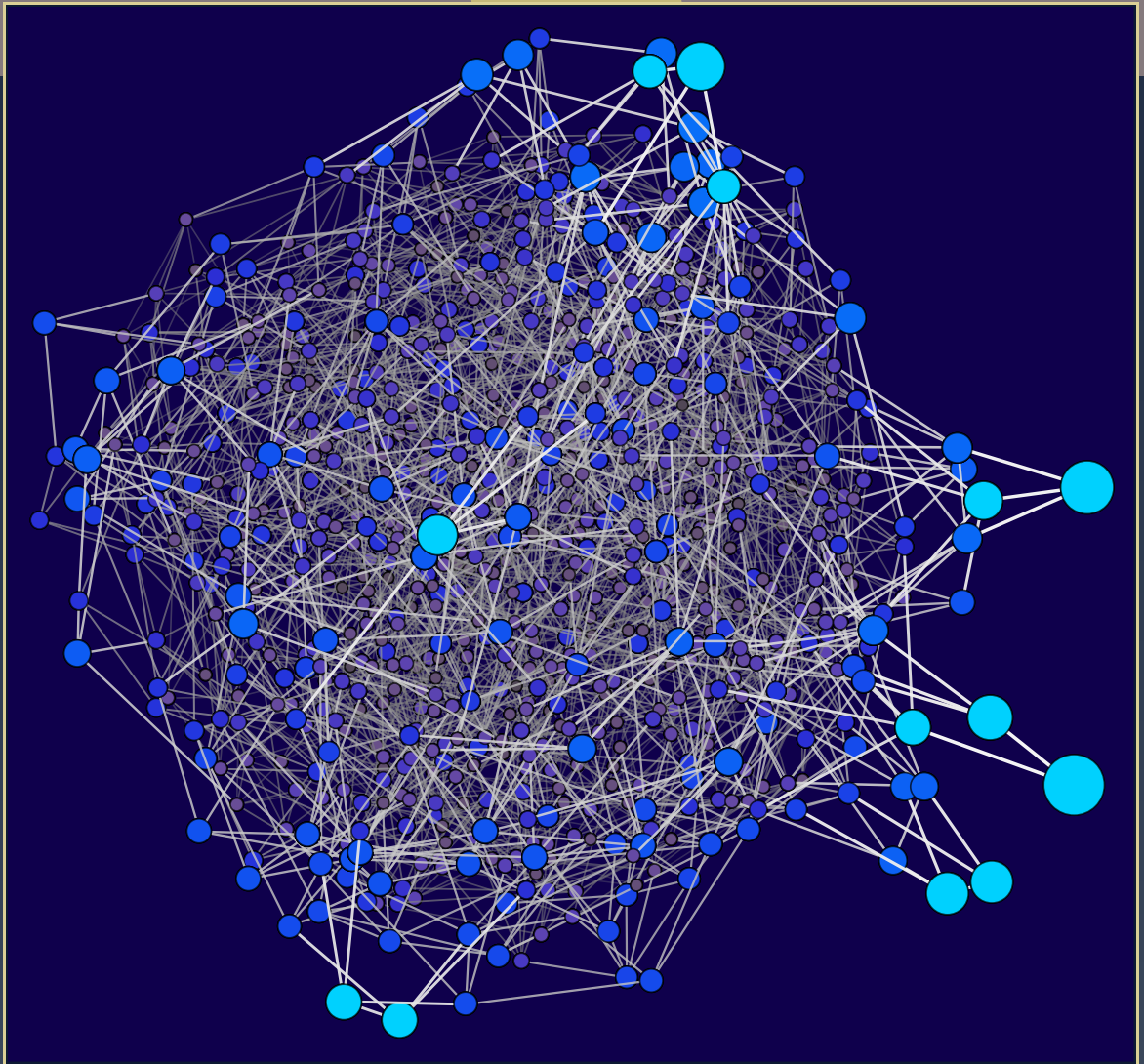


# ANTS XIV

## Proceedings of the Fourteenth Algorithmic Number Theory Symposium

University of Auckland, 2020

edited by  
Steven D. Galbraith





ANTS XIV  
Proceedings of the Fourteenth  
Algorithmic Number Theory Symposium







# **ANTS XIV**

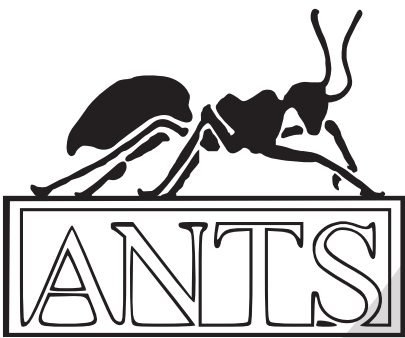
## Proceedings of the Fourteenth Algorithmic Number Theory Symposium

University of Auckland

<https://www.math.auckland.ac.nz/~sgal018/ANTS>

Edited by

Steven D. Galbraith



*Volume Editor:*

Steven D. Galbraith  
Mathematics Department  
University of Auckland  
New Zealand

---

The cover image is based on an illustration from the article “Supersingular curves with small noninteger endomorphisms”, by Jonathan Love and Dan Boneh (see p. 9).

The contents of this work are copyrighted by MSP or the respective authors.  
All rights reserved.

Electronic copies can be obtained free of charge from <http://msp.org/obs/4>  
and printed copies can be ordered from MSP ([contact@msp.org](mailto:contact@msp.org)).

The Open Book Series is a trademark of Mathematical Sciences Publishers.

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-07-1 (print), 978-1-935107-08-8 (electronic)

First published 2020.

---



**MATHEMATICAL SCIENCES PUBLISHERS**

798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840  
[contact@msp.org](mailto:contact@msp.org) <http://msp.org>

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational and algorithmic number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the fourteenth ANTS meeting, which took place June 29 to July 4, 2020 via video conference, the plans for holding it at the University of Auckland, New Zealand, having been disrupted by the COVID-19 pandemic. The volume contains revised and edited versions of 24 refereed papers and one invited paper presented at the conference.



# Contents

<i>Commitment schemes and diophantine equations</i>	1
José Felipe Voloch	
<i>Supersingular curves with small noninteger endomorphisms</i>	7
Jonathan Love and Dan Boneh	
<i>Cubic post-critically finite polynomials defined over <math>\mathbb{Q}</math></i>	23
Jacqueline Anderson, Michelle Manes and Bella Tobin	
<i>Faster computation of isogenies of large prime degree</i>	39
Daniel J. Bernstein, Luca De Feo, Antonin Leroux and Benjamin Smith	
<i>On the security of the multivariate ring learning with errors problem</i>	57
Carl Bootland, Wouter Castryck and Frederik Vercauteren	
<i>Two-cover descent on plane quartics with rational bitangents</i>	73
Nils Bruin and Daniel Lewis	
<i>Abelian surfaces with fixed 3-torsion</i>	91
Frank Calegari, Shiva Chidambaram and David P. Roberts	
<i>Lifting low-gonal curves for use in Tuitman's algorithm</i>	109
Wouter Castryck and Floris Vermeulen	
<i>Simultaneous diagonalization of incomplete matrices and applications</i>	127
Jean-Sébastien Coron, Luca Notarnicola and Gabor Wiese	
<i>Hypergeometric L-functions in average polynomial time</i>	143
Edgar Costa, Kiran S. Kedlaya and David Roe	
<i>Genus 3 hyperelliptic curves with CM via Shimura reciprocity</i>	161
Bogdan Adrian Dina and Sorina Ionica	
<i>A canonical form for positive definite matrices</i>	179
Mathieu Dutour Sikirić, Anna Haensch, John Voight and Wessel P.J. van Woerden	
<i>Computing Igusa's local zeta function of univariates in deterministic polynomial-time</i>	197
Ashish Dwivedi and Nitin Saxena	
<i>Computing endomorphism rings of supersingular elliptic curves and connections to path-finding in isogeny graphs</i>	215
Kirsten Eisenträger, Sean Hallgren, Chris Leonardi, Travis Morrison and Jennifer Park	
<i>New rank records for elliptic curves having rational torsion</i>	233
Noam D. Elkies and Zev Klagsbrun	
<i>The nearest-colattice algorithm: Time-approximation tradeoff for approx-CVP</i>	251
Thomas Espitau and Paul Kirchner	

<i>Cryptanalysis of the generalised Legendre pseudorandom function</i>	267
Novak Kaluđerović, Thorsten Kleinjung and Dušan Kostić	
<i>Counting Richelot isogenies between superspecial abelian surfaces</i>	283
Toshiyuki Katsura and Katsuyuki Takashima	
<i>Algorithms to enumerate superspecial Howe curves of genus 4</i>	301
Momonari Kudo, Shushi Harashita and Everett W. Howe	
<i>Divisor class group arithmetic on <math>C_{3,4}</math> curves</i>	317
Evan MacNeil, Michael J. Jacobson Jr. and Renate Scheidler	
<i>Reductions between short vector problems and simultaneous approximation</i>	335
Daniel E. Martin	
<i>Computation of paramodular forms</i>	353
Gustavo Rama and Gonzalo Tornaría	
<i>An algorithm and estimates for the Erdős–Selfridge function</i>	371
Brianna Sorenson, Jonathan Sorenson and Jonathan Webster	
<i>Totally <math>p</math>-adic numbers of degree 3</i>	387
Emerald Stacy	
<i>Counting points on superelliptic curves in average polynomial time</i>	403
Andrew V. Sutherland	

# Commitment schemes and diophantine equations

José Felipe Voloch

Motivated by questions in cryptography, we look for diophantine equations that are hard to solve but for which determining the number of solutions is easy.

## 1. Commitment schemes

Solving a diophantine equation is typically hard but, given a point, it is typically easy to find a variety containing that point. This is an example of a “one-way function” with potential applications to cryptography. Our current (lack of) knowledge suggests that such a function is possibly quantum resistant and, therefore, cryptosystems based on these could be used for postquantum cryptography [BL17].

An encryption system based on this principle was proposed by Akiyama and Goto [AG06; AG08], then broken by Ivanov and the author [IV09]. It was then fixed, broken again, fixed again... Current status unclear.

The purpose of a commitment scheme is for a user to commit to a message without revealing it (e.g., vote, auction bid) by making public a value obtained from the message in such a way that one can check, after the message is revealed, that the public value confirms the message.

Using such diophantine one-way functions for commitment schemes was proposed by Boneh and Corrigan-Gibbs [BCG14]. They also suggested working modulo an RSA modulus  $N$ . This could conceivably weaken the system. It will definitely no longer be quantum resistant. Some partial attacks on this particular system are presented in [ZW17].

Here is the general format of a diophantine commitment scheme. Encode a message as point  $P$  over some field  $F$ . Make public a variety  $V/F$  with  $P \in V$ , with  $V$  taken from some fixed family of varieties. To check the commitment, one verifies that  $P$  satisfies the equations of  $V$ . We need the following conditions to be satisfied for this to work:

- Given  $P$ , it is easy to construct  $V$ .
- Given  $V$ , it is hard to find  $V(F)$  (hence  $P$ ).
- Given  $V$  (and perhaps  $P$ ), it is easy to verify that  $\#V(F) = 1$ .

MSC2020: 11D45, 94A60.

Keywords: commitment schemes, diophantine equations, algebraic varieties.

The last condition is important to prevent cheating. It proves that  $P$  was indeed the committed message. In general, a commitment scheme consists of two algorithms  $\text{Commit}(m, r)$ ,  $\text{Reveal}(m, r, c)$ . The first takes as input a message  $m$  and a random string  $r$  to produce an output  $c$ , which is then made public. The second takes as input  $m, r, c$  as before and outputs yes or no, depending on whether  $c$  is the correct output of  $\text{Commit}(m, r)$ . The randomness is needed, e.g., if the list of possible messages is small enough that it can be brute force searched. Note that our requirement that  $\#V(F) = 1$  corresponds to the notion of perfect binding for a commitment scheme. There is a weaker notion of computational binding in which the condition is relaxed to only hold with probability close to one. See [BCG14, Section 4.1] for the precise definition of a commitment scheme and some discussion.

These commitment schemes are similar in spirit to the class of multivariate polynomial cryptosystems. In analogy to what is done there, it is conceivable to have encryption by selecting a subset of varieties  $V/F$  such that  $V(F)$  can be easily found but that  $V$  can be disguised as a general member of the collection of varieties. We do not address the interesting problem of doing this for schemes we consider.

## 2. Diophantine equations

Answering a question of Friedman, Poonen [Poo10] proved:

**Theorem 2.1.** *Assuming the Bombieri–Lang conjecture, there exists  $f(x, y) \in \mathbb{Q}[x, y]$  inducing an injection  $\mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}$ .*

Boneh and Corrigan-Gibbs [BCG14] then use the following construction from such a function. For  $P = (a, b)$ , take  $V : f(x, y) = f(a, b)$  to get a commitment scheme fitting the general setting of Section 1. Unfortunately, Poonen’s proof, besides being conditional on a conjecture, is also nonconstructive!

Zagier suggested  $f(x, y) = x^7 + 3y^7$  as a polynomial defining an injective function. But we don’t have a proof. With exponent 13 instead of 7, the abcd conjecture implies that this function essentially injective.

**Question 2.2.** Is solving  $x^7 + 3y^7 = k$  over  $\mathbb{Q}$  hard?

Pasten [Pas20] proved that there exists an affine surface  $S$  of the form  $U \times U$  with  $S(\mathbb{Q})$  Zariski-dense in  $S$  and a morphism  $S \rightarrow \mathbb{A}^1$  inducing an injection  $S(\mathbb{Q}) \rightarrow \mathbb{Q}$ . But,  $S(\mathbb{Q})$  is too sparse to be cryptographically useful.

Cornelissen [Cor99], using that the abcd conjecture is true for function fields of characteristic 0, noted that  $x^m + ty^m$  is injective in  $K(t)$ ,  $\text{char } K = 0$  for  $m$  large.

**Question 2.3.** Is solving  $x^m + ty^m = k$  over  $\mathbb{Q}(t)$  hard?

My guess is that the answer is no.

Cornelissen also noted that  $x^p + ty^p$  is injective in  $K(t)$ ,  $\text{char } K = p$ . But solving  $x^p + ty^p = k$  is easy.

The following was noted in [SV20], with the proof being an extension of [Vol85] (see also [Wan] for a related result without a hypothesis on the degree of the morphism):



**Theorem 2.4.** *Let  $F$  be a function field of a curve  $C$  of genus  $g$  with field of constants  $K$  of characteristic  $p > 0$  and let  $S$  be a finite set of places of  $F$ . If  $u_1, \dots, u_t$  are  $S$ -units of  $F$ , linearly independent over  $K$ , such that the degree of the morphism  $(u_1 : \dots : u_t) : C \rightarrow \mathbb{P}^{t-1}$  is less than  $p$  and satisfy*

$$u_1 + \dots + u_t = 1$$

*then*

$$\max\{\deg u_i \mid i = 1, \dots, t\} \leq \frac{t(t-1)}{2}(2g-2+\#S)$$

The above result implies the injectivity of  $x^{13} + ty^{13}$  in the set of pairs of elements of  $K(t) - K$  of degree at most  $p/13$  if  $13 \nmid p(p-1)$ .

This is enough for the application to commitment schemes by taking a sufficiently large finite field  $K$  and considering the function  $x^{13} + ty^{13}$  restricted to the above set where the function is injective.

But the function is not injective in the whole of  $K(t)$ . Indeed, if  $x^{13} + ty^{13} = k$ ,  $q = p^{12}$ , then

$$(x^q / k^{(q-1)/13})^{13} + t(t^{(q-1)/13} y^q / k^{(q-1)/13})^{13} = k$$

### 3. Curves on surfaces

The cryptosystem of Akiyama and Goto [AG06; AG08] actually uses curves on surfaces over finite fields. We now consider the use of rational curves on surfaces in  $\mathbb{P}^3$  over a finite field for commitment schemes.

We start with a rational curve  $P$  parametrized by  $(f_0 : f_1 : f_2 : f_3)$  in  $\mathbb{P}^3$  over a finite field  $\mathbb{F}_q$ , where the  $f_i$  are polynomials of degree at most  $m$  (i.e., a point in  $\mathbb{P}^3$  over  $\mathbb{F}_q(t)$ ). Such a curve will include the message and randomness and our commitment will be a smooth surface  $S/\mathbb{F}_q$  of degree  $d$  containing  $P$ . This is a bit different from previous schemes as the surface is constant (i.e., independent of  $t$ ). If  $S$  is given by an homogeneous equation  $F = 0$ , the condition that  $P \subset S$  is simply  $F(f_0, f_1, f_2, f_3) = 0$  which can be viewed as a system of linear equations on the coefficients of  $F$ , once the  $f_i$  are given. There are  $\binom{d+3}{3}$  coefficients and  $dm + 1$  equations. One has solutions to the system as soon as there are more coefficients than equations but these are not guaranteed to be smooth. Poonen [Poo08] has proved that, for  $d$  large, a positive proportion of those solutions do indeed give smooth surfaces. One expects in practice that, as long as the finite field is big enough, there will be plenty of smooth surfaces.

To guarantee uniqueness of the curve  $P$  inside  $S$ , we prove the following result.

**Theorem 3.1.** *Let  $S/\mathbb{F}_q$  be a smooth surface in  $\mathbb{P}^3$  of degree  $d > 3$  with Picard number two. Then  $S$  contains at most one smooth rational curve of degree  $m$ , if  $m < 2d(d-4)/(d-2)$ .*

*Proof.* Let  $H$  be a hyperplane section and  $D_1, D_2$  two distinct smooth rational curves of degree  $m$  contained in  $S$ . We compute the determinant of the matrix of intersection pairings for  $H, D_1, D_2$  and show it is nonzero, hence these curves are independent in the Néron–Severi group, contradicting the hypothesis on the Picard number.

Clearly,  $H^2 = d$ ,  $HD_i = m$ ,  $i = 1, 2$ . The canonical class of  $S$  is  $(d-4)H$ , so the adjunction formula gives  $D_i^2 + (d-4)HD_i = -2$ , hence  $D_i^2 = -(2 + (d-4)m)$ . Let  $\delta = D_1 D_2$ . The determinant of the

matrix of intersection pairings is therefore

$$\begin{vmatrix} H^2 & HD_1 & HD_2 \\ D_1H & D_1^2 & D_1D_2 \\ D_2H & D_2D_1 & D_2^2 \end{vmatrix} = \begin{vmatrix} d & m & m \\ m & -(2 + (d-4)m) & \delta \\ m & \delta & -(2 + (d-4)m) \end{vmatrix} \\ = -d\delta^2 + 2m^2\delta + d(2 + (d-4)m)^2 + m^2(2 + (d-4)m).$$

This vanishes precisely when  $\delta = -(2 + (d-4)m)$ ,  $2m^2/d + (2 + (d-4)m)$ . The first value is negative so cannot be  $D_1D_2$  and the second value is bigger than  $m^2$  by our hypothesis but  $D_1D_2 \leq m^2$  by Bézout's theorem so cannot be  $D_1D_2$  either.  $\square$

To apply the theorem, we need to know that the Picard number of  $S$  is at most two. For a given surface, this can be done using the algorithm of [Cos15], for example. This algorithm computes the  $L$ -function of  $S$  and the Picard number of  $S$  is the multiplicity of  $q$  as a root of the  $L$ -function, conditional on the Tate conjecture. However, the surfaces we construct will have Picard number at least two and a theorem of Tate shows that the multiplicity of  $q$  as a root of the  $L$ -function is an upper bound for the Picard number. So, if this multiplicity is two, it is verified that the Picard number is two. There is a parity condition coming from the functional equation for  $L$ -functions which implies that this will not work if  $d$  is odd. It is reasonable to expect that a sizable proportion of such surfaces have Picard number two if  $d$  is even, but this is not currently known and is worthy of further investigation.

In sum, our commitment scheme is as follows, with a finite field  $\mathbb{F}_q$  and integers  $m, d$  selected a priori:

- (1) Encode a message as well as some randomness within  $(f_0, f_1, f_2, f_3)$ ,  $f_i \in \mathbb{F}_q[t]$ ,  $\deg f_i \leq m$ .
- (2) Choose a random  $F \in \mathbb{F}_q[x_0, x_1, x_2, x_3]$  homogeneous of degree  $d$  with  $F(f_0, f_1, f_2, f_3) = 0$ .
- (3) Check whether the surface defined by  $F = 0$  is smooth and has Picard number two. If so, publish  $F$  as the commitment. If not, pick a different  $F$  in step (2).

For an explicit example, consider  $m = 3, d = 6$ . For a sextic surface to contain a given twisted cubic, one needs to satisfy a system of 19 equations in 84 variables and, hopefully, many of those will give rise to smooth surfaces with Picard number two. The space of available messages depends on 16 variables.

One can also use  $m = 3, d = 4$ . The inequality in the theorem is not satisfied but the second value for  $\delta$  is  $13/2$ , which is not an integer so cannot be  $D_1D_2$  and the result holds. In this case, we have a system of 13 equations in 35 variables for the coefficients of the surface and again, the space of available messages depends on 16 variables.

The expansion from 16 variables to 84 (or 35) from the message to the commitment is potentially wasteful and it is worth investigating whether a priori setting many of these variables to zero will still allow enough variability so that step (3) above succeeds. Another, less explicit way, of achieving the same result is to require that  $F$  vanishes at a prespecified set of points  $Z_0$  not lying on the curve  $P$ . Poonen (personal communication) informs me that the results of [Poo08] can be adapted to show that, for  $d$  large, a positive proportion of the surfaces containing both  $P$  and  $Z_0$  are smooth.

Another issue worth studying is the choice of  $q$ . In some ways, small  $q$  is better for computations. But, if a very small value of  $q$ , such as  $q = 2$  is chosen, then  $m = 3$  is too small, as it allows brute force searching for the rational curve.

Given a surface, to find a rational curve inside it, one can either do a brute force search on the coefficients of the parametrization, or set up a system of equations for these coefficients and try to solve it, e.g., using Gröbner bases. Neither option seem particularly efficient. Neither option also appears to be much improved by the use of quantum computers. There are general algorithms in the literature (e.g., [PTvL15]) that compute the Néron–Severi group of a variety but these make no claim of practicality.

### Acknowledgements

This work was supported by MBIE. I would also like to thank Steven Galbraith for suggesting that I look into commitment schemes and for helpful comments as well as Edgar Costa and Bjorn Poonen for suggestions.

### References

- [AG06] K. Akiyama and A. Goto, *A public-key cryptosystem using algebraic surfaces*, (extended abstract), PQCrypto Workshop Record.
- [AG08] K. Akiyama and A. Goto, *An improvement of the algebraic surface public-key cryptosystem*, Proceedings of SCIS.
- [BCG14] Dan Boneh and Henry Corrigan-Gibbs, *Bivariate polynomials modulo composites and their applications*, 42–62.
- [BL17] Daniel J. Bernstein and Tanja Lange, *Post-quantum cryptography*, Nature **549** (2017), no. 7671, 188–194.
- [Cor99] Gunther Cornelissen, *Stockage diophantien et hypothèse abc généralisée*, C. R. Acad. Sci. Paris Sér. I Math. **328** (1999), no. 1, 3–8.
- [Cos15] Edgar Costa, *Effective computations of Hasse–Weil zeta functions*, 2015, Ph.D. Thesis, p. 78.
- [IV09] Petar Ivanov and José Felipe Voloch, *Breaking the Akiyama–Goto cryptosystem*, 113–118.
- [Pas20] Hector Pasten, *Bivariate polynomial injections and elliptic curves*, Selecta Math. (N.S.) **26** (2020), no. 2, Paper No. 22, 13.
- [Poo08] Bjorn Poonen, *Smooth hypersurface sections containing a given subscheme over a finite field*, Math. Res. Lett. **15** (2008), no. 2, 265–271.
- [Poo10] Bjorn Poonen, *Multivariable polynomial injections on rational numbers*, Acta Arith. **145** (2010), no. 2, 123–127.
- [PTvL15] Bjorn Poonen, Damiano Testa, and Ronald van Luijk, *Computing Néron–Severi groups and cycle class groups*, Compos. Math. **151** (2015), no. 4, 713–734.
- [SV20] Igor E. Shparlinski and José Felipe Voloch, *Value sets of sparse polynomials*, Canad. Math. Bull. **63** (2020), no. 1, 187–196.
- [Vol85] José Felipe Voloch, *Diagonal equations over function fields*, Bol. Soc. Brasil. Mat. **16** (1985), no. 2, 29–39.
- [Wan] Julie Tzu-Yueh Wang, *A note on Wronskians and the ABC theorem in function fields of prime characteristic*, Manuscripta Math. **98**, no. 2, 255–264.
- [ZW17] Xiaona Zhang and Li-Ping Wang, *Partial bits exposure attacks on a new commitment scheme based on the Zagier polynomial*, 357–366.

Received 3 Aug 2020.

JOSÉ FELIPE VOLOCH: [felipe.voloch@canterbury.ac.nz](mailto:felipe.voloch@canterbury.ac.nz)

School of Mathematics and Statistics, University of Canterbury, Christchurch, New Zealand



# Supersingular curves with small noninteger endomorphisms

Jonathan Love and Dan Boneh

We introduce a special class of supersingular curves over  $\mathbb{F}_{p^2}$ , characterized by the existence of noninteger endomorphisms of small degree. We prove a number of properties about this set. Most notably, we can partition this set into subsets such that curves within each subset have small-degree isogenies between them, but curves in distinct subsets have no small-degree isogenies between them. Despite this, we show that isogenies between distinct subsets can heuristically be computed efficiently, giving a technique for computing isogenies between certain prescribed curves that cannot be efficiently found by searching on  $\ell$ -isogeny graphs.

## 1. Introduction

Given an elliptic curve  $E$  over a field  $k$ , let  $\text{End}(E)$  denote the ring of endomorphisms of  $E$  that are defined over  $\bar{k}$ . The curve  $E$  is *supersingular* if  $\text{End}(E)$  is noncommutative; this can only occur if  $E$  is defined over  $\mathbb{F}_{p^2}$  for some prime  $p$  [19, Theorem V.3.1]. The set  $\text{SS}(p)$  of all supersingular curves up to  $\mathbb{F}_p$ -isomorphism can be quite complicated, but in this paper we define subsets of  $\text{SS}(p)$  which are relatively straightforward to compute with and to classify.

**Definition 1.1.** Given  $M < p$ , an elliptic curve  $E$  over a finite field of characteristic  $p$  is *M-small* (we also say that the  $j$ -invariant of  $E$  is *M-small*) if there exists  $\alpha \in \text{End}(E)$  with  $\deg \alpha \leq M$  such that  $\alpha$  is not multiplication by an integer. The set of  $\mathbb{F}_p$ -isomorphism classes of *supersingular M-small* curves over  $\mathbb{F}_{p^2}$  is denoted  $\text{SS}^M(p)$ .

Assume for the rest of this paper that  $p \geq 5$ . We will study the structure of the set  $\text{SS}^M(p)$  of supersingular *M-small* curves, and in particular, we will discuss the following properties of this set:

- (a) If  $M < \sqrt{p}/2$ , the set  $\text{SS}^M(p)$  of *M-small* supersingular curves partitions into  $O(M)$  subsets, each connected by small-degree isogenies, such that there is no isogeny of degree less than  $\sqrt{p}/(2M)$  between distinct subsets ([Theorem 1.3](#)).

---

This research was supported by NSF grant #1701567.

MSC2010: 11G20, 11R52, 11T71.

**Keywords:** supersingular, elliptic curve, isogeny graph, M-small, endomorphism, quaternion, maximal order, Deuring correspondence, partition, archipelago, island, airport, orientation, Hilbert class polynomial.

- (b) The endomorphism rings of  $M$ -small supersingular curves, and isogenies between any two of them, can heuristically be computed in time polynomial in  $M$  and  $\log p$  (Section 7).

Let us state point (a) more precisely. Given an elliptic curve  $E$  over  $\mathbb{F}_{p^2}$ , let  $E^{(p)}$  denote its image under the  $p$ -th power Frobenius map  $(x, y) \mapsto (x^p, y^p)$ . If  $E$  is defined over  $\mathbb{F}_p$ , then  $E = E^{(p)}$ ; otherwise we have  $E = (E^{(p)})^{(p)}$  and so this map will swap conjugate pairs of curves.<sup>1</sup>

**Definition 1.2.** Let  $E$  and  $E'$  be supersingular elliptic curves over  $\mathbb{F}_{p^2}$ . The *distance from  $E$  to  $E'$* , denoted  $d(E, E')$ , is the minimum degree of an isogeny  $E \rightarrow E'$  or  $E \rightarrow E'^{(p)}$  defined over  $\overline{\mathbb{F}}_p$ .

By basic properties of isogenies (e.g., [19, Chapter III]),  $\log d$  is a pseudometric on the set of supersingular curves over  $\mathbb{F}_{p^2}$ , and it descends to a metric on the set of Galois orbits  $\{E, E^{(p)}\}$ .

Given a positive integer  $M$  and a fundamental discriminant  $D$ , we can define the following subset of  $\text{SS}^M(p)$ :

$$T_D^M := \{E \in \text{SS}(p) : \mathbb{Q}(\alpha) \cong \mathbb{Q}(\sqrt{D}) \text{ for some } \alpha \in \text{End}(E) - \mathbb{Z} \text{ with } \deg \alpha \leq M\}.$$

**Theorem 1.3.** *Let  $M$  be a positive integer. Then  $\text{SS}^M(p)$  is a union*

$$\text{SS}^M(p) = \bigcup_D T_D^M,$$

*of nonempty subsets  $T_D^M$ , indexed by fundamental discriminants  $-4M \leq D < 0$  which are not congruent to a square mod  $p$ . These sets have the following properties:*

- (a) *If  $E, E'$  are in distinct subsets  $T_D^M \neq T_{D'}^M$ , then*

$$d(E, E') \geq \frac{\sqrt{p}}{2M}.$$

- (b) *If  $E, E'$  are in the same  $T_D^M$ , then there is a sequence  $E = E_0, E_1, \dots, E_r = E'$  of elements of  $T_D^M$  such that*

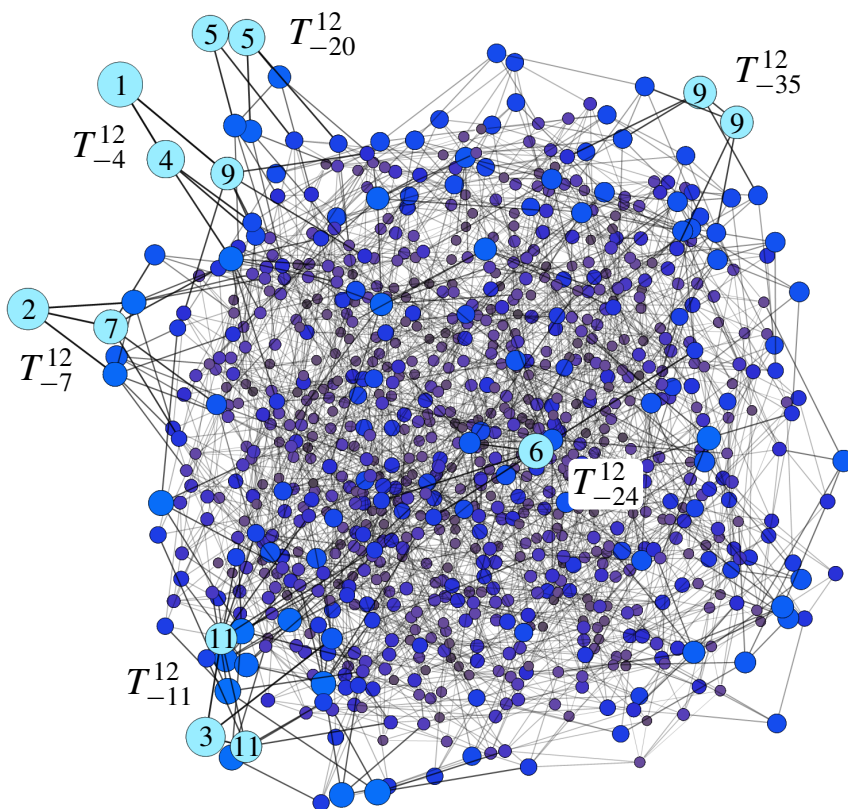
$$d(E_{i-1}, E_i) \leq \frac{2}{3}\sqrt{3M}$$

*for all  $i = 1, \dots, r$ . We can take  $r \leq 3$ , or alternatively, we can take  $r \leq 3 \log_2(\frac{2}{3}\sqrt{3M})$  and require all  $d(E_{i-1}, E_i)$  to be prime.*

**Remark 1.4.** If  $M < \frac{1}{2}\sqrt{p}$ , then Theorem 1.3(a) implies that the sets  $T_D^M$  are disjoint, and hence form a partition of  $\text{SS}^M(p)$ .

Figure 1 illustrates Theorem 1.3 for  $p = 20011$  and  $M = 12$ . In particular, since  $\sqrt{20011}/(2 \cdot 12) \approx 5.9$ , Theorem 1.3(a) predicts that curves in distinct sets  $T_D^M$  are at least two steps apart in the graph. Also, as the primes less than  $\frac{2}{3}\sqrt{3 \cdot 12}$  are 2 and 3, Theorem 1.3(b) predicts that the sets  $T_D^M$  are connected components of the subgraph of 12-small curves. One can see that both these claims are true in the figure.

<sup>1</sup>The map  $E \rightarrow E^{(p)}$  on supersingular curves is called the “mirror involution” in [1], where the relationship between conjugate pairs, along with many other structural properties of supersingular isogeny graphs, is studied in detail.



**Figure 1.** Supersingular curves in characteristic 20011 with conjugate pairs  $\{E, E^{(p)}\}$  identified. The 12-small curves are highlighted and labeled with the smallest degree of a noninteger endomorphism. The sets  $T_D^M$  from Theorem 1.3 are indicated. Two curves  $E, E'$  are connected by an edge if there is an isogeny  $E \rightarrow E'$  of degree 2 or 3. Data computed using Magma, plotted using Mathematica.

If we think of  $M$  minus the degree of the smallest noninteger endomorphism as a measure of elevation, then the set of supersingular curves can be thought of as an archipelago. The  $M$ -small curves are above sea level, and hence are easy to find and to study (Section 2). Each set  $T_D^M$  is an island: curves on the same island are close enough to walk between, but distinct islands are very far from each other. We shall see in Section 5 that the islands  $T_D^M$  are closely related to the craters of isogeny volcanoes (which appear in ordinary isogeny graphs [22] and in oriented supersingular isogeny graphs [7; 16]), so perhaps we can say that this archipelago was formed by volcanic activity! In Section 7 we will construct “airports” that allow us to efficiently travel between the islands, allowing us to find isogenies between any two  $M$ -small supersingular curves. Unfortunately, most supersingular curves remain deep underwater, shrouded in mystery.

The fact that the sets  $T_D^M$  are connected by small-degree isogenies (as described in Theorem 1.3(b)) will not be evident if we only consider isogenies of a single prime degree. In fact, if  $\ell$  is a small prime, then under relatively mild conditions on  $M$  (Remark 6.2), there are two  $M$ -small curves that are connected by a degree  $\ell$  isogeny, but such that any isogeny of degree relatively prime to  $\ell$  will have degree greater



than  $p\ell/(4M)$ . So if we exclude isogenies of degree divisible by  $\ell$  for any sufficiently small prime  $\ell$ , the sets  $T_D^M$  will no longer be connected by short paths.

**1A. Motivation.** We say that a supersingular elliptic curve  $E$  over  $\mathbb{F}_{p^2}$  is “hard” if it is computationally infeasible to compute its endomorphism ring. A number of applications in cryptography (e.g., [9]) need an explicit hard curve  $E$  where no one, including the party who generated the curve, can compute its endomorphism ring. Currently, there is no known method to generate such a curve.

To illustrate the problem, suppose  $p \equiv 2 \pmod{3}$  and let  $E_0$  be the supersingular curve with  $j$ -invariant 0. One can generate a large number of supersingular curves by starting at  $E_0$  and taking a random walk along the graph of degree  $\ell$  isogenies for some small prime  $\ell$ . However, for any curve  $E$  found in this way, we can compute  $\text{End}(E)$  using the isogeny path from  $E_0$  to  $E$ .

We may consider using the set of  $M$ -small supersingular elliptic curves, for some polynomial size  $M$ , as a candidate set of explicit hard curves. If  $E$  is a typical  $M$ -small curve, then point (a) tells us that  $E$  could not reasonably be found by searching from  $E_0$  on  $\ell$ -isogeny graphs for any small primes  $\ell$ . A priori, this might suggest that it would be difficult to compute the isogeny path from  $E_0$  to  $E$ , and therefore there is hope that the endomorphism ring of  $E$  will remain unknown.

However, point (b) suggests that this is likely not the case, and that a hard curve will not be  $M$ -small. By the classification results of Section 2, this rules out using roots of low-degree Hilbert class polynomials as a reasonable candidate for a method of constructing hard curves. It remains an open problem to construct a single explicit hard supersingular curve.

**1B. Organization.** We briefly discuss how to generate  $M$ -small curves in Section 2, and begin the proof of Theorem 1.3 with Lemma 2.3. An overview of some concepts we will need from the theory of quaternion algebras<sup>2</sup> can be found in Section 3. In Section 4 we define a notion of distance for maximal orders of quaternion algebras, and use it to prove Theorem 1.3(a). We review the theory of orientations of supersingular curves in Section 5 and use this theory to prove Theorem 1.3(b). In Section 6 we show that certain isogenies of degree  $\ell$  cannot be replaced by short isogenies of degree relatively prime to  $\ell$ . We finish by describing an algorithm for computing isogenies between elliptic curves in Section 7.

A list of (mostly standard) results on the sizes of various sets of  $M$ -small curves can be found in an appendix, available with the unpublished version of this paper [15].

## 2. Hilbert class polynomials and $M$ -small curves

Most well-known examples of supersingular curves are  $M$ -small for relatively small values of  $M$ . For instance, supersingular curves with a nontrivial automorphism are 1-small. This includes the curve  $y^2 = x^3 + x$  with  $j$ -invariant 1728 when  $p \equiv 3 \pmod{4}$ , and the curve  $y^2 = x^3 + 1$  with  $j$ -invariant 0 when  $p \equiv 2 \pmod{3}$ . More generally, Bröker in [2] proposes a general algorithm for producing a supersingular

<sup>2</sup>Many prior papers on supersingular isogenies use the structure of quaternion algebras to study supersingular isogenies; see for instance [13] and [10].



curve over an arbitrary finite field. We will show that his algorithm returns  $M$ -small curves, and then discuss how to generalize his approach to generate all  $M$ -small curves.

A ring  $\mathcal{O}$  is a *quadratic order* if it is a finite-index subring of the ring of integers  $\mathcal{O}_K$  of some imaginary quadratic field  $K$ . To each quadratic order  $\mathcal{O}$ , we can associate its *Hilbert class polynomial*  $H_{\mathcal{O}}(x) \in \mathbb{Z}[x]$ , which has the property that  $z \in \mathbb{C}$  is a root of  $H_{\mathcal{O}}$  if and only if  $z$  is the  $j$ -invariant of an elliptic curve  $\tilde{E}$  over  $\mathbb{C}$  with endomorphism ring isomorphic to  $\mathcal{O}$  [8, Proposition 13.2]. The degree of  $H_{\mathcal{O}}$  equals the class number of  $\mathcal{O}$ .

Bröker's algorithm [2, Algorithm 2.4] proceeds as follows. To construct a supersingular curve over  $\mathbb{F}_p$  with  $p \equiv 1 \pmod{4}$ ,<sup>3</sup> one first finds a small prime  $q \equiv 3 \pmod{4}$  with Legendre symbol  $(-q/p) = -1$ . We compute the Hilbert class polynomial  $H_{\mathcal{O}_K}(x)$  for  $K = \mathbb{Q}(\sqrt{-q})$ , and find a root of  $H_{\mathcal{O}_K}(x) \pmod{p}$  in  $\mathbb{F}_p$ . The condition  $(-q/p) = -1$  then guarantees that this root is the  $j$ -invariant of a supersingular curve. This algorithm generates  $M$ -small curves for a reasonably small value of  $M$ , as the following proposition shows.

**Proposition 2.1.** *The supersingular curves found by Algorithm 2.4 of [2] are  $((q+1)/4)$ -small. Assuming GRH, they are  $M$ -small for  $M = O(\log^2 p)$ .*

*Proof.* The output of the algorithm is a curve  $E$  over  $\mathbb{F}_p$  with the following property: there is curve  $\tilde{E}$  over the Hilbert class field of  $\mathbb{Q}(\sqrt{-q})$  such that  $\text{End}(\tilde{E}) \cong \mathcal{O}_K$ , and  $E$  is the reduction of  $\tilde{E}$  modulo some prime of  $\mathcal{O}_L$ . In particular,  $(1 + \sqrt{-q})/2 \in \mathcal{O}_K$  is a noninteger endomorphism of  $\tilde{E}$ . The reduction map  $\text{End}(\tilde{E}) \rightarrow \text{End}(E)$  is a degree-preserving injection [20, Proposition II.4.4], so  $\text{End}(E)$  contains a noninteger endomorphism of norm  $(q+1)/4$ , proving that  $E$  is  $((q+1)/4)$ -small. As discussed in the proof of [2, Lemma 2.5], under GRH we can take  $q = O(\log^2 p)$ .  $\square$

A natural generalization of Bröker's algorithm is to compute all roots (not just those in  $\mathbb{F}_p$ ) of  $H_{\mathcal{O}}(x) \pmod{p}$ , for all imaginary quadratic orders  $\mathcal{O}$  with sufficiently small discriminant. By Proposition 2.2, this process can be used to generate the set of all  $M$ -small elliptic curves. Note that if  $M$  is an integer, then an imaginary quadratic order  $\mathcal{O}$  has discriminant  $|\text{disc } \mathcal{O}| \leq 4M$  if and only if  $\mathcal{O} - \mathbb{Z}$  has an element with norm at most  $M$ .

**Proposition 2.2.** *Let  $M \in \mathbb{Z}$  satisfy  $3 \leq M < p$ , let  $E$  be an elliptic curve over a finite field of characteristic  $p$ , and let  $z \in \overline{\mathbb{F}}_p$  be the  $j$ -invariant of  $E$ . Then  $E$  is  $M$ -small if and only if  $H_{\mathcal{O}}(z) = 0$  for some quadratic order  $\mathcal{O}$  with discriminant  $-4M \leq \text{disc } \mathcal{O} < 0$ . In this setting  $\text{End}(E)$  contains an isomorphic copy of  $\mathcal{O}$ , and  $E$  is supersingular if and only if  $p$  does not split in the field of fractions of  $\mathcal{O}$ .*

The proof is analogous to that of Proposition 2.1, applying Deuring's lifting theorem [14, Theorem 13.14] to show that every  $M$ -small curve arises in this way. This result allows us to prove the first portion of Theorem 1.3.

**Lemma 2.3.** *The sets  $T_D^M$  appearing in Theorem 1.3 are nonempty, and their union is  $\text{SS}^M(p)$ .*

<sup>3</sup>For  $p = 2$ , the curve  $y^2 + y = x^3$  is supersingular, and for  $p \equiv 3 \pmod{4}$  the curve  $y^2 = x^3 + x$  is supersingular.

*Proof.* Given any fundamental discriminant  $-4M \leq D < 0$  with  $(D/p) = -1$ ,  $p$  does not split in the quadratic field  $K$  with discriminant  $D$ . So by [Proposition 2.2](#), the roots of  $H_{\mathcal{O}_K}(x) \pmod{p}$  are  $j$ -invariants of  $M$ -small supersingular curves in  $T_D^M$ .

Now consider  $E \in \text{SS}^M(p)$ . By [Proposition 2.2](#),  $\text{End}(E)$  contains a quadratic order  $\mathcal{O}$  with discriminant  $-4M < \text{disc } \mathcal{O} < 0$ , and  $p$  does not split in the field of fractions of  $\mathcal{O}$ . Letting  $D$  be the discriminant of the field of fractions of  $\mathcal{O}$ , we hence have  $-4M \leq D < 0$  and  $(D/p) = -1$ . Since  $M$  is an integer,  $\mathcal{O} - \mathbb{Z}$  contains an element with norm at most  $M$ , so that  $E \in T_D^M$ .  $\square$

### 3. Maximal orders of quaternion algebras

Unless otherwise cited, all the material in this section can be found in [\[25\]](#).

There is a quaternion algebra  $B$  over  $\mathbb{Q}$ , unique up to isomorphism, that ramifies exactly at  $p$  and  $\infty$ . For  $p \neq 2$ , we can take

$$B := \{w + xi + yj + zk : w, x, y, z \in \mathbb{Q}\}, \quad i^2 = -q, \quad j^2 = -p, \quad ij = -ji = k$$

for an appropriate integer  $q$  depending on  $p \pmod{8}$  [\[17, Proposition 5.1\]](#).

Given  $\alpha = w + xi + yj + zk \in B$ , we define its *conjugate*,  $\bar{\alpha} := w - ix - jy - kz$ , its *reduced norm*,  $\text{nrd}(\alpha) := \alpha\bar{\alpha} = w^2 + qx^2 + py^2 + qpz^2$ , and its *reduced trace*,  $\text{trd}(\alpha) := \alpha + \bar{\alpha} = 2w$ . Any  $\alpha \in B$  is the root of a polynomial

$$x^2 - \text{trd}(\alpha)x + \text{nrd}(\alpha)$$

with rational coefficients; if  $\alpha \notin \mathbb{Q}$ , this is the *minimal polynomial* of  $\alpha$ . Any  $\alpha \notin \mathbb{Q}$  generates an imaginary quadratic subfield  $\mathbb{Q}(\alpha) \subseteq B$ . Conversely, an imaginary quadratic field  $K$  embeds into  $B$  if and only if  $p$  does not split in  $K$  [\[25, Proposition 14.6.7\]](#), or equivalently, if the Legendre symbol  $((\text{disc } K)/p)$  is not equal to 1.

An *ideal*  $I \subseteq B$  is a subgroup under addition which is generated by a basis of  $B$  considered as a vector space over  $\mathbb{Q}$ . An *order*  $\mathfrak{O} \subseteq B$  is an ideal which contains 1 and is closed under multiplication. An order is *maximal* if there are no orders properly containing it. An element  $\alpha \in B$  with  $\text{trd}(\alpha), \text{nrd}(\alpha) \in \mathbb{Z}$  is called *integral*;  $\alpha$  is integral if and only if it is contained in some order of  $B$ .

Given an ideal  $I \subseteq B$ , we can define *left and right orders of  $I$* ,

$$\mathfrak{O}_L(I) := \{x \in B : xI \subseteq I\}, \quad \mathfrak{O}_R(I) := \{x \in B : Ix \subseteq I\}.$$

We say that  $I$  is a *left ideal of  $\mathfrak{O}$*  if  $\mathfrak{O}_L(I) = \mathfrak{O}$ , and that  $I$  is a *right ideal of  $\mathfrak{O}'$*  if  $\mathfrak{O}_R(I) = \mathfrak{O}'$ . In this scenario we say  *$I$  links  $\mathfrak{O}$  to  $\mathfrak{O}'$* .

An ideal  $I$  that is closed under multiplication is called an *integral ideal*. An integral ideal is necessarily contained in its left and right orders, and hence  $\text{nrd}(\alpha) \in \mathbb{Z}$  for all  $\alpha$  in an integral ideal. Given an integral ideal  $I \subseteq B$ , the *reduced norm of  $I$*  is defined to be

$$\text{nrd}(I) := \gcd\{\text{nrd}(\alpha) \mid \alpha \in I\}.$$

Given a quadratic order  $\mathcal{O}$  and a maximal order  $\mathfrak{D} \subseteq B$ , we say that  $\mathcal{O}$  is *optimally embedded* in  $\mathfrak{D}$  if  $\mathcal{O} \cong \mathfrak{D} \cap K$  for some subfield  $K \subseteq B$ . The map  $\mathcal{O} \rightarrow B$  with image  $\mathfrak{D} \cap K$  is an *optimal embedding*.

**3A. The Deuring correspondence.** Let  $\text{SS}(p) \subseteq \mathbb{F}_{p^2}$  denote the set of supersingular curves up to  $\overline{\mathbb{F}}_p$ -isomorphism. Given  $E \in \text{SS}(p)$ ,  $\text{End}(E)$  will be isomorphic to a maximal order in  $B$ . If  $E$  and  $E^{(p)}$  are Frobenius conjugates, then  $\text{End}(E)$  and  $\text{End}(E^{(p)})$  will be isomorphic orders. Aside from this relation, nonisomorphic curves will always have nonisomorphic endomorphism rings. In fact, we have a bijection, known as the *Deuring correspondence*

$$\text{SS}(p)/(E \sim E^{(p)}) \leftrightarrow \{\text{maximal orders of } B\}/\cong$$

sending  $E$  to the set of maximal orders isomorphic to  $\text{End}(E)$ . The degree (resp. trace, resp. dual) of an endomorphism is equal to the norm (resp. trace, resp. conjugate) of the corresponding element of  $B$ , and composition of endomorphisms corresponds to multiplication of elements of  $B$ . Further, if we fix  $E \in \text{SS}(p)$  and a maximal order  $\mathfrak{D}_E \cong \text{End}(E)$ , then we have a one-to-one correspondence

$$\{\text{separable isogenies out of } E\}/\cong \leftrightarrow \{\text{left ideals of } \mathfrak{D}_E\}.$$

An isogeny  $\phi : E \rightarrow E'$  will correspond to an ideal  $I$  linking  $\mathfrak{D}_E$  to some maximal order  $\mathfrak{D}_{E'}$  isomorphic to  $\text{End}(E')$ , and  $\deg \phi = \text{nrd}(I)$ .

#### 4. Large distances between $T_D^M$

We first define a notion of distance between maximal orders and prove some of its properties. We will then use this notion to prove part (a) of [Theorem 1.3](#).

##### 4A. Distance between maximal orders.

**Definition 4.1.** Given maximal orders  $\mathfrak{D}, \mathfrak{D}' \subseteq B$ , the *distance from  $\mathfrak{D}$  to  $\mathfrak{D}'$* ,  $d(\mathfrak{D}, \mathfrak{D}')$ , is any of the following quantities:

- (a)  $|\mathfrak{D} : \mathfrak{D} \cap \mathfrak{D}'|$  (the index of  $\mathfrak{D} \cap \mathfrak{D}'$  in  $\mathfrak{D}$ ).
- (b)  $|\mathfrak{D}' : \mathfrak{D} \cap \mathfrak{D}'|$  (the index of  $\mathfrak{D} \cap \mathfrak{D}'$  in  $\mathfrak{D}'$ ).
- (c) The smallest reduced norm of an integral ideal linking  $\mathfrak{D}$  to  $\mathfrak{D}'$ .

**Lemma 4.2.** *The three quantities in [Definition 4.1](#) are all equal.*

*Proof.* We observe that these values are equal if and only if the corresponding quantities obtained by localizing at each prime are all equal [\[25, Lemma 9.5.7\]](#). There is a unique maximal order at the ramified prime  $p$ , and so all three of the local quantities at  $p$  are equal to 1.

For  $\ell \neq p$ , the statement follows from the theory of the Bruhat–Tits tree [\[25, Section 23.5\]](#). Specifically, we have  $B_\ell \cong M_2(\mathbb{Q}_\ell)$ . With respect to an appropriate basis, if we set  $\varpi = \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}$ , we will have  $\mathfrak{D}_\ell = M_2(\mathbb{Z}_\ell)$  and  $\mathfrak{D}'_\ell = \varpi^{-e} \mathfrak{D}_\ell \varpi^e$  for some exponent  $e$  [\[25, Lemma 23.5.14\]](#). Then  $\mathfrak{D}_\ell \varpi^e = \varpi^e \mathfrak{D}'_\ell$  is the

linking ideal of smallest reduced norm, and we can check directly that

$$|\mathfrak{D}_\ell : \mathfrak{D}_\ell \cap \mathfrak{D}'_\ell| = |\mathfrak{D}'_\ell : \mathfrak{D}_\ell \cap \mathfrak{D}'_\ell| = \text{nrd}(\mathfrak{D}_\ell \varpi^e) = \ell^e. \quad \square$$

Note that  $\log d$  defines a metric on the set of maximal orders of  $B$ ; the triangle inequality follows because  $\text{nrd}(IJ) \leq \text{nrd}(I) \text{nrd}(J)$  for any compatible ideals  $I$  and  $J$  [25, Example 16.3.6]. Unlike distances between elliptic curves, Definition 4.1 is *not* isomorphism-invariant, but we can relate the two notions of distance as follows.

**Lemma 4.3.** *Let  $E$  and  $E'$  be supersingular curves. Then*

$$d(E, E') = \min\{d(\mathfrak{D}, \mathfrak{D}') \mid \mathfrak{D} \cong \text{End}(E), \mathfrak{D}' \cong \text{End}(E')\}.$$

*Proof.* By the Deuring correspondence, both sides are equal to

$$\min\{\deg \phi \mid \phi : E \rightarrow E'' \text{ for some } E'' \in \text{SS}(p) \text{ with } \text{End}(E'') \cong \text{End}(E')\}. \quad \square$$

**4B. Proof of Theorem 1.3(a).** Suppose that  $E \in T_D^M$  and  $E' \in T_{D'}^M$ . Let  $\mathfrak{D} \cong \text{End}(E)$  and  $\mathfrak{D}' \cong \text{End}(E')$  be maximal orders in  $B$ . Thus there exist  $\alpha \in \mathfrak{D} - \mathbb{Z}$  and  $\alpha' \in \mathfrak{D}' - \mathbb{Z}$ , each with reduced norm at most  $M$ . The quadratic orders

$$\mathcal{O} := \mathbb{Q}(\alpha) \cap \mathfrak{D} \quad \text{and} \quad \mathcal{O}' := \mathbb{Q}(\alpha') \cap \mathfrak{D}$$

are both optimally embedded in  $\mathfrak{D}$ . Since  $\mathbb{Q}(\alpha) \not\cong \mathbb{Q}(\alpha')$ ,  $\mathcal{O}$  and  $\mathcal{O}'$  are distinct. Hence

$$\text{disc } \mathcal{O} \text{ disc } \mathcal{O}' \geq 4p,$$

as a result of the following theorem due to Kaneko.

**Theorem 4.4** [12, Theorem 2']. *Let  $\mathfrak{D} \subseteq B$  be a maximal order. If  $\mathcal{O}$  and  $\mathcal{O}'$  are quadratic orders of imaginary quadratic fields, optimally embedded into  $\mathfrak{D}$  with distinct images, then  $\text{disc } \mathcal{O} \text{ disc } \mathcal{O}' \geq 4p$ . If in addition  $\mathcal{O}$  and  $\mathcal{O}'$  have isomorphic fields of fractions, then  $\text{disc } \mathcal{O} \text{ disc } \mathcal{O}' \geq p^2$ .*

Let  $D$  denote the discriminant of  $K = \mathbb{Q}(\alpha)$ . Since  $\alpha \in \mathcal{O} - \mathbb{Z}$ , and the quadratic order  $\mathcal{O}$  must be of the form  $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$  for some positive integer  $f$ , we have

$$\text{nrd}(\alpha) \geq N_{K/\mathbb{Q}}\left(\frac{1}{2}f\sqrt{D}\right) = \frac{1}{4} \text{disc } \mathcal{O}.$$

Letting  $d = d(\mathfrak{D}, \mathfrak{D}') = |\mathfrak{D}' : \mathfrak{D} \cap \mathfrak{D}'|$ , we have  $d\alpha' \in \mathfrak{D} \cap \mathfrak{D}' \subseteq \mathfrak{D}$ . As we did with  $\text{nrd}(\alpha)$ , we can compute  $d^2 \text{nrd}(\alpha') \geq \frac{1}{4} \text{disc } \mathcal{O}'$ . Hence

$$d^2 M^2 \geq d^2 \text{nrd}(\alpha) \text{nrd}(\alpha') \geq \frac{1}{16} \text{disc } \mathcal{O} \text{ disc } \mathcal{O}' \geq \frac{p}{4}.$$

This implies that  $d(\mathfrak{D}, \mathfrak{D}') \geq \sqrt{p}/(2M)$ . Since this bound holds for all maximal orders  $\mathfrak{D} \cong \text{End}(E)$  and  $\mathfrak{D}' \cong \text{End}(E')$ , Lemma 4.3 allows us to conclude that  $d(E, E') \geq \sqrt{p}/(2M)$ , concluding the proof of Theorem 1.3(a).

## 5. Short paths within $T_D^M$

We first introduce the theory of orientations<sup>4</sup> as defined by Colò and Kohel [7]. We then use these results to prove part (b) of Theorem 1.3.

### 5A. Orientations.

**Definition 5.1.** Given a supersingular curve  $E \in \text{SS}(p)$  and an imaginary quadratic field  $K$ , a  $K$ -orientation of  $E$  is a fixed embedding  $\iota : K \hookrightarrow \text{End}(E) \otimes \mathbb{Q}$ . Given a quadratic order  $\mathcal{O} \subseteq K$ , a  $K$ -orientation is a *primitive  $\mathcal{O}$ -orientation* if  $\text{End}(E) \cap \iota(K) \cong \mathcal{O}$ , or in other words, if  $\iota$  restricted to  $\mathcal{O}$  is an optimal embedding of  $\mathcal{O}$  in  $\text{End}(E)$ .

**Definition 5.2.** If  $E, E' \in \text{SS}(p)$  have  $K$ -orientations  $\iota$  and  $\iota'$ , respectively, an isogeny  $\phi : E \rightarrow E'$  is  $K$ -oriented if

$$\iota'(x) = \frac{1}{\deg \phi} \phi \circ \iota(x) \circ \widehat{\phi}, \quad x \in K,$$

where  $\widehat{\phi}$  denotes the dual isogeny of  $\phi$ .

Let  $\text{SS}_{\mathcal{O}}(p)$  denote the set of elliptic curves equipped with a primitive  $\mathcal{O}$ -orientation, up to  $K$ -oriented isomorphism. Onuki describes two types of isogenies that we will use to construct paths. First there are “ascending” isogenies, which can be used to decrease the conductor of the optimally embedded quadratic order.

**Proposition 5.3** [16, Proposition 4.1]. *Suppose  $\ell$  is a prime and  $f$  is a positive integer. Let  $\mathcal{O} \subseteq K$  have conductor  $\ell f$ , and  $\mathcal{O}' \subseteq K$  have conductor  $f$ . Then for any  $(E, \iota) \in \text{SS}_{\mathcal{O}}(p)$ , there exists  $(E', \iota') \in \text{SS}_{\mathcal{O}'}(p)$  with a  $K$ -oriented isogeny  $E \rightarrow E'$  of degree  $\ell$ .*

In order to describe “horizontal” isogenies, we first describe an action of the class group  $\text{Cl}(\mathcal{O})$  on  $\text{SS}_{\mathcal{O}}(p)$ . Given an invertible ideal  $\mathfrak{a} \subseteq \mathcal{O}$  relatively prime to  $p$ , and a curve  $E$  with a primitive  $\mathcal{O}$ -orientation, define the  $\mathfrak{a}$ -torsion subgroup

$$E[\mathfrak{a}] := \bigcap_{x \in \mathfrak{a}} \ker \iota(x).$$

Up to  $K$ -oriented isomorphism, there is a unique elliptic curve  $(\mathfrak{a} * E)$  with a primitive  $\mathcal{O}$ -orientation and a separable isogeny  $\phi_{\mathfrak{a}} : E \rightarrow (\mathfrak{a} * E)$  such that  $\ker \phi_{\mathfrak{a}} = E[\mathfrak{a}]$  [16, Proposition 3.5]. Since principal ideals act by endomorphisms, the action  $(\mathfrak{a}, E) \mapsto \mathfrak{a} * E$  is well-defined on ideal classes.

**Proposition 5.4** [16, Proposition 3.3 and Theorem 3.4]. *Suppose  $p$  does not divide the conductor of  $\mathcal{O}$ . Either the ideal class group  $\text{Cl}(\mathcal{O})$  acts transitively on  $\text{SS}_{\mathcal{O}}(p)$ , or  $\text{SS}_{\mathcal{O}}(p)$  splits into two conjugate orbits:  $(E, \iota)$  is in one orbit if and only if  $(E^{(p)}, \iota^{(p)})$  is in the other.*

<sup>4</sup>A previous version of this paper took a different approach to proving analogues of Propositions 5.3 and 5.4. While the underlying ideas are similar, we have found that the language of orientations provides a much cleaner framework for these results.

Suppose  $E \in \text{SS}_{\mathcal{O}}(p)$  and  $\mathfrak{a}$  is an invertible ideal of  $\mathcal{O}$  relatively prime to  $p$ . The proof of [16, Proposition 3.5] shows that the dual isogeny of  $\phi_{\mathfrak{a}}$  has kernel  $(\mathfrak{a} * E)[\bar{\mathfrak{a}}]$ , and so by the proof of [16, Proposition 3.6],  $\widehat{\phi}_{\mathfrak{a}} \circ \phi_{\mathfrak{a}}$  has kernel  $E[\bar{\mathfrak{a}}\mathfrak{a}] = E[N(\mathfrak{a})]$ . Thus

$$\begin{aligned} (\deg \phi_{\mathfrak{a}})^2 &= \deg(\widehat{\phi}_{\mathfrak{a}} \circ \phi_{\mathfrak{a}}) \\ &= |E[N(\mathfrak{a})]| = N(\mathfrak{a})^2, \end{aligned}$$

so we can conclude that  $\deg \phi_{\mathfrak{a}} = N(\mathfrak{a})$ .

**5B. Proof of Theorem 1.3(b).** Suppose  $E, E' \in T_D^M$ , so there exist  $\alpha \in \text{End}(E) - \mathbb{Z}$  and  $\alpha' \in \text{End}(E') - \mathbb{Z}$  with  $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\alpha')$ . Set  $K \cong \mathbb{Q}(\alpha)$ .

*Ascending isogenies.* We may equip  $E$  with a  $K$ -orientation  $\iota$  that has image  $\mathbb{Q}(\alpha) \subseteq \text{End}(E) \otimes \mathbb{Q}$ . This  $K$ -orientation is a primitive  $\mathcal{O}$ -orientation for some quadratic order  $\mathcal{O} \subseteq K$ . By Proposition 5.3, a sequence of  $K$ -oriented isogenies of prime degree can take us from  $E$  to a curve  $F \in \text{SS}_{\mathcal{O}_K}(p)$ , successively dividing the conductor of the optimally embedded order by one prime factor at a time. We can use the fact that  $\alpha \in \iota(\mathcal{O})$  to bound the conductor  $f$  of  $\mathcal{O}$ :

$$\frac{3}{4}f^2 \leq \frac{f^2|D|}{4} \leq \deg(\alpha) \leq M,$$

so that  $f \leq b := \frac{2}{3}\sqrt{3M}$ . Hence, the isogeny  $E \rightarrow F$  obtained by composing all the prime-degree isogenies has degree at most  $b$ .

In the same way, we can find a sequence of prime-degree isogenies from  $E'$  to a curve  $F' \in \text{SS}_{\mathcal{O}_K}(p)$ , and the degree of their composition is at most  $b$ . Take the dual to obtain an isogeny  $F' \rightarrow E'$ .

*Horizontal isogenies.* We first consider the case that  $F$  and  $F'$  are in the same orbit under the action of  $\text{Cl}(\mathcal{O}_K)$ . By Proposition 5.4, there is an ideal  $\mathfrak{a}$  of  $\mathcal{O}_K$  such that  $\mathfrak{a} * F = F'$ . Since this action depends only on the ideal class, we may take  $\mathfrak{a}$  to have norm at most  $\frac{1}{\sqrt{3}}\sqrt{|D|}$ ,<sup>5</sup> which is at most  $b = \frac{2}{3}\sqrt{3M}$  since  $|D| \leq 4M$ . Hence there is an isogeny  $F \rightarrow F'$  of degree at most  $b$ .

Combining this isogeny with the vertical isogenies found above, the sequence  $E, F, F', E'$  has consecutive distances at most  $b$ . The curves  $F$  and  $F'$  are in  $T_D^M$  because they have an optimally embedded quadratic order strictly larger than  $\mathcal{O}$  and  $\mathcal{O}'$ . This shows that we can find a sequence as in Theorem 1.3(b) with  $r = 3$ .

If  $F$  and  $F'$  are in different orbits, first apply Frobenius conjugation to  $F'$  and  $E'$  (as well as to the isogeny connecting them). Then  $F$  and  $F'^{(p)}$  are in the same  $\text{Cl}(\mathcal{O}_K)$ -orbit, so the argument above shows that the sequence  $E, F, F'^{(p)}, E'^{(p)}$  has consecutive distances at most  $b$ . But by Definition 1.1, replacing  $E'^{(p)}$  with  $E'$  does not change distances.

<sup>5</sup>Minkowski's bound has the coefficient  $\frac{2}{\pi}$  instead of  $\frac{1}{\sqrt{3}}$ , but we get a stronger bound using the Hermite constant  $\gamma_2 = \frac{2}{\sqrt{3}}$ . Namely, the fractional ideal  $\mathfrak{a}^{-1}$  must contain an element  $x$  of norm at most  $\gamma_2(\frac{1}{2}\sqrt{|D|})N(\mathfrak{a})^{-1}$ , and we can take the ideal  $x\mathfrak{a} \sim \mathfrak{a}$ .

**Prime-degree isogenies.** We decompose each of the isogenies  $E \rightarrow F$ ,  $F \rightarrow F'$ , and  $F' \rightarrow E'$  into isogenies of prime degree. Note that  $E \rightarrow F$  and  $E' \rightarrow F'$  were defined as compositions of prime-degree isogenies to begin with, and every curve along the way is in  $T_D^M$  because the optimally embedded quadratic order grows at each step. For the isogeny  $F \rightarrow F'$ , write the ideal  $\mathfrak{a}$  as a product of prime ideals. We can choose  $\mathfrak{a}$  so that none of its prime ideal factors will be principal, so that they will all have prime norm. These ideals therefore induce prime-degree isogenies, and their composition is an isogeny  $F \rightarrow F'$ .

Since the isogenies  $E \rightarrow F$ ,  $F \rightarrow F'$ , and  $F' \rightarrow E'$  each have degree  $b$ , the full sequence of prime-degree isogenies

$$E = E_0 \rightarrow E_1 \rightarrow \cdots \rightarrow E_r \cong E'$$

must satisfy

$$2^r \leq \prod_{i=1}^r d(E_{i-1}, E_i) \leq b^3,$$

which gives us the bound  $r \leq 3 \log_2 b$ .

Combining [Lemma 2.3](#), [Section 4B](#), and [Section 5B](#), we have a complete proof of [Theorem 1.3](#).

## 6. Vertical $\ell$ -isogenies have no short detours

As discussed in [Section 5](#),  $M$ -small curves within a single set  $T_D^M$  may be given a  $\mathbb{Q}(\sqrt{D})$ -orientation, and then connected by “horizontal” or “vertical” isogenies. In this section we prove that if two oriented curves are connected by a vertical  $\ell$ -isogeny, then there is no short isogeny between them with degree relatively prime to  $\ell$ .<sup>6</sup> As a result, the short paths described in [Theorem 1.3\(b\)](#) will only exist if all sufficiently small primes are allowed as degrees of isogenies.

**Proposition 6.1.** *Let  $\ell$  be a prime,  $M \in \mathbb{Z}$ , and  $\beta$  be an imaginary quadratic integer with norm at most  $M/\ell^2$ . Suppose  $E, E' \in \text{SS}^M(p)$  have  $\mathbb{Z}[\beta]$  optimally embedded in  $\text{End}(E)$  and  $\mathbb{Z}[\ell\beta]$  optimally embedded in  $\text{End}(E')$ . If  $\phi : E \rightarrow E'$  is any isogeny with degree relatively prime to  $\ell$ , then*

$$\deg \phi \geq \frac{p\ell}{4M}.$$

**Remark 6.2.** Given  $M \in \mathbb{Z}$  and prime  $\ell$ , if  $\text{SS}^{M/\ell^2}(p)$  is nonempty then there are  $E, E' \in \text{SS}^M(p)$  satisfying the conditions of [Proposition 6.1](#): we can take  $E \in \text{SS}^{M/\ell^2}(p)$  and follow a “descending”  $\ell$ -isogeny [[16](#), [Proposition 4.1](#)] to  $E'$ .

*Proof of Proposition 6.1.* Let  $\phi : E \rightarrow E'$  be an isogeny with degree relatively prime to  $\ell$ . Fix a maximal order  $\mathfrak{O} \subseteq B$  with  $\mathfrak{O} \cong \text{End}(E)$ . By the Deuring correspondence,  $\phi$  corresponds to an ideal  $I$  linking  $\mathfrak{O}$  to some maximal order  $\mathfrak{O}' \cong \text{End}(E')$ . Since  $I$  is a sublattice of  $\mathfrak{O} \cap \mathfrak{O}'$ ,  $\text{nrd}(I)^2 = |\mathfrak{O} : I|$  [[25](#), [Main Theorem 16.1.3](#)] is a multiple of  $d(\mathfrak{O}, \mathfrak{O}') = |\mathfrak{O} : \mathfrak{O} \cap \mathfrak{O}'|$ . Thus, since  $\text{nrd}(I) = \deg \phi$  is not divisible by  $\ell$ , neither is  $d(\mathfrak{O}, \mathfrak{O}')$ .

<sup>6</sup>A result of this form does not hold for horizontal isogenies, because a single ideal class may have multiple representatives with small, relatively prime norms.



If the optimal embeddings  $\mathbb{Z}[\beta] \hookrightarrow \mathfrak{D}$  and  $\mathbb{Z}[\ell\beta] \hookrightarrow \mathfrak{D}'$  were to land in the same subfield of  $B$ , then  $|\mathfrak{D} : \mathfrak{D} \cap \mathfrak{D}'|$  would be divisible by  $\ell$ , a contradiction. Hence we must have  $\mathfrak{D} \cap K \cong \mathbb{Z}[\ell\beta]$  and  $\mathfrak{D}' \cap K' \cong \mathbb{Z}[\beta]$  for distinct but isomorphic fields  $K$  and  $K'$ . Let  $\mathcal{O} := \mathfrak{D} \cap K$  and  $\mathcal{O}' := \mathfrak{D}' \cap K'$  both be optimally embedded in  $\mathfrak{D}$ . Since  $K$  and  $K'$  are isomorphic but distinct, [Theorem 4.4](#) tells us that  $\text{disc } \mathcal{O} \text{ disc } \mathcal{O}' \geq p^2$ .

Letting  $d := d(\mathfrak{D}, \mathfrak{D}')$ , we have  $\ell\beta \in \mathcal{O}$  and  $d\beta \in \mathcal{O}'$ . So just as in [Section 4B](#),

$$d^2 \ell^2 \text{nrd}(\beta)^2 \geq \frac{1}{16} \text{disc } \mathcal{O} \text{ disc } \mathcal{O}' \geq \frac{p^2}{16}.$$

Finally, applying [Definition 4.1\(c\)](#),

$$\deg \phi = \text{nrd}(I) \geq d(\mathfrak{D}, \mathfrak{D}') \geq \frac{p}{4\ell \text{nrd}(\beta)} \geq \frac{p\ell}{4M}. \quad \square$$

## 7. Isogenies between $M$ -small supersingular curves

Despite the large distances between  $M$ -small curves in distinct subsets  $T_D^M$ , we show that isogenies between them can nonetheless be computed efficiently under certain heuristic assumptions. On each “island”  $T_D^M$ , we will construct an “airport,” a curve with known endomorphism ring. To find an isogeny between two  $M$ -small curves, we will apply [Theorem 1.3\(b\)](#) to find a path from each curve to the airport on its respective island, and then compute an isogeny between the airports.

**7A. Locating the airports.** From our definition of  $B$ , we have  $j^2 = -p$  and  $i^2 = -q$  for some relatively small value of  $q$ ; for  $p \equiv 3 \pmod{4}$  we can use  $q = 1$ , and for  $p \equiv 1 \pmod{4}$  we can use the same  $q$  as in [Proposition 2.1](#), so that under GRH we have  $q = O(\log^2 p)$ . Let  $K \neq \mathbb{Q}(i)$  be a quadratic field of discriminant  $-4M \leq D < 0$ . We must make an assumption which we leave unproven, but is plausible both heuristically and experimentally (see [Remark 7.3](#)).

**Assumption 7.1.** Let  $\alpha \in B$  satisfy  $4\alpha^2 = D$  (if  $D \equiv 0 \pmod{4}$ ) or  $4\alpha^2 - 4\alpha + 1 = D$  (if  $D \equiv 1 \pmod{4}$ ). Then it is feasible to find an integral element  $\beta \in B$  with the following property: if  $n$  is the denominator of  $\text{trd}(\alpha\beta)$ , then the discriminant of the order  $\mathbb{Z}\langle\alpha, n\beta\rangle$  can be efficiently factored into primes.<sup>7</sup>

**Lemma 7.2.** Assume GRH and an oracle for [Assumption 7.1](#). Given a fundamental discriminant  $-4M \leq D < 0$  with  $(D/p) = -1$ , a maximal order of  $B$  containing an integral element  $\alpha$  with  $\text{nrd}(\alpha) \leq M$  and  $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\sqrt{D})$  can be computed in probabilistic polynomial time in  $M$  and  $\log p$ .

*Proof.* The computation is as follows. First find  $x, y, z, w \in \mathbb{Q}$  such that

$$(x + y\sqrt{D})^2 + q(z + w\sqrt{D})^2 = -p. \quad (1)$$

If we set

$$\gamma = pi + qzj + xk \quad \text{and} \quad \delta = qwj + yk,$$

<sup>7</sup>The definition of  $n$  guarantees that  $\mathbb{Z}\langle\alpha, n\beta\rangle$  is in fact an order. Aside from the fact that the discriminant will be divisible by  $p^2$  (since any order is contained in a maximal order), we expect this discriminant to behave in some sense as a “random integer” as we vary  $\beta$ . In the range of values that seem to arise in practice, integers that can be easily factored are relatively common.



the proof of [25, Lemma 5.4.7] shows that  $(\gamma\delta^{-1})^2 = D$ , giving us an explicit embedding of  $\mathbb{Q}(\sqrt{D})$  into  $B$ . Let  $\alpha = \frac{1}{2}\gamma\delta^{-1}$  or  $\alpha = \frac{1}{2}(1 + \gamma\delta^{-1})$ , whichever is integral. Then  $\alpha$  satisfies the conditions for Assumption 7.1, so we can use the oracle to find an order containing  $\alpha$  and a factorization of its discriminant. Then use [24, Proposition 4.3.4] to construct a maximal order containing this order. The resulting maximal order contains  $\alpha$ , and so the required conditions are satisfied.

We now discuss the validity and runtime of this process. If we set  $K = \mathbb{Q}(\sqrt{D})$ , there exists an embedding of  $K = \mathbb{Q}(\sqrt{D})$  into  $B$  [25, Proposition 14.6.7]. This implies that  $B \otimes_{\mathbb{Q}} K$  is split [25, Lemma 5.4.7], so there exists a solution  $v \in K(i)^{\times}$  to the relative norm equation  $N_{K(i)/K}(v) = -p$  [25, Theorem 5.4.6(vi)], implying that (1) has a solution.

We can solve (1) using an algorithm due to Simon [21, Algorithm 6.5], which requires computing the relative class group of  $K(i)/K$ , factoring the norms of the generators of the relative class group into prime ideals of  $K$ , factoring  $p$  into prime ideals of  $K$ , and linear algebra. Under GRH, the discriminant  $\Delta$  of  $K(i) \cong \mathbb{Q}(\sqrt{D}, \sqrt{-q})$  is polynomial in  $M$  and  $\log p$ , so the first two of these tasks can be done in polynomial time.<sup>8</sup> Since  $(D/p) = -1$ ,  $p$  is already prime in  $K$ , and the necessary linear algebra can also be done in polynomial time.

Constructing a maximal order containing  $\text{disc } \mathbb{Z}\langle\alpha, n\beta\rangle$  takes polynomial time in  $\log p$  and the bit-lengths of  $\alpha$  and  $n\beta$ , assuming the factorization of  $\text{disc } \mathbb{Z}\langle\alpha, n\beta\rangle$  is given, and a probabilistic algorithm (e.g., [18]) is used for factoring polynomials over finite fields.  $\square$

**Remark 7.3.** We checked Assumption 7.1 experimentally using Magma, by computing the maximal order of Lemma 7.2 for  $p = 2^{256} + 297$  (in this case we can take  $q = 7$ ),  $M = 100$ , and all 62 allowable values of  $D$ . We used the function `NormEquation` to solve the relative norm equation, and `MaximalOrder` to find a maximal order containing a given order. In every case, either  $\beta = i$  or  $\beta = j$  satisfied Assumption 7.1. Constructing all of these maximal orders took 60 seconds on a generic personal laptop (16 GB RAM, 1.80 GHz CPU).

**7B. An algorithm for computing isogenies.** We describe an algorithm<sup>9</sup> for computing an isogeny between any two curves  $E, E' \in \text{SS}(p)$ . In general, the runtime will be exponential in  $\log p$ , but it is efficient when  $E$  and  $E'$  are both  $M$ -small for relatively small  $M$ . Note that the algorithm does not require knowledge of any noninteger endomorphisms of  $E$  or  $E'$ , or even a nontrivial bound on  $M$ .

**Lemma 7.4.** *Let  $M < p$  be such that  $E, E' \in \text{SS}^M(p)$  (the value of  $M$  may not be known to the algorithm).<sup>10</sup> Assuming GRH and an oracle for Assumption 7.1, Algorithm 1 runs successfully in probabilistic polynomial time in  $M$  and  $\log p$ .*

<sup>8</sup>The (absolute) class groups  $\text{Cl}(K(i))$  and  $\text{Cl}(K)$  can be computed in probabilistic subexponential time in  $\log|\Delta|$  [3], and the relative class group can be efficiently computed from this data using linear algebra [6, Algorithm 7.3.1]. Under GRH, generators of the relative class group will have (absolute) norm  $O(\log^2|\Delta|)$  [6, p. 369] and so factoring their (relative) norms can also be done efficiently.

<sup>9</sup>This algorithm is primarily a proof of concept; there is a lot of optimization that can be done if it is to be used in practice.

<sup>10</sup>Every  $E \in \text{SS}(p)$  is  $M$ -small for  $M = \lfloor \frac{1}{2}p^{2/3} + \frac{1}{4} \rfloor$  [11, Section 4].

---

**Algorithm 1:** Computing isogenies between supersingular curves.

---

**Input** :  $E, E' \in \text{SS}(p)$ .

**Output** : An isogeny  $E \rightarrow E'$ .

- (1) Find the roots in  $\mathbb{F}_{p^2}$  of the Hilbert class polynomials  $H_{\mathcal{O}}(x) \pmod{p}$ , for quadratic orders  $\mathcal{O}$  of successively increasing discriminant. Stop when the  $j$ -invariant of  $E$  is found as a root of  $H_{\mathcal{O}_E}(x) \pmod{p}$ , for some order  $\mathcal{O}_E$ . Let  $S$  denote the set of all roots in  $\mathbb{F}_{p^2}$  of all quadratic orders considered.
- (2) Let  $D$  be the discriminant of the field of fractions of  $\mathcal{O}_E$ . Compute a maximal order  $\mathfrak{O}_D \subseteq B$  as in [Lemma 7.2](#).
- (3) Compute an elliptic curve  $E_D \in \text{SS}(p)$  such that  $\text{End}(E_D) \cong \mathfrak{O}_D$ .
- (4) Find an isogeny in  $S$  from  $E$  to  $E_D$  by breadth-first search. That is, from the current curve, use modular polynomials to find all curves in  $S$  that are connected to the current curve by an isogeny of prime degree at most

$$\frac{2}{3}\sqrt{3\lceil \frac{1}{4}|\text{disc } \mathcal{O}_E| \rceil}.$$

Continue until either  $E_D$  or  $E_D^{(p)}$  is found. If  $E_D^{(p)}$  is found, replace  $E_D$  with  $E_D^{(p)}$ .

- (5) Repeat Steps (1) to (4) for  $E'$ , obtaining a curve  $E_{D'}$  with known endomorphism ring, as well as a path from  $E'$  to  $E_{D'}$ .
  - (6) Compute an isogeny from  $E_D$  to  $E_{D'}$ .
  - (7) Compose the isogeny  $E \rightarrow E_D$  (from Step (4)), the isogeny  $E_D \rightarrow E_{D'}$  (from Step (6)), and the isogeny  $E_{D'} \rightarrow E'$  (dual of the isogeny from Step (5)).
- 

*Proof.* First we examine Step (1). Each polynomial  $H_{\mathcal{O}}(x) \pmod{p}$  can be computed in  $O(|\text{disc } \mathcal{O}|^{1+\varepsilon})$  time [\[23, Theorem 1\]](#). The roots of this polynomial in  $\mathbb{F}_{p^2}$  can be found by factoring it over  $\mathbb{F}_p$ , and keeping the linear and quadratic factors. There is a probabilistic algorithm for factoring which is polynomial time in  $\deg H_{\mathcal{O}}(x)$  and  $\log p$  [\[18\]](#). The degree of  $H_{\mathcal{O}}(x)$  equals the class number of  $\mathcal{O}$ , which is  $O(|\text{disc } \mathcal{O}|^{1/2+\varepsilon})$ . By [Proposition 2.2](#), the  $j$ -invariant of  $E$  is a root of  $H_{\mathcal{O}_E}(x) \pmod{p}$  for an order  $\mathcal{O}_E$  with  $|\text{disc } \mathcal{O}_E| \leq 4M$ , so Step (1) computes  $S$  and  $\mathcal{O}_E$  in time polynomial in  $M$  and  $\log p$ .

Step (2) requires an oracle for [Assumption 7.1](#) but otherwise runs in polynomial time in  $M$  and  $\log p$ ; note that  $(D/p) = -1$  by [Proposition 2.2](#) so the conditions of [Lemma 7.2](#) are met. There are known algorithms for performing Steps (3) [\[10, Proposition 13\]](#) and (6) [\[10, Proposition 7\]](#) in polynomial time.

Now consider Step (4). Let  $\widehat{M} = \lceil \frac{1}{4}|\text{disc } \mathcal{O}_E| \rceil$ , so that  $-\widehat{M} \leq \text{disc } \mathcal{O}_E < 0$ . Thus  $E \in T_D^{\widehat{M}}$ , and  $E_D \in T_D^{\widehat{M}}$  by the properties of  $\mathfrak{O}$  described in [Lemma 7.2](#). Since  $S$  contains  $\text{SS}^{\widehat{M}}(p)$  by construction, [Theorem 1.3\(b\)](#) guarantees that Step (4) will find a path from  $E$  to either  $E_D$  or  $E_D^{(p)}$ . Since the number of elements of  $S$  is polynomial in  $M$ , the process can be done in time polynomial in  $M$  and  $\log p$ . Replacing  $E_D$  with  $E_D^{(p)}$  does not change the endomorphism ring, and so Step (6) can still be done.  $\square$

**7C. Isogenies defined over  $\mathbb{F}_p$ .** Suppose  $E$  and  $E'$  are  $M$ -small curves defined over  $\mathbb{F}_p$ . Some situations, such as key recovery for the CSIDH protocol [\[4\]](#), require being able to find an  $\mathbb{F}_p$ -isogeny  $E \rightarrow E'$ . While [Algorithm 1](#) allows us to construct an isogeny between these curves, this isogeny will not necessarily be

defined over  $\mathbb{F}_p$ . This is solved by concurrent work of Castryck, Panny, and Vercauteren [5], in which they provide an algorithm to compute an  $\mathbb{F}_p$ -isogeny  $E \rightarrow E'$ , given the endomorphism rings of  $E$  and  $E'$  (which can be computed from the isogenies  $E \rightarrow E_D$  and  $E' \rightarrow E_{D'}$ , found in Steps (4) and (5) of Algorithm 1).

## Acknowledgments

We would like to thank John Voight for crucial insights behind the results of Section 7, and Akshay Venkatesh for pointing us towards the key ideas necessary for Section 5. We also thank the anonymous reviewers for many improvements, including a local proof for Lemma 4.2, a significant improvement to the bound in Theorem 1.3(a), and catching many errors.

Several attendees of the XIVth Algorithmic Number Theory Symposium also helped to improve this paper after its initial presentation. We especially thank Boris Fouotsa Tako, Lorenz Panny, and Noam Elkies for pointing out ways to improve the presentation of Section 5, and Frederik Vercauteren and Steven Galbraith for attentive editing and constructive feedback.

## References

- [1] Sarah Arpin, Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Travis Scholl, and Jana Sotáková, *Adventures in Supersingularland*, 2019. [arXiv 1909.07779](#)
- [2] Reinier Bröker, *Constructing supersingular elliptic curves*, J. Comb. Number Theory **1** (2009), no. 3, 269–273. [MR 2681311](#)
- [3] Johannes A. Buchmann, *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields*, Séminaire de Théorie des Nombres, Paris 1988–89 (Catherine Goldstein, ed.), Progress in Mathematics, no. 91, Birkhäuser Boston, Boston, MA, 1990, pp. 27–41.
- [4] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes, *CSIDH: an efficient post-quantum commutative group action*, Advances in Cryptology – ASIACRYPT 2018 (Thomas Peyrin and Steven Galbraith, eds.), Springer International Publishing, 2018, pp. 395–427.
- [5] Wouter Castryck, Lorenz Panny, and Frederik Vercauteren, *Rational isogenies from irrational endomorphisms*, Advances in Cryptology – EUROCRYPT 2020 (Anne Canteaut and Yuval Ishai, eds.), Springer International Publishing, 2020, pp. 523–548.
- [6] Henri Cohen, *Advanced topics in computational number theory*, Springer, 2000.
- [7] Leonardo Colò and David Kohel, *Orienting supersingular isogeny graphs*, Number-Theoretic Methods in Cryptology 2019, 2019.
- [8] David A. Cox, *Primes of the form  $x^2 + ny^2$ : Fermat, class field theory, and complex multiplication*, 2 ed., Wiley, 2013.
- [9] Luca De Feo, Simon Masson, Christophe Petit, and Antonio Sanso, *Verifiable delay functions from supersingular isogenies and pairings*, Advances in Cryptology – ASIACRYPT 2019 (Steven D. Galbraith and Shihō Moriai, eds.), Springer International Publishing, 2019, pp. 248–277.
- [10] Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit, *Supersingular isogeny graphs and endomorphism rings: reductions and solutions*, Advances in Cryptology – EUROCRYPT 2018 (Jesper Buus Nielsen and Vincent Rijmen, eds.), Springer International Publishing, 2018, pp. 329–368.
- [11] Noam D. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over  $\mathbb{Q}$* , *Inventiones mathematicae* **89** (1987), no. 3, 561–567.
- [12] Masanobu Kaneko, *Supersingular  $j$ -invariants as singular moduli mod  $p$* , *Osaka Journal of Mathematics* **26** (1989), no. 4, 849–855.

- [13] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol, *On the quaternion  $\ell$ -isogeny path problem*, LMS Journal of Computation and Mathematics **17** (2014), 418–432.
- [14] Serge Lang, *Elliptic functions*, Springer, 1987.
- [15] Jonathan Love and Dan Boneh, *Supersingular curves with smal non-integer endomorphisms*, 2020. [arXiv 1910.03180](#)
- [16] Hiroshi Onuki, *On oriented supersingular elliptic curves*, 2020. [arXiv 2002.09894](#)
- [17] Arnold Pizer, *An algorithm for computing modular forms on  $\Gamma_0(N)$* , Journal of Algebra **64** (1980), 340–390.
- [18] Michael O. Rabin, *Probabilistic algorithms in finite fields*, SIAM J. Comput. **9** (1980), 273–280.
- [19] Joseph H. Silverman, *The arithmetic of elliptic curves*, 2 ed., Springer-Verlag, 2009.
- [20] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, 1994.
- [21] Denis Simon, *Solving norm equations in relative number fields using  $S$ -units*, Mathematics of Computation **71** (2002), 1287–1305.
- [22] Andrew V. Sutherland, *Isogeny volcanoes*, The Open Book Series **1** (2012).
- [23] Andrew V. Sutherland, *Computing Hilbert class polynomials with the Chinese remainder theorem*, Mathematics of Computation **80** (2011), no. 273, 501–538.
- [24] John Voight, *Quadratic forms and quaternion algebras: algorithms and arithmetic*, Ph.D. thesis, Berkeley, CA, USA, 2005.
- [25] John Voight, *Quaternion algebras*, 2020.

Received 20 Feb 2020.

JONATHAN LOVE: [jonlove@stanford.edu](mailto:jonlove@stanford.edu)

Department of Mathematics, Stanford University, Stanford, CA, United States

DAN BONEH: [dabo@cs.stanford.edu](mailto:dabo@cs.stanford.edu)

Computer Science Department, Stanford University, Stanford, CA, United States

# Cubic post-critically finite polynomials defined over $\mathbb{Q}$

Jacqueline Anderson, Michelle Manes, and Bella Tobin

We find all post-critically finite (PCF) cubic polynomials defined over  $\mathbb{Q}$ , up to conjugacy over  $\mathrm{PGL}_2(\overline{\mathbb{Q}})$ . We describe normal forms that classify equivalence classes of cubic polynomials while respecting the field of definition. Applying known bounds on the coefficients of post-critically bounded polynomials to these normal forms simultaneously at all places of  $\mathbb{Q}$ , we create a finite search space of cubic polynomials over  $\mathbb{Q}$  that may be PCF. Using a computer search of these possibly PCF cubic polynomials, we find fifteen which are in fact PCF.

## 1. Introduction

Let  $K$  be a number field, and let  $f(z) \in K[z]$  have degree  $d \geq 2$ . Consider iterates of  $f$ :

$$f^n(z) := \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ times}}(z), \quad \text{and} \quad f^0(z) := z.$$

The orbit of a point  $\alpha \in \overline{K}$  is the set  $\mathcal{O}_f(\alpha) = \{f^n(\alpha) \mid n \geq 0\}$ .

Rather than studying individual polynomials, we consider equivalence classes of polynomials under conjugation by affine elements  $\phi \in \mathrm{PGL}_2(\overline{K})$ . For  $\phi(z) = az + b \in \overline{K}[z]$ , we define

$$f^\phi = \phi \circ f \circ \phi^{-1}.$$

Note that  $f$  and  $f^\phi$  have the same dynamical behavior over  $\overline{K}$  in the sense that  $\phi$  maps the orbit  $\mathcal{O}_f(\alpha)$  to  $\mathcal{O}_{f^\phi}(\phi(\alpha))$ .

Critical points of  $f$  are the points  $\alpha \in \overline{K}$  such that  $f'(\alpha) = 0$ . Branner and Hubbard write in [6] “the main question to ask about a rational map is: *what are the orbits under iteration of the critical points?*” Of particular interest are functions for which all critical points have either a bounded or finite orbit.

**Definition 1.1.** A polynomial  $f$  is *postcritically finite* (PCF) if the orbit of each critical point is finite. A polynomial is *postcritically bounded* with respect to a given absolute value if the orbit of each critical point is bounded with respect to that absolute value.

Manes’ work partially supported by Simons collaboration grant #359721.

MSC2010: 37P05.

*Keywords:* arithmetic dynamics, post-critically finite, cubic polynomials.

The study of PCF maps has a long history in complex dynamics, from Thurston's work in the early 1980s and continuing to the present day, for example [3; 9; 10; 11; 12; 13]. In [18], Silverman describes PCF maps as an analog of abelian varieties with complex multiplication, so these maps are of particular interest in arithmetic dynamics as well. For example, all quadratic post-critically finite rational maps over  $\mathbb{Q}$  have been found in [15], and many cubic post-critically finite polynomials over  $\mathbb{Q}$  have been found in [14].

**Theorem.** *There are exactly fifteen  $\overline{\mathbb{Q}}$  conjugacy classes of cubic PCF polynomials defined over  $\mathbb{Q}$ :*

(1) $z^3$	(2) $-z^3 + 1$	(3) $-2z^3 + 3z^2 + \frac{1}{2}$
(4) $-2z^3 + 3z^2$	(5) $-z^3 + \frac{3}{2}z^2 + 1$	(6) $2z^3 - 3z^2 + 1$
(7) $2z^3 - 3z^2 + \frac{1}{2}$	(8) $z^3 - \frac{3}{2}z^2$	(9) $-3z^3 + \frac{9}{2}z^2$
(10) $-4z^3 + 6z^2 - \frac{1}{2}$	(11) $4z^3 - 6z^2 + \frac{3}{2}$	(12) $3z^3 - \frac{9}{2}z^2 + 1$
(13) $-z^3 + \frac{3}{2}z^2 - 1$	(14) $-\frac{1}{4}z^3 + \frac{3}{2}z + 2$	(15) $-\frac{1}{28}z^3 - \frac{3}{4}z + \frac{7}{2}$

Of these, (1), (4), (6), (8), (10), and (11) were found by Ingram in [14]. To complete the list, we adapt Ingram's techniques as described below.

Let  $K$  be a number field, and let  $f(z) \in K[z]$  be a cubic polynomial. Critical points of  $f$  are roots of the quadratic polynomial  $f'(z) \in K[z]$ , so there are three possibilities:

- (a) There are two distinct critical points:  $\gamma_1 \neq \gamma_2$ , and they are both  $K$ -rational.
- (b) There are two distinct critical points  $\gamma_1 \neq \gamma_2$  with  $K(\gamma_1) = K(\gamma_2)$  a quadratic extension of  $K$ .
- (c) There is exactly one critical point,  $\gamma \in K$ .

In the first two cases, we say that  $f$  is *bicritical*. In the third case, we say  $f$  is *unicritical*. In determining a complete list of cubic PCF polynomials defined over  $\mathbb{Q}[z]$ , we treat each of these cases separately:

- (1) For each of cases (a)–(c) above, find a normal form for cubic polynomials such that every cubic polynomial over  $\mathbb{Q}[z]$  is conjugate to a map in one of these forms, and the conjugation respects the field of definition for the given case.
- (2) For a map to be PCF, it must be post-critically bounded in each absolute value. Find archimedean and  $p$ -adic bounds on the coefficients for maps in the normal forms to be post-critically bounded.
- (3) Use the bounds in (2) to create a finite search space of possibly PCF maps.
- (4) For each map in the finite search space, test if it is PCF or not.

**1A. Outline.** We begin in Section 2 by treating the special case of a polynomial with a unique critical point. In Section 3, we find the normal forms needed in Step (1) of the algorithm above. Section 4 provides the coefficient bounds described in Step (2). Finally, Section 5 describes the algorithms and provides the complete list of PCF cubic polynomials defined over  $\mathbb{Q}$ .

## 2. Unicritical PCF polynomials

We begin by considering unicritical PCF polynomials. First, we will determine a normal form for unicritical polynomials of arbitrary degree defined over a number field  $K$ . In [8], Buff studied unicritical polynomials from a complex dynamics point of view, and he used that work to answer questions of Milnor and of Baker and DeMarco. Some of his preliminary work overlaps with the work here, specifically the normal form in Theorem 2.1 and the bound on  $|a|$  in Proposition 2.2. Because Buff was working over  $\mathbb{C}$ , he did not consider questions about field of definition. Therefore, we provide full proofs of these results from a more arithmetic point of view.

**Theorem 2.1.** *Let  $f(z) \in K[z]$  be a degree  $d$  unicritical polynomial. Then either  $f(z)$  is  $\bar{K}$ -conjugate to  $z^d$ , or  $f$  is conjugate to a unique polynomial of the form*

$$az^d + 1 \in K[z].$$

*Proof.* Without loss of generality, we may replace  $f$  by a conjugate map where the unique critical point  $\gamma$  is moved to 0. Since  $\gamma \in K$ , this does not change the field of definition. So we assume that  $f(z) = bz^d + c \in K[z]$ .

If  $c = 0$ , then  $f(z) = bz^d$  for  $b \in K^\times$ . Letting  $\phi(z) = b^{1/(d-1)}z$ , we have  $f^\phi(z) = z^d$ .

Now, assume  $c \neq 0$ . Conjugating by  $\phi(z) = z/c$  gives

$$f^\phi(z) = bc^{d-1}z^d + 1.$$

Since  $b, c \in K^\times$ , then  $bc^{d-1} \in K^\times$ . Letting  $a = bc^{d-1}$  gives the result.

Finally,  $\phi$  is the only affine map in  $\text{PGL}_2(\bar{K})$  fixing 0 and satisfying  $f^\phi(0) = 1$ . Therefore,  $f(z)$  is  $\bar{K}$ -conjugate to  $az^d + 1 \in K[z]$  for a unique  $a \in K^\times$ .  $\square$

Theorem 2.1 implies that up to conjugacy every unicritical polynomial  $f \in K[z]$  is a power map or of the form  $az^d + 1$ . In both cases  $\text{Crit}(f) = \{0\}$ . If  $f$  is a power map then  $f(0) = 0$ , hence  $f$  is PCF. Therefore, in order to completely describe all other PCF unicritical polynomials in  $\mathbb{Q}[z]$  (of any degree), we need only consider those of the form  $f(z) = az^d + 1$  for  $a \in \mathbb{Q}^\times$ .

**Proposition 2.2** [8, Corollary 8]. *If  $f(z) = az^d + 1 \in K[z]$  is post-critically finite, then  $|a| \leq 2$ .*

*Proof.* Suppose  $|a| > 2$  and  $|\alpha| \geq 1$ . Then

$$|f(\alpha)| = |a\alpha^d + 1| > |\alpha|.$$

Inductively,  $\alpha$  must be a wandering point. Since  $\text{Crit}(f) = \{0\}$  and  $f(0) = 1$ , we see that  $f$  is not PCF. Therefore, if  $f \in K[z]$  is PCF it must be that  $|a| \leq 2$ .  $\square$

**Theorem 2.3.** *Let  $f(z) = az^d + 1 \in \mathbb{Q}[z]$  and  $d \geq 2$ . For  $d$  even,  $f$  is PCF if and only if  $a \in \{-2, -1\}$ . For  $d$  odd,  $f$  is PCF if and only if  $a = -1$ .*

*Proof.* Suppose  $|a|_p > 1$  for some prime  $p$ . If  $|z|_p \geq 1$ , then  $|f(z)|_p = |az^d + 1|_p = |az^d|_p > |z|_p$ , so  $\alpha$  is a wandering point if there exists  $n \geq 0$  such that  $|f^n(\alpha)|_p \geq 1$ . In particular,  $f(0) = 1$ , so the critical

point 0 is a wandering point and  $f$  is not PCF. We conclude that for all primes  $p$ ,  $|a|_p \leq 1$ ; hence  $a \in \mathbb{Z}$ . By [Proposition 2.2](#),  $|a| \leq 2$ , so  $a \in \{\pm 1, \pm 2\}$ .

Suppose that  $|\alpha| > 2$ . Then

$$|f(\alpha)| = |a\alpha^d + 1| > 2^{d-1}|\alpha| - 1 > |\alpha|.$$

Inductively,  $\alpha$  must be a wandering point for  $f$ .

If  $a = 1$ , then  $f^3(0) = 2^d + 1$ , so 0 must be a wandering point. If  $a = 2$ , then  $f^2(0) = 3$ , so 0 must be a wandering point. If  $a = -1$ , then  $f^2(0) = 0$ , so  $f$  is PCF.

Finally, consider the case  $a = -2$ . If  $d$  is even then  $f^2(0) = f^3(0) = -1$ , so  $f$  is PCF. If  $d$  is odd, then  $f^3(0) = 3$ , so 0 is a wandering point.  $\square$

### 3. Normal forms for bicritical polynomials

Cubic polynomials have been studied extensively in complex dynamics, e.g., [\[5; 4; 6; 7; 16\]](#), and in arithmetic dynamics, e.g., [\[14\]](#). All of these use the Branner–Hubbard normal form, sometimes also called the monic centered form:

$$F(z) = z^3 + Az + B \quad \text{with critical points } \pm\alpha \text{ where } \alpha = \sqrt{\frac{-A}{3}}.$$

This form may be preferred in complex dynamics, but it is not ideal in arithmetic dynamics because it does not preserve the field of definition of the polynomial. For example, in [\[14\]](#), Ingram shows that if  $K$  is a number field and  $F(z) \in K[z]$  is PCF, then the pairs  $(A, B)$  are in a finite computable set, and he finds the set in the case  $F(z) \in \mathbb{Q}(z)$ . However, our [Table 1](#) shows that fewer than half of the PCF cubic polynomials defined over  $\mathbb{Q}$  are conjugate to some  $F(z) \in \mathbb{Q}[z]$  in the Branner–Hubbard form.

**Example 3.1.** Consider the PCF polynomial  $f \in \mathbb{Q}[z]$  given by  $f(z) = 3z^3 - \frac{9}{2}z^2 + 1$ . Conjugating by

$$\phi(z) = \sqrt{3}z - \frac{\sqrt{3}}{2} \text{ gives } f^\phi(z) = z^3 - \frac{9}{4}z - \frac{\sqrt{3}}{4} \notin \mathbb{Q}[z].$$

In this section, we describe normal forms for cubic bicritical polynomials, one for the case of rational critical points and one for the case of irrational critical points. These cases are not disjoint, but both are necessary to exhaustively list all PCF cubic polynomials. It is a simple matter to check that our final list of cubic polynomials contains no conjugate maps, so this is of no concern.

**Example 3.2.** Let

$$f_1(z) = \frac{z^3}{4} - \frac{3z}{2}, \quad \text{so } \text{Crit}(f_1) = \{\pm\sqrt{2}\}.$$

Moving the two critical points to 0 and 1 gives the polynomial  $g_1(z) = 2z^3 - 3z^2 + 1$ . These conjugate polynomials—one with rational critical points and one with irrational critical points—are both defined over  $\mathbb{Q}$ .



If  $f(z) \in K[z]$  has two rational critical points, we may conjugate to move them to 0 and 1 without changing the field of definition. From [2, Proposition 2.3], we know that there is a *unique* conjugacy class of bicritical polynomials of degree  $d \geq 3$  with fixed critical points  $\gamma_1$  and  $\gamma_2$ , and with prescribed ramification at the two critical points. Moreover, we have a formula for this polynomial when  $\{\gamma_1, \gamma_2\} = \{0, 1\}$ . Call the polynomial  $\mathcal{B}_{d,k}(z)$ . Since the critical points are at 0 and 1 and the polynomial has degree  $d$ , we have

$$\mathcal{B}'_{d,k}(z) = cz^{d-k-1}(z-1)^k$$

for some  $1 \leq k < d-1$  and some constant  $c$ . So  $d-k$  is the ramification index of  $\mathcal{B}_{d,k}(z)$  at the critical point 0, and  $k+1$  is the ramification index at the critical point 1. Expanding with the binomial theorem, integrating term-by-term, and requiring that the two critical points are fixed gives

$$\mathcal{B}_{d,k}(z) = \left( \frac{1}{k!} \prod_{j=0}^k (d-j) \right) z^{d-k} \sum_{i=0}^k \frac{(-1)^i}{(d-k+i)} \binom{k}{i} z^i. \quad (3-1)$$

Since we are concerned with the case  $d = 3$ , necessarily  $k = 1$ , giving the polynomial

$$\mathcal{B}_{3,1}(z) = -2z^3 + 3z^2. \quad (3-2)$$

**Proposition 3.3.** *Let  $g \in K[z]$  be a bicritical polynomial of degree  $d \geq 3$  with  $\text{Crit}(g) = \{\gamma_1, \gamma_2\} \subseteq K$ . There exists an element  $\phi \in \text{PGL}_2(K)$  such that  $g^\phi = a\mathcal{B}_{d,k} + c$  for some  $k \in \mathbb{N}$  and some  $a, c \in K$ .*

*Proof.* Let  $g \in K[z]$  with critical points  $\gamma_1, \gamma_2 \in K$ . Choose  $k \in \mathbb{N}$  such that  $d-k$  is the ramification index of  $\gamma_1$  and  $k+1$  is the ramification index of  $\gamma_2$ . Define  $\phi(z) = (z-\gamma_1)/(\gamma_2-\gamma_1) \in \text{PGL}_2(K)$ , which moves the critical points to 0 and 1, respectively.

If  $f(z) = g^\phi(z)$ , then  $f$  has critical points at 0 and 1 and degree  $d$ , so

$$f'(z) = \alpha z^{d-k-1}(z-1)^k = a\mathcal{B}'_{d,k}(z)$$

for some  $a \in \bar{K}^\times$ .

Then  $f(z) = a\mathcal{B}_{d,k}(z) + c$ , and since  $f = g^\phi$  where both  $g, \phi \in K[z]$ , we have  $a, c \in K$ . □

We now consider a normal form for cubic polynomials  $g \in K[z]$  with critical points in a quadratic extension of  $K$ .

Let  $D \in \mathcal{O}_K^\times$  and let  $d \geq 3$  be odd. We define a polynomial  $\mathcal{P}_{d,D}(z) \in K[z]$  by the following conditions:

- $\mathcal{P}'_{d,D}(z) = (z^2 - D)^{(d-1)/2}$ .
- $\mathcal{P}_{d,D}(0) = 0$ .

Then  $\mathcal{P}_{d,D}(z)$  is a bicritical polynomial having critical points  $\{\pm\sqrt{D}\}$  each with ramification index  $(d+1)/2$ . Just as with the polynomials  $\mathcal{B}_{d,k}(z)$ , we expand the derivative  $\mathcal{P}'_{d,D}(z)$  using the binomial theorem, integrate term-by-term, and use the fact that 0 is fixed to find a formula for these polynomials:

$$\mathcal{P}_{d,D}(z) = \sum_{j=0}^{(d-1)/2} (-D)^{(d-1)/2-j} \binom{\frac{d-1}{2}}{j} \frac{z^{2j+1}}{2j+1}. \quad (3-3)$$

Of particular interest in the sequel is the cubic case

$$\mathcal{P}_{3,D}(z) = \frac{z^3}{3} - Dz. \quad (3-4)$$

**Proposition 3.4.** *Let  $g(z) \in K[z]$  be a bicritical polynomial of degree  $d \geq 3$ . Suppose that  $\text{Crit}(g) = \{\gamma_1, \gamma_2\} \not\subset K$ . Then  $g$  is conjugate to a map of the form  $a\mathcal{P}_{d,D}(z) + c$  for some  $a, c \in K$  and some  $D \in \mathcal{O}_K^\times / \mathcal{O}_K^2$ .*

*Proof.* By definition,  $\{\gamma_1, \gamma_2\}$  are roots of the polynomial  $g'(z) \in K[z]$ . Since they are not in  $K$ , we must have  $g'(z) = \alpha(h(z))^\beta$  where  $h \in K[z]$  is an irreducible quadratic polynomial. Note: In this case,  $d$  is odd and the ramification index of each critical point is  $(d+1)/2$ .

Therefore there are  $m, n \in K$  with  $n \neq 0$  and  $D \in \mathcal{O}_K^\times / \mathcal{O}_K^2$  such that  $\gamma_1 = m + n\sqrt{D}$  and  $\gamma_2 = m - n\sqrt{D}$ . Consider

$$\phi(z) = \frac{z-m}{n} \in K[z], \quad \text{which satisfies } \phi(\gamma_1) = \sqrt{D} \text{ and } \phi(\gamma_2) = -\sqrt{D}.$$

Define  $f(z) = g^\phi(z)$ . Since  $g, \phi \in K[z]$ , we have  $f(z) \in K[z]$ . Hence  $f'(z) \in K[z]$ . Furthermore,  $\text{Crit}(f) = \text{Crit}(g^\phi) = \phi(\text{Crit}(g)) = \{\pm\sqrt{D}\}$ . Therefore,  $f'(z) = a(z^2 - D)^{(d-1)/2}$  for some  $a \in K$ , which means that  $f(z) = a\mathcal{P}_{d,D}(z) + c \in K[z]$ .  $\square$

#### 4. Coefficient bounds for PCF cubic polynomials over $\mathbb{Q}$

From Corollary 1.2 in [14], for any number field  $K$  there are finitely many conjugacy classes of post-critically finite polynomial maps of degree  $d$  in  $K[z]$ . We would like to use the normal forms in Section 3 to determine a representative of each conjugacy class of PCF cubic polynomials over  $\mathbb{Q}$ . Many of these results can be extended to bicritical maps of arbitrary degree (see [19]).

Let  $f(z) = a_d z^d + a_{d-1} z^{d-1} + \cdots + a_1 z + a_0 \in K[z]$ . Following Ingram [14], we set the following notation:

$$(2d)_v = \begin{cases} 1 & v \text{ is nonarchimedean,} \\ 2d & v \text{ is archimedean,} \end{cases}$$

$$C_{f,v} = (2d)_v \max_{0 \leq i < d} \left\{ 1, \left| \frac{a_i}{a_d} \right|_v^{1/(d-i)}, |a_d|_v^{-1/(d-1)} \right\}.$$

The following lemma show that  $C_{f,v}$  gives an effective  $v$ -adic bound for preperiodic points (points with finite orbit) of a polynomial  $f(z) \in \mathbb{Q}[z]$ . Applying this bound to the critical points will, in turn, give  $v$ -adic bounds on the coefficients for PCF polynomials. Ingram uses  $C_{f,v}$  in exactly this way in [14] without stating and proving a lemma of this sort. We provide Lemma 4.1 and its proof for clarity and completeness.

**Lemma 4.1.** *Let  $f(z) \in \mathbb{Q}[z]$  be a polynomial of degree  $d \geq 2$ . For  $\alpha \in \mathbb{Q}$ , if there exists  $v \in M_{\mathbb{Q}}$  and  $n \in \mathbb{N}$  such that*

$$|f^n(\alpha)|_v > C_{f,v},$$

*then  $\alpha$  must be a wandering point (have infinite orbit) for  $f$ .*

*Proof.* First, notice that  $\alpha$  is a wandering point if and only if  $f^n(\alpha)$  is a wandering point for all  $n \in \mathbb{N}$ , so without loss of generality, assume  $|\alpha|_v > C_{f,v}$  for some  $v \in M_K$ . We will show that  $\alpha$  is a wandering point by proving that whenever  $|\alpha|_v > C_{f,v}$ , we must have  $|f(\alpha)|_v > |\alpha|_v$ .

If  $v$  is nonarchimedean, then  $|\alpha|_v > |a_i/a_d|_v^{1/(d-i)}$  guarantees that  $|a_d\alpha^d|_v > |a_i\alpha^i|_v$  for all  $i < d$ , so we have

$$|f(\alpha)|_v = \left| \sum_{i=0}^d a_i \alpha^i \right|_v = |a_d \alpha^d|_v > |\alpha|_v.$$

The inequality above comes from the fact that  $|\alpha|_v > C_{f,v} \geq |a_d|_v^{-1/(d-1)}$ .

If  $v$  is archimedean, then starting with  $|\alpha|_v > 2d|a_i/a_d|_v^{1/(d-i)}$ , we see that

$$|a_d \alpha^d|_v > \max_{0 \leq i < d} \{(2d)^{d-i} |a_i \alpha^i|_v\} \geq 2d \max_{0 \leq i < d} \{|a_i \alpha^i|_v\},$$

and so we have

$$|f(\alpha)|_v = \left| \sum_{i=0}^d a_i \alpha^i \right|_v \geq |a_d \alpha^d|_v - d \max_{0 \leq i < d} |a_i \alpha^i|_v > \frac{1}{2} |a_d \alpha^d|_v.$$

Finally, it follows from  $|\alpha|_v > 2d|a_d|_v^{-1/(d-1)}$  that

$$\frac{1}{2} |a_d \alpha^d|_v > \frac{1}{2} (2d)^{d-1} |\alpha|_v > |\alpha|_v,$$

as desired. □

**4A. PCF cubics with rational critical points.** We begin by specializing [Lemma 4.1](#) to bicritical cubic polynomials with rational critical points, using the normal form in [Proposition 3.3](#).

**Lemma 4.2.** *Let*

$$f(z) = a\mathcal{B}_{3,1} + c = a(-2z^3 + 3z^2) + c \in \mathbb{Q}[z]$$

*be a bicritical polynomial and let  $\alpha \in \mathbb{Q}$ . If there exist  $v \in M_{\mathbb{Q}}$  and  $n \in \mathbb{N}$  such that*

$$|f^n(\alpha)|_v > C_{f,v} = (6)_v \max\left\{1, \left|\frac{3}{2}\right|_v, \left|\frac{1}{2a}\right|_v^{1/2}, \left|\frac{c}{2a}\right|_v^{1/3}\right\},$$

*then  $\alpha$  is a wandering point for  $f$ .*

*Proof.* The result follows immediately from applying the definition of  $C_{f,v}$  and [Lemma 4.1](#) to the coefficients of  $f(z)$ . □

**Remark 4.3.** Let  $f(z) = a(-2z^3 + 3z^2) + c \in \mathbb{Q}[z]$ , so  $\text{Crit}(f) = \{0, 1\}$ . If  $f$  is PCF then every element in the orbits of 0 and 1 must be bounded by  $C_{f,v}$ . In particular,

$$|f(1)|_v = |a + c|_v \leq C_{f,v} \quad \text{and} \quad |f(0)|_v = |c|_v \leq C_{f,v}.$$

Thus if  $f$  is PCF, then  $\max\{|c|_v, |a + c|_v\} \leq C_{f,v}$  for all  $v \in M_{\mathbb{Q}}$ . For every nonarchimedean place  $v$ , this means  $\max\{|a|_v, |c|_v\} \leq C_{f,v}$ .

Using the bound given above, we can find bounds on the absolute values of the parameters  $a$  and  $c$  of a PCF polynomial of the form  $f(z) = a(-2z^3 + 3z^2) + c \in \mathbb{Q}[z]$ . We begin with an archimedean bound on the parameter  $a$ .

**Lemma 4.4.** *Let  $f(z) = a(-2z^3 + 3z^2) + c \in \mathbb{Q}[z]$ . If  $f$  is PCF, then  $|a| < 4$ .*

*Proof.* Suppose  $|a| \geq 4$  and  $|\alpha| \geq \max\{|c|, 2\}$ . Then

$$|f(\alpha)| = |a\alpha^{d-1}(-(d-1)\alpha + d) + c|,$$

and a straightforward calculation shows that  $|f(\alpha)| > |\alpha|$ . If  $|c| \geq 2$ , then 0 must be a wandering point. If  $|c| < 2$ , then

$$|a + c| \geq |a| - |c| > 2,$$

so 1 must be a wandering point. Thus, if  $f$  is PCF, we must have  $|a| < 4$ . □

The following lemmas give  $p$ -adic bounds on the parameters  $a$  and  $c$  when  $f$  is PCF.

**Lemma 4.5.** *If  $f(z) = a(-2z^3 + 3z^2) + c \in \mathbb{Q}[z]$  is PCF then for nonarchimedean  $v \in M_{\mathbb{Q}}$*

$$C_{f,v} = \max\left\{1, \left|\frac{3}{2}\right|_v, \left|\frac{1}{2a}\right|_v^{1/2}\right\}.$$

*Proof.* Let  $f(z) = a(-2z^3 + 3z^2) + c \in \mathbb{Q}[z]$  and  $v \in M_{\mathbb{Q}}$  be nonarchimedean. From [Lemma 4.2](#),

$$C_{f,v} = \max\left\{1, \left|\frac{3}{2}\right|_v, \left|\frac{1}{2a}\right|_v^{1/2}, \left|\frac{c}{2a}\right|_v^{1/3}\right\}.$$

Suppose

$$C_{f,v} = \left|\frac{c}{2a}\right|_v^{1/3} > \left|\frac{1}{2a}\right|_v^{1/2}; \quad \text{then } |c|_v^2 > \left|\frac{1}{2a}\right|_v.$$

However, since  $f$  is PCF,

$$|c|_v \leq C_{f,v} = \left|\frac{c}{2a}\right|_v^{1/3}, \quad \text{so } |c|_v^2 \leq \left|\frac{1}{2a}\right|_v,$$

giving a contradiction. □

Notice that the statement above holds for  $a, c \in K$  and  $v \in M_K$  for any number field  $K$  and the proof is identical.

**Lemma 4.6.** *Let  $f(z) = a(-2z^3 + 3z^2) + c \in \mathbb{Q}[z]$  be PCF, let  $p$  be an odd prime, and let  $|\cdot|_p$  be the  $p$ -adic absolute value. Then  $|a|_p \leq 1$  and  $|c|_p^2 \leq |a|_p^{-1}$ .*

*Proof.* From [Lemma 4.5](#),

$$C_{f,p} = \max\left\{1, \left|\frac{3}{2}\right|_p, \left|\frac{1}{2a}\right|_p^{1/2}\right\} = \max\{1, |3|_p, |a|_p^{-1/2}\} = \max\{1, |a|_p^{-1/2}\}.$$

There are two distinct cases

- (1)  $C_{f,p} = 1$ , or
- (2)  $C_{f,p} = |a|_p^{-1/2} > 1$ .

First, suppose  $C_{f,p} = 1 \geq |a|_p^{-1/2}$ . Then  $|a|_p \geq 1$ . However, since  $f$  is PCF,

$$|a|_p, |c|_p \leq C_{f,p} = 1.$$

Therefore  $|a|_p = 1$ ,  $|a|_p^{-1} = 1$ , and  $|c|_p^2 \leq 1 = |a|_p^{-1}$ .

Now, suppose  $C_{f,p} = |a|_p^{-1/2} > 1$ . Then  $|a|_p < 1$ , as desired. Furthermore, since  $f$  is PCF,

$$|c|_p \leq C_{f,p} = |a|_p^{-1/2}. \quad \square$$

**Lemma 4.7.** *Let  $f(z) = a(-2z^3 + 3z^2) + c \in \mathbb{Q}[z]$  be PCF. Then*

$$|2a|_2 \leq 1 \quad \text{and} \quad |2c|_2 \leq 1.$$

*In fact,  $2a \in \mathbb{Z}$ .*

*Proof.* From Lemma 4.6, we have  $|2a|_p \leq 1$  for all odd primes  $p$ , so  $2a \in \mathbb{Z}$  will follow immediately once we know that  $|2a|_2 \leq 1$ .

From Lemma 4.5,

$$C_{f,2} = \max\left\{1, \left|\frac{3}{2}\right|_2, \left|\frac{1}{2a}\right|_2^{1/2}\right\} = \max\left\{2, \left|\frac{1}{2a}\right|_2^{1/2}\right\}. \quad (4-1)$$

Suppose  $C_{f,2} = 2$ : Since  $f$  is PCF, both  $|a|_2$  and  $|c|_2 \leq 2$ . Therefore, both  $|2a|_2$  and  $|2c|_2 \leq 1$  as desired.

Suppose  $C_{f,2} = |1/(2a)|_2^{1/2} > 2$ : Then

$$|2a|_2 < \frac{1}{4} < 1. \quad (4-2)$$

By Lemma 4.4,  $|a| < 4$ , so since  $2a \in \mathbb{Z}$ , we must have

$$a \in \left\{\frac{n}{2} : 1 \leq |n| < 8\right\}. \quad (4-3)$$

However, all of these possible  $a$ -values fail to satisfy equation (4-2), so the case  $C_{f,2} = |1/(2a)|_2^{1/2} > 2$  does not happen. Therefore, if  $f$  is PCF then  $C_{f,2} = 2$ , and both  $|2a|_2$  and  $|2c|_2 \leq 1$  as desired.  $\square$

**Proposition 4.8.** *If  $f$  is a cubic PCF polynomial of the form  $a\mathcal{B}_{d,k}(z) + c \in \mathbb{Q}[z]$ , then*

$$\pm a \in \left\{\frac{1}{2}, 1, \frac{3}{2}, 2, \frac{5}{2}, 3, \frac{7}{2}\right\} \quad \text{and} \quad \pm c \in \left\{0, 1, \frac{1}{2}, \frac{3}{2}, 2\right\}.$$

*Proof.* The result for  $a$  follows from equation (4-3) and Lemma 4.7.

Given the list for  $a$ , we see that  $|a|_p = 1$  for any prime  $p \notin \{2, 3, 5, 7\}$ . For  $p \in \{3, 5, 7\}$ , we have  $|a|_p \geq \frac{1}{p}$ , so  $|a|_p^{-1} \leq p$ . Using Lemma 4.6, we conclude that  $|c|_p \leq 1$  in both cases. Combining this with the fact that  $|2c|_2 \leq 1$  from Lemma 4.7, we see that  $|2c|_p \leq 1$  for all primes  $p$ . That is,  $2c \in \mathbb{Z}$ .

We will show that  $|c| < \frac{5}{2}$ . Suppose that  $a$  is contained in the above list and  $|\alpha| \geq |c| \geq \frac{5}{2}$ . Then

$$|f(\alpha)| \geq |a||\alpha|^2 - 2\alpha + 3 - |c|,$$

and this implies  $|f(\alpha)| > |\alpha|$ . Hence  $\alpha$  is a wandering point for  $f$ . Then  $c = f(0)$  must be a wandering point for  $f$ , in which case  $f$  would not be PCF. The result for  $c$  follows.  $\square$

**4B. PCF cubics with irrational critical points.** As in [Section 4A](#), we can use the bound  $C_{f,v}$  to find bounds on the (archimedean and nonarchimedean) absolute values of the parameters  $a, c$  and  $D$  of a PCF polynomial of the form  $f(z) = a\mathcal{P}_{3,D} + c \in \mathbb{Q}[z]$ . Unlike in [Section 4A](#), the bounds are not given explicitly. Instead, we will determine restrictions on the relationships between the three parameters. In [Theorem 5.2](#), we use these relationships to implement an algorithm that determines a finite set of triples  $(D, a, c)$  for which the polynomial  $f(z) = a\mathcal{P}_{3,D} + c \in \mathbb{Q}[z]$  is possibly PCF.

**Proposition 4.9.** *Let  $f(z) = a(z^3/3 - Dz) + c \in \mathbb{Q}[z]$ . If  $f$  is PCF, then*

$$\pm aD \in \left\{ \frac{3}{4}, \frac{3}{2}, \frac{9}{4}, 3, \frac{15}{4}, \frac{9}{2}, \frac{21}{4} \right\}.$$

*Proof.* Let  $\phi(z) = (z - \sqrt{D})/(-2\sqrt{D})$ . Then

$$f^\phi(z) = \frac{-2}{3}aD(-2z^3 + 3z^2) + \frac{aD}{3} - \frac{c - \sqrt{D}}{2\sqrt{D}}.$$

None of the bounds on  $a$  in the previous section depended on the fact that  $c \in \mathbb{Q}$ , so we may apply them to  $f^\phi$ . From [Proposition 4.8](#), we have that

$$\pm \frac{2}{3}aD \in \left\{ \frac{1}{2}, 1, \frac{3}{2}, 2, \frac{5}{2}, 3, \frac{7}{2} \right\}. \quad \square$$

**Lemma 4.10.** *Let  $f(z) = a(z^3/3 - Dz) + c \in \mathbb{Q}[z]$  with  $\pm aD \in \left\{ \frac{3}{4}, \frac{3}{2}, \frac{9}{4}, 3, \frac{15}{4}, \frac{9}{2}, \frac{21}{4} \right\}$ . If  $f$  is postcritically finite, then  $|c|^2 < 11|D|$ .*

*Proof.*  $\text{Crit}(f) = \{\pm\sqrt{D}\}$  and

$$f(\pm\sqrt{D}) = \mp \frac{2}{3}aD^{3/2} + c.$$

A calculation shows that if  $|c|^2 \geq 11|D|$  and  $\alpha \in \mathbb{C}$  with  $|\alpha| > |c|$ , then  $|f(\alpha)| > |\alpha|$ . Since  $a \neq 0$  then at least one of the critical points  $\gamma$  must satisfy  $|f(\gamma)| > |c|$ .  $\square$

**Lemma 4.11.** *Let  $f(z) = a(z^3/3 - Dz) + c \in \mathbb{Q}[z]$ . If  $f$  is  $p$ -adically post-critically bounded, then*

$$|c\sqrt{a}|_p \leq \begin{cases} 1 & \text{if } p \geq 5, \\ 3^{-1/2} & \text{if } p = 3, \\ 2^3 & \text{if } p = 2. \end{cases}$$

*Proof.* Let  $g = f^\phi$  for some  $\phi \in \text{PGL}_2(\overline{\mathbb{Q}})$  so that  $f^\phi$  is monic and has a fixed point at 0. Then  $g$  is of the form

$$g(z) = z^3 + 3\alpha z^2 + (3\alpha^2 - aD)z \quad (4-4)$$

where  $\alpha$  is a root of the polynomial

$$z^3 - (aD + 1)z + c\sqrt{\frac{a}{3}}. \quad (4-5)$$

The critical points for  $g$  are now  $-\alpha \pm \sqrt{aD/3}$ .

From [1, Theorems 1.2 and 4.1], we know that if  $g$  is  $p$ -adically post-critically bounded, the critical points must satisfy

$$\left| -\alpha \pm \sqrt{\frac{aD}{3}} \right|_p \leq \begin{cases} 1 & \text{if } p > 2, \\ 2 & \text{if } p = 2. \end{cases}$$

First consider  $p \geq 3$ . Add the critical points to see that

$$|-2\alpha|_p \leq 1, \quad \text{so } |\alpha|_p \leq 1.$$

Therefore, the polynomial in equation (4-5) is monic and all three roots lie in the  $p$ -adic unit disk. A Newton polygon argument says that the coefficients of that polynomial must also lie in the  $p$ -adic unit disk: if any coefficient had negative valuation, some segment of the Newton polygon would have positive slope, which would imply that the polynomial has a root of absolute value greater than one.

Since the constant term lies in the  $p$ -adic unit disk,

$$\left| c\sqrt{\frac{a}{3}} \right|_p \leq 1.$$

That gives the following bounds for  $p \neq 2$ :

$$|c\sqrt{a}|_p \leq \begin{cases} 1 & \text{if } p \geq 5, \\ 3^{-1/2} & \text{if } p = 3. \end{cases}$$

Now consider the case  $p = 2$ . We have

$$\left| -\alpha \pm \sqrt{\frac{aD}{3}} \right|_2 \leq 2. \tag{4-6}$$

Using the list of possible  $aD$  values from Proposition 4.9, we see that

$$\left| \sqrt{\frac{aD}{3}} \right|_2 \leq 2.$$

Applying the ultrametric triangle inequality to equation (4-6) yields  $|\alpha|_2 \leq 2$ . Therefore the Newton polygon for that polynomial at  $p = 2$  can have a segment of slope at most 1. Since the polynomial in equation (4-5) is cubic, that means the constant term must satisfy

$$v_2\left(c\sqrt{\frac{a}{3}}\right) \geq -3.$$

So  $|c\sqrt{a}|_2 \leq 2^3$ , which completes the proof.  $\square$

## 5. The algorithms

This section presents algorithms for finding all bicritical cubic PCF polynomials over  $\mathbb{Q}[z]$ ; the algorithms depend on normal forms found in Section 3 and coefficient bounds proven in Section 4.

**5A. Case 1: Rational critical points.** Results in [Section 4](#) give a finite set of coefficients to test, so the first algorithm is straightforward.

**Theorem 5.1.** *If  $f(z) \in \mathbb{Q}[z]$  is a cubic bicritical PCF polynomial with rational critical points, then  $f(z)$  is conjugate to  $f_{a,c}(z) = a(-2z^3 + 3z^2) + c$  where*

$$(a, c) \in \left\{ (1, 0), (\pm 1, \frac{1}{2}), (\frac{1}{2}, \pm 1), (2, -\frac{1}{2}), (\frac{3}{2}, 0), (-1, 1), (-2, \frac{3}{2}), (-\frac{3}{2}, 1), (-\frac{1}{2}, 0) \right\}.$$

*Proof.* From [Proposition 3.3](#), we know that every cubic polynomial in  $\mathbb{Q}[z]$  with rational critical points is conjugate to a map of the form  $f_{a,c}(z) = a(-2z^3 + 3z^2) + c$  for some  $a, c \in \mathbb{Q}$ .

From [Proposition 4.8](#), if  $f_{a,c}$  is post-critically bounded in every place, then

$$\pm a \in \left\{ \frac{1}{2}, 1, \frac{3}{2}, 2, \frac{5}{2}, 3, \frac{7}{2} \right\} \quad \text{and} \quad \pm c \in \left\{ 0, 1, \frac{1}{2}, \frac{3}{2}, 2 \right\}.$$

This gives 126 possibilities for  $(a, c)$ . The authors used built-in Sage [\[17\]](#) functionality to test all such pairs.<sup>1</sup> □

**5B. Case 3: Irrational critical points.** This case is more delicate. Results in [Section 4](#) give relationships between absolute values of the coefficients for cubic PCF maps. We must disentangle these relationships to build a finite search space.

**Theorem 5.2.** *If  $f(z) \in \mathbb{Q}[z]$  is a cubic bicritical PCF polynomial that is not conjugate to a polynomial with rational critical points, then  $f(z)$  is conjugate to  $f_{D,a,c}(z) = a(\frac{z^3}{3} - Dz) + c$  where*

$$(D, a, c) \in \left\{ (2, -\frac{3}{4}, 2), (-7, -\frac{3}{28}, \frac{7}{2}) \right\}.$$

*Proof.* From [Proposition 3.4](#), we know that every cubic polynomial in  $\mathbb{Q}[z]$  with irrational critical points is conjugate to a map of the form

$$f_{D,a,c}(z) = a(z^3/3 - Dz) + c$$

for some  $a, c \in \mathbb{Q}$  and a squarefree integer  $D$ .

Note that if  $c = 0$ , then  $f_{D,a,c}(z)$  is conjugate to a cubic polynomial with rational critical points via conjugation by  $\phi(z) = (a - \sqrt{D})/(-z\sqrt{D})$ . Furthermore,  $f_{D,a,-c}(z)$  is conjugate to  $f_{D,a,c}(z)$ , so we may assume that  $c > 0$ . Therefore, we build a list of triples  $(D, a, c)$  with  $D, a, c > 0$ , and each triple corresponds to four possibly PCF polynomials (varying the signs of  $D$  and  $a$ ). We split the algorithm into two cases corresponding to  $D$  even and  $D$  odd.

Step 1: *Loop over possible  $aD$  values.* From [Proposition 4.9](#), if  $f_{D,a,c}$  is PCF then:

$$\pm aD \in \left\{ \frac{3}{4}, \frac{3}{2}, \frac{9}{4}, 3, \frac{15}{4}, \frac{9}{2}, \frac{21}{4} \right\}.$$

---

<sup>1</sup>Sage code is available with the arXiv distribution of this article.



Step 2: *Compute  $|a|_2$ .* We use the value of  $aD$  in Step 1 and the parity of  $D$ .

Step 3: *Find an upper bound for  $|c|_p$  for each prime  $p$ .* From [Lemma 4.11](#), we know that if  $f_{D,a,c}(z)$  is  $p$ -adically post-critically bounded, then

$$|c\sqrt{a}|_p \leq \begin{cases} 1 & \text{if } p \geq 5, \\ 3^{-1/2} & \text{if } p = 3, \\ 2^3 & \text{if } p = 2. \end{cases} \quad (5-1)$$

So from Step 2 we can find  $e \leq 3$  such that  $|c|_2 \leq 2^e$ . Also using the list in Step 1, we conclude that  $|c|_p \leq 1$  for each prime  $p \geq 3$ .

Step 4: *Factor  $D$  and  $c$ .* Write  $D = mP$  or  $D = 2mP$ , where  $m$  and  $P$  are relatively prime odd squarefree integers such that  $m$  divides the numerator of  $aD$  and  $P$  divides the denominator of  $a$ . By equation (5-1),  $P$  must also divide the numerator of  $c$ . Thus,  $c = \frac{Pk}{2^e}$  for some positive integer  $k$ . Note: For a fixed  $aD$  from the list above,  $m$  comes from a finite set, but for now  $P$  and  $k$  can be arbitrarily large.

Step 5: *Bound the factors of  $D$  and  $c$ .* From [Lemma 4.10](#), we know that if  $f_{D,a,c}(z)$  is post-critically bounded at the archimedean place, then  $|c|^2 < 11|D|$ . Depending on the parity of  $D$ , this gives

$$\frac{P^2k^2}{2^{2e}} < 11mP \quad \text{or} \quad \frac{P^2k^2}{2^{2e}} < 22mP.$$

So  $Pk^2 < B$  where  $B = 11m \cdot 2^{2e}$  when  $D$  is odd, and  $B = 11m \cdot 2^{2e+1}$  when  $D$  is even. We know  $e$  from Step 3, so for each  $m$  we have an explicit value for the upper bound  $B$ .

Step 6: *Loop over  $P$  values.* For all odd, squarefree integers  $P < B$ , we determine the set of possible  $k$  values such that  $Pk^2 < B$ .

Step 7: *Create the triple.* Each triple  $(m, P, k)$  yields a triple  $(D, a, c) = (mP, aD/(mP), Pk/2^e)$  or  $(D, a, c) = (2mP, aD/(2mP), Pk/2^e)$ . Finally, check that  $3 \mid ac$  to verify that the triple satisfies the 3-adic condition in equation (5-1). If so, add  $(D, a, c)$  to the list of possible PCF triples.

This algorithm yields a list of 5,957 triples corresponding to 23,828 possibly PCF polynomials. The authors used built-in Sage [\[17\]](#) functionality to test all such triples. Only the two listed in the theorem statement above are actually PCF and are not conjugate to a polynomial already found in [Theorem 5.1](#). □

Combining the results in Theorems [2.3](#), [5.1](#), and [5.2](#) yields a total of 15 conjugacy classes of PCF cubic polynomials over  $\mathbb{Q}[z]$ , and this list is exhaustive. In the table below, we provide one representative of each conjugacy class along with the critical portrait for the polynomial. In the portrait, the critical points are given by  $\gamma$  and other points in the post-critical set are denoted  $\bullet$ . The monic centered form is given when it is defined over  $\mathbb{Q}[z]$ ; these appeared in [\[14\]](#).



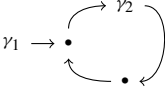
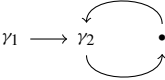

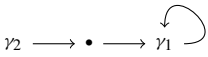


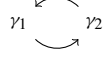
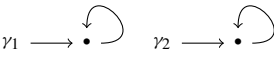
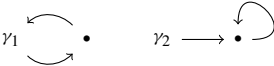
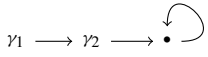
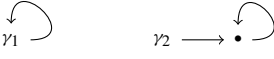
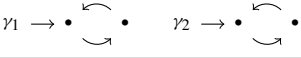

PCF polynomial	Critical portrait	Monic centered form
$z^3$		$z^3$
$-z^3 + 1$		
$-2z^3 + 3z^2 + \frac{1}{2}$		
$-z^3 + \frac{3}{2}z^2 + 1$		
$-2z^3 + 3z^2$		$z^3 + \frac{3}{2}z$
$-3z^3 + \frac{9}{2}z^2$		
$-z^3 + \frac{3}{2}z^2 - 1$		
$-4z^3 + 6z^2 - \frac{1}{2}$		$z^3 + 3z$
$2z^3 - 3z^2 + 1$		$z^3 - \frac{3}{2}z$
$4z^3 - 6z^2 + \frac{3}{2}$		$z^3 - 3z$
$2z^3 - 3z^2 + \frac{1}{2}$		
$3z^3 - \frac{9}{2}z^2 + 1$		
$z^3 - \frac{3}{2}z^2$		$z^3 - \frac{3}{4}z + \frac{3}{4}$ and $z^3 - \frac{3}{4}z - \frac{3}{4}$
$-\frac{1}{4}z^3 + \frac{3}{2}z + 2$		
$-\frac{1}{28}z^3 - \frac{3}{4}z + \frac{7}{2}$		

Table 1. Critical Portraits of Cubic PCF Polynomials over  $\mathbb{Q}$

**Acknowledgements.** Material from this article forms a part of the third author’s Ph.D. thesis. The authors thank the committee members for helpful comments: Rosie Alegado, Pavel Guerzhoy, Piper H, Ruth Haas, and Rob Harron. We thank Sarah Koch for helpful comments and conversation.

The project was completed during a SQuaRE at the American Institute for Mathematics. The authors thank AIM for providing a supportive environment.

This material is based upon work supported by and while the second author served at the National Science Foundation. Any opinion, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

## References

- [1] Jacqueline Anderson, *Bounds on the radius of the  $p$ -adic Mandelbrot set*, Acta Arith. **158** (2013), no. 3, 253–269. [MR 3040666](#)
- [2] Jacqueline Anderson, Irene I. Bouw, Ozlem Ejder, Neslihan Girgin, Valentijn Karemaker, and Michelle Manes, *Dynamical Belyi maps*, Women in numbers Europe II, Assoc. Women Math. Ser., vol. 11, Springer, Cham, 2018, pp. 57–82. [MR 3882706](#)
- [3] James Belk and Sarah Koch, *Iterated monodromy for a two-dimensional map*, In the tradition of Ahlfors-Bers. V, Contemp. Math., vol. 510, Amer. Math. Soc., Providence, RI, 2010, pp. 1–11. [MR 2581826](#)
- [4] Araceli Bonifant, Jan Kiwi, and John Milnor, *Errata for “Cubic polynomial maps with periodic critical orbit, part II: Escape regions”*, Conform. Geom. Dyn. **14** (2010), 190–193. [MR 2670510](#)
- [5] Araceli Bonifant, Jan Kiwi, and John Milnor, *Cubic polynomial maps with periodic critical orbit. II. Escape regions*, Conform. Geom. Dyn. **14** (2010), 68–112. [MR 2600536](#)
- [6] Bodil Branner and John H. Hubbard, *The iteration of cubic polynomials. I. The global topology of parameter space*, Acta Math. **160** (1988), no. 3–4, 143–206. [MR 945011](#)
- [7] Bodil Branner and John H. Hubbard, *The iteration of cubic polynomials. II. Patterns and parapatterns*, Acta Math. **169** (1992), no. 3–4, 229–325. [MR 1194004](#)
- [8] Xavier Buff, *On postcritically finite unicritical polynomials*, New York J. Math. **24** (2018), 1111–1122. [MR 3890968](#)
- [9] Laura De Marco, *Dynamical moduli spaces and elliptic curves*, Ann. Fac. Sci. Toulouse Math. (6) **27** (2018), no. 2, 389–420. [MR 3831028](#)
- [10] C. Favre and T. Gauthier, *Distribution of postcritically finite polynomials*, Israel J. Math. **209** (2015), no. 1, 235–292. [MR 3430241](#)
- [11] William Floyd, Walter Parry, and Kevin M. Pilgrim, *Modular groups, Hurwitz classes and dynamic portraits of NET maps*, Groups Geom. Dyn. **13** (2019), no. 1, 47–88. [MR 3900764](#)
- [12] Thomas Gauthier and Gabriel Vigny, *Distribution of postcritically finite polynomials II: Speed of convergence*, J. Mod. Dyn. **11** (2017), 57–98. [MR 3627118](#)
- [13] Thomas Gauthier and Gabriel Vigny, *Distribution of postcritically finite polynomials III: Combinatorial continuity*, Fund. Math. **244** (2019), no. 1, 17–48. [MR 3874664](#)
- [14] Patrick Ingram, *A finiteness result for post-critically finite polynomials*, International Mathematics Research Notices (2010).
- [15] David Lukas, Michelle Manes, and Diane Yap, *A census of quadratic post-critically finite rational functions defined over  $\mathbb{Q}$* , LMS J. Comput. Math. **17** (2014), no. suppl. A, 314–329. [MR 3240812](#)
- [16] John Milnor, *Cubic polynomial maps with periodic critical orbit. I*, Complex dynamics, A K Peters, Wellesley, MA, 2009, pp. 333–411. [MR 2508263](#)
- [17] Inc. SageMath, *CoCalc: Collaborative Computation Online*, 2016, <https://cocalc.com/>.

- [18] Joseph H. Silverman, *Moduli spaces and arithmetic dynamics*, CRM Monograph Series, vol. 30, American Mathematical Society, Providence, RI, 2012. [MR 2884382](#)
- [19] Bella Tobin, *Arithmetic dynamics of bicritical polynomials*, In progress.

Received 3 Feb 2020.

JACQUELINE ANDERSON: [jacqueline.anderson@bridgew.edu](mailto:jacqueline.anderson@bridgew.edu)

*Department of Mathematics, Bridgewater State University, Bridgewater, MA, United States*

MICHELLE MANES: [mmanes@math.hawaii.edu](mailto:mmanes@math.hawaii.edu)

*Department of Mathematics, University of Hawai‘i at Mānoa, Honolulu, HI, United States*

BELLA TOBIN: [bella.tobin@okstate.edu](mailto:bella.tobin@okstate.edu)

*Department of Mathematics, Oklahoma State University, Stillwater, OK, United States*

# Faster computation of isogenies of large prime degree

Daniel J. Bernstein, Luca De Feo, Antonin Leroux, and Benjamin Smith

*Dedicated to the memory of Peter Lawrence Montgomery*

Let  $\mathcal{E}/\mathbb{F}_q$  be an elliptic curve, and  $P$  a point in  $\mathcal{E}(\mathbb{F}_q)$  of prime order  $\ell$ . Vélu's formulæ let us compute a quotient curve  $\mathcal{E}' = \mathcal{E}/\langle P \rangle$  and rational maps defining a quotient isogeny  $\phi : \mathcal{E} \rightarrow \mathcal{E}'$  in  $\tilde{O}(\ell)$   $\mathbb{F}_q$ -operations, where the  $\tilde{O}$  is uniform in  $q$ . This article shows how to compute  $\mathcal{E}'$ , and  $\phi(Q)$  for  $Q$  in  $\mathcal{E}(\mathbb{F}_q)$ , using only  $\tilde{O}(\sqrt{\ell})$   $\mathbb{F}_q$ -operations, where the  $\tilde{O}$  is again uniform in  $q$ . As an application, this article speeds up some computations used in the isogeny-based cryptosystems CSIDH and CSURF.

## 1. Introduction

Let  $\mathcal{E}$  be an elliptic curve over a finite field  $\mathbb{F}_q$  of odd characteristic, and let  $P$  be a point in  $\mathcal{E}(\mathbb{F}_q)$  of order  $n$ . The point  $P$  generates a cyclic subgroup  $\mathcal{G} \subseteq \mathcal{E}(\mathbb{F}_q)$ , and there exists an elliptic curve  $\mathcal{E}'$  over  $\mathbb{F}_q$  and a separable degree- $n$  quotient isogeny

$$\phi : \mathcal{E} \longrightarrow \mathcal{E}' \quad \text{with} \quad \ker \phi = \mathcal{G} = \langle P \rangle ;$$

the isogeny  $\phi$  is also defined over  $\mathbb{F}_q$ . We want to compute  $\phi(Q)$  for a point  $Q$  in  $\mathcal{E}(\mathbb{F}_q)$  as efficiently as possible.

If  $n$  is composite, then we can decompose  $\phi$  into a series of isogenies of prime degree. Computationally, this assumes that we can factor  $n$ , but finding a prime factor  $\ell$  of  $n$  is not a bottleneck compared to the computation of an  $\ell$ -isogeny by the techniques considered here. We thus reduce to the case where  $n = \ell$  is prime.

*Date:* 2020.09.30.

For the long version of this article see [6]. Thanks to the anonymous referees for their comments. Author list in alphabetical order; see <https://www.ams.org/profession/leaders/culture/CultureStatement04.pdf>. Part of this work was carried out while the first author was visiting the Simons Institute for the Theory of Computing. This work was supported by the Cisco University Research Program, by DFG Cluster of Excellence 2092 “CASA: Cyber Security in the Age of Large-Scale Adversaries”, and by the U.S. National Science Foundation under grant 1913167. “Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation” (or other funding agencies). Permanent ID of this document: 44d5ade1c1778d86a5b035ad20f880c08031a1dc.

*MSC2020:* 11Y16.

*Keywords:* isogenies, resultants.

Vélu introduced formulæ for  $\phi$  and  $\mathcal{E}'$  (see [56] and [38, §2.4]): for  $\mathcal{E}$  defined by  $y^2 = x^3 + a_2x^2 + a_4x + a_6$  and  $\ell \geq 3$ , we have

$$\phi : (X, Y) \mapsto \left( \frac{\Phi_{\mathcal{G}}(X)}{\Psi_{\mathcal{G}}(X)^2}, \frac{Y\Omega_{\mathcal{G}}(X)}{\Psi_{\mathcal{G}}(X)^3} \right)$$

where

$$\begin{aligned} \Psi_{\mathcal{G}}(X) &= \prod_{s=1}^{(\ell-1)/2} (X - x([s]P)), \\ \Phi_{\mathcal{G}}(X) &= 4(X^3 + a_2X^2 + a_4X + a_6)(\Psi'_{\mathcal{G}}(X)^2 - \Psi''_{\mathcal{G}}(X)\Psi_{\mathcal{G}}(X)) \\ &\quad - 2(3X^2 + 2a_2X + a_4)\Psi'_{\mathcal{G}}(X)\Psi_{\mathcal{G}}(X) + (\ell X - \sum_{s=1}^{\ell-1} x([s]P))\Psi_{\mathcal{G}}(X)^2, \\ \Omega_{\mathcal{G}}(X) &= \Phi'_{\mathcal{G}}(X)\Psi_{\mathcal{G}}(X) - 2\Phi_{\mathcal{G}}(X)\Psi'_{\mathcal{G}}(X). \end{aligned}$$

The obvious way to compute  $\phi(Q)$  is to compute the rational functions shown above, i.e., to compute the coefficients of the polynomials  $\Psi_{\mathcal{G}}$ ,  $\Phi_{\mathcal{G}}$ ,  $\Omega_{\mathcal{G}}$ ; and then evaluate those polynomials. This takes  $\tilde{O}(\ell)$  operations. (If we need the defining equation of  $\mathcal{E}'$ , then we can obtain it by evaluating  $\phi(Q)$  for a few  $Q$  outside  $\mathcal{G}$ , possibly after extending  $\mathbb{F}_q$ , and then interpolating a curve equation through the resulting points. Alternatively, Vélu gives further formulas for the defining equation.) We emphasize, however, that the goal is not to compute the coefficients of these functions; the goal is to evaluate the functions at a specified point.

The core algorithmic problem falls naturally into a more general framework: the efficient evaluation of polynomials and rational functions over  $\mathbb{F}_q$  whose roots are values of a function from a cyclic group to  $\mathbb{F}_q$ .

Fix a cyclic group  $\mathcal{G}$  (which we will write additively), a generator  $P$  of  $\mathcal{G}$ , and a function  $f : \mathcal{G} \rightarrow \mathbb{F}_q$ . For each finite subset  $S$  of  $\mathbb{Z}$ , we define a polynomial

$$h_S(X) = \prod_{s \in S} (X - f([s]P)),$$

where  $[s]P$  denotes the sum of  $s$  copies of  $P$ . The kernel polynomial  $\Psi_{\mathcal{G}}(x)$  above is an example of this, with  $f = x$  and  $S = \{1, \dots, (\ell-1)/2\}$ . Another example is the cyclotomic polynomial  $\Phi_n$ , where  $f$  embeds  $\mathbb{Z}/n\mathbb{Z}$  in the roots of unity of  $\mathbb{F}_q$ , and  $\Phi_n(X) = h_S(X)$  where  $S = \{i \mid 0 \leq i < n, \gcd(i, n) = 1\}$ . More generally, if  $f$  maps  $i \mapsto \zeta^i$  for some  $\zeta$ , then  $h_S(X)$  is a polynomial whose roots are various powers of  $\zeta$ ; similarly, if  $f$  maps  $i \mapsto i\beta$  for some  $\beta$ , then  $h_S(X)$  is a polynomial whose roots are various integer multiples of  $\beta$ .

Given  $f$  and  $S$ , then, we want to compute  $h_S(\alpha) = \prod_{s \in S} (\alpha - f([s]P))$  for any  $\alpha$  in  $\mathbb{F}_q$ . One can always directly compute  $h_S(\alpha)$  in  $O(\#S)$   $\mathbb{F}_q$ -operations; this is the standard way to compute  $\Psi_{\mathcal{G}}(\alpha)$ . But if  $S$  has enough additive structure, and if  $f$  is sufficiently compatible with the group structure on  $\mathcal{G}$ , then we can compute  $h_S(\alpha)$  in  $\tilde{O}(\sqrt{\#S})$   $\mathbb{F}_q$ -operations, as we will see in §2, §3, and §4. Our main theoretical result is Theorem 4.11, which shows how to achieve this quasi-square-root complexity for a large class of

$S$  when  $f$  is the  $x$ -coordinate on an elliptic curve. We apply this to the special case of efficient  $\ell$ -isogeny computation in §5. We discuss applications in isogeny-based cryptography in §6.

Most of this paper focuses on asymptotic exponents, in particular improving  $\ell$ -isogeny evaluation from cost  $\tilde{O}(\ell)$  to cost  $\tilde{O}(\sqrt{\ell})$ . However, this analysis hides polylogarithmic factors that can swamp the exponent improvement for small  $\ell$ . In the full version [6], we instead analyze costs for concrete values of  $\ell$ , and ask how large  $\ell$  needs to be for the  $\tilde{O}(\sqrt{\ell})$  algorithms to outperform conventional algorithms.

**1.1. Model of computation.** We state our framework for  $\mathbb{F}_q$  for concreteness. All time complexities are in  $\mathbb{F}_q$ -operations, with the  $O$  and  $\tilde{O}$  uniform over  $q$ .

The ideas are more general. The algorithms here are algebraic algorithms in the sense of [16], and can further be lifted to algorithms defined over  $\mathbb{Z}[1/2]$  and in some cases over  $\mathbb{Z}$ . In other words, the algorithms are agnostic to the choice of  $q$  in  $\mathbb{F}_q$ , except for sometimes requiring  $q$  to be odd; and the algorithms can also be applied to more general rings, as long as all necessary divisions can be carried out.

Restricting to algebraic algorithms can damage performance. For example, for most input sizes, the fastest known algorithms to multiply polynomials over  $\mathbb{F}_q$  are faster than the fastest known algebraic algorithms for the same task. This speedup is only polylogarithmic and hence is not visible at the level of detail of our analysis (the full version [6] contains a detailed analysis of concrete performances), but implementors should be aware that simply performing a sequence of separate  $\mathbb{F}_q$ -operations is not always the best approach.

## 2. Strassen’s deterministic factorization algorithm

As a warmup, we review a deterministic algorithm that provably factors  $n$  into primes in time  $\tilde{O}(n^{1/4})$ . There are several such algorithms in the literature using fast polynomial arithmetic, including [53], [12], [23], and [34]; there is also a separate series of lattice-based algorithms surveyed in, e.g., [4]. Strassen’s algorithm from [53] has the virtue of being particularly simple, and is essentially the algorithm presented in this section.

The state of the art in integer factorization has advanced far beyond  $\tilde{O}(n^{1/4})$ . For example, ECM [39], Lenstra’s elliptic-curve method of factorization, is plausibly conjectured to take time  $n^{o(1)}$ . We present Strassen’s algorithm because Strassen’s main subroutine is the simplest example of a much broader speedup that we use.

**2.1. Factorization via modular factorials.** Computing  $\gcd(n, \ell! \bmod n)$  reveals whether  $n$  has a prime factor  $\leq \ell$ . Binary search through all  $\ell \leq \sqrt{n}$  then finds the smallest prime factor of  $n$ . Repeating this process completely factors  $n$  into primes.

The rest of this section focuses on the problem of computing  $\ell! \bmod n$ , given positive integers  $\ell$  and  $n$ . The algorithm of §2.3 uses  $\tilde{O}(\sqrt{\ell})$  additions, subtractions, and multiplications in  $\mathbb{Z}/n\mathbb{Z}$ , plus negligible overhead. For comparison, a straightforward computation would use  $\ell - 1$  multiplications modulo  $n$ . The  $\tilde{O}$  here is uniform over  $n$ .

**2.2. Modular factorials as an example of the main problem.** Define  $\mathcal{G}$  as the additive group  $\mathbb{Z}$ , define  $P = 1$ , define  $f : \mathcal{G} \rightarrow \mathbb{Z}/n\mathbb{Z}$  as  $s \mapsto s$ , and define  $h_S(X) = \prod_{s \in S} (X - f([s]P)) \in (\mathbb{Z}/n\mathbb{Z})[X]$ . Then, in particular,  $h_S(X) = (X - 1) \cdots (X - \ell)$  for  $S = \{1, \dots, \ell\}$ , and one can compute  $\ell! \bmod n$  by computing  $h_S(\ell + 1)$  or, alternatively, by computing  $(-1)^\ell h_S(0)$ . This fits the modular-factorials problem, in the special case that  $n$  is a prime number  $q$ , into the framework of §1.

**2.3. An algorithm for modular factorials.** Compute  $b = \lfloor \sqrt{\ell} \rfloor$ , and define  $I = \{0, 1, 2, \dots, b - 1\}$ . Use a product tree to compute the polynomial  $h_I(X) = X(X - 1)(X - 2) \cdots (X - (b - 1)) \in (\mathbb{Z}/n\mathbb{Z})[X]$ .

Define  $J = \{b, 2b, 3b, \dots, b^2\}$ . Compute  $h_J(X)$ , and then compute the resultant of  $h_J(X)$  and  $h_I(X)$ . This resultant is  $h_I(b)h_I(2b)h_I(3b) \cdots h_I(b^2)$ , i.e.,  $(b^2)! \bmod n$ .

One can compute the resultant of two polynomials via continued fractions; see, e.g., [54]. An alternative here, since  $h_J$  is given as a product of linear polynomials, is to use a remainder tree to compute  $h_I(b), h_I(2b), \dots, h_I(b^2) \in \mathbb{Z}/n\mathbb{Z}$ , and then multiply. Either approach uses  $\tilde{O}(\sqrt{\ell})$  operations.

Finally, multiply by  $(b^2 + 1)(b^2 + 2) \cdots \ell$  modulo  $n$ , obtaining  $\ell! \bmod n$ .

### 3. Evaluation of polynomials whose roots are powers

Pollard [49] introduced a deterministic algorithm that provably factors  $n$  into primes in time  $O(n^{1/4+\epsilon})$ . Strassen's algorithm from [53] was a streamlined version of Pollard's algorithm, replacing  $O(n^{1/4+\epsilon})$  with  $\tilde{O}(n^{1/4})$ .

This section reviews Pollard's main subroutine, a fast method to evaluate a polynomial whose roots (with multiplicity) form a geometric progression. For comparison, Strassen's main subroutine is a fast method to evaluate a polynomial whose roots form an arithmetic progression. See §2.3 above.

**3.1. A multiplicative version of modular factorials.** Fix  $\zeta \in (\mathbb{Z}/n\mathbb{Z})^*$ . Define  $\mathcal{G} = \mathbb{Z}$ , define  $P = 1$ , define  $f : \mathcal{G} \rightarrow (\mathbb{Z}/n\mathbb{Z})^*$  as  $s \mapsto \zeta^s$ , and define  $h_S(X) = \prod_{s \in S} (X - f([s]P)) = \prod_{s \in S} (X - \zeta^s) \in (\mathbb{Z}/n\mathbb{Z})[X]$ . (For comparison, in §2,  $f$  was  $s \mapsto s$ , and  $h_S(X)$  was  $\prod_{s \in S} (X - s)$ .)

In particular,  $h_S(X) = \prod_{s=1}^\ell (X - \zeta^s)$  for  $S = \{1, 2, 3, \dots, \ell\}$ . Given  $\alpha \in \mathbb{Z}/n\mathbb{Z}$ , one can straightforwardly evaluate  $h_S(\alpha)$  for this  $S$  using  $O(\ell)$  algebraic operations in  $\mathbb{Z}/n\mathbb{Z}$ . The method in §3.2 accomplishes the same result using only  $\tilde{O}(\sqrt{\ell})$  operations. The  $O$  and  $\tilde{O}$  are uniform in  $n$ , and all of the algorithms here can take  $\zeta$  as an input rather than fixing it. There are some divisions by powers of  $\zeta$ , but divisions are included in the definition of algebraic operations.

Pollard uses the special case  $h_S(1) = \prod_{s=1}^\ell (1 - \zeta^s)$ . This is  $(1 - \zeta)^\ell$  times the quantity  $(1 + \zeta)(1 + \zeta + \zeta^2) \cdots (1 + \zeta + \cdots + \zeta^{\ell-1})$ . It would be standard to call the latter quantity a “ $q$ -factorial” if the letter “ $q$ ” were used in place of “ $\zeta$ ”; beware, however, that it is not standard to call this quantity a “ $\zeta$ -factorial”. For a vast generalization of Pollard's algorithm to  $q$ -holonomic sequences, see [11]; in §4, we will generalize it in a different direction.

**3.2. An algorithm for the multiplicative version of modular factorials.** Compute  $b = \lfloor \sqrt{\ell} \rfloor$ , and define  $I = \{1, 2, 3, \dots, b\}$ . Use a product tree to compute the polynomial  $h_I(X) = \prod_{i=1}^b (X - \zeta^i)$ .



Define  $J = \{0, b, 2b, \dots, (b-1)b\}$ , and use a remainder tree to compute  $h_I(\alpha/\zeta^j)$  for all  $j \in J$ . Pollard uses the chirp- $z$  transform [50] (Bluestein's trick) instead of a remainder tree, saving a logarithmic factor in the number of operations, and it is also easy to save a logarithmic factor in computing  $h_I(X)$ , but these speedups are not visible at the level of detail of the analysis in this section.

Multiply  $\zeta^{jb}$  by  $h_I(\alpha/\zeta^j)$  to obtain  $\prod_{i=1}^b (\alpha - \zeta^{i+j})$  for each  $j$ , and then multiply across  $j \in J$  to obtain  $\prod_{s=1}^{b^2} (\alpha - \zeta^s)$ . Finally, multiply by  $\prod_{s=b^2+1}^\ell (\alpha - \zeta^s)$  to obtain the desired  $h_S(\alpha)$ .

One can view the product  $\prod_{s=1}^{b^2} (\alpha - \zeta^s)$  here, like the product  $(b^2)!$  in §2, as the resultant of two degree- $b$  polynomials. Specifically,  $\prod_j h_I(\alpha/\zeta^j)$  is the resultant of  $\prod_j (X - \alpha/\zeta^j)$  and  $h_I$ ; and  $\prod_j \zeta^{jb} h_I(\alpha/\zeta^j)$  is the resultant of  $\prod_j (\zeta^j X - \alpha)$  and  $h_I$ . One can, if desired, use continued-fraction resultant algorithms rather than multipoint evaluation via a remainder tree.

**3.3. Structures in  $S$  and  $f$ .** We highlight two structures exploited in the above computation of  $\prod_{s=1}^\ell (\alpha - \zeta^s)$ . First, the set  $S = \{1, 2, \dots, \ell\}$  has enough additive structure to allow most of it to be decomposed as  $I + J$ , where  $I$  and  $J$  are much smaller sets. Second, the map  $s \mapsto \zeta^s$  is a group homomorphism, allowing each  $\zeta^{i+j}$  to be computed as the product of  $\zeta^i$  and  $\zeta^j$ ; we will return to this point in §4.1.

We now formalize the statement regarding additive structure, focusing on the  $\mathbb{F}_q$  case that we will need later in the paper. First, some terminology: we say that sets of integers  $I$  and  $J$  have *no common differences* if  $i_1 - i_2 \neq j_1 - j_2$  for all  $i_1 \neq i_2$  in  $I$  and all  $j_1 \neq j_2$  in  $J$ . If  $I$  and  $J$  have no common differences, then the map  $I \times J \rightarrow I + J$  sending  $(i, j)$  to  $i + j$  is a bijection.

**Lemma 3.4.** *Let  $q$  be a prime power. Let  $\zeta$  be an element of  $\mathbb{F}_q^*$ . Define  $h_S(X) = \prod_{s \in S} (X - \zeta^s) \in \mathbb{F}_q[X]$  for each finite subset  $S$  of  $\mathbb{Z}$ . Let  $I$  and  $J$  be finite subsets of  $\mathbb{Z}$  with no common differences. Then*

$$h_{I+J}(X) = \text{Res}_Z(h_I(Z), H_J(X, Z))$$

where  $\text{Res}_Z(\cdot, \cdot)$  is the bivariate resultant, and

$$H_J(X, Z) := \prod_{j \in J} (X - \zeta^j Z).$$

*Proof.*  $\text{Res}_Z(h_I(Z), H_J(X, Z)) = \prod_{i \in I} \prod_{j \in J} (X - \zeta^i \zeta^j) = \prod_{(i,j) \in I \times J} (X - \zeta^{i+j}) = h_{I+J}(X)$  since the map  $I \times J \rightarrow I + J$  sending  $(i, j)$  to  $i + j$  is bijective.  $\square$

Algorithm 1 is an algebraic algorithm that outputs  $h_S(\alpha)$  given  $\alpha$ . The algorithm is parameterized by  $\zeta$  and the set  $S$ , and also by finite subsets  $I, J \subset \mathbb{Z}$  with no common differences such that  $I + J \subseteq S$ . The algorithm and the proof of Proposition 3.5 are stated using generic resultant computation (via continued fractions), but, as in §2.3 and §3.2, one can alternatively use multipoint evaluation.

**Proposition 3.5.** *Let  $q$  be a prime power. Let  $\zeta$  be an element of  $\mathbb{F}_q^*$ . Let  $I, J$  be finite subsets of  $\mathbb{Z}$  with no common differences. Let  $K$  be a finite subset of  $\mathbb{Z}$  disjoint from  $I + J$ . Given  $\alpha$  in  $\mathbb{F}_q$ , Algorithm 1 outputs  $\prod_{s \in S} (\alpha - \zeta^s)$  using  $\tilde{O}(\max(\#I, \#J, \#K))$   $\mathbb{F}_q$ -operations, where  $S = (I + J) \cup K$ .*

---

**Algorithm 1:** Computing  $h_S(\alpha) = \prod_{s \in S} (\alpha - \zeta^s)$ 


---

**Parameters:** a prime power  $q$ ;  $\zeta \in \mathbb{F}_q^*$ ; finite subsets  $I, J, K \subseteq \mathbb{Z}$  such that  $I$  and  $J$  have no common differences and  $(I + J) \cap K = \{\}$ ;  $\zeta^s$  for each  $s \in I \cup J \cup K$

**Input:**  $\alpha$  in  $\mathbb{F}_q$

**Output:**  $h_S(\alpha)$  where  $h_S(X) = \prod_{s \in S} (X - \zeta^s)$  and  $S = (I + J) \cup K$

```

1  $h_I \leftarrow \prod_{i \in I} (Z - \zeta^i) \in \mathbb{F}_q[Z]$ 
2  $H_J \leftarrow \prod_{j \in J} (\alpha - \zeta^j Z) \in \mathbb{F}_q[Z]$ 
3  $h_{I+J} \leftarrow \text{Res}_Z(h_I, H_J) \in \mathbb{F}_q$ 
4  $h_K \leftarrow \prod_{k \in K} (\alpha - \zeta^k) \in \mathbb{F}_q$ 
5 return  $h_{I+J} \cdot h_K$ 
```

---

The  $\tilde{O}$  is uniform in  $q$ . Instead of taking  $\zeta$  and various precomputed powers of  $\zeta$  as parameters, the algorithm can take  $\zeta$  as an input, at the cost of computing  $\zeta^i$  for  $i \in I$ ,  $\zeta^j$  for  $j \in J$ , and  $\zeta^k$  for  $k \in K$ . This preserves the time bound if the elements of  $I, J, K$  each have  $\text{polylog}(\max(\#I, \#J, \#K))$  bits.

*Proof.* Since  $S \setminus K = I + J$ , we have  $h_S(\alpha) = h_{I+J}(\alpha) \cdot h_K(\alpha)$ , and Lemma 3.4 shows that  $h_{I+J}(\alpha) = \text{Res}_Z(h_I(Z), H_J(\alpha, Z))$ . Line 1 computes  $h_I(Z)$  in  $\tilde{O}(\#I)$   $\mathbb{F}_q$ -operations; Line 2 computes  $H_J(\alpha, Z)$  in  $\tilde{O}(\#J)$   $\mathbb{F}_q$ -operations; Line 3 computes  $h_{I+J}(\alpha)$  in  $\tilde{O}(\max(\#I, \#J))$   $\mathbb{F}_q$ -operations; and Line 4 computes  $h_K(\alpha)$  in  $\tilde{O}(\#K)$   $\mathbb{F}_q$ -operations. The total is  $\tilde{O}(\max(\#I, \#J, \#K))$   $\mathbb{F}_q$ -operations.  $\square$

**3.6. Optimization.** The best conceivable case for the time bound in Proposition 3.5, as a function of  $\#S$ , is  $\tilde{O}(\sqrt{\#S})$ . Indeed,  $\#S = \#I + \#J + \#K$ , so  $\max(\#I, \#J, \#K) \geq \sqrt{\#S + 1/4} - 1/2$ .

To reach  $\tilde{O}(\sqrt{\#S})$  for a given set of exponents  $S$ , we need sets  $I$  and  $J$  with no common differences such that  $I + J \subseteq S$  with  $\#I, \#J$ , and  $\#(S \setminus (I + J))$  in  $\tilde{O}(\sqrt{\#S})$ . Such  $I$  and  $J$  exist for many useful sets  $S$ . Example 3.7 shows a simple form for  $I$  and  $J$  when  $S$  is an arithmetic progression.

**Example 3.7.** Suppose  $S$  is an arithmetic progression of length  $n$ : that is,

$$S = \{m, m + r, m + 2r, \dots, m + (n - 1)r\}$$

for some  $m$  and some nonzero  $r$ . Let  $b = \lfloor \sqrt{n} \rfloor$ , and set

$$I := \{ir \mid 0 \leq i < b\} \quad \text{and} \quad J := \{m + jbr \mid 0 \leq j < b\};$$

then  $I$  and  $J$  have no common differences, and  $I + J = \{m + kr \mid 0 \leq k < b^2\}$ , so

$$I + J = S \setminus K \quad \text{where} \quad K = \{m + kr \mid b^2 \leq k < n\}.$$

Now  $\#I = \#J = b$ , and  $\#K = n - b^2 \leq 2b$ , so we can use these sets to compute  $h_S(\alpha)$  in  $\tilde{O}(b) = \tilde{O}(\sqrt{n})$   $\mathbb{F}_q$ -operations, following Proposition 3.5. (In the case  $r = 1$ , we recognise the index sets driving Shanks' baby-step giant-step algorithm.)

#### 4. Elliptic resultants

The technique in §3 for evaluating polynomials whose roots are powers is well known. Our main theoretical contribution is to adapt this to polynomials whose roots are functions of more interesting groups: in particular, functions of elliptic-curve torsion points. The most important such function is the  $x$ -coordinate. The main complication here is that, unlike in §3, the function  $x$  is not a homomorphism.

**4.1. The elliptic setting.** Let  $\mathcal{E}/\mathbb{F}_q$  be an elliptic curve, let  $P \in \mathcal{E}(\mathbb{F}_q)$ , and define  $\mathcal{G} = \langle P \rangle$ . Let  $S$  be a finite subset of  $\mathbb{Z}$ . We want to evaluate

$$h_S(X) = \prod_{s \in S} (X - f([s]P)), \quad \text{where} \quad f : Q \mapsto \begin{cases} 0 & \text{if } Q = 0, \\ x(Q) & \text{if } Q \neq 0, \end{cases}$$

at some  $\alpha$  in  $\mathbb{F}_q$ . Here  $x : \mathcal{E} \rightarrow \mathcal{E}/\langle \pm 1 \rangle \cong \mathbb{P}^1$  is the usual map to the  $x$ -line.

Adapting Algorithm 1 to this setting is not a simple matter of replacing the multiplicative group with an elliptic curve. Indeed, Algorithm 1 explicitly uses the homomorphic nature of  $f : s \mapsto \zeta^s$  to represent the roots  $\zeta^s$  as  $\zeta^i \zeta^j$  where  $s = i + j$ . This presents an obstacle when moving to elliptic curves:  $x([i + j]P)$  is not a rational function of  $x([i]P)$  and  $x([j]P)$ , so we cannot apply the same trick of decomposing most of  $S$  as  $I + J$  before taking a resultant of polynomials encoding  $f(I)$  and  $f(J)$ .

This obstacle does not matter in the factorization context. For example, in §3, a straightforward resultant  $\prod_{i,j} (\alpha/\zeta^j - \zeta^i)$  detects collisions between  $\alpha/\zeta^j$  and  $\zeta^i$ ; our rescaling to  $\prod_{i,j} (\alpha - \zeta^{i+j})$  was unnecessary. Similarly, Montgomery's FFT extension [44] to ECM computes a straightforward resultant  $\prod_{i,j} (x([i]P) - x([j]P))$ , detecting any collisions between  $x([i]P)$  and  $x([j]P)$ ; this factorization method does not compute, and does not need to compute, a product of functions of  $x([i + j]P)$ . The isogenies context is different: we need a product of functions of  $x([i + j]P)$ .

Fortunately, even if the  $x$ -map is not homomorphic, there is an algebraic relation between  $x(P)$ ,  $x(Q)$ ,  $x(P + Q)$ , and  $x(P - Q)$ , which we will review in §4.2. The introduction of the difference  $x(P - Q)$  as well as the sum  $x(P + Q)$  requires us to replace the decomposition of most of  $S$  as  $I + J$  with a decomposition involving  $I + J$  and  $I - J$ , which we will formalize in §4.5. We define the resultant required to tie all this together and compute  $h_{I \pm J}(\alpha)$  in §4.8.

**4.2. Biquadratic relations on  $x$ -coordinates.** Lemma 4.3 recalls the general relationship between  $x(P)$ ,  $x(Q)$ ,  $x(P + Q)$ , and  $x(P - Q)$ . Example 4.4 gives explicit formulæ for the case that is most useful in our applications.

**Lemma 4.3.** *Let  $q$  be a prime power. Let  $\mathcal{E}/\mathbb{F}_q$  be an elliptic curve. There exist biquadratic polynomials  $F_0$ ,  $F_1$ , and  $F_2$  in  $\mathbb{F}_q[X_1, X_2]$  such that*

$$(X - x(P + Q))(X - x(P - Q)) = X^2 + \frac{F_1(x(P), x(Q))}{F_0(x(P), x(Q))}X + \frac{F_2(x(P), x(Q))}{F_0(x(P), x(Q))}$$

for all  $P$  and  $Q$  in  $\mathcal{E}$  such that  $0 \notin \{P, Q, P + Q, P - Q\}$ .

*Proof.* The existence of  $F_0$ ,  $F_1$ , and  $F_2$  is classical (see e.g. [17, p. 132] for the  $F_i$  for Weierstrass models); indeed, the existence of such biquadratic systems is a general phenomenon for theta functions of level 2 on abelian varieties (see e.g. [47, §3]).  $\square$

**Example 4.4** (biquadratics for Montgomery models). If  $\mathcal{E}$  is defined by an affine equation  $By^2 = x(x^2 + Ax + 1)$ , then the polynomials of Lemma 4.3 are

$$\begin{aligned} F_0(X_1, X_2) &= (X_1 - X_2)^2, \\ F_1(X_1, X_2) &= -2((X_1X_2 + 1)(X_1 + X_2) + 2AX_1X_2), \\ F_2(X_1, X_2) &= (X_1X_2 - 1)^2. \end{aligned}$$

The symmetric triquadratic polynomial  $(X_0X_1 - 1)^2 + (X_0X_2 - 1)^2 + (X_1X_2 - 1)^2 - 2X_0X_1X_2(X_0 + X_1 + X_2 + 2A) - 2$  is  $X_0^2F_0(X_1, X_2) + X_0F_1(X_1, X_2) + F_2(X_1, X_2)$ .

Montgomery curves  $By^2 = x(x^2 + Ax + 1)$ , and the remarkably simple formula  $(X_1X_2 - 1)^2 / (X_1 - X_2)^2$  for the product  $x(P + Q)x(P - Q)$  on these curves, were introduced by Montgomery in [43, Section 10.3.1]. See [7] for more information about Montgomery curves.

**4.5. Index systems.** In §3, we represented most of  $S$  as  $I + J$ ; requiring  $I$  and  $J$  to have no common differences ensured this representation had no redundancy. Now we will represent most elements of  $S$  as elements of  $(I + J) \cup (I - J)$ , so we need a stronger restriction on  $I$  and  $J$  to avoid redundancy.

**Definition 4.6.** Let  $I$  and  $J$  be finite sets of integers.

- (1) We say that  $(I, J)$  is an *index system* if the maps  $I \times J \rightarrow \mathbb{Z}$  defined by  $(i, j) \mapsto i + j$  and  $(i, j) \mapsto i - j$  are both injective and have disjoint images.
- (2) If  $S$  is a finite subset of  $\mathbb{Z}$ , then we say that an index system  $(I, J)$  is an *index system for  $S$*  if  $I + J$  and  $I - J$  are both contained in  $S$ .

If  $(I, J)$  is an index system, then the sets  $I + J$  and  $I - J$  are both in bijection with  $I \times J$ . We write  $I \pm J$  for the union of  $I + J$  and  $I - J$ .

**Example 4.7.** Let  $m$  be an odd positive integer, and consider the set

$$S = \{1, 3, 5, \dots, m\}$$

in arithmetic progression. Let

$$I := \{2b(2i + 1) \mid 0 \leq i < b'\} \quad \text{and} \quad J := \{2j + 1 \mid 0 \leq j < b\}$$

where  $b = \lfloor \sqrt{m+1}/2 \rfloor$ ;  $b' = \lfloor (m+1)/4b \rfloor$  if  $b > 0$ ; and  $b' = 0$  if  $b = 0$ . Then  $(I, J)$  is an index system for  $S$ , and  $S \setminus (I \pm J) = K$  where  $K = \{4bb' + 1, \dots, m - 2, m\}$ . If  $b > 0$  then  $\#I = b' \leq b + 2$ ,  $\#J = b$ , and  $\#K \leq 2b - 1$ .

**4.8. Elliptic resultants.** We are now ready to adapt the results of §3 to the setting of §4.1. Our main tool is Lemma 4.9, which expresses  $h_{I \pm J}$  as a resultant of smaller polynomials.

**Lemma 4.9.** *Let  $q$  be a prime power. Let  $\mathcal{E}/\mathbb{F}_q$  be an elliptic curve. Let  $P$  be an element of  $\mathcal{E}(\mathbb{F}_q)$ . Let  $n$  be the order of  $P$ . Let  $(I, J)$  be an index system such that  $I, J, I + J$ , and  $I - J$  do not contain any elements of  $n\mathbb{Z}$ . Then*

$$h_{I \pm J}(X) = \frac{1}{\Delta_{I,J}} \cdot \text{Res}_Z(h_I(Z), E_J(X, Z))$$

where

$$E_J(X, Z) := \prod_{j \in J} (F_0(Z, x([j]P))X^2 + F_1(Z, x([j]P))X + F_2(Z, x([j]P)))$$

and  $\Delta_{I,J} := \text{Res}_Z(h_I(Z), D_J(Z))$  where  $D_J(Z) := \prod_{j \in J} F_0(Z, x([j]P))$ .

*Proof.* Since  $(I, J)$  is an index system,  $I + J$  and  $I - J$  are disjoint, and therefore we have  $h_{I \pm J}(X) = h_{I+J}(X) \cdot h_{I-J}(X)$ . Expanding and regrouping terms, we get

$$\begin{aligned} h_{I \pm J}(X) &= \prod_{(i,j) \in I \times J} (X - x([i+j]P)) (X - x([i-j]P)) \\ &= \prod_{i \in I} \prod_{j \in J} \left( X^2 + \frac{F_1(x([i]P), x([j]P))}{F_0(x([i]P), x([j]P))} X + \frac{F_2(x([i]P), x([j]P))}{F_0(x([i]P), x([j]P))} \right) \end{aligned}$$

by Lemma 4.3. Factoring out the denominator, we find

$$h_{I \pm J}(X) = \frac{\prod_{i \in I} E_J(X, x([i]P))}{\prod_{i \in I} \prod_{j \in J} F_0(x([i]P), x([j]P))} = \frac{\prod_{i \in I} E_J(X, x([i]P))}{\prod_{i \in I} D_J(x([i]P))};$$

and finally  $\prod_{i \in I} E_J(X, x([i]P)) = \text{Res}_Z(h_I(Z), E_J(X, Z))$  and  $\prod_{i \in I} D_J(x([i]P)) = \text{Res}_Z(h_I(Z), D_J(Z)) = \Delta_{I,J}$ , which yields the result.  $\square$

**4.10. Elliptic polynomial evaluation.** Algorithm 2 is an algebraic algorithm for computing  $h_S(\alpha)$ ; it is the elliptic analogue of Algorithm 1. Theorem 4.11 proves its correctness and runtime.

**Theorem 4.11.** *Let  $q$  be a prime power. Let  $\mathcal{E}/\mathbb{F}_q$  be an elliptic curve. Let  $P$  be an element of  $\mathcal{E}(\mathbb{F}_q)$ . Let  $n$  be the order of  $P$ . Let  $(I, J)$  be an index system for a finite set  $S \subset \mathbb{Z}$ . Assume that  $I, J$ , and  $S$  contain no elements of  $n\mathbb{Z}$ . Given  $\alpha$  in  $\mathbb{F}_q$ , Algorithm 2 computes*

$$h_S(\alpha) = \prod_{s \in S} (\alpha - x([s]P))$$

in  $\tilde{O}(\max(\#I, \#J, \#K)) \mathbb{F}_q$ -operations, where  $K = S \setminus (I \pm J)$ .

In particular, if  $\#I, \#J$ , and  $\#K$  are in  $\tilde{O}(\sqrt{\#S})$ , then Algorithm 2 computes  $h_S(\alpha)$  in  $\tilde{O}(\sqrt{\#S}) \mathbb{F}_q$ -operations. The  $\tilde{O}$  is uniform in  $q$ . Instead of taking  $P$  and various  $x([s]P)$  as parameters, Algorithm 2 can take  $P$  as an input, at the cost of computing the relevant multiples of  $P$ .

---

**Algorithm 2:** Computing  $h_S(\alpha) = \prod_{s \in S} (\alpha - x([s]P))$  for  $P \in \mathcal{E}(\mathbb{F}_q)$

---

**Parameters:** a prime power  $q$ ; an elliptic curve  $\mathcal{E}/\mathbb{F}_q$ ;  $P \in \mathcal{E}(\mathbb{F}_q)$ ; a finite subset  $S \subset \mathbb{Z}$ ; an index system  $(I, J)$  for  $S$  such that  $S \cap n\mathbb{Z} = I \cap n\mathbb{Z} = J \cap n\mathbb{Z} = \{\}$ , where  $n$  is the order of  $P$ ;  $x([s]P)$  for each  $s \in I \cup J \cup K$

**Input:**  $\alpha$  in  $\mathbb{F}_q$

**Output:**  $h_S(\alpha)$  where  $h_S(X) = \prod_{s \in S} (X - x([s]P))$

- 1  $h_I \leftarrow \prod_{i \in I} (Z - x([i]P)) \in \mathbb{F}_q[Z]$
  - 2  $D_J \leftarrow \prod_{j \in J} F_0(Z, x([j]P)) \in \mathbb{F}_q[Z]$
  - 3  $\Delta_{I,J} \leftarrow \text{Res}_Z(h_I, D_J) \in \mathbb{F}_q$
  - 4  $E_J \leftarrow \prod_{j \in J} (F_0(Z, x([j]P))\alpha^2 + F_1(Z, x([j]P))\alpha + F_2(Z, x([j]P))) \in \mathbb{F}_q[Z]$
  - 5  $R \leftarrow \text{Res}_Z(h_I, E_J) \in \mathbb{F}_q$
  - 6  $h_K \leftarrow \prod_{k \in S \setminus (I \pm J)} (\alpha - x([k]P)) \in \mathbb{F}_q$
  - 7 **return**  $h_K \cdot R / \Delta_{I,J}$
- 

*Proof.* The proof follows that of Proposition 3.5. Since  $S \setminus K = I \pm J$ , we have  $h_S(\alpha) = h_{I \pm J}(\alpha) \cdot h_K(\alpha)$ . Using the notation of Lemma 4.9: Line 1 computes  $h_I(Z)$  in  $\tilde{O}(\#I)$   $\mathbb{F}_q$ -operations; Line 2 computes  $D_J(Z)$  in  $\tilde{O}(\#J)$   $\mathbb{F}_q$ -operations; Line 3 computes  $\Delta_{I,J}$  in  $\tilde{O}(\max(\#I, \#J))$   $\mathbb{F}_q$ -operations; Line 4 computes  $E_J(\alpha, Z)$  in  $\tilde{O}(\#J)$   $\mathbb{F}_q$ -operations; Line 5 computes  $\text{Res}_Z(h_I(Z), E_J(\alpha, Z))$ , which is the same as  $\Delta_{I,J} h_{I \pm J}(\alpha)$  by Lemma 4.9, in  $\tilde{O}(\max(\#I, \#J))$   $\mathbb{F}_q$ -operations; Line 6 computes  $h_K(\alpha)$  in  $\tilde{O}(\#K)$   $\mathbb{F}_q$ -operations; and Line 7 returns  $h_S(\alpha) = h_K(\alpha) \cdot h_{I \pm J}(\alpha)$ . The total number of  $\mathbb{F}_q$ -operations is in  $\tilde{O}(\max(\#I, \#J, \#K))$ .  $\square$

**Example 4.12** (evaluating kernel polynomials). We now address a problem from the introduction: evaluating  $\Psi_{\mathcal{G}}$ , the radical of the denominators of the rational functions defining the  $\ell$ -isogeny  $\phi : \mathcal{E} \rightarrow \mathcal{E}'$  with kernel  $\mathcal{G} = \langle P \rangle$ , for  $\ell$  odd. Here

$$\Psi_{\mathcal{G}}(X) = h_S(X) = \prod_{s \in S} (X - x([s]P)) \quad \text{where} \quad S = \{1, 3, \dots, \ell - 2\}$$

(the set  $S$  may be replaced by any set of representatives of  $((\mathbb{Z}/\ell\mathbb{Z}) \setminus \{0\})/\langle \pm 1 \rangle$ ). Following Example 4.7, let  $I = \{2b(2i + 1) \mid 0 \leq i < b'\}$  and  $J = \{1, 3, \dots, 2b - 1\}$  with  $b = \lfloor \sqrt{\ell - 1}/2 \rfloor$  and (for  $b > 0$ )  $b' = \lfloor (\ell - 1)/4b \rfloor$ ; then  $(I, J)$  is an index system for  $S$ , and Algorithm 2 computes  $h_S(\alpha) = \Psi_{\mathcal{G}}(\alpha)$  for any  $\alpha$  in  $\mathbb{F}_q$  in  $\tilde{O}(\sqrt{\ell})$   $\mathbb{F}_q$ -operations.

**Example 4.13** (evaluating derivatives of polynomials). Algorithm 2 can evaluate  $h_S$  at points in any  $\mathbb{F}_q$ -algebra, at the cost of a slowdown that depends on how large the algebra is. These algebras need not be fields. For example, we can evaluate  $h_S(\alpha + \epsilon)$  in the algebra  $\mathbb{F}_q[\epsilon]/\epsilon^2$  of 1-jets, obtaining  $h_S(\alpha) + \epsilon h'_S(\alpha)$ . We can thus evaluate derivatives, sums over roots, etc. The algebra of 1-jets was used the same way in, e.g., [46; 40; 5]; [2] also notes Zagier's suggested terminology "jet plane".

**4.14. Irrational generators.** The point  $P$  in Lemma 4.9, Algorithm 2, and Theorem 4.11 need not be in  $\mathcal{E}(\mathbb{F}_q)$ : everything is defined over  $\mathbb{F}_q$  if  $x(P)$  is in  $\mathbb{F}_q$ . More generally, take  $P$  in  $\mathcal{E}(\mathbb{F}_{q^e})$  with  $x(P)$  in  $\mathbb{F}_{q^e}$  for some minimal  $e \geq 1$ . The  $q$ -power Frobenius  $\pi$  on  $\mathcal{E}$  maps  $P$  to  $\pi(P) = [\lambda]P$  for some eigenvalue  $\lambda$  in  $\mathbb{Z}/n\mathbb{Z}$  of order  $e$  in  $(\mathbb{Z}/n\mathbb{Z})^*$ . Let  $L = \{\lambda^a \mid 0 \leq a < e\}$ . For  $h_S(X)$  to be in  $\mathbb{F}_q[X]$ , we need  $S = LS'$  for some  $S' \subseteq \mathbb{Z}$  (modulo  $n$ ): that is,  $S = \{\lambda^a s' \mid 0 \leq a < e, s' \in S'\}$ . Then

$$h_S(X) = \prod_{s' \in S'} \prod_{a=0}^{e-1} (X - x([\lambda^a s']P)) = \prod_{s' \in S'} g_{s'}(X)$$

where the polynomial

$$g_{s'}(X) = \prod_{a=0}^{e-1} (X - x([\lambda^a s']P)) = \prod_{a=0}^{e-1} (X - x(\pi^a([s']P))) = \prod_{a=0}^{e-1} (X - x([s']P)^{q^a})$$

is in  $\mathbb{F}_q[X]$ , and can be easily computed from  $x([s]P)$ .

To write  $h_I$ ,  $D_J$ , and  $E_J$  as products of polynomials over  $\mathbb{F}_q$ , we need the index system  $(I, J)$  for  $S$  to satisfy  $(I, J) = (LI', LJ')$  for some index system  $(I', J')$  for  $S'$ . While this does not affect the asymptotic complexity of the resulting evaluation algorithms at our level of analysis, it should be noted that the requirement that  $(I, J) = (LI', LJ')$  is quite strong: typically  $e$  is in  $O(\ell)$ , so  $\#L$  is not in  $\tilde{O}(\sqrt{\#S})$ , and a suitable index system  $(I, J)$  with  $\#I$  and  $\#J$  in  $\tilde{O}(\sqrt{\#S})$  does not exist.

**4.15. Other functions on  $\mathcal{E}$ .** We can replace  $x$  with more general functions on  $\mathcal{E}$ , though for completely general  $f$  there may be no useful analogue of Lemma 4.3, or at least not one that allows a Lemma 4.9 with conveniently small index system. However, everything above adapts easily to the case where  $x$  is composed with an automorphism of  $\mathbb{P}^1$  (that is,  $f = (ax + b)/(cx + d)$  with  $a, b, c, d$  in  $\mathbb{F}_q$  such that  $ad \neq bc$ ). Less trivially, we can take  $f = \psi_x$  for any isogeny  $\psi : \mathcal{E} \rightarrow \mathcal{E}''$ . In this case, the  $F_0$ ,  $F_1$ , and  $F_2$  of Lemma 4.3 are derived from the curve  $\mathcal{E}''$ , not  $\mathcal{E}$ .

**4.16. Abelian varieties.** It is tempting to extend our results to higher-dimensional principally polarized abelian varieties (PPAVs), replacing  $\mathcal{E}$  with a PPAV  $\mathcal{A}/\mathbb{F}_q$ , and  $x$  with some coordinate on  $\mathcal{A}$ , but evaluating the resulting  $h_S$  using our methods is more complicated. The main issue is the analogue of Lemma 4.3. If we choose any even coordinate  $x$  on  $\mathcal{A}$ , then the classical theory of theta functions yields quadratic relations between  $x(P + Q)$ ,  $x(P - Q)$ , and the coordinates of  $P$  and  $Q$ , but not *only*  $x(P)$  and  $x(Q)$ : they also require the other even coordinates of  $P$  and  $Q$ . (The simplest example of this is seen in the differential addition formulæ for Kummer surfaces: see [22, §6], [31, §3.2], and [18, §4.4].) This means that an analogue of Algorithm 2 for PPAVs would require multivariate polynomials and resultants; an investigation of this is well beyond the scope of this article.

## 5. Computing elliptic isogenies

We now apply the techniques of §4 to the problem of efficient isogeny computation. The task is divided in two parts: evaluating isogenies on points (§5.1), and computing codomain curves (§5.2). Our cryptographic applications use isogenies between Montgomery models of elliptic curves, and we concentrate exclusively on this case here; but our methods adapt easily to Weierstrass and other models.

**5.1. Evaluating isogenies.** Let  $\mathcal{E}/\mathbb{F}_q : y^2 = x(x^2 + Ax + 1)$  be an elliptic curve in Montgomery form, and let  $P$  be a point of prime order  $\ell \neq 2$  in  $\mathcal{E}(\mathbb{F}_q)$ . Costello and Hisil give explicit formulæ in [25] for a quotient isogeny  $\phi : \mathcal{E} \rightarrow \mathcal{E}'$  with kernel  $\mathcal{G} = \langle P \rangle$  such that  $\mathcal{E}'/\mathbb{F}_q : y^2 = x(x^2 + A'x + 1)$  is a Montgomery curve:

$$\phi : (X, Y) \mapsto (\phi_x(X), c_0 Y \phi'_x(X))$$

where  $c_0 = \prod_{0 < s < \ell/2} x([s]P)$  and

$$\phi_x(X) = X \prod_{0 < s < \ell} \frac{x([s]P)X - 1}{X - x([s]P)}. \quad (1)$$

See [51] for generalizations and a different proof, and see the earlier paper [45] for analogous Edwards-coordinate formulas.

Our main goal is to evaluate  $\phi$  on the level of  $x$ -coordinates: that is, to compute  $\phi_x(\alpha)$  given  $\alpha = x(Q)$  for  $Q$  in  $\mathcal{E}(\mathbb{F}_q)$ . This is sufficient for our cryptographic applications. Applications that also need the  $y$ -coordinate of  $\phi(Q)$ , namely  $c_0 y(Q) \phi'_x(\alpha)$ , can compute  $c_0$  as  $(-1)^{(\ell-1)/2} h_S(0)$ , and can compute  $\phi'_x(\alpha)$  together with  $\phi_x(\alpha)$  by the technique of Example 4.13. To compute  $\phi_x(\alpha)$ , we rewrite Eq. (1) as

$$\phi_x(X) = \frac{X^\ell \cdot h_S(1/X)^2}{h_S(X)^2} \quad \text{where} \quad S = \{1, 3, \dots, \ell-2\}.$$

Computing  $\phi_x(\alpha)$  thus reduces to two applications of Algorithm 4.11, using (for example) the index system  $(I, J)$  for  $S$  in Example 4.7. The constant  $\Delta_{I,J}$  appears with the same multiplicity in the numerator and denominator, so we need not compute it. All divisions in the computation are by nonzero field elements except in the following cases, which can be handled separately: if  $Q = 0$  then  $\phi(Q) = 0$ ; if  $Q \neq 0$  but  $h_S(\alpha) = 0$  for  $\alpha = x(Q)$  then  $\phi(Q) = 0$ ; if  $Q = (0, 0)$  then  $\phi(Q) = (0, 0)$ .

**5.2. Computing codomain curves.** Our other main task is to determine the coefficient  $A'$  in the defining equation of  $\mathcal{E}'$ .

One approach is as follows. We can now efficiently compute  $\phi(Q)$  for any  $Q$  in  $\mathcal{E}(\mathbb{F}_q)$ . Changing the base ring from  $\mathbb{F}_q$  to  $R = \mathbb{F}_q[\alpha]/(\alpha^2 + A\alpha + 1)$  (losing a small constant factor in the cost of evaluation) gives us  $\phi(Q)$  for any  $Q$  in  $\mathcal{E}(R)$ . In particular,  $Q = (\alpha, 0)$  is a point in  $\mathcal{E}[2](R)$ , and computing  $\phi(Q) = (\alpha', 0)$  reveals  $A' = -(\alpha' + 1/\alpha')$ . An alternative—at the expense of taking a square root, which is no longer a  $q$ -independent algebraic computation—is to find a point  $(\alpha, 0)$  in  $\mathcal{E}(\mathbb{F}_{q^2})$  with  $\alpha \neq 0$ . Sometimes  $\alpha$  is in  $\mathbb{F}_q$ , and then extending to  $\mathbb{F}_{q^2}$  is unnecessary.



Another approach is to use explicit formulas for  $A'$ . The formulas from [25] give  $A' = c_0^2(A - 3\sigma)$  where  $c_0^2 = \prod_{0 < s < \ell} x([s]P)$  and  $\sigma = \sum_{0 < s < \ell} (x([s]P) - 1/x([s]P))$ . As pointed out in [42] in the context of CSIDH, one can instead transform to twisted Edwards form and use the formulas from [45], obtaining  $A' = 2(1 + d)/(1 - d)$  where

$$d = \left( \frac{A-2}{A+2} \right)^\ell \left( \prod_{s \in S} \frac{x([s]P) - 1}{x([s]P) + 1} \right)^8 = \left( \frac{A-2}{A+2} \right)^\ell \left( \frac{h_S(1)}{h_S(-1)} \right)^8.$$

We can thus compute  $A'$  using  $\tilde{O}(\sqrt{\ell})$  operations: every task we need can be performed by some evaluations of  $h_S$  and some (asymptotically negligible) operations.

## 6. Applications in isogeny-based cryptography

With the notable exception of SIDH/SIKE [36; 27; 1], most isogeny-based cryptographic protocols need to evaluate large-degree isogenies. Specifically, CRS [52; 26], CSIDH [20], CSURF [19], etc. use large-degree isogenies, since not enough keys are fast compositions of isogenies of a few small prime degrees. The largest isogeny degree, with standard optimizations, grows quasi-linearly in the pre-quantum security level. For the same post-quantum security level, known quantum attacks require an asymptotically larger base field but do not affect the largest isogeny degree; see [20, Remark 11].

Concretely, targeting 128 bits of pre-quantum security, CSIDH-512 fixes

$$p = 4 \cdot \underbrace{(3 \cdot 5 \cdots 373)}_{73 \text{ first odd primes}} \cdot 587 - 1$$

and uses isogenies of all odd prime degrees  $\ell \mid p + 1$ . Similarly, CSURF-512 fixes

$$p = 8 \cdot 9 \cdot \underbrace{(5 \cdot 7 \cdots 337)}_{66 \text{ consecutive primes}} \cdot 349 \cdot 353 \cdot \underbrace{(367 \cdots 389)}_{6 \text{ consecutive primes}} - 1$$

and uses isogenies of all prime degrees  $\ell \mid p + 1$ , including  $\ell = 2$ .

The CSIDH and CSURF algorithms repeatedly sample a random point of order dividing  $p + 1$  in  $\mathcal{E}/\mathbb{F}_p$ , multiply it by an appropriate cofactor to get  $P$ , and then apply Vélu's formulas for each of the primes  $\ell \mid \text{ord}(P)$  to obtain  $\mathcal{E}' = \mathcal{E}/\langle P \rangle$ . Our algorithm seamlessly replaces Vélu's formulas in both systems. Computing  $\mathcal{E}'$  is easy in CSURF: all curves involved have rational 2-torsion, and can thus be represented by a root of  $\alpha^2 + A\alpha - 1$  in  $\mathbb{F}_p$ . For CSIDH, we can apply the techniques of §5.2; alternatively, we can walk to the surface and represent curves as in CSURF.

B-SIDH [24] is an SIDH variant using smaller prime fields, at the cost of much larger prime isogeny degrees. One participant uses isogenies of degree  $\ell \mid p + 1$ , and the other uses  $\ell \mid p - 1$ . Since primes  $p$  such that  $p - 1$  and  $p + 1$  both have many small prime factors are rare, some of the  $\ell$  involved in B-SIDH tend to be even larger than in CSIDH and CSURF. The B-SIDH algorithm starts from a single point  $P$  and computes  $\mathcal{E}/\langle P \rangle$  together with the evaluation of  $\phi : \mathcal{E} \rightarrow \mathcal{E}/\langle P \rangle$  at three points. Unlike CSIDH and

CSURF, there is no repeated random sampling of points: a single  $\ell$ -isogeny evaluation for each prime  $\ell \mid p \pm 1$  is needed.

Our asymptotic speedup in isogeny evaluation implies asymptotic speedups for CRS, CSIDH, CSURF, and B-SIDH as the security level increases. This does not imply, however, that there is a speedup for (e.g.) pre-quantum security  $2^{128}$ .

The Appendix of this paper’s full version [6] addresses the question of how large  $\ell$  needs to be before our algorithms become faster than the conventional algorithms. It looks more closely at performance and quantifies the cross-over point by considering different metrics such as time in several software or the number of multiplications. More precisely, we present four implementations: one in magma [10], one in julia [9] (with nemo [29] for the underlying arithmetic) and two in C (a first one using the underlying arithmetic of FLINT [32] and the second one on top of the arithmetic subroutines of [20]). In each of the metrics considered there, the cross-over point is within the range of primes used in CSIDH-512. The new  $\ell$ -isogeny algorithm sets new speed records for CSIDH-512 and CSIDH-1024 by small but measurable percentages, and has more effect on protocols that use larger  $\ell$ -isogenies. Our code is available from <https://velusqrt.isogeny.org>.

Cryptographic protocols that exploit the KLPT algorithm [37] for isogeny path renormalization, such as the signature scheme [30] and the encryption scheme SÉTA [28], need to work with irrational torsion points. They may thus benefit from the technique of §4.14. We did not investigate these protocols further.

## References

- [1] Reza Azarderakhsh, Brian Koziel, Matt Campagna, Brian LaMacchia, Craig Costello, Patrick Longa, Luca De Feo, Michael Naehrig, Basil Hess, Joost Renes, Amir Jalali, Vladimir Soukharev, David Jao, and David Urbanik. Supersingular isogeny key encapsulation, 2017. <https://sike.org>.
- [2] Karim Belabas, Hendrik W. Lenstra, Jr., and Don B. Zagier. Explicit methods in number theory, 2011. Oberwolfach report 35/2011. <https://publications.mfo.de/handle/mfo/3250>.
- [3] Daniel J. Bernstein. Scaled remainder trees, 2004. <https://cr.yp.to/papers.html#scaledmod>.
- [4] Daniel J. Bernstein. Reducing lattice bases to find small-height values of univariate polynomials. In Joe Buhler and Peter Stevenhagen, editors, *Algorithmic number theory: lattices, number fields, curves and cryptography*, pages 421–446. Cambridge University Press, 2008. <https://cr.yp.to/papers.html#smallheight>.
- [5] Daniel J. Bernstein. Jet list decoding, 2011. <https://cr.yp.to/talks/2011.11.24/slides.pdf>.
- [6] Daniel J. Bernstein, Luca De Feo, Antonin Leroux, and Benjamin Smith. Faster computation of isogenies of large prime degree. Cryptology ePrint Archive, Report 2020/341, 2020. <https://eprint.iacr.org/2020/341>.
- [7] Daniel J. Bernstein and Tanja Lange. Montgomery curves and the Montgomery ladder. In Joppe W. Bos and Arjen K. Lenstra, editors, *Topics in computational number theory inspired by Peter L. Montgomery*, pages 82–115. Cambridge University Press, 2017. <https://eprint.iacr.org/2017/293>.
- [8] Daniel J. Bernstein, Tanja Lange, Chloe Martindale, and Lorenz Panny. Quantum circuits for the CSIDH: optimizing quantum evaluation of isogenies. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT*, volume 11477 of *Lecture Notes in Computer Science*, pages 409–441, 2019. <https://ia.cr/2018/1059>.
- [9] Jeff Bezanson, Alan Edelman, Stefan Karpinski, and Viral B. Shah. Julia: A fresh approach to numerical computing. *SIAM Review*, 59(1):65–98, 2017. <https://arxiv.org/abs/1411.1607>.

- [10] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3–4):235–265, 1997. Computational algebra and number theory (London, 1993). <https://www.math.ru.nl/~bosma/pubs/JSC1997Magma.pdf>.
- [11] Alin Bostan. Computing the N-th term of a q-holonomic sequence. In *Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation*, ISSAC '20, page 46–53, New York, NY, USA, 2020. Association for Computing Machinery.
- [12] Alin Bostan, Pierrick Gaudry, and Éric Schost. Linear recurrences with polynomial coefficients and application to integer factorization and Cartier–Manin operator. *SIAM Journal on Computing*, 36(6):1777–1806, 2007. <https://hal.inria.fr/inria-00514132>.
- [13] Alin Bostan, Grégoire Lecerf, Bruno Salvy, Éric Schost, and Bernd Wiebelt. Complexity issues in bivariate polynomial factorization. ISSAC 2004, pages 42–49. Association for Computing Machinery, 2004. <https://specfun.inria.fr/bostan/publications/BoLeSaScWi04.pdf>.
- [14] Alin Bostan, Grégoire Lecerf, and Éric Schost. Tellegen’s principle into practice. ISSAC 2003, pages 37–44. Association for Computing Machinery, 2003. <https://specfun.inria.fr/bostan/publications/BoLeSc03.pdf>.
- [15] Richard P. Brent and H. T. Kung. The area-time complexity of binary multiplication. *Journal of the ACM*, 28:521–534, 1981. <https://maths-people.anu.edu.au/~brent/pub/pub055.html>.
- [16] Peter Bürgisser, Michael Clausen, and Mohammad Amin Shokrollahi. *Algebraic complexity theory*, volume 315 of *Grundlehren der mathematischen Wissenschaften*. Springer, 1997.
- [17] J. W. S. Cassels. *Lectures on Elliptic Curves*, volume 24 of *London Mathematical Society Student Texts*. Cambridge University Press, 1991.
- [18] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus 2*, volume 230 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, 1996.
- [19] Wouter Castryck and Thomas Decru. CSIDH on the surface. 2019. <https://ia.cr/2019/1404>.
- [20] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: an efficient post-quantum commutative group action. In *ASIACRYPT (3)*, volume 11274 of *Lecture Notes in Computer Science*, pages 395–427, 2018. <https://ia.cr/2018/383>.
- [21] Daniel Cervantes-Vázquez, Mathilde Chenu, Jesús-Javier Chi-Domínguez, Luca De Feo, Francisco Rodríguez-Henríquez, and Benjamin Smith. Stronger and faster side-channel protections for CSIDH. In *Progress in Cryptology – LATINCRYPT 2019*, pages 173–193, 2019. <https://ia.cr/2019/837>.
- [22] David V. Chudnovsky and Gregory V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Advances in Applied Mathematics*, 7(4):385–434, 1986. <https://core.ac.uk/download/pdf/82012348.pdf>.
- [23] Edgar Costa and David Harvey. Faster deterministic integer factorization. *Mathematics of Computation*, 83(285):339–345, 2014. <https://arxiv.org/abs/1201.2116>.
- [24] Craig Costello. B-SIDH: supersingular isogeny Diffie-Hellman using twisted torsion, 2019. <https://ia.cr/2019/1145>.
- [25] Craig Costello and Hüseyin Hisil. A simple and compact algorithm for SIDH with arbitrary degree isogenies. In *ASIACRYPT (2)*, volume 10625 of *Lecture Notes in Computer Science*, pages 303–329, 2017. <https://eprint.iacr.org/2017/504>.
- [26] Jean-Marc Couveignes. Hard homogeneous spaces, 2006. <https://ia.cr/2006/291>.
- [27] Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology*, 8(3):209–247, 2014. <https://ia.cr/2011/506>.
- [28] Cyprien Delpech de Saint Guilhem, Péter Kutas, Christophe Petit, and Javier Silva. SÉTA: supersingular encryption from torsion attacks, 2019. <https://ia.cr/2019/1291>.
- [29] Claus Fieker, William Hart, Tommy Hofmann, and Fredrik Johansson. Nemo/Hecke: Computer algebra and number theory packages for the Julia programming language. ISSAC 2017, pages 157–164, New York, NY, USA, 2017. ACM. <https://arxiv.org/abs/1705.06134v1>.
- [30] Steven D. Galbraith, Christophe Petit, and Javier Silva. Identification protocols and signature schemes based on supersingular isogeny problems. In *ASIACRYPT*, 2017. <https://ia.cr/2016/1154>.

- [31] Pierrick Gaudry. Fast genus 2 arithmetic based on Theta functions. *J. Mathematical Cryptology*, 1(3):243–265, 2007. <https://ia.cr/2005/314>.
- [32] William B. Hart, Fredrik Johansson, and Sebastian Pancratz. FLINT: Fast Library for Number Theory, 2020. Development version, <http://flintlib.org>.
- [33] David Harvey. Faster algorithms for the square root and reciprocal of power series. *Mathematics of Computation*, 80(273):387–394, 2011. <https://arxiv.org/abs/0910.1926>.
- [34] Markus Hittmeir. A babystep-giantstep method for faster deterministic integer factorization. *Mathematics of Computation*, 87(314):2915–2935, 2018. <https://arxiv.org/abs/1608.08766v1>.
- [35] Aaron Hutchinson, Jason LeGrow, Brian Koziel, and Reza Azarderakhsh. Further optimizations of CSIDH: A systematic approach to efficient strategies, permutations, and bound vectors, 2019. <https://ia.cr/2019/1121>.
- [36] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *PQCrypto 2011*, pages 19–34, 2011. <https://ia.cr/2011/506>.
- [37] David Kohel, Kristin E. Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion  $\ell$ -isogeny path problem. <https://ia.cr/2014/505>.
- [38] David R. Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California at Berkeley, 1996. <http://iml.univ-mrs.fr/kohel/pub/thesis.pdf>.
- [39] Hendrik W. Lenstra, Jr. Factoring integers with elliptic curves. *Annals of mathematics*, pages 649–673, 1987. <https://www.math.leidenuniv.nl/hwl/PUBLICATIONS/1987c/art.pdf>.
- [40] Gregorio Malajovich and Jorge P. Zubelli. Tangent Graeffe iteration. *Numerische Mathematik*, 89(4):749–782, 2001. <https://arxiv.org/abs/math/9908150>.
- [41] Michael Meyer, Fabio Campos, and Steffen Reith. On lions and elligators: An efficient constant-time implementation of CSIDH. In Jintai Ding and Rainer Steinwandt, editors, *PQCrypto 2019*, pages 307–325, 2019. <https://ia.cr/2018/1198>.
- [42] Michael Meyer and Steffen Reith. A faster way to the CSIDH. In *INDOCRYPT*, volume 11356 of *Lecture Notes in Computer Science*, pages 137–152. Springer, 2018. <https://ia.cr/2018/782>.
- [43] Peter L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Mathematics of Computation*, 48(177):243–264, 1987.
- [44] Peter Lawrence Montgomery. *An FFT extension of the elliptic curve method of factorization*. PhD thesis, UCLA, 1992. <https://cr.yp.to/bib/1992/montgomery.pdf>.
- [45] Dustin Moody and Daniel Shumow. Analogues of Vélú’s formulas for isogenies on alternate models of elliptic curves. *Mathematics of Computation*, 85(300):1929–1951, 2016. <https://ia.cr/2011/430>.
- [46] Jacques Morgenstern. Algorithmes linéaires tangents et complexité. *Comptes Rendus Hebdomadaires des Séances de l’Académie des Sciences, Série A*, 277:367–369, septembre 1973. <https://gallica.bnf.fr/ark:/12148/cb34416987n/date>.
- [47] David B. Mumford. On the equations defining abelian varieties. I. *Inventiones Mathematicae*, 1(4):287–354, 1966. <https://dash.harvard.edu/handle/1/3597241>.
- [48] Hiroshi Onuki, Yusuke Aikawa, Tsutomu Yamazaki, and Tsuyoshi Takagi. (Short Paper) A faster constant-time algorithm of CSIDH keeping two points. In Nuttapon Attrapadung and Takeshi Yagi, editors, *Advances in Information and Computer Security*, pages 23–33, 2019. <https://ia.cr/2019/353>.
- [49] John M. Pollard. Theorems on factorization and primality testing. *Mathematical Proceedings of the Cambridge Philosophical Society*, 76(3):521–528, 1974. <https://doi.org/10.1017/S0305004100049252>.
- [50] Lawrence R. Rabiner, R. W. Schafer, and Charles M. Rader. The chirp-z transform algorithm. *IEEE Transactions on Audio and Electroacoustics*, 17:86–92, 1969. [https://www.ece.ucsb.edu/Faculty/Rabiner/ece259/Reprints/015\\_czt.pdf](https://www.ece.ucsb.edu/Faculty/Rabiner/ece259/Reprints/015_czt.pdf).
- [51] Joost Renes. Computing isogenies between Montgomery curves using the action of  $(0, 0)$ . *PQCrypto 2018*, pages 229–247, 2018. <https://ia.cr/2017/1198>.
- [52] Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies, 2006. <https://ia.cr/2006/145>.
- [53] Volker Strassen. Einige Resultate über Berechnungskomplexität. *Jahresbericht der Deutschen Mathematiker-Vereinigung*, 78:1–8, 1976.

- [54] Volker Strassen. The computational complexity of continued fractions. *SIAM Journal on Computing*, 12:1–27, 1983.
- [55] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.0)*, 2020. <https://www.sagemath.org>.
- [56] Jacques Vélú. Isogénies entre courbes elliptiques. *Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences, Série A*, 273:238–241, juillet 1971. <https://gallica.bnf.fr/ark:/12148/cb34416987n/date>.

Received 28 Feb 2020. Revised 28 Feb 2020.

DANIEL J. BERNSTEIN: *Department of Computer Science, University of Illinois at Chicago, USA*  
and

*Horst Görtz Institute for IT Security, Ruhr University Bochum, Germany*  
[djb@cr.yp.to](mailto:djb@cr.yp.to)

LUCA DE FEO: *IBM Research Zürich, Switzerland*  
[antsXIV@defeo.lu](mailto:antsXIV@defeo.lu)

ANTONIN LEROUX: [antonin.leroux@polytechnique.org](mailto:antonin.leroux@polytechnique.org)  
*DGA, Inria and École Polytechnique, Institut Polytechnique de Paris, Palaiseau, France*

BENJAMIN SMITH: [smith@lix.polytechnique.fr](mailto:smith@lix.polytechnique.fr)  
*Inria and École Polytechnique, Institut Polytechnique de Paris, Palaiseau, France*



# On the security of the multivariate ring learning with errors problem

Carl Bootland, Wouter Castryck, and Frederik Vercauteren

The multivariate ring learning with errors ( $m$ -RLWE) problem was introduced in 2015 by Pedrouzo-Ulloa, Troncoso-Pastoriza and Pérez-González. Instead of working over a polynomial residue ring with one variable as in RLWE, it works over a polynomial residue ring in several variables. However, care must be taken when choosing the multivariate rings for use in cryptographic applications as they can be either weak or simply equivalent to univariate RLWE. For example, Pedrouzo-Ulloa et al. suggest using tensor products of cyclotomic rings, in particular power-of-two cyclotomic rings. They claim incorrectly that the security increases with the product of the individual degrees. We present simple methods to solve the search  $m$ -RLWE problem far more efficiently than was claimed in the previous literature by reducing the problem to the RLWE problem in dimension equal to the maximal degree of its components (and not the product) and where the noise increases with the square-root of the degree of the other components. Our methods utilise the fact that the defining cyclotomic polynomials share algebraically related roots. We use these methods to successfully attack the search variant of the  $m$ -RLWE problem for a set of parameters estimated to offer more than 2600 bits of security, and being equivalent to solving the bounded distance decoding problem in a highly structured lattice of dimension 16384, in less than two weeks of computation time or just a few hours if parallelized on 128 cores. Finally, we also show that optimizing module-LWE cryptosystems by introducing an extra ring structure as is common practice to optimize LWE, can result in a total breakdown of security.

## 1. Introduction

In concurrent and independent work, Stehlé et al. [22] and Lyubashevsky et al. [14] introduced ring variants of the learning with errors (LWE) problem. The problem in the former is known as the polynomial learning with errors (PLWE) problem while the latter is known as the ring learning with errors (RLWE) problem. The main advantage of using a ring variant over the original problem is that the schemes are much more efficient and the size of the public keys is significantly smaller. Later, a module variant was introduced in [4] where it is called the general learning with errors problem and captures both previous problems as extremes of a broader class of problems.

---

*MSC2010:* primary 11T71; secondary 11R18, 94A60.

*Keywords:* multivariate, ring learning with errors, cyclotomic rings, module-LWE.

For a ring  $R$ , free and of finite rank (as a module) over  $\mathbb{Z}$ , and positive integers  $n$  and  $q$  set  $R_q = R/qR$ . Samples from the module-LWE distribution are of the form  $(\mathbf{a}, b)$  where  $\mathbf{a} \leftarrow R_q^n$  is uniformly sampled and  $b = \langle \mathbf{a}, \mathbf{s} \rangle + e \bmod q$  where  $e \leftarrow \chi$  is sampled from an error distribution and  $\mathbf{s} \in R_q^n$  is the secret vector. LWE is the case when  $R = \mathbb{Z}$  and the ring variant is when  $n = 1$  but now the ring  $R$  can be thought of as a polynomial residue ring. Thus in going from LWE to its ring variant we replace the inner product of vectors by the product of polynomials (modulo some polynomial modulus). The module-LWE problem is used in cryptographic primitives such as the NIST submissions Saber [8] and Kyber [3].

As previously stated, module-LWE bridges the gap between LWE and RLWE, but is still not as efficient as RLWE. It is thus tempting to replace the inner product in module-LWE by a product of polynomials, just like RLWE, but where now the coefficients are from a polynomial residue ring (in an independent variable) rather than simply integers. This idea naturally leads to the multivariate ring learning with errors ( $m$ -RLWE) problem as introduced by Pedrouzo-Ulloa, Troncoso-Pastoriza and Pérez-González in a series of papers [18; 19; 20] between 2015 and 2017. Essentially this does to module-LWE what RLWE does to LWE—by adding more structure they are able to construct more efficient schemes with smaller key sizes.

Originally, only the simplest case of the problem in two variables was formulated. They define this problem in [18], which they call the bivariate RLWE (2-RLWE) problem using the ring  $R_q[x, y] = \mathbb{Z}_q[x, y]/(f(x), g(y))$  as follows:

**Problem 1.1.** Given a bivariate polynomial residue ring  $R_q[x, y]$  with  $f(x) = x^{n_1} + 1$ ,  $g(y) = y^{n_2} + 1$  and an error distribution  $\chi[x, y]$  on  $R_q[x, y]$  that generates small-norm random bivariate polynomials in  $R_q[x, y]$ ,<sup>1</sup> 2-RLWE relies upon the computational indistinguishability between samples  $(a_i, b_i = a_i \cdot s + e_i)$  and  $(a_i, u_i)$  where  $a_i, u_i \leftarrow R_q[x, y]$  are chosen uniformly at random from the ring  $R_q[x, y]$ , and  $s, e_i \leftarrow \chi[x, y]$  are drawn from the error distribution.

Although not explicitly stated in [18],  $f$  and  $g$  are taken to be two-power cyclotomics, i.e.,  $n_1$  and  $n_2$  are powers of two.

The authors then construct a method for encrypted image processing whose security is based on the 2-RLWE problem. The sample parameters proposed for use are  $n_1 = n_2 = 2^i$ ,  $\lceil \log_2 q \rceil = 22 + 3i$  for  $i = 7, 8, 9, 10$ . Using the lower bound given in [13, Equation (5.2)] these instances are estimated to have bit security 2663, 10288, 38880 and 146675 respectively, though these parameters fall well outside the range of parameters for which the bound was derived, so these security levels are unlikely to be accurate; however, using the LWE-estimator of Albrecht et al. [1] gives even larger security estimates. Thus it is clear Pedrouzo-Ulloa et al. believe these parameter suggestions give a very high security level. However, in light of our attack, which we will see works in dimension  $n_1 = n_2$ , the LWE-estimator gives the estimated security levels as 32, 33, 35 and 98 bits respectively.

<sup>1</sup>Technically, there is no norm on the ring  $R_q[x, y]$  so this statement does not make mathematical sense. What is meant by  $\chi[x, y]$  is to sample an element in  $\mathbb{Z}[x, y]$  whose degree in  $x$  is at most  $n_1 - 1$  and whose degree in  $y$  is at most  $n_2 - 1$  and whose coefficient vector has small-norm, smallness being a function of  $q$ , and then reducing the polynomial modulo  $q$ ,  $f$  and  $g$ .



Further, in [19], Pedrouzo-Ulloa et al. reformulate the  $m$ -RLWE problem in terms of the tensor product of number fields and consider the ring  $R$  now as the tensor product of the corresponding rings of integers. They proceed by generalising the security reductions of Lyubashevsky et al. from RLWE to standard problems on ideal lattices to the multivariate case, now reducing them to multivariate ideal lattice problems.

Finally, in [20], Pedrouzo-Ulloa et al. build upon the  $m$ -RLWE problem, this time again specialised to power-of-two cyclotomics, and give a number of useful multidimensional signal processing operations and optimizations for use with their  $m$ -RLWE based homomorphic encryption scheme.

For the security of their multivariate schemes, the authors claim and give a sketch proof in [20, Proposition 1] that the 2-RLWE problem above is equivalent to the RLWE problem in the ring  $\mathbb{Z}_q[z]/(h(z))$  where  $h(z) = z^{n_1 n_2} + 1$ , however, as will become obvious, this is not true, as we can solve the 2-RLWE problem far more easily. The flaw is that while  $\mathbb{Q}[z]/(h(z))$  certainly contains isomorphic copies of  $\mathbb{Q}[x]/(f(x))$  and  $\mathbb{Q}[y]/(g(y))$ , it is not the smallest number field which does so. If we assume  $n_1 \geq n_2$  then in this specific case,  $\mathbb{Q}[x]/(f(x))$  itself has this property. This shows that we expect to be able to solve the 2-RLWE problem by solving  $\max\{n_1, n_2\}$  dimensional problems, not dimension  $n_1 n_2$ . This logic can be made to work more generally with any cyclotomic fields, not just power of two cyclotomics, as detailed in Section 3A.

In this paper, we give a simple assessment of the security of the  $m$ -RLWE problem and present an efficient attack when the polynomial moduli are related in a certain way. The basic idea of the attack is to apply a number of “smallness”-preserving ring homomorphisms which reduce the problem to standard RLWE problems of much lower dimension and with a slightly larger error distribution. Solving the search variant in each case gives us enough information to recover the secret in the original  $m$ -RLWE problem. For example, for the 2-RLWE problem above with  $n_1 \geq n_2$  the problem is reduced to  $n_2$  instances of the RLWE problem in dimension  $n_1$ , the same modulus  $q$  and with the noise growing only by a factor of  $\sqrt{n_2}$ . This attack shows that the stated hardness of the problem is much lower than had been previously asserted in the literature which claimed security equivalent to RLWE in dimension  $n_1 n_2$ .

We remark that shortly after our results appeared in an online preprint, Cheon, Kim and Yhee [7] used the  $m$ -RLWE problem in defining a generalisation of the HEAAN homomorphic encryption scheme suitable for approximate matrix arithmetic. They also pointed out our evaluation attack and hence used cyclotomic polynomials of coprime order. Furthermore, the original authors of  $m$ -RLWE, together with Gama and Georgieva suggested redefining the problem to instead use modular functions of the form  $x^{n_1} + d_1, y^{n_2} + d_2, \dots$ , where the  $d_i$  are small integers, in order to avoid our attack [17].

The remainder of the paper is organised as follows: in Section 2 we recall the required background and in Section 3 we define the  $m$ -RLWE problem and show that in many cases it is equivalent to the standard RLWE problem. In Section 4 we present our attack on the remaining cases of  $m$ -RLWE and the results of our implementation, and in Section 5 we remark that the standard optimization trick of going from LWE to RLWE, when applied to module-LWE, can result in a total breakdown of security. Finally, we conclude the paper in Section 6.

## 2. Preliminaries

Let  $[n]$  denote the set  $\{0, 1, 2, \dots, n-1\}$ . For a commutative ring  $R$  and an element  $r \in R$  we denote by  $(r)$  the principal ideal of  $R$  generated by  $r$ ; namely,

$$(r) = \{rs \mid s \in R\}.$$

For a finite set  $S$  we denote by  $U(S)$  the uniform distribution on  $S$ .

**2A. Subgaussians.** We also require the notion of a subgaussian random variable. We follow the approach in [15, Section 2.3] and say that a random variable  $X$  over  $\mathbb{R}$  is subgaussian with parameter  $s > 0$  if for all  $t \in \mathbb{R}$  we have

$$\mathbb{E}(e^{2\pi i t X}) \leq e^{\pi s^2 t^2}.$$

We also use the same notation for the probability distribution of  $X$ . It is a simple exercise to show that the sum of subgaussian distributions is also subgaussian:

**Lemma 2.1.** *Let  $s_i \geq 0$  and suppose that we have independent and identically distributed random variables  $X_i$  which are subgaussian with parameter  $s_i$ . Define  $X$  to be the random variable that is the sum of the  $X_i$  and set  $s = (\sum_i s_i^2)^{1/2}$ , then  $X$  is subgaussian with parameter  $s$ .*

We can also apply Markov's inequality to the subgaussian random variable  $X$  with parameter  $s$  which shows that

$$\Pr(|X| \geq t) \leq 2e^{-\pi t^2/s^2}.$$

**2B. RLWE and its variants.** Here we also introduce the distinction between the so-called dual- and primal-RLWE problems as well as the polynomial RLWE problem, abbreviated to PLWE. The starting point for the first two problems is a number field  $K$  and its ring of integers  $\mathcal{O}_K$  and an integer modulus  $q \geq 2$ . Typically  $K$  is a cyclotomic number field but this need not be the case. Samples are of the form  $(a_i, b_i)$  where  $b_i = a_i s + e_i$  and  $a_i \in \mathcal{O}_K/q\mathcal{O}_K$  is sampled uniformly at random and  $e_i$  is sampled from an error distribution on  $K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R}$ . The difference between the two cases is that in the dual-RLWE case the secret  $s$  is sampled from  $\mathcal{O}_K^{\vee}/q\mathcal{O}_K^{\vee}$ , with  $\mathcal{O}_K^{\vee}$  the fractional ideal dual to  $\mathcal{O}_K$ , while in the primal-RLWE case it is sampled from  $\mathcal{O}_K/q\mathcal{O}_K$ . Finally, in the PLWE case  $a_i, s \in \mathbb{Z}_q[x]/(f)$  for some monic irreducible polynomial  $f$  and the error term is an element of  $\mathbb{R}[x]/(f)$ .

The actual problems come in two variants; a decision version where one has to determine whether the second component of the samples is computed according to the RLWE distribution or chosen randomly as in [Problem 1.1](#), and a search version where one is asked to find the secret  $s$ .

It has been shown by Ducas and Durmus [9] for cyclotomic fields, and by Rosca, Stehlé, and Wallet [21] more generally, that one can reduce dual-RLWE to primal-RLWE with only a limited growth in the error term. Also in [21] they show that the reduction can be extended from primal-RLWE to PLWE. Since  $m$ -RLWE is defined to use exclusively cyclotomic rings, for simplicity, we will focus on the PLWE problem in this paper. Our attack is, however, more general and we explain the modifications needed to generalise this to the other more general RLWE problems where appropriate.

**2C. Search RLWE as a BDD problem.** In this section we recall a simple and well-known lattice attack on the search variant of the RLWE problem by considering it as a special case of the bounded distance decoding problem (BDD). The attack works given enough samples and is practical for low-dimensional problems.

Suppose we are given  $\ell$  samples  $\{(a_i, b_i)\}_{i \in [\ell]}$  from the PLWE distribution and suppose we are working in the ring  $R = \mathbb{Z}_q[x]/(f(x))$ ,  $\deg(f) = n$ . Then we know that if  $s$  is the secret polynomial we have  $b_i = sa_i + e_i$  for some  $e_i$  with small coefficients. We can rewrite this as a vector-matrix equation by replacing the elements of  $R$  by their (row) vector of coefficients (with respect to the standard power basis in  $x$ ) which we denote in bold; if  $M_{a_i}$  is the matrix of multiplication by  $a_i$  then we have  $\mathbf{b}_i = s M_{a_i} + \mathbf{e}_i$ . Since  $s$  is the same for each sample we can concatenate all of the samples into one equation:

$$(\mathbf{b}_1 \cdots \mathbf{b}_\ell) = s(M_{a_1} \cdots M_{a_\ell}) + (\mathbf{e}_1 \cdots \mathbf{e}_\ell).$$

This is an instance of the bounded distance decoding (BDD) problem in the  $q$ -ary lattice  $\mathcal{L}$  spanned by the rows of  $(M_{a_1} \cdots M_{a_\ell})$  (with entries taken as integers) and  $qI_{n\ell}$ ; the target vector being  $\mathbf{v} = (\mathbf{b}_1 \cdots \mathbf{b}_\ell)$ . Any BDD-solver, such as Kannan's embedding technique [12] or Babai's nearest plane algorithm [2], can thus be used to solve search PLWE. In general, both the ring  $R$  and its dual  $R^\vee$  can be written as an integral lattice with a suitable choice of basis and the same approach can be taken to write the search problem as a BDD problem.

Two samples will in practice uniquely define  $s$ , and the more samples one has, the better the chance of solving the problem. Since we will use the BDD-solver as a black box in our algorithm, we simply refer to the tool of Albrecht et al. [1] which can be used to estimate the running time of these algorithms.

### 3. The $m$ -RLWE Problem

In [19] the authors define the multivariate RLWE distribution, in its dual formulation, in terms of a tensor product of number fields  $K = \bigotimes_{i \in [m]} K_i$  where each  $K_i$  is a cyclotomic field; not necessarily distinct. The ring  $R$  used is now the tensor product,  $R = \bigotimes_{i \in [m]} \mathcal{O}_{K_i}$ , where  $\mathcal{O}_{K_i}$  is the ring of integers of the number field  $K_i$ . Further, one defines  $\mathbb{T} := K_{\mathbb{R}}/R^\vee$  where  $R^\vee$  is the dual fractional ideal of  $R$  called the codifferent ideal. Finally, for an integer modulus  $q \geq 2$ , set  $R_q = R/qR$  and  $R_q^\vee = R^\vee/qR^\vee$ .

**Definition 3.1** (multivariate RLWE distribution). For  $s \in R_q^\vee$  and an error distribution  $\psi$  over  $K_{\mathbb{R}}$ , a sample from the  $m$ -RLWE distribution  $A_{s,\psi}$  over  $R_q \times \mathbb{T}$  is generated by sampling  $a \leftarrow R_q$  uniformly at random,  $e \leftarrow \psi$ , and outputting  $(a, b = (a \cdot s)/q + e \bmod R^\vee)$ .

One can then define the multivariate RLWE search and decision problems in the standard way.

**Definition 3.2** (multivariate RLWE search problem). Let  $\Psi$  be a family of distributions over  $K_{\mathbb{R}}$ . Denote by  $m$ -RLWE $_{q,\psi}$  the search version of the  $m$ -RLWE problem: given access to arbitrarily many independent samples from  $A_{s,\psi}$  for some fixed uniformly random  $s \in R_q^\vee$  and  $\psi \in \Psi$ , find  $s$ .

**Definition 3.3** (multivariate RLWE decision problem). Let  $\Gamma$  be a distribution over a family of error distributions, each over  $K_{\mathbb{R}}$ . The average-case-decision version of the  $m$ -RLWE problem, denoted by

$m$ -R-DLWE $_{q,\Gamma}$ , is to distinguish with nonnegligible advantage between arbitrarily many independent samples from  $A_{s,\psi}$ , for a random choice of  $(s, \psi) \leftarrow U(R_q^\vee) \times \Gamma$ , and the same number of uniformly random and independent samples from  $R_q \times \mathbb{T}$ .

**3A. Decomposition of  $m$ -RLWE and the compositum field.** It is well known that the  $n$ -th cyclotomic ring (respectively, field) can be split into a tensor product of prime-power cyclotomic rings (respectively, fields), with these prime powers being those appearing in the factorisation of  $n$ . In the case of rings, if we denote the  $j$ -th cyclotomic polynomial by  $\Phi_j$ , we have that if the prime power factorisation of  $n$  is  $n = p_1^{e_1} \cdots p_m^{e_m}$  then,

$$\frac{\mathbb{Z}[x]}{(\Phi_n(x))} \cong \frac{\mathbb{Z}[x]}{(\Phi_{p_1^{e_1}}(x))} \otimes \cdots \otimes \frac{\mathbb{Z}[x]}{(\Phi_{p_m^{e_m}}(x))}.$$

If  $\varphi$  is the isomorphism from the right-hand side to the left, and we have an instance of the  $m$ -RLWE problem in the right-hand tensor product of rings modulo  $q$  then lifting the coefficients to  $\mathbb{Z}$ , applying  $\varphi$  and reducing modulo  $q$  will give an instance of the RLWE problem since  $\varphi(q) = q$  and  $\varphi$  is a linear map when considering the rings as  $\mathbb{Z}$ -lattices. Furthermore, this map is “smallness”-preserving so the resulting error distribution is still a distribution of small elements, though possibly with some degradation in precisely how small. As a result we obtain the following observation.

**Observation.** The  $m$ -RLWE problem for cyclotomic fields with defining polynomials  $\Phi_{n_i}$  is only distinct from the RLWE problem when the  $n_i$  are not all pairwise coprime.

Going back to the more general case of arbitrary number fields  $K_i$ , the way to view the problem is via the notion of the compositum of fields; in our case this is the smallest number field which contains isomorphic copies of each  $K_i$ . Then there is a natural algebra homomorphism from the tensor product of the  $K_i$  to the compositum; in fact, there can be many such homomorphisms: if we fix one then we can first apply any automorphisms of the  $K_i$  before applying this homomorphism to give the others.

We can then distinguish two cases. The first case is the so-called *linearly disjoint* case: the map is injective (and, as such, automatically bijective in our case) and so the tensor product and the compositum are isomorphic. We remark this is only true in terms of the number fields themselves and not the corresponding rings of integers. However, only when this map is not injective is the  $m$ -RLWE problem distinct from the RLWE problem and this is the crux of the flaw in the reduction from  $m$ -RLWE to RLWE given in [19]. Instead of having to solve a lattice problem in the tensor product of fields whose dimension is the product of the degrees of the defining polynomials, one can work in the compositum field where the lattice problem now has dimension the degree of the compositum as a number field which can be much smaller.

For well-behaved number fields, the natural linear map from the tensor product of the  $K_i$  to the compositum is again somewhat “smallness”-preserving. This means that the corresponding RLWE problems in the compositum field may still have small enough error polynomials to be able to mount an attack against them. We note that the  $m$ -RLWE problem was introduced to improve the efficiency of certain applications of somewhat homomorphic encryption; the number fields which can be used in these advanced cryptographic primitives are well-behaved in this sense.

Since the RLWE problem is widely deemed to be a hard problem in large dimensions, we will only be interested in the case when the fields  $K_i$  are not linearly disjoint. The simplest case of this for cyclotomic fields is when  $m = 2$  and the two fields are prime-power cyclotomic fields for the same prime. In particular we will focus on the prime 2 as this is a very popular choice for efficiency reasons.

## 4. Attacks

**4A. A distinguishing attack.** Our attack is inspired by the “evaluation at one” attack and its variants on nonstandard decisional PLWE problems [10; 11; 5]. These attacks work if the defining polynomial  $f$  of the ring  $R = \mathbb{Z}[x]/(f(x))$  has a small root modulo  $q$ , say  $f(\theta) \equiv 0 \pmod{q}$ . Then evaluation at  $x = \theta$  is well defined and guessing the value of  $s(\theta)$  one can test if  $e(\theta) = b(\theta) - a(\theta)s(\theta)$  is distributed according to the error distribution evaluated at  $\theta$ . This requires  $e(\theta)$  to be distinguishable from uniform, which it is if  $e(\theta)$  remains small enough; hence  $\theta$  should also be small, e.g.,  $\theta = \pm 1$ .

Note that evaluation at  $\theta$  is equivalent to reduction modulo the ideal generated by  $x - \theta$  and on further reduction by  $q$  the ring is nontrivial if and only if  $f(\theta)$  and  $q$  are not coprime. To stand any chance of distinguishing though,  $f(\theta)$  and  $q$  should have a large common factor so that the quotient ring is not too small; this is the case when  $f(\theta) \equiv 0 \pmod{q}$ . More generally, for the attack to succeed we really only need that  $\mathbb{Z}[x]/(f(x), q, x - \theta) = \mathbb{Z}/(f(\theta), q)$  is large enough to distinguish the distribution of  $e(\theta)$  from uniform.

In our setting, the ring  $R$  is equal to  $\mathbb{Z}[x, y]/(f(x), g(y))$  so we look for an ideal  $\mathcal{I}$  of  $R$  such that  $\mathcal{I}$  and  $(q)$  are not coprime. In particular, viewing  $R$  as

$$\frac{\mathbb{Z}[x]}{(f(x))}[y] \bigg/ (g(y))$$

we can try to find a root of  $g(y)$  modulo  $q$  in the ring  $\mathbb{Z}[x]/(f(x))$ . If such a root  $\theta(x)$  exists, we can try to distinguish between  $e(x, \theta(x))$  of the form  $b(x, \theta(x)) - a(x, \theta(x))s(x, \theta(x))$ , hence coming from genuine  $m$ -RLWE samples, and  $e(x, \theta(x))$  coming from uniformly random samples.

**Example 4.1.** As a small example let us take  $f(x) = x^4 + 1$  and  $g(y) = y^2 + 1$ . We look for a solution to  $y^2 + 1 \equiv 0 \pmod{q}$  in the ring  $\mathbb{Z}[x]/(x^4 + 1)$ . It is easy to see that a solution is  $y = x^2$ ; hence we have found a root. Thus the mapping  $a(x, y) \mapsto a(x, x^2)$  is a ring homomorphism from  $\mathbb{Z}[x, y]/(x^4 + 1, y^2 + 1)$  to  $\mathbb{Z}[x]/(x^4 + 1)$ . The error polynomials will be sampled coefficient-wise with respect to the standard power basis  $x^i y^j$  which we use throughout this paper. Thus writing  $e(x, y) = \sum_{i=0}^3 \sum_{j=0}^1 e_{i,j} x^i y^j$  we see that under this homomorphism the error polynomial  $e(x, y)$  is mapped to

$$\sum_{i=0}^3 \sum_{j=0}^1 e_{i,j} x^{i+2j} = (e_{0,0} - e_{2,1}) + (e_{1,0} - e_{3,1})x + (e_{2,0} + e_{0,1})x^2 + (e_{3,0} + e_{1,1})x^3.$$

We thus see that the image of the error polynomial also has small coefficients as they are just a signed sum of two of the original coefficients. In particular, the coefficients of the error term are distinguishable from

random elements modulo  $q$  for large enough  $q$ . This means a distinguishing attack can be successfully mounted against the decisional  $m$ -RLWE problem in this setting.

We can in fact go a step further in the above example as  $y = -x^2$  is another solution to  $y^2 + 1 \equiv 0 \pmod{q}$ . This may not seem to add much but using this second solution we can perform an attack on the search variant of the problem making the attack much more powerful. More generally, having multiple roots may make a direct attack on the search variant feasible. This will be demonstrated in practice in the next section.

**4B. Multiple roots.** Take the example of the 2-RLWE problem of [Problem 1.1](#) with  $f(x) = x^{n_1} + 1$  and  $g(y) = y^{n_2} + 1$  for  $n_1$  and  $n_2$  powers of two so that without loss of generality we can assume that  $n_2 \mid n_1$  and let  $k = n_1/n_2$ . Here we have many roots of  $g(y)$  in  $\mathbb{Z}[x]/(f(x))$  even before reducing modulo  $q$ . Namely we have  $g(x^{(2i+1)k}) = 0$  for  $i \in [n_2]$  and each of the roots is distinct. We can thus define the map

$$\begin{aligned} \Theta : \mathbb{Z}[x, y]/(f(x), g(y)) &\rightarrow (\mathbb{Z}[x]/(f(x)))^{n_2}, \\ a(x, y) &\mapsto (a(x, x^k), a(x, x^{3k}), \dots, a(x, x^{(2n_2-1)k})). \end{aligned}$$

This map is essentially the canonical embedding of  $\mathbb{Z}[y]/(y^{n_2} + 1)$  where, instead of mapping into  $\mathbb{Z}[e^{\pi i/n_2}]^{n_2} \subset \mathbb{C}^{n_2}$ , each component maps into the ring of integers of the compositum of fields which is isomorphic to  $\mathbb{Z}[x]/(x^{n_1} + 1)$  in our case. Thus we see that  $\Theta$  is a ring homomorphism. We denote by  $\Theta_i$  the  $i$ -th component of  $\Theta$  which is again a ring homomorphism.

Just like the canonical embedding, the map  $\Theta$  is injective. Write  $a(x, y) = \sum_{j=0}^{n_2-1} a_j(x) y^j$  and let  $\mathbf{a}$  be the vector of coefficients with respect to the power basis in  $y$ :  $\mathbf{a} = (a_0(x), \dots, a_{n_2-1}(x))$ . Then,

$$\Theta(a(x, y)) = \mathbf{a} \begin{pmatrix} 1 & 1 & \dots & 1 \\ x^k & x^{3k} & \dots & x^{(2n_2-1)k} \\ x^{2k} & x^{6k} & \dots & x^{(2n_2-1)2k} \\ \vdots & \vdots & \ddots & \vdots \\ x^{(n_2-1)k} & x^{3(n_2-1)k} & \dots & x^{(2n_2-1)(n_2-1)k} \end{pmatrix}.$$

This matrix is a Vandermonde matrix and thus has determinant  $\prod_{0 \leq i < j < n_2} (x^{(2j+1)k} - x^{(2i+1)k})$  which is nonzero as the  $x^{(2i+1)k}$  are distinct for  $i \in [n_2]$ . Hence  $\Theta$  is injective and can thus be inverted. Further, for  $n_2 > 2$ , the absolute value of this determinant is a square root of the discriminant of the number field  $\mathbb{Q}(e^{\pi i/n_2})$ . It is well known (see, for example, [\[24, Proposition 2.1\]](#)) that the discriminant is  $n_2^{n_2}$  so the determinant is one of  $\pm n_2^{n_2/2}$ . Hence for odd  $q$  the corresponding map  $\Theta$  modulo  $q$  which we denote by  $\bar{\Theta}$  is also invertible; here we mean the map

$$\begin{aligned} \bar{\Theta} : \mathbb{Z}_q[x, y]/(f(x), g(y)) &\rightarrow (\mathbb{Z}_q[x]/(f(x)))^{n_2}, \\ a(x, y) &\mapsto (a(x, x^k), a(x, x^{3k}), \dots, a(x, x^{(2n_2-1)k})). \end{aligned}$$

The inverse mapping from the image of  $\Theta$  (or  $\bar{\Theta}$  if it exists) is given by multiplying by the inverse of the Vandermonde matrix on the right. If we denote the Vandermonde matrix by  $T = (T_{i,j})_{i,j \in [n_2]}$  then

its inverse is given by  $U = (U_{i,j})_{i,j \in [n_2]}$  where  $U_{i,j} = \frac{1}{n_2} x^{-2jk} T_{j,n_2-i} = \frac{1}{n_2} x^{-j(2i+1)k}$  where the indices are taken modulo  $n_2$ . To see this we compute

$$\begin{aligned} (TU)_{i,j} &= \sum_{m=0}^{n_2-1} T_{i,m} U_{m,j} = \sum_{m=0}^{n_2-1} x^{i(2m+1)k} \frac{1}{n_2} x^{-j(2m+1)k} \\ &= \frac{1}{n_2} \sum_{m=0}^{n_2-1} x^{(i-j)(2m+1)k} = \delta_{i,j}. \end{aligned}$$

We now look at how large the coefficients of the  $t$ -th component of  $\Theta(e(x, y))$ , denoted  $\Theta_t(e(x, y))$ , are if  $e(x, y)$  is sampled from the  $m$ -RLWE error distribution. We suppose that this error distribution has coefficients, with respect to the basis  $x^i y^j$ , sampled independently from a distribution that is subgaussian with parameter  $\sigma$  so writing  $e(x, y) = \sum_{i=0}^{n_2-1} \sum_{j=0}^{n_1-1} e_{i,j} x^j y^i$ , each  $e_{i,j}$  is an independent subgaussian random variable with parameter  $\sigma$ . Then applying  $\Theta_t$  for some  $t \in [n_2]$  gives

$$\Theta_t(e(x, y)) = \sum_{i=0}^{n_2-1} \sum_{j=0}^{n_1-1} e_{i,j} x^{j+i(2t+1)k} = \sum_{l=0}^{n_1-1} \left( \sum_{i=0}^{n_2-1} (-1)^{q_{i,l}} e_{i,r_{i,l}} \right) x^l,$$

where we define  $q_{i,l}$  and  $r_{i,l}$  as the quotient and remainder of  $l - i(2t+1)k$  on division by  $n_1$  (which depends on  $t$ ):  $l - i(2t+1)k = q_{i,l}n_1 + r_{i,l}$  with  $r_{i,l} \in [n_1]$ . This can be seen by rewriting  $j$  as  $j = l - i(2t+1)k \bmod n_1$  for some  $l \in [n_1]$  (for each  $i$  separately) and noting that as  $j$  runs over  $[n_1]$  so does  $l$ , after which one swaps the order of summation.

Thus we see that the coefficients of  $\Theta_t(e(x, y))$  are the sum of  $n_2$  subgaussians with parameter  $\sigma$  and so are themselves subgaussian with parameter  $\sqrt{n_2}\sigma$ .

**4C. Our attack.** Here we present a simple attack on the 2-RLWE problem. It combines both the simple lattice attack and the distinguishing attack. We stress that the attack is much more powerful than the distinguishing attack alone as firstly it solves a search rather than a decisional problem and secondly there is no need for any guessing during the attack. We point out that our attack has a strong similarity to Nussbaumer's algorithm for fast convolution [16].

We start with a number of samples  $\{(a_j(x, y), b_j(x, y))\}_{j \in [\ell]}$  where

$$b_j(x, y) = a_j(x, y)s(x, y) + e_j(x, y).$$

The attack starts by evaluating the map  $\bar{\Theta}$  on each sample; we define  $\alpha_{i,j}(x) := \bar{\Theta}_i(a_j(x, y))$  and  $\beta_{i,j}(x) := \bar{\Theta}_i(b_j(x, y))$ . We note that since  $\bar{\Theta}$  is a ring homomorphism we have, on defining  $\epsilon_{i,j}(x) := \bar{\Theta}_i(e_j(x, y))$  and  $\sigma_i(x) := \bar{\Theta}_i(s(x, y))$ , that

$$\beta_{i,j}(x) = \alpha_{i,j}(x)\sigma_i(x) + \epsilon_{i,j}(x) \quad \text{for } i \in [n_2], j \in [\ell].$$

Our first goal is to find the  $\sigma_i(x)$  and to do this we use the simple lattice attack from Section 2C since for a fixed  $i$  the samples  $(\alpha_{i,j}(x), \beta_{i,j}(x))$  follow an  $\text{RLWE}_{q, \sqrt{n_2}\Psi}$  distribution. This means we need to simply solve  $n_2$  instances of an RLWE problem in dimension  $n_1$  with noise distribution that is  $\sqrt{n_2}$  times



		$n_1$											
		4		8		16		32		64		128	
instances block size		100		100		100		10		1		1	
		30		30		30		30		10		10	
		$\ell$	$p$	$\ell$	$p$	$\ell$	$p$	$\ell$	$p$	$\ell$	$p$	$\ell$	$p$
$n_2$	4	2	13	2	13	2	13	2	13	2	15	2	21
		3	9	3	10	3	10	3	11	3	13	3	20
	8			2	13	2	13	2	14	2	17	2	22
				3	10	3	10	3	11	3	15	3	20
	16					2	14	2	15	2	18	2	23
						3	11	3	12	3	16	3	22
	32							2	15	2	19	2	24
								3	12	3	17	3	22
	64									2	20	2	31
										3	18	3	24

**Table 1.** The number of samples  $\ell \leq 3$  and the minimal  $p \in \mathbb{N}$ ,  $p \approx \log_2(q)$ , for which our attack succeeded in each of the stated number of attempts for the stated block size, given  $n_1$ ,  $n_2$  and  $q = 2^p + 1$ , and where the secret polynomial is sampled uniformly at random in  $R_q$ .

wider than for the  $m$ -RLWE problem; each instance is independent so can be solved in parallel. If this succeeds we have computed the image of  $s(x, y)$  under  $\bar{\Theta}$  and since  $\bar{\Theta}$  is invertible for odd  $q$  we can compute  $s(x, y)$  and solve the 2-RLWE problem.

**4D. Implementation results.** We implemented and tested our attack in SageMath [23], using the NTL library for lattice reduction. We tested our attack on the smallest parameter set given in [18], namely for  $n_1 = n_2 = 128$  and  $q$  being the smallest prime larger than  $2^{42}$ . The secret polynomial is sampled from the error distribution which samples coefficients independently from a discrete Gaussian with  $\sigma = 8/\sqrt{2\pi} \approx 3.19$  (the default in SEAL [6]), larger than the stated  $\sigma = 1$  in [18]. We were able to successfully recover the secret polynomial with just one sample using BKZ reduction with block size 10 to solve the BDD problem instances. This clearly shows that the estimated security level of over 2500 bits is a significant overestimate. We can see from the estimates given by the LWE estimator [1] that the parameter sets with  $n_1 = n_2 = 256$  and  $n_1 = n_2 = 512$  also offer little to no security (33 and 35 bits, respectively) while that for  $n_1 = n_2 = 1024$  offers at most 98 bits.

In Table 1 we report on a run of our attack with  $n_1 \geq n_2$  and  $q$  of the form  $2^p + 1$  for  $p \in \mathbb{N}$ . The secret polynomial  $s$  we try to find is chosen uniformly at random from  $\mathbb{Z}_q[x, y]/(x^{n_1} + 1, y^{n_2} + 1)$  so the minimum number of 2-RLWE samples possible to recover  $s$  is two. We give the minimum  $q$  of the stated form for which the attack succeeded in a fixed number of consecutive instances with the stated number of samples; here we used the embedding approach combined with BKZ reduction to attempt to solve the BDD instances. Further, the coefficients of the error polynomials were sampled independently using a discrete Gaussian sampler with  $\sigma = 3.19$ . The results are heuristic as we only attempted to solve



		$n_1$												
		4		8		16		32		64		128		
instances		100		100		100		10		1		1		
block size		30		30		30		30		10		10		
		$\ell$	$p$	$\ell$	$p$	$\ell$	$p$	$\ell$	$p$	$\ell$	$p$	$\ell$	$p$	
$n_2$	4	1	11	1	12	1	12	1	13	1	14	1	22	
		2	9	2	9	2	10	2	11	2	13	2	20	
	8			1	13	1	13	1	14	1	15	1	22	
				2	10	2	10	2	11	2	14	2	21	
	16					1	14	1	14	1	17	1	22	
						2	11	2	12	2	15	2	21	
	32							1	15	1	18	1	23	
								2	12	2	16	2	22	
	64										1	20	1	25
											2	17	2	23

**Table 2.** The number of samples  $\ell \leq 2$  and the minimal  $p \in \mathbb{N}$ ,  $p \approx \log_2(q)$  for which our attack succeeded in the stated number of instances and with the stated block size, given  $n_1$ ,  $n_2$  and  $q = 2^p + 1$ , and where the secret polynomial is sampled coefficient-wise with each coefficient uniformly random in  $\{-1, 0, 1\}$ .

a limited number of instances for each choice of  $n_1$ ,  $n_2$  and  $q$ . It is certainly possible to find the secret for smaller  $q$  by increasing the block size used, and in specific instances this may not even be necessary.

In Table 2 we performed the same attack but this time with the coefficients of the secret polynomial taken from the uniform distribution on  $\{-1, 0, 1\}$ ; hence a successful attack is possible with only one sample. While the case of the secret being sampled from the error distribution, as in the proposed image processing scheme of [20], can be viewed as having an extra sample  $(1, 0 = 1 \cdot s - s)$  whose error is  $-s$ , it is often the case in practical applications of somewhat homomorphic encryption that the secret is sampled from this narrower distribution to get the most efficiency out of the scheme. It is therefore interesting to see how this choice affects our attack.

**4E. The case of the general  $m$ -RLWE problem.** The previous subsection showed that the 2-RLWE problem can be readily attacked with the combination of an evaluation attack and simple lattice reduction techniques. More generally, if the defining polynomials of the 2-RLWE problem are both  $p$ -th power cyclotomic polynomials of degree  $\phi(p^{r_i})$ , where  $\phi$  is the Euler-totient function, then our attack straightforwardly applies to this case with the caveat that  $\bar{\Theta}$  must be invertible modulo  $q$  which holds if  $q$  is coprime with  $\phi(p^{r_2}) = p^{r_2-1}(p-1)$ . We remark that if  $h = \gcd(q, \phi(p^{r_2}))$  and  $\phi(p^{r_2})$  are small, it is possible to compute all possible preimages of  $\bar{\Theta}$  and test each of them in turn to determine the correct value of the secret, however this rather quickly becomes prohibitively expensive the larger  $h$  and  $r_2$  become as there are  $h^{\phi(p^{r_2})}$  possibilities to check.

Increasing the value of  $m$  when each of the defining polynomials is a  $p$ -th power cyclotomic polynomial of degree  $n_i = \phi(p^{r_i})$  increases the difficulty of the problem since the error grows by a multiplicative

factor of  $\sqrt{\prod_{i=j+1}^m n_i}$  in a lattice of dimension  $\prod_{i=1}^j n_i$  for some  $1 \leq j \leq m$ ; here we can choose the order of the  $n_i$  which best suits the attack. We therefore see that a trade-off can be made in choosing  $j$ : if  $j = 1$  means the error is already too large for the lattice reduction attack to succeed, we can choose a larger  $j$  at the cost of having to perform lattice reduction in a lattice of larger dimension. In this way, taking large  $m$  offers some security but at a loss of efficiency if such a large  $m$  is not needed specifically for the application in mind.

When instantiating  $m$ -RLWE with an arbitrary tensor product of number fields we again wish to find an analogue for the map  $\Theta$ . This will consist of algebra homomorphisms from  $K = \bigotimes_{i \in [m]} K_i$  to the compositum field, which we denote by  $L$ . These algebra homomorphisms can naturally be extended to maps from  $K_{\mathbb{R}}$  to  $L \otimes_{\mathbb{Q}} \mathbb{R}$  which fix  $q$  so we can evaluate them on the components of samples from the  $m$ -RLWE distribution.

In the case that all the number fields  $K_i$  are Galois extensions then there are exactly

$$n := \prod_{i \in [m]} [K_i : \mathbb{Q}] = \prod_{i \in [m]} n_i$$

such algebra homomorphisms from  $K$  to  $L$ . Since all of the  $K_i$  are Galois, so is  $L$ ; if we define  $N := |\text{Aut}(L)| = [L : \mathbb{Q}]$  as the number of automorphisms of  $L$  then up to automorphism in  $L$  there are  $k := n/N$  distinct algebra homomorphisms which we denote by  $\Theta = (\Theta_i)_{i \in [k]}$ .

Again,  $\Theta$  is injective so can be inverted; however for the attack to work we need  $\bar{\Theta}$  to be invertible, that is,  $\Theta$  to be invertible modulo  $q$ . Further, we also require  $\Theta$  to map the error distribution  $\psi$  over  $K_{\mathbb{R}}$  to elements of  $L_{\mathbb{R}}$  which have small coefficients with respect to a known basis for  $L$  as a  $\mathbb{Q}$ -vector space. If these conditions are met then we can carry out the same attack of applying  $\bar{\Theta}$  to the  $m$ -RLWE samples, solving  $k$  instances of the reduced problem in a lattice of dimension  $N$  and applying  $\bar{\Theta}^{-1}$  to recover the secret.

To summarise the requirements for the full attack, we require for the number fields  $K_i$  to be Galois, for the map  $\bar{\Theta}$  to be invertible and for  $\Theta$  to map small elements to small elements. Nevertheless, if either of the first two conditions are not met it may still be possible to recover partial information about the secret using our approach.

## 5. The dangers of optimizing module based cryptosystems

We take the example of Kyber [3] which, when reduced to its simplest form, has a public key which is a module-LWE sample where the secret  $s$  is a small element of the module  $R_q^k$  where  $R = \mathbb{Z}[x]/(x^n + 1)$  with  $n$  a power of two. Such a public key is then a pair  $(A, b)$  with  $A$  a  $k \times k$  matrix whose entries are chosen uniformly at random from  $R_q$  and  $b \in R_q^k$  with  $b = As + e$  for some small error element  $e \in R_q^k$ . This means a public key consists of  $k(k+1)$  elements of  $R_q$ . One might be tempted to use a structured matrix, such as a negacyclic one, instead of a uniformly random one; after all this is essentially how one goes from LWE to its ring based counterpart RLWE and with our current understanding this latter optimization only incurs a negligible deterioration in security.

Let us fix some parameters and observe what happens. The suggested “paranoid” parameters from [3] are to take  $k = 4$  and  $n = 256$  and  $q = 6781$  which gives a (post-quantum) security level of 218 bits, the largest given by the authors. Taking the matrix  $A$  to be negacyclic, that is a matrix of the form

$$\begin{pmatrix} a_0 & -a_{k-1} & -a_{k-2} & \cdots & -a_1 \\ a_1 & a_0 & -a_{k-1} & \cdots & -a_2 \\ a_2 & a_1 & a_0 & \cdots & -a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{k-1} & a_{k-2} & a_{k-3} & \cdots & a_0 \end{pmatrix},$$

means that only 5 elements of  $R_q$  are needed to define the public key instead of 20. Further, as shown below, the scheme can be interpreted as adding a ring structure on top of  $R_q$  in a new variable  $y$  satisfying  $y^4 + 1$  and replacing matrix multiplication by ring multiplication. Hence, we are in the  $m$ -RLWE setting and working in the tensor product of two power-of-two cyclotomic fields of degrees 256 and 4, respectively.

Formally, we can define the negacyclic module-LWE problem as follows. Let  $R = \mathbb{Z}[x]/(x^n + 1)$  with  $n$  a power of two and let  $q \geq 2$  and  $k$  be positive integers. Let  $s$  be an element of  $R_q^k$  and  $\chi$  a distribution of small elements in  $R_q^k$ . A sample from the negacyclic module-LWE distribution with secret  $s$  is of the form  $(A, \mathbf{b} = As + \mathbf{e})$ , where  $A \in R_q^{k \times k}$  is a negacyclic matrix and  $\mathbf{e} \leftarrow \chi$ . The negacyclic module-LWE decision problem is to decide whether a given set of samples of the form  $(A_i, \mathbf{b}_i) \in R_q^{k \times k} \times R_q^k$ , with each  $A_i$  a negacyclic matrix are sampled from the negacyclic module-LWE distribution or with each  $\mathbf{b}_i$  sampled uniformly at random from  $R_q^k$  instead. The negacyclic module-LWE search problem is, given samples from the negacyclic module-LWE distribution with secret  $s$ , to recover  $s$ .

Given a negacyclic matrix  $A \in R_q^{k \times k}$  whose first column is  $(a_0, \dots, a_{k-1})^T$ , we can write  $a(y) = \sum_{i=0}^{k-1} a_i y^i$  so that the equality  $\mathbf{b} = As$  is equivalent to

$$b(y) = a(y)s(y) \bmod y^k + 1,$$

where  $b(y) = \sum_{i=0}^{k-1} b_i y^i$  and  $s(y) = \sum_{i=0}^{k-1} s_i y^i$  with the  $b_i$  and  $s_i$  the coordinates of the vectors  $\mathbf{b}$  and  $\mathbf{s}$ , respectively. We therefore see that the negacyclic module-LWE problem is equivalent to the  $m$ -RLWE problem in the ring  $\mathbb{Z}[x, y]/(x^n + 1, y^k + 1)$ .

Returning to our example of a structured Kyber variant, we can thus apply our attack with  $n_1 = 256$  and  $n_2 = 4$  which shows that we can recover  $s$  by solving four RLWE problems in dimension 256 from one sample where the error distribution has variance twice that of the original error distribution. Using the LWE-estimator [1], we find that this basic version of a structured Kyber offers at most 107 bits of security, essentially halving the bit security when compared to the original version of Kyber without any additional structure. Thus there is a large difference in terms of security between going from LWE to RLWE and going from module-LWE to  $m$ -RLWE if one is not careful.

We note this structured Kyber would also be weak with the “light” parameter set where  $k = 2$ , but for the standard parameters where  $k = 3$  the above attack does not apply as 3 is not a power of two;

that is,  $x^3 + 1$  has no roots in a power-of-two cyclotomic field. This again shows the subtlety of the problem of trying to optimize module-LWE. Care needs to be taken in choosing which method and for which parameters such an optimization can be applied without severely damaging the security of the problem.

## 6. Conclusion

In this paper we reconsidered the  $m$ -RLWE problem and its security. We showed that, with a combination of simple evaluation and lattice attacks, the security of the  $m$ -RLWE problem was dramatically less than had been previously estimated in the literature. We would therefore not recommend using 2-RLWE for values of  $n_1$  or  $n_2$  less than those used in standard RLWE based schemes for cryptographic purposes. More generally, we conclude that the  $m$ -RLWE problem using number fields with a small degree compositum field is insecure. Finally, this paper should also serve as a warning to implementers of module-LWE based cryptosystems to not blindly apply the standard optimization trick that is used to transform LWE into RLWE.

## Acknowledgements

This work was supported in part by the Research Council KU Leuven grants C14/18/067 and STG/17/019, by CyberSecurity Research Flanders with reference number VR20192203 as well as by the Research Foundation Flanders (FWO) through WOG Coding Theory and Cryptography. Bootland was supported by a PhD fellowship of the Research Foundation Flanders (FWO).

## References

- [1] Martin R. Albrecht, Rachel Player, and Sam Scott. On the concrete hardness of Learning with Errors. *Journal of Mathematical Cryptology*, 9(3):169–203, 2015.
- [2] László Babai. On Lovász’ lattice reduction and the nearest lattice point problem. *Combinatorica*, 6(1):1–13, 1986.
- [3] Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM. In *2018 IEEE European Symposium on Security and Privacy*, pages 353–367, 2018.
- [4] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. Fully Homomorphic Encryption without Bootstrapping. Cryptology ePrint Archive, Report 2011/277, 2011. <https://eprint.iacr.org/2011/277>.
- [5] Wouter Castryck, Ilia Iliashenko, and Frederik Vercauteren. Provably Weak Instances of Ring-LWE Revisited. In *EUROCRYPT 2016*, pages 147–167. Springer-Verlag, 2016.
- [6] Hao Chen, Kim Laine, and Rachel Player. Simple Encrypted Arithmetic Library - SEAL v2.1. In Michael Brenner, Kurt Rohloff, Joseph Bonneau, Andrew Miller, Peter Y.A. Ryan, Vanessa Teague, Andrea Bracciali, Massimiliano Sala, Federico Pintore, and Markus Jakobsson, editors, *Financial Cryptography and Data Security*, pages 3–18. Springer International Publishing, 2017.
- [7] Jung Hee Cheon, Andrey Kim, and Donggeon Yhee. Multi-dimensional packing for HEAAN for approximate matrix arithmetics. Cryptology ePrint Archive, Report 2018/1245, 2018. <https://eprint.iacr.org/2018/1245>.
- [8] Jan-Pieter D’Anvers, Angshuman Karmakar, Sujoy Sinha Roy, and Frederik Vercauteren. Saber: Module-LWR Based Key Exchange, CPA-Secure Encryption and CCA-Secure KEM. In Antoine Joux, Abderrahmane Nitaj, and Tajjeeddine Rachidi, editors, *AFRICACRYPT 2018*, pages 282–305. Springer International Publishing, 2018.

- [9] Léo Ducas and Alain Durmus. Ring-LWE in Polynomial Rings. In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, *PKC 2012*, pages 34–51. Springer Berlin Heidelberg, 2012.
- [10] Kirsten Eisenträger, Sean Hallgren, and Kristin Lauter. Weak Instances of PLWE. In Antoine Joux and Amr Youssef, editors, *SAC 2014*, pages 183–194. Springer International Publishing, 2014.
- [11] Yara Elias, Kristin E. Lauter, Ekin Özman, and Katherine E. Stange. Provably Weak Instances of Ring-LWE. In Rosario Gennaro and Matthew Robshaw, editors, *CRYPTO 2015*, pages 63–92. Springer Berlin Heidelberg, 2015.
- [12] Ravi Kannan. Minkowski’s Convex Body Theorem and Integer Programming. *Mathematics of Operations Research*, 12(3):415–440, 1987.
- [13] Richard Lindner and Chris Peikert. Better Key Sizes (and Attacks) for LWE-Based Encryption. In Aggelos Kiayias, editor, *CT-RSA 2011*, pages 319–339. Springer Berlin Heidelberg, 2011.
- [14] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On Ideal Lattices and Learning with Errors over Rings. In Henri Gilbert, editor, *EUROCRYPT 2010*, pages 1–23. Springer Berlin Heidelberg, 2010.
- [15] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. A Toolkit for Ring-LWE Cryptography. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, pages 35–54. Springer Berlin Heidelberg, 2013.
- [16] H. Nussbaumer. Fast polynomial transform algorithms for digital convolution. *IEEE Transactions on Acoustics, Speech, and Signal Processing*, 28(2):205–215, 1980.
- [17] Alberto Pedrouzo-Ulloa, Juan Ramón Troncoso-Pastoriza, Nicolas Gama, Mariya Georgieva, and Fernando Pérez-González. Revisiting Multivariate Ring Learning with Errors and its Applications on Lattice-based Cryptography. Cryptology ePrint Archive, Report 2019/1109, 2019. <https://eprint.iacr.org/2019/1109>.
- [18] Alberto Pedrouzo-Ulloa, Juan Ramón Troncoso-Pastoriza, and Fernando Pérez-González. Multivariate lattices for encrypted image processing. In *IEEE International Conference on Acoustics, Speech and Signal Processing*, pages 1707–1711. IEEE, 2015.
- [19] Alberto Pedrouzo-Ulloa, Juan Ramón Troncoso-Pastoriza, and Fernando Pérez-González. On Ring Learning with Errors over the Tensor Product of Number Fields. <https://arxiv.org/abs/1607.05244>, 2016.
- [20] Alberto Pedrouzo-Ulloa, Juan Ramón Troncoso-Pastoriza, and Fernando Pérez-González. Multivariate Cryptosystems for Secure Processing of Multidimensional Signals. <https://arxiv.org/abs/1712.00848>, 2017.
- [21] Miruna Rosca, Damien Stehlé, and Alexandre Wallet. On the Ring-LWE and Polynomial-LWE Problems. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018*, pages 146–173. Springer International Publishing, 2018.
- [22] Damien Stehlé, Ron Steinfeld, Keisuke Tanaka, and Keita Xagawa. Efficient public key encryption based on ideal lattices. In Mitsuru Matsui, editor, *Advances in Cryptology – ASIACRYPT 2009*, pages 617–635. Springer Berlin Heidelberg, 2009.
- [23] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 7.5.1)*, 2017. <http://www.sagemath.org>.
- [24] Lawrence C. Washington. *Introduction to Cyclotomic Fields*. Graduate Texts in Mathematics. Springer New York, 1997.

Received 28 Feb 2020.

CARL BOOTLAND: [carl.bootland@kuleuven.be](mailto:carl.bootland@kuleuven.be)  
 imec – COSIC, KU Leuven, Heverlee, Belgium

WOUTER CASTRYCK: [wouter.castrycck@kuleuven.be](mailto:wouter.castrycck@kuleuven.be)  
 imec – COSIC, KU Leuven, Leuven, Belgium

and

Department of Mathematics: Algebra and Geometry, Ghent University, Ghent, Belgium

FREDERIK VERCAUTEREN: [frederik.vercauteran@kuleuven.be](mailto:frederik.vercauteran@kuleuven.be)  
 imec – COSIC, KU Leuven, Heverlee, Belgium



# Two-cover descent on plane quartics with rational bitangents

Nils Bruin and Daniel Lewis

We implement two-cover descent for plane quartics over  $\mathbb{Q}$  with all 28 bitangents rational and show that on a significant collection of test cases, it resolves the existence of rational points. We also review a classical description of the relevant moduli space and use it to generate examples. We observe that local obstructions are quite rare for such curves and only seem to occur in practice at primes of good reduction. In particular, having good reduction at 11 implies having no rational points. We also gather numerical data on two-Selmer ranks of Jacobians of these curves, providing evidence these behave differently from those of general abelian varieties due to the frequent presence of an everywhere locally trivial torsor.

## 1. Introduction

A central problem in arithmetic geometry is to determine if a variety  $C$  over a number field  $k$ , for instance a nonsingular projective curve, has any  $k$ -rational points. The most elementary way of showing that  $C(k)$  is empty is by showing that  $C(k_v) = \emptyset$  for some completion  $k_v$  of  $k$ . In that case, we say  $C$  has a *local obstruction* to having rational points.

We consider a more refined *descent obstruction* here. Our construction can be read in elementary terms, but the theoretical motivation is enlightening. Suppose we have an unramified cover  $\pi : D \rightarrow C$  of nonsingular proper varieties over  $k$  with geometric automorphism group  $\Gamma = \text{Aut}_{k^{\text{alg}}}(D/C)$  satisfying  $\#\Gamma = \deg(\pi)$ . The *twisting principle* [Mil80, III.4.3(a)] gives us that the Galois cohomology set  $H^1(k, \Gamma)$  parametrizes *twists*  $\pi_\gamma : D_\gamma \rightarrow C$ , as well as a map  $\gamma : C(k) \rightarrow H^1(k, \Gamma)$  such that for  $P \in C(k)$  and  $\gamma = \gamma(P)$ , we have  $Q \in D_\gamma(k)$  such that  $\pi_\gamma(Q) = P$ . This leads us to consider the associated Selmer set

$$\text{Sel}^{(\pi)}(C/k) = \{\gamma \in H^1(k, \Gamma) : D_\gamma(k_v) \neq \emptyset \text{ for all completions } k_v \text{ of } k\}.$$

Since the map  $\gamma$  takes values in  $\text{Sel}^{(\pi)}(C/k)$ , we see that if the latter is empty then  $C(k)$  is empty too. In that case we say that  $C$  has a  $\pi$ -*cover obstruction* to having rational points:  $C$  has no rational points because a collection of covering varieties all have local obstructions.

---

Bruin acknowledges the support of the Natural Sciences and Engineering Research Council of Canada (NSERC), funding reference number RGPIN-2018-04191.

*MSC2010:* primary 11G30, 14H30; secondary 11D41, 14H50.

*Keywords:* plane quartics, rational points, local-to-global obstructions, bitangents, descent obstructions, two-covers.

The proof of the Chevalley–Weil theorem [CW32] implies that  $\text{Sel}^{(\pi)}(C/k) \subset H^1(k, \Gamma; S)$ , where the latter denotes the classes that are unramified outside the set  $S$  of bad places for the cover  $\pi : D \rightarrow C$ . The set  $H^1(k, \Gamma; S)$  is finite and explicitly computable. This means that to compute  $\text{Sel}^{(\pi)}(C/k)$  one only needs to check the local solvability of finitely many  $D_\gamma$ . Hence,  $\text{Sel}^{(\pi)}(C/k)$  is explicitly computable, although not necessarily efficiently.

For hyperelliptic curves, there is a well-developed theory of *two-covers* in [BS09], where  $\Gamma = \text{Jac}_C[2]$ . Their associated Selmer sets are relatively practical to compute and, as is described there, many genus two curves over  $\mathbb{Q}$  have no local obstruction, but can be shown to have  $\text{Sel}^{(2)}(C/\mathbb{Q}) = \emptyset$ . In fact it has since been shown [BGW17] that in a precise way, *most* hyperelliptic curves have a two-cover obstruction.

Results beyond hyperelliptic curves are sparse. The general descent theory is available in [BPS16], which also provides some genus three examples, but in its full generality, the need to compute class group information of degree 28 extensions limits large-scale experiments significantly. There has also been some progress on creating an appropriate setting for arithmetic statistical techniques [Tho16] to two-descent on Jacobians of curves of genus three, but it is presently not clear how to generalize the Bhargava–Gross–Wang approach to this setting.

In this article we endeavour to start a more systematic study by considering plane quartics  $C$  with a restricted 2-level structure; in particular  $\text{Jac}_C[2](\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^6$ . This forces the 28 bitangents of  $C$  to be defined over  $\mathbb{Q}$  and has the computational and expository advantage that all required data can be expressed over  $\mathbb{Q}$ ; no algebraic number theory is required.

**Remark 1.1.** For a hyperelliptic curve  $C$  of genus  $g$ , having  $\text{Jac}_C[2](k) = (\mathbb{Z}/2\mathbb{Z})^{2g}$  implies that all  $2g + 2$  Weierstrass points on  $C$  are rational, making two-cover descent rather uninteresting. In this sense, two-cover descent on plane quartics has simpler nontrivial applications than on hyperelliptic curves.

In Section 3 we review an explicit description of the moduli space of smooth plane quartics with labelled bitangents as the space of seven labelled points in general position in  $\mathbb{P}^2$ . For small fields we prove:

**Proposition 1.2.** *For  $p = 3, 5, 7$ , there exist no nonsingular plane quartics over  $\mathbb{F}_p$  with all bitangents defined over  $\mathbb{F}_p$ . Over  $\mathbb{F}_9$ , there is only one isomorphism class, represented by the Fermat quartic*

$$C_9 : x^4 + y^4 + z^4 = 0, \text{ with } \#C_9(\mathbb{F}_9) = 28.$$

*Over  $\mathbb{F}_{11}$ , there is only one isomorphism class, represented by*

$$C_{11} : x^4 + y^4 + z^4 + x^2y^2 + x^2z^2 + y^2z^2 = 0, \text{ and } C_{11}(\mathbb{F}_{11}) = \emptyset.$$

In particular, a plane quartic  $C$  over  $\mathbb{Q}$  with rational bitangents has bad reduction at 3, 5, and 7. If it has good reduction at 11, then it has a local obstruction there. The curve  $C_9$  attains the maximum number of rational points for a genus three curve over  $\mathbb{F}_9$ . Its rational points are contacts of the 28 hyperflexes. Both  $C_9$  and  $C_{11}$  are reductions of the Klein quartic  $x^4 + y^4 + z^4 - \frac{3}{2}(1 + \sqrt{-7})(x^2y^2 + x^2z^2 + y^2z^2)$ .



[Section 4](#) describes, given a smooth plane quartic  $C$  with rational bitangents, an explicit model for a two-cover  $\pi_\gamma : D_\gamma \rightarrow C$ , with  $\Gamma = (\mathbb{Z}/2\mathbb{Z})^6$  as a Galois-module. This directly establishes a description of two-covers and their twists, without appealing to étale cohomology.

In [Section 5](#) we describe an algorithm to compute, with reasonable efficiency, sets

$$\mathrm{Sel}^{(2)}(C/k, N) \supset \mathrm{Sel}^{(2)}(C/k),$$

for integers  $N \geq 1$ , with equality holding for  $N \geq 66569$ , and, in practice, for much smaller values of  $N$  already.

In [Section 6](#) we describe a numerical experiment, where we tabulate the behaviour of  $\mathrm{Sel}^{(2)}(C/\mathbb{Q})$  for various quartics  $C$ . We consider a systematic collection of 81070 moduli points with coordinates from  $\{-6, \dots, 6\}$ , as well as a collection of 70000 randomly selected points with coordinates from  $\{-40, \dots, 40\}$ .

**Observation 1.3.** For all curves  $C$  in our collections with  $\mathrm{Sel}^{(2)}(C/\mathbb{Q}) \neq \emptyset$ , we can find a point  $P \in C(\mathbb{Q})$ .

This leaves the following question, which we fully expect to have an affirmative answer, but remains open for now.

**Question 1.4.** Is it possible to construct a smooth plane quartic  $C$  over  $\mathbb{Q}$  with rational bitangents such that  $\mathrm{Sel}^{(2)}(C/\mathbb{Q}) \neq \emptyset$  but  $C(\mathbb{Q}) = \emptyset$ ?

**Remark 1.5.** For a considerable number of curves in our collections we also get information on the 2-Selmer groups of their Jacobians. The data matches the distribution conjectured in [\[PR12, Conjecture 1.1\]](#) quite closely, but only after taking into account that the  $\mathrm{Jac}_C$ -torsor representing  $\mathrm{Pic}^1$  is very frequently everywhere locally trivial. Since nonhyperelliptic curves often have points everywhere locally, this phenomenon should be general: one should expect Jacobians to exhibit special arithmetic behaviour.

This work is based on the master's thesis [\[Lew19\]](#) of the second author.

## 2. Plane quartics and their bitangents

In this section we collect the classical combinatorics and geometry of bitangents and theta characteristics on nonhyperelliptic curves of genus three. See [\[Dol12, Chapter 6\]](#) or [\[GH04\]](#) for a more comprehensive modern treatment.

Let  $k$  be a field of characteristic different from 2 and let  $C$  be a curve of genus three over  $k$ . Then  $\mathrm{Jac}(C)[2]$  is a 0-dimensional separated group scheme of degree 64 and exponent 2, equipped with a nondegenerate alternating bilinear pairing. Indeed, the automorphism group of  $\mathrm{Jac}(C)[2]$  is  $\mathrm{Sp}_6(\mathbb{F}_2)$ .

**Definition 2.1.** A *theta characteristic* on a curve  $C$  of genus  $g$  is a divisor class  $\theta \in \mathrm{Pic}^{g-1}(C)$  such that  $2\theta$  is the canonical class. The *parity* of  $\theta$  is determined by the parity of the dimension of the Riemann–Roch space  $H^0(C, \theta)$ .

It is a classical result [GH04, Proposition 1.11] that a curve of genus  $g$  has  $2^{g-1}(2^g + 1)$  even and  $2^{g-1}(2^g - 1)$  odd theta characteristics. For  $g = 3$  and  $C$  nonhyperelliptic it is easily checked that  $h^0(C, \theta) \leq 1$ , so the odd theta characteristics are exactly the ones that admit a (unique) effective representative.

The canonical model of a nonhyperelliptic genus three curve  $C$  is a quartic in  $\mathbb{P}^2$ :

$$C : f(x, y, z) = 0, \text{ with } f \in k[x, y, z] \text{ homogeneous of degree four.}$$

Since canonical classes are exactly line sections  $C \cdot l$ , we see there are 28 lines  $l$  such that  $C \cdot l = 2\theta$ , where  $\theta$  is a degree two effective divisor representing a theta characteristic: we recover the 28 bitangents of a smooth plane quartic. Fix for each bitangent line  $l$ , a linear form  $\ell$  describing the line.

**Lemma 2.2.** *Let  $C$  be a smooth plane quartic. Then no seven distinct bitangents pass through a single point.*

*Proof.* Suppose  $l_1, \dots, l_7$  intersect in  $P_0$ . If  $P_0$  were to lie on  $C$  it would be singular, so it does not. Hence projecting away from  $P_0$  gives a degree four map  $C \rightarrow \mathbb{P}^1$ . Since  $l_i \cdot C$  is a fibre of this projection, the ramification divisor has degree at least  $2 \cdot 7$ . But that exceeds the degree 12 given by the Riemann–Hurwitz formula.  $\square$

Let  $\theta_1, \theta_2$  be two odd theta-characteristics. Then  $2(\theta_1 - \theta_2) = \text{div}(\ell_1/\ell_2)$ , where we regard the quotient of linear forms as a rational function on  $C$ . We see that

$$[\theta_2 - \theta_1] \in \text{Pic}^0(C)[2].$$

As it turns out, all nonzero 2-torsion classes admit such a representative; in fact,  $\binom{28}{2}/63 = 6$  of them. We see that  $\theta_1 - \theta_2$  and  $\theta_3 - \theta_4$  are linearly equivalent precisely when  $\theta_1 + \dots + \theta_4$  is twice canonical. For bitangent forms, this leads to the following concept.

**Definition 2.3.** We say a quadruple of bitangent forms  $\mathbf{q} = \{\ell_1, \dots, \ell_4\}$  is a *syzygetic quadruple* if their contact points with  $C$  lie on a conic. This means there are constants  $\delta_{\mathbf{q}}, c_{\mathbf{q}} \in k^*$  and a quadratic form  $Q_{\mathbf{q}} \in k[x, y, z]$  such that

$$\ell_1 \ell_2 \ell_3 \ell_4 = \delta_{\mathbf{q}} Q_{\mathbf{q}}^2 + c_{\mathbf{q}} f. \quad (2-1)$$

There are 315 syzygetic quadruples. We say a triple of bitangents is *syzygetic* if it is part of a syzygetic quadruple. If it is, then it is part of only one.

**Definition 2.4.** We say that a set of seven bitangent forms  $\{\ell_1, \dots, \ell_7\}$  is an *Aronhold set* if none of its triples are syzygetic.

There are 288 Aronhold sets. For an Aronhold set, write  $\{\theta_1, \dots, \theta_7\}$  for the corresponding theta characteristics. Then  $\theta_1 + \dots + \theta_7 - 3\kappa_C$  is again a theta characteristic: an even one. We see that each even theta characteristic has  $288/36 = 8$  Aronhold sets associated with it. Additionally, one can check that  $\{\theta_1 - \theta_7, \dots, \theta_6 - \theta_7\}$  forms a basis for  $\text{Pic}(C)[2]$ .

It follows that specifying a labelled Aronhold set on a smooth plane quartic amounts to marking a 2-level structure on its Jacobian. The converse holds too.

**Proposition 2.5** [GH04]. *The following two moduli spaces are naturally isomorphic:*

- *Nonhyperelliptic genus three curves with a labelled Aronhold set*
- *Nonhyperelliptic genus three curves with full 2-level structure.*

There is a unique conjugacy class  $\text{Sym}(8) \subset \text{Sp}_6(\mathbb{F}_2)$ . It is of length 36 and it corresponds to the stabilizer of an even theta characteristic. The action can be made explicit by labelling the bitangents by

$$\{\ell_{ij} = \ell_{\{i,j\}} : i \in \{0, \dots, 7\}, j \in \{i+1, \dots, 7\}\}, \quad (2-2)$$

with  $\text{Sym}(8)$  acting in the obvious way on the subscripts. This labelling can be chosen in such a way that the syzygetic quadruples come in two  $\text{Sym}(8)$ -orbits: one of length 210 and one of length 105, represented by, respectively,

$$\{\ell_{01}, \ell_{12}, \ell_{23}, \ell_{03}\} \quad \text{and} \quad \{\ell_{01}, \ell_{23}, \ell_{45}, \ell_{67}\}. \quad (2-3)$$

We see that for  $i = 0, \dots, 7$ , we have the Aronhold sets  $\{\ell_{ij} : j \neq i\}$ . We sometimes suppress  $i = 0$  in our indices, so  $\ell_{0j} = \ell_j$ .

**Proposition 2.6.** *Let  $\ell_1, \dots, \ell_7$  be an Aronhold set of bitangent forms on a smooth plane quartic  $C : f(x, y, z) = 0$ . Then the square class of each of the other bitangents  $\ell_{ij}$  is determined in the sense that there is a constant  $\delta_{ij} \in k^\times$  and a cubic form  $g_{ij} \in k[x, y, z]$  such that*

$$\left( \prod_{n \notin \{i,j\}} \ell_n \right) \ell_{ij} \equiv \delta_{ij} g_{ij}^2 \pmod{fk[x, y, z]}.$$

*Proof.* To ease notation, set  $\{i, j\} = \{6, 7\}$ . By combining the syzygetic quadruples

$$\{\ell_1, \ell_{23}, \ell_{45}, \ell_{67}\}, \{\ell_2, \ell_7, \ell_{23}, \ell_{37}\}, \{\ell_4, \ell_7, \ell_{45}, \ell_{57}\}, \{\ell_3, \ell_5, \ell_{37}, \ell_{57}\},$$

we get that the left-hand side has a divisor with even multiplicities. The existence of  $g_{ij}$  follows from the projective normality of  $C$ .  $\square$

### 3. Generating plane quartics with rational bitangents

We use del Pezzo surfaces of degree two (see [Dol12, 6.3.3] or [GH04]) to describe a classical link between nonhyperelliptic genus three curves with 2-level structure and point configurations in the plane.

**Definition 3.1.** We say seven points  $p_1, \dots, p_7 \in \mathbb{P}^2$  lie in *general position* if no three are collinear and no six lie on a conic.

Given seven points  $p_1, \dots, p_7 \in \mathbb{P}^2$  in general position, we obtain a del Pezzo surface  $X$  of degree two by blowing up the seven points. In fact we obtain a labelling of the 56 exceptional curves on  $X$ :

- 7 exceptional components  $E'_i$  above the blown-up points  $p_i$ .

- 7 proper transforms  $E_i$  of cubics  $\tilde{E}_i$  through the seven points with a nodal singularity at  $p_i$ .
- 21 proper transforms  $E_{ij}$  of lines  $\tilde{E}_{ij}$  connecting  $p_i$  and  $p_j$ .
- 21 proper transforms  $E'_{ij}$  of conics  $\tilde{E}'_{ij}$  through  $\{p_1, \dots, p_7\} \setminus \{p_i, p_j\}$ .

A del Pezzo surface  $X$  of degree 2 comes equipped with a  $2:1$  map  $X \rightarrow \mathbb{P}^2$ , given by the anticanonical system  $|\kappa_X|$  on  $X$ . The branch locus  $C$  in  $\mathbb{P}^2$  is a smooth plane quartic.

If  $X$  is obtained as the blow-up of  $p_1, \dots, p_7 \in \mathbb{P}^2$  then there is an induced rational map  $\phi$  making the following diagram commute:

$$\begin{array}{ccc} & X & \\ \text{bl} \swarrow & & \searrow 2:1 \\ \mathbb{P}^2 & \xrightarrow{\phi} & \mathbb{P}^2 \end{array}$$

Let  $\phi_1, \phi_2, \phi_3$  generate the space of cubics passing through  $p_1, \dots, p_7$ . It is straightforward to check that the  $\text{bl}^* \phi_i$  generate  $|\kappa_X|$ , so  $\phi = (\phi_1 : \phi_2 : \phi_3)$ . The branch locus of  $\phi$  is contained in the plane sextic curve

$$C' : \det \left( \frac{\partial \phi_i}{\partial x_j} \right)_{ij} = 0 \quad (3-1)$$

and indeed,  $C = \phi(C')$  turns out to be a plane quartic.

Since  $\tilde{E}_i$  and  $\tilde{E}_{ij} \cup \tilde{E}'_{ij}$  are loci described by cubics in the span of  $\phi_1, \phi_2, \phi_3$ , they map to lines, whose defining forms we denote by  $\ell_i$  and  $\ell_{ij}$  respectively.

**Lemma 3.2.** *The labelling described above is compatible with (2-2), so  $\{\ell_1, \dots, \ell_7\}$  is an Aronhold set and Definition 2.3 describes the syzygetic quadruples.*

*Proof.* The deeper reason is that the configuration of seven points in  $\mathbb{P}^2$  has the same moduli as seven points in  $\mathbb{P}^3$  by *association* of point sets [Cob22]. The sextic model  $C'$  actually arises as the projection from a linear system  $|\theta_{\text{even}} + \kappa_C|$  (see [GH04]), so the labelling is indeed directly linked to the choice of an even theta characteristic on  $C$ . However, it is also sufficient to just verify the statement for a particular case and then argue via connectedness of the moduli space.  $\square$

The construction above provides a very explicit description of the moduli space of nonhyperelliptic genus three curves with full 2-level structure. For explicitly parametrizing it, we lose no generality by setting  $p_1, p_2, p_3, p_4$  to be the standard simplex and choosing  $p_5, p_6, p_7 = (u_1 : v_1 : 1), (u_2 : v_2 : 1), (u_3 : v_3 : 1)$ . General position means the  $3 \times 3$ , respectively  $6 \times 6$  minors of

$$\begin{pmatrix} 1 & 0 & 0 & 1 & u_1 & u_2 & u_3 \\ 0 & 1 & 0 & 1 & v_1 & v_2 & v_3 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 & 1 & u_1^2 & u_2^2 & u_3^2 \\ 0 & 1 & 0 & 1 & v_1^2 & v_2^2 & v_3^2 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & u_1 v_1 & u_2 v_2 & u_3 v_3 \\ 0 & 0 & 0 & 1 & u_1 & u_2 & u_3 \\ 0 & 0 & 0 & 1 & v_1 & v_2 & v_3 \end{pmatrix},$$

do not vanish.

*Proof of Proposition 1.2.* With the description given above, it is a finite amount of work to check all the possibilities for  $p = 3, 5, 7, 11$ . For  $p = 3, 5, 7$  there are no 7 points over  $\mathbb{F}_p$  in general position (see also [BFL19, Proposition 4.4]). For  $\mathbb{F}_9$  there are 40 triples  $\{(u_1 : v_1 : 1), (u_2 : v_2 : 1), (u_3 : v_3 : 1)\}$  that complement the standard simplex to 7 points in general position. The construction (3-1) requires lifting to characteristic 0, but the rest of the construction remains valid. We find all resulting curves are isomorphic to  $C_9$ . For  $\mathbb{F}_{11}$  there are 1440 triples, all giving curves isomorphic to  $C_{11}$ .  $\square$

#### 4. Two-covers of smooth plane quartics with rational bitangents

Let  $C : f(x, y, z) = 0$  be a smooth plane quartic with an Aronhold set  $\ell_1, \dots, \ell_7$ . We adopt the notation of Proposition 2.6. For  $\gamma = (\gamma_1, \dots, \gamma_7) \in (k^\times)^7$  we define the following curve in weighted projective space  $\mathbb{P}[2^3, 1^{28}]$  with coordinates  $x, y, z$  of weight 2 and  $w_1, \dots, w_7, w_{12}, \dots, w_{67}$  of weight 1:

$$D'_\gamma : \begin{cases} f(x, y, z) = 0, \\ \ell_i(x, y, z) = \gamma_i w_i^2 & \text{for } i = 1, \dots, 7, \\ \ell_{ij}(x, y, z) = \delta_{ij} / (\prod_{n \neq i, j} \gamma_n) w_{ij}^2 & \text{for } 1 \leq i < j \leq 7, \\ g_{ij}(x, y, z) = w_{ij} \prod_{n \neq i, j} w_n & \text{for } 0 \leq i < j \leq 7. \end{cases}$$

Thanks to the relations from Proposition 2.6 we have a well-defined projection  $D'_\gamma \rightarrow C$ . In fact, from the sign changes on  $w_1, \dots, w_7$  we see that  $\text{Aut}(D'_\gamma/C) = (\mathbb{Z}/2\mathbb{Z})^7$ . Furthermore, from the fact that the representation of the automorphism group on  $w_{12}, w_{23}, \dots, w_{67}, w_{17}$  is faithful and for any fibre of  $D'_\gamma \rightarrow C$  at most one of  $w_i$  or  $w_{ij}$  is zero, it follows the cover is unramified and that  $D'_\gamma$  is not geometrically connected. Indeed the involution on  $D'_\gamma$  that swaps the signs of all of  $w_1, \dots, w_7$  interchanges geometric components. We consider the projection  $\mathbb{P}[2^3, 1^{28}] \rightarrow \mathbb{P}^{27}$  away from the weight 2 part and consider the image  $D_\gamma$  of  $D'_\gamma$ .

Lemma 2.2 yields three linearly independent linear forms  $\ell_i, \ell_j, \ell_n$ , so that we can express  $x, y, z$  as linear forms in  $w_i^2, w_j^2, w_k^2$ . Eliminating  $x, y, z$  from the equations gives us  $D_\gamma$  as an intersection of an octic equation, 25 quadratic equations, and 28 sextic equations. Alternatively we derive quartic relations from the syzygetic quadruples and their described relations (see Definition 2.3).

We introduce notation for a group naturally isomorphic to  $(k^\times/k^{\times 2})^6$ , but presented in a way more natural for our purposes.

**Definition 4.1.** We define  $L'(2, k) \simeq (k^\times/k^{\times 2})^6$  by the exact sequence

$$1 \rightarrow (k^\times/k^{\times 2}) \xrightarrow{\text{diagonal}} (k^\times/k^{\times 2})^7 \rightarrow L'(2, k) \rightarrow 1$$

and we usually represent elements in  $L'(2, k)$  by  $(\gamma_1, \dots, \gamma_7) \in (k^\times)^7$ .

**Proposition 4.2.** *The two-covers of  $C$  are exactly*

$$\{\pi_\gamma : D_\gamma \rightarrow C, \text{ where } \gamma \in L'(2, k)\}.$$

*Proof.* The projection of  $D_\gamma$  onto the coordinates  $(w_1 : \dots : w_7)$  gives a birational map to an intersection  $\tilde{D}_\gamma$  of four quadrics and an octic hypersurface. Its singular locus is the pull-back along  $\pi_\gamma$  of the contact locus of the bitangents  $\ell_1, \dots, \ell_7$ . We see that  $\tilde{\pi} : \tilde{D}_\gamma \rightarrow C$  is a finite rational cover of degree  $2^6$  and that  $\tilde{\pi}^*(\ell_i/\ell_7) = (\gamma_i/\gamma_7)(w_i/w_7)^2$ . This shows that a basis for  $\text{Pic}^0(C)[2]$  pulls back to principal divisors, and hence that  $\tilde{D}_\gamma$  is a birational model of a two-cover, and therefore so is  $D_\gamma$ . To see that  $D_\gamma$  is nonsingular, we use that for  $P \in D_\gamma(k^{\text{alg}})$  we can find an Aronhold set of bitangents that do not meet  $\pi_\gamma(P)$ .

In order to show that all 2-covers arise as  $D_\gamma$ , we observe that  $\text{Pic}(C/k)[2] = (\mu_2)^6$ , where we write  $\mu_2$  for the Galois module  $\{-1, 1\}$ . By the Kummer sequence we have

$$H^1(k, \text{Pic}(C/k)[2]) = (k^\times/k^{\times 2})^6 \simeq L'(2, k).$$

For  $\sigma \in \text{Gal}(k^{\text{sep}}/k)$  we define the cocycle

$$\xi_\gamma(\sigma) : (w_1 : \dots : w_7) \mapsto \left( \frac{\sqrt{\gamma_1}^\sigma}{\sqrt{\gamma_1}} w_1 : \dots : \frac{\sqrt{\gamma_7}^\sigma}{\sqrt{\gamma_7}} w_7 \right).$$

This gives an isomorphism  $L'(2, k) \simeq H^1(k, \text{Aut}(D_1/C)) \simeq H^1(k, \text{Pic}^0(C)[2])$ , and  $D_\gamma$  is the twist of  $D_1$  by the Galois cocycle  $\xi_\gamma$ .  $\square$

We define a partial map

$$\gamma : C(k) \dashrightarrow L'(2, k); \quad P \mapsto (\ell_1(P), \dots, \ell_7(P))$$

and extend it to a full map by observing that by [Definition 2.3](#), for any syzygetic quadruple  $\mathfrak{q} = \{\ell_i, \ell_a, \ell_b, \ell_c\}$  we have that

$$\ell_i(P) \equiv \delta_{\mathfrak{q}} \ell_a(P) \ell_b(P) \ell_c(P) \pmod{\text{squares}}$$

whenever both sides are nonzero, so if  $\ell_i(P) = 0$ , we assign the appropriate value by taking the right-hand side for a suitable quadruple  $\mathfrak{q}$ . We obtain:

**Proposition 4.3.** *The map  $\gamma : C(k) \rightarrow L'(2, k)$  assigns to  $P \in C(k)$  the cover  $D_{\gamma(P)}$  for which there is a point  $Q \in D_{\gamma(P)}(k)$  such that  $\pi_{\gamma(P)}(Q) = P$ .*

## 5. Selmer sets

We restrict to the case where  $k$  is a number field, but our method applies to any global field of characteristic different from 2. We write  $\mathcal{O}$  for its ring of integers,  $\Omega$  for the set of places of  $k$ , and  $k_v$  for the completion of  $k$  at  $v \in \Omega$ . For nonarchimedean  $v$  we write  $\mathcal{O}_v \subset k_v$  for its ring of integers,  $\mathfrak{p}_v$  for its maximal ideal, and  $\mathcal{O}_v/\mathfrak{p}_v$  for its residue field.

The map  $\gamma$  from [Proposition 4.3](#) and its local variant  $\gamma_v$  fit in the commutative diagram

$$\begin{array}{ccc} C(k) & \xrightarrow{\gamma} & L'(2, k) \\ \downarrow & & \downarrow \rho_v \\ C(k_v) & \xrightarrow{\gamma_v} & L'(2, k_v). \end{array}$$

We define

$$\mathrm{Sel}^{(2)}(C/k) = \{\gamma \in L'(2, k) : \rho_v(\gamma) \in \gamma_v(C(k_v)) \text{ for all } v \in \Omega_k\}.$$

Clearly we have  $\gamma(C(k)) \subset \mathrm{Sel}^{(2)}(C/k)$  and in particular, if  $\mathrm{Sel}^{(2)}(C/k) = \emptyset$  then  $C(k) = \emptyset$ .

Let us now fix an integral model  $C : f(x, y, z) = 0$  with  $f \in \mathcal{O}[x, y, z]$ , as well as 28 bitangent forms  $\ell_{ij} \in \mathcal{O}[x, y, z]$ . The *discriminant*  $D_{27}(f)$  of a quartic (see [GKZ08, Chapter 13, Proposition 1.7]) is an integer form of degree 27 in the coefficients of  $f$  that vanishes precisely when  $f$  describes a singular curve. Thus, if we take

$$S = \{v \in \Omega_k : \mathrm{ord}_v(2D_{27}(f)) > 0, \text{ or } \ell_{ij} \in \mathfrak{p}_v[x, y, z], \text{ or } v \text{ is archimedean}\}$$

then  $C$  has good reduction at all  $v$  not in  $S$ , meaning that the coefficient-wise reductions of  $f$  and  $\ell_{ij}$  describe a nonsingular plane quartic and its bitangents over  $\mathcal{O}_v/\mathfrak{p}_v$ . We consider the *unramified part*

$$L'(2, k_v)^{\mathrm{unr}} = \{\gamma \in L'(2, k_v) : \mathrm{ord}_v(\gamma_i) \equiv \mathrm{ord}_v(\gamma_j) \pmod{2} \text{ for all } i, j\}.$$

**Proposition 5.1.** *If  $C/k_v$  has good reduction as a plane quartic and the residue characteristic of  $k_v$  is odd, then  $\gamma_v(C(k_v)) \subset L'(2, k_v)^{\mathrm{unr}}$ . If furthermore  $\#\mathcal{O}_v/\mathfrak{p}_v \geq 66562$  then  $\gamma_v(C(k_v)) = L'(2, k_v)^{\mathrm{unr}}$ .*

*Proof.* Let  $\bar{C}$  be the reduction of  $C$ . Any point  $P \in C(k_v)$  reduces to a point  $\bar{P} \in \bar{C}(\mathcal{O}_v/\mathfrak{p}_v)$ . Since the bitangents do not share contact points,  $\mathrm{ord}_v(\ell_i(P)) > 0$  for at most one  $i$ . Let  $\mathfrak{q} = \{\ell_i, \ell_a, \ell_b, \ell_c\}$  be a syzygetic quadruple. The good reduction properties imply  $\mathrm{ord}_v(\delta_{\mathfrak{q}}) = 0$ , in the notation of Definition 2.3. We see  $\ell_i(P)\ell_a(P)\ell_b(P)\ell_c(P)$  must have even valuation, but that implies  $\mathrm{ord}_v(\ell_i(P))$  is even.

For the second part, we observe that for  $\gamma \in L'(2, k_v)^{\mathrm{unr}}$ , the curve  $D_\gamma$  has good reduction as well. This curve has genus 129 and, writing  $q = \#\mathcal{O}_v/\mathfrak{p}_v$ , the Hasse–Weil bounds give

$$\#\bar{D}_\gamma(\mathcal{O}_v/\mathfrak{p}_v) \geq q + 1 - 2 \cdot 129\sqrt{q},$$

so if  $q \geq 66562$ , then there is a (necessarily smooth) point on  $\bar{D}_\gamma$ , so Hensel lifting gives a point in  $D_\gamma(k_v)$ . The image of that point on  $C$  maps to  $\gamma$ .  $\square$

We define

$$L'(2, k; S) = \{\gamma \in L'(2, k) : \rho_v(\gamma) \in L'(2, k_v)^{\mathrm{unr}} \text{ for all } v \in \Omega_k \setminus S\}.$$

Let  $\mathcal{O}_S$  be the ring obtained by inverting the primes of the finite places in  $S$ . If  $\mathcal{O}_S$  has odd ideal class number then  $L'(2, k; S)$  is generated by  $(\mathcal{O}_S^\times/\mathcal{O}_S^{\times 2})^7$ , so it is a finite group. Note that by enlarging  $S$ , we can ensure that  $\mathcal{O}_S$  has odd class number.

It follows from Proposition 5.1 that  $\mathrm{Sel}^{(2)}(C/k) \subset L'(2, k; S)$ . Furthermore, if we set

$$T = S \cup \{v \in \Omega_k : \#\mathcal{O}_v/\mathfrak{p}_v < 66562\},$$

then we obtain

$$\mathrm{Sel}^{(2)}(C/k) = \{\gamma \in L'(2, k; S) : \rho_v(\gamma) \in \gamma_v(C(k_v)) \text{ for } v \in T\}. \quad (5-1)$$

Hence, if we can compute generators for  $\mathcal{O}_S^\times$ , which is a standard task in algebraic number theory, and compute  $\gamma_v(C(k_v))$  for finite and real  $v$ , then we can compute the Selmer set.

**5.1. Computing the local image for archimedean places.** For  $k_v = \mathbb{C}$  we have that  $\mathbb{C}^\times = \mathbb{C}^{\times 2}$  and  $C(\mathbb{C}) \neq \emptyset$ , so there is nothing to compute; the local image is the whole (trivial) group  $L'(2, \mathbb{C})$ .

For  $k = \mathbb{R}$  we have that  $\mathbb{R}^\times / \mathbb{R}^{\times 2}$  is represented by  $\{\pm 1\}$ . Furthermore, a smooth plane quartic  $C/\mathbb{R}$  with all bitangents defined over  $\mathbb{R}$  has four components [GH81, Proposition 5.1], and the map  $\gamma : C(\mathbb{R}) \rightarrow L'(2, \mathbb{R}) \simeq \mathbb{F}_2^6$  is continuous and therefore constant on components. In order to find  $\gamma(C(\mathbb{R}))$  we only need to find points on each component and evaluate  $\gamma$  there. Each pair of components has four bitangents touching each, so these contact points must be real. The remaining four bitangents might have complex conjugate contact points. Each pair of components is separated by a bitangent, so  $\gamma$  actually takes different values on the components; we know that  $\#\gamma(C(\mathbb{R})) = 4$ .

Since we need to compute the bitangents anyway, we can use the real contact points to evaluate  $\gamma$ . Once we have found four different images, we know we have determined the entire image.

**5.2. Computing the local image for finite places.** In this section, we take  $k$  to be a local field with ring of integers  $\mathcal{O}$ , uniformizer  $\pi$  with  $\mathfrak{p} = \pi\mathcal{O}$ , and a set  $D$  of representatives of  $\mathcal{O}/\mathfrak{p}$ .

We have  $k^\times \simeq \mathbb{Z} \oplus \mathcal{O}^\times$ . The map  $\mu : k^\times \rightarrow k^\times / k^{\times 2} \simeq (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathcal{O}^\times / \mathcal{O}^{\times 2})$  is constant on sets of the form  $x_0 + \mathfrak{p}^{\text{ord}(4)+1}$ , with  $x_0 \in \mathcal{O}^\times$ , as can easily be checked from the fact that Newton iteration for finding the roots of  $y^2 - x_0$  amounts to iterating the map  $y \mapsto \frac{1}{2}(y + \frac{x_0}{y})$ , which converges for  $y \in 1 + 2\mathfrak{p}$  if  $\text{ord}((x_0 - 1)/4) > 1$ .

We assume we have  $f, \ell_{ij} \in \mathcal{O}[x, y, z]$  representing a quartic curve  $C : f(x, y, z) = 0$  and its bitangents. Furthermore, we assume we have the  $\delta_q$  from Definition 2.3 for all syzygetic quadruples  $q$ , or at least the 210 that involve  $\ell_1, \dots, \ell_7$ .

Note any  $P \in C(k)$  admits a representative of one of the forms  $(x_0 : y_0 : 1)$ ,  $(x_0 : 1 : \pi y_0)$ ,  $(1 : \pi x_0 : \pi y_0)$ , with  $x_0, y_0 \in \mathcal{O}$ , so it is sufficient to restrict ourselves to  $\mathcal{O}$ -valued points on affine plane quartics.

We say a set of the form  $\mathcal{B} = (x_0 + \mathfrak{p}^e) \times (y_0 + \mathfrak{p}^e)$  is a *Hensel-liftable ball* for  $f(x, y) = 0$  if  $0 \in f(\mathcal{B})$  and  $(0, 0) \notin \nabla_{xy} f(\mathcal{B})$ , with  $\nabla_{xy}$  denoting the gradient. In that case, applying Newton iteration to any point in  $\mathcal{B}$  converges to an  $\mathcal{O}$ -valued point of  $f(x, y) = 0$ . It is a standard result that the  $\mathcal{O}$ -valued points on a nonsingular curve can be covered with finitely many Hensel-liftable balls (see Algorithm 2 in the Appendix).

In addition, we require that  $\gamma$  is constant on  $\mathcal{B} \cap C(k)$ . For this we use that the component  $\gamma_i(P)$  can be computed via either  $\mu(\ell_i(P))$  or, for a syzygetic quadruple  $q = \{\ell_i, \ell_a, \ell_b, \ell_c\}$ , by  $\mu(\delta_q \ell_a(P) \ell_b(P) \ell_c(P))$ . Since bitangents do not share contact points, we see that for sufficiently small balls, at least one of the descriptions will be constant. We can then evaluate the map at a single representative. We start with a covering of Hensel-liftable balls and refine it as required. With Algorithm 3 (see the Appendix) we find

$$\gamma(C(k)) = \text{LOCALIMAGE}(f(x, y, 1)) \cup \text{LOCALIMAGE}(f(x, 1, \pi y)) \cup \text{LOCALIMAGE}(f(1, \pi x, \pi y)).$$

**Remark 5.2.** The additional condition that  $\gamma$  be constant on our Hensel-liftable balls  $\mathcal{B}$  is surprisingly easily satisfied. In experiments with  $\mathcal{O} = \mathbb{Z}_p$ , including for  $p = 2$ , we find that refinement is only rarely required.



This happens because there are many syzygetic quadruples: each  $\ell_i$  is involved in 45. Hence, if  $P$  lies close to a zero of  $\ell_i$ , then there is likely a quadruple  $q$  such that  $P$  lies far away from the contact points of the other three bitangents.

This is in stark contrast with the hyperelliptic case, where the role of the bitangent contact points is played by the Weierstrass points. They are fewer in number, but there are also fewer relations between them, necessitating higher lifting.

**5.3. Overcoming combinatorial explosion.** If  $k$  is a number field, then we can compute  $L'(2, k; S)$  and the algorithms from Sections 5.1 and 5.2 allow us to compute the local images, so using (5-1) we can compute  $\text{Sel}^{(2)}(C/k)$ . However, as an  $\mathbb{F}_2$ -vector space, we have  $\dim_2 L'(2, k; S) = 6(\#S)$ , and  $S$  tends to have considerable size. For instance, if  $k = \mathbb{Q}$  and  $C$  has points everywhere locally, then Proposition 1.2 yields that  $\{2, 3, 5, 7, 11, \infty\} \subset S$ , so  $\#L'(\mathbb{Q}, 2; S) \geq 2^{36}$ . Consequently, the pointwise iteration over  $L'(k, 2; S)$  that (5-1) suggests, is usually practically infeasible. We use some linear algebra first.

We extend  $\gamma$  linearly to divisors, while also keeping track of the parity of the degree,

$$\tilde{\gamma} : \text{Div}(C) \rightarrow \mathbb{F}_2 \times L'(2, k); \quad \tilde{\gamma}\left(\sum n_P P\right) = \left(\sum n_P, \prod \gamma(P)^{n_P}\right)$$

(see [BPS16, §6]). One finds that principal divisors lie in the kernel, so  $\tilde{\gamma}$  descends to a map on  $\text{Pic}(C/k)$ . We write  $W_v = \langle \tilde{\gamma}(C(k_v)) \rangle$  for the  $\mathbb{F}_2$ -span. We write  $W_v^0$  for the kernel of the projection  $W_v \rightarrow \mathbb{F}_2$  on the first coordinate, and  $W_v^1$  for its complement.

Given explicit representations for  $L'(2, k; S)$  and  $L'(2, k_v)$  as  $\mathbb{F}_2$ -vector spaces, it is easy to find a description of  $\tilde{\rho}_v : \mathbb{F}_2 \times L'(2, k; S) \rightarrow \mathbb{F}_2 \times L'(2, k_v)$  as a linear transformation. We immediately obtain

$$\text{Sel}^{(2)}(C/k) \subset W_C^1 := \bigcap_{v \in S} \tilde{\rho}_v^{-1}(W_v^1), \quad (5-2)$$

where the intersection on the right-hand side is easily computed as an affine subset using standard linear algebra tools, even if  $\#S \sim 100$ .

On  $\text{Pic}^0(C/k_v)$ , the kernel of  $\tilde{\gamma}_v$  is exactly  $2\text{Pic}^0(C/k_v)$ . Furthermore, with the presence of a point  $P_0 \in C(k_v)$  we have that  $\text{Pic}^0(C/k_v) = \text{Jac}_C(k_v)$ , and since the latter is a compact  $k_v$ -Lie group we have

$$\#(\text{Jac}_C(k_v)/2\text{Jac}_C(k_v)) = (\#\text{Jac}_C[2](k_v))/|2|_v^3, \quad (5-3)$$

where we normalize

$$|2|_v = \begin{cases} 2 & \text{if } v \text{ is a real place,} \\ 4 & \text{if } v \text{ is a complex place,} \\ (\#\mathcal{O}_v/\mathfrak{p}_v)^{-\text{ord}_v(2)} & \text{if } v \text{ is a finite place.} \end{cases}$$

**Lemma 5.3.** *Suppose  $C$  is defined over a completion  $\mathbb{Q}_v$  of  $\mathbb{Q}$ . If  $\{P_0, \dots, P_r\} \subset C(\mathbb{Q}_v)$  are such that*

$$\dim_2 \langle \gamma_v(P_i) - \gamma_v(P_0) : i = 1, \dots, r \rangle = \begin{cases} 3 & \text{if } \mathbb{Q}_v = \mathbb{R}, \\ 9 & \text{if } \mathbb{Q}_v = \mathbb{Q}_2, \\ 6 & \text{otherwise,} \end{cases}$$

*then  $\tilde{\gamma}_v(\text{Pic}^0(C/\mathbb{Q}_v)) = W_v^0$  and  $W_v = \langle \tilde{\gamma}(P_0), \dots, \tilde{\gamma}(P_r) \rangle$ .*

*Proof.* We have  $\#\text{Jac}_C[2](\mathbb{Q}_v) = 64$ , so the dimension bound is just (5-3). Thus the condition is that the divisor classes  $[P_1 - P_0], \dots, [P_r - P_0]$  generate  $\text{Pic}^0(C/\mathbb{Q}_v)/2\text{Pic}^0(C/\mathbb{Q}_v)$ . The second statement follows simply from  $W_v = W_v^0 + \tilde{\gamma}(P_0)$ .  $\square$

This lemma provides us in many cases with a way to compute  $W_v$  directly and quickly. An alternative is to determine  $\tilde{\gamma}_v(C(k_v))$  using the algorithm sketched in Section 5.2. This has a complexity proportional to the size of the residue field  $\mathcal{O}_v/\mathfrak{p}_v$ , which is rather bad.

In many cases the  $k_v$ -valued contact points of the bitangents are already sufficient to generate  $W_v$ . In fact for real places this is always the case by the argument in Section 5.1.

It may be the case that  $\text{Pic}^0(C/k_v)/2\text{Pic}^0(C/k_v)$  really does need divisors with higher degree places in their support. In that case, if the residue field is small enough, we can compute  $W_v$  via Section 5.2 or we can search for these higher degree places and use

$$\langle \tilde{\gamma}_v(P_0) \rangle + \tilde{\gamma}_v(\text{Pic}^0(C/k_v))$$

as an upper bound for  $W_v$  in (5-2).

**Remark 5.4.** If Lemma 5.3 applies to all  $v \in S$  then we compute the 2-Selmer group of  $\text{Jac}_C$  as well, via

$$\text{Sel}^{(2)}(\text{Jac}_C/\mathbb{Q}) = \bigcap_{v \in S} \tilde{\rho}_v^{-1}(W_v^0),$$

and in any case the right-hand side gives a subgroup of the Selmer group, so we get a lower bound in all cases. See Section 6.2.

**5.4. Information at good primes.** Let  $k_v$  be a local field of odd residue characteristic, with  $q = \#(\mathcal{O}_v/\mathfrak{p}_v)$ . Then

$$\#L'(2, k_v)^{\text{unr}} = 64.$$

If  $C/k_v$  has good reduction  $\bar{C}$ , then  $\gamma_v(P)$  is already determined by the reduction of  $P$ , so using the Hasse–Weil bounds, we obtain

$$\#\gamma_v(C(k_v)) \leq \#\bar{C}(\mathcal{O}_v/\mathfrak{p}_v) \leq q + 1 + 6\sqrt{q}.$$

If  $q \leq 29$  then  $\gamma_v(C(k_v)) \subsetneq L'(2, k_v)^{\text{unr}}$ , and even if  $q$  is larger, it is quite likely that the local image is not the entire unramified set. Hence, for small residue class field, many of the two-covers  $D_\gamma$  fail to have points locally, even at primes of good reduction. We see that in the intersection (5-1), the primes of small norm actually impose significant conditions.

Because computing local images for primes of larger norm is expensive, we define a more easily computed set that contains  $\text{Sel}^{(2)}(C/k)$ , by

$$\text{Sel}^{(2)}(C/k; N) = \{ \gamma \in L'(2, k; S) :$$

$$(1, \gamma) \in W_C^1 \text{ for } v \in S \text{ and } \rho_v(\gamma) \in \gamma_v(C(k_v)) \text{ for } v \text{ such that } \#(\mathcal{O}_v/\mathfrak{p}_v) \leq N \}.$$

We compute this set using Algorithm 1. If the resulting set is empty, then  $C(k)$  is empty.

**Algorithm 1:** TwoCoverDescent

---

**Input:** Quartic  $f \in \mathcal{O}[x, y, z]$  describing a nonsingular plane quartic  $C$  with bitangent forms  $\{\ell_{ij} \in \mathcal{O}[x, y, z] : 0 \leq i < j \leq 7\}$  and the  $\delta_q$  according to [Definition 2.3](#), and a norm bound  $N$

**Output:**  $\text{Sel}^{(2)}(C/k; N)$

```

1  $S \leftarrow \{v \in \Omega_k : \text{ord}_v(2D_{27}(f)) > 0, \text{ or } \ell_{ij} \in \mathfrak{p}_v[x, y, z], \text{ or } v \text{ is archimedean}\}$ 
2  $W \leftarrow \mathbb{F}_2 \times L'(2, k; S)$ 
3 for  $v \in S$ :
4    $\mathcal{P} \leftarrow \{\tilde{\mathcal{Y}}_v(P) \in C(k_v) : \ell_{ij}(P) = 0 \text{ for some } i, j\}$ 
5   if  $\dim_2 \langle P - Q : P, Q \in \mathcal{P} \rangle$  equals the bound in Lemma 5.3:
6      $W_v \leftarrow \langle \mathcal{P} \rangle$ 
7   else:
8      $W_v \leftarrow \langle \tilde{\mathcal{Y}}_v(C(k_v)) \rangle$  as computed in Sections 5.1 and 5.2
9    $W \leftarrow W \cap \rho_v^{-1}(W_v)$ 
10  $W^1 \leftarrow \{w \in W : w_1 = 1\}$ , where  $w_1$  is the image of  $w$  in  $\mathbb{F}_2$  from line 2
11 for  $v \in \Omega_k : v \text{ is finite and } \#(\mathcal{O}_v/\mathfrak{p}_v) \leq N$ :
12    $W^1 \leftarrow \{w \in W^1 : \tilde{\rho}_v(w) \in \tilde{\mathcal{Y}}_v(C(k_v))\}$ 
13 return  $W$ 
```

---

## 6. Results

We implemented [Algorithm 1](#) for  $k = \mathbb{Q}$  in Magma and tested it on two sample sets:

### A. Curves parameterized by

$$\{(u_1, \dots, v_3) \in \{-6, \dots, 6\} : u_1 < u_2 < u_3 \text{ and } u_1 < v_1\}.$$

The inequalities normalize some of the permutations possible on the points that lead to isomorphic curves. We found 81070 configurations in general position. However, because of the small values of the coefficients, there are many configurations with extra symmetries, so we find many isomorphic curves in the configurations. We find 33471 distinct values for  $D_{27}$ , indicating that the collection contains many nonisomorphic curves as well.

**B.** 70000 curves with  $u_1, \dots, v_3$  chosen uniformly randomly from  $\{-40, \dots, 40\}$ , while discarding configurations not in general position. We originally found two quartics with matching  $D_{27}$ . Their configurations differed by a permutation, so the curves were isomorphic. We replaced one of them.

In each case, we used Magma's `MinimizeReducePlaneQuartic` to find a nicer plane model, with smaller discriminant. Since isomorphisms change  $D_{27}$  by a 27-th power, it is easy to tell from discriminants when curves are not isomorphic.

Typical examples take less than 2 seconds to execute, with the quartic reduction step being one of the more expensive and less predictable steps. Occasional anomalies arise, where computation of a local image at a large prime is required. The whole experiment represents about 126 CPU hours of work.

	$C(\mathbb{Q}_v) = \emptyset$	$\text{Sel}^{(2)}(C/\mathbb{Q}) = \emptyset$	rational bitangent contact point	other rational point	total
<b>A</b>	3654	42477	34025	4568	81070
	4.5%	52%	42%	5.6%	100%
<b>B</b>	521	63926	4830	1244	70000
	0.7%	91%	6.9%	1.8%	100%

**Table 6.1.** Two-cover descent results

**Example 6.1.** As a small, typical, example, take

$$\begin{pmatrix} u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \end{pmatrix} = \begin{pmatrix} 17 & -7 & -9 \\ 35 & 3 & 9 \end{pmatrix}.$$

We find

$$C : 9x^4 - 60x^3y + 357x^2y^2 + 246xy^3 + 16y^4 - 42x^3z + 259x^2yz - 168xy^2z \\ - 141y^3z + 31x^2z^2 - 492xyz^2 + 207y^2z^2 + 42xz^3 - 27yz^3 + 9z^4 = 0$$

and  $D_{27}(C) = 2^{34} \cdot 3^{20} \cdot 5^{10} \cdot 7^8 \cdot 11^2 \cdot 13^6 \cdot 17^4 \cdot 19^4 \cdot 29^2 \cdot 37^2 \cdot 41^2$ . The curve  $C$  has points everywhere locally. We have  $\dim_2 L'(2, \mathbb{Q}; S) = 72$  and  $W_C = \bigcap_{v \in S} \tilde{\rho}_v^{-1}(W_v)$  has  $\dim_2 W_C = 10$ . We find that  $W_C^1$  is nonempty, so it has  $2^9$  elements. Computing

$$W_{C,T}^1 = \{w \in W_C^1 : \tilde{\rho}_v(w) \in \tilde{\mathcal{Y}}_v(C(k_v)) \text{ for } v \in T\}$$

is quite doable, for various sets  $T$ . We conclude that  $C(\mathbb{Q}) = \emptyset$  from, for example,

$$\text{Sel}^{(2)}(C/\mathbb{Q}) \subset W_{C,T}^1 = \emptyset \text{ for } T = \{2, 3, 5\} \text{ or } \{31, 43, 47, 53, 71, 83\}.$$

Furthermore, from the data computed we can conclude that

$$\dim_2 \text{Sel}^{(2)}(\text{Jac}_C/\mathbb{Q}) = \dim_2 W_C^0 = 9,$$

so either  $\text{Jac}_C(\mathbb{Q})$  has free rank 3 or  $\text{III}(\text{Jac}_C/\mathbb{Q})[2]$  is nontrivial.

**6.1. Results of two-cover descent.** We executed [Algorithm 1](#) on our samples, with  $N = 50$ . This allowed us to determine the existence of rational points on each of the curves. We summarize our findings in [Table 6.1](#).

When  $\text{Sel}^{(2)}(C/\mathbb{Q}) \neq \emptyset$  and  $C$  has no rational bitangent contact points (possibly a hyperflex), we search for a low-height nonsingular point using `PointSearch` on either the sextic model (3-1) or the plane quartic model we construct from it. These are the curves reported in the “other rational point” column. For two curves we needed to search up to a height bound of  $10^7$ .

Another interesting fact is that local obstructions are quite rare (having a local obstruction implies  $\text{Sel}^{(2)}(C/\mathbb{Q}) = \emptyset$ ). Furthermore we only found  $C(\mathbb{Q}_p) = \emptyset$  for  $p = 2, 11, 23$ , and only when  $C$  has good reduction at those places. [Proposition 1.2](#) gives a partial explanation of this fact. This is quite contrary to the case of hyperelliptic curves, where local obstructions do tend to occur at primes of bad reduction.

	6	7	8	9	10	11	12	13	
<b>A</b>	0.05%	18.7%	39.4%	29.1%	10.1%	2.28%	0.29%	0.006%	( $n = 31990$ )
<b>B</b>	0	20.2%	41.8%	27.9%	8.71%	1.27%	0.10%	0.006%	( $n = 51685$ )

**Table 6.2.** Distribution of  $\dim_2 \text{Sel}^{(2)}(\text{Jac}_C / \mathbb{Q})$  where our data allowed its computation

## 6.2. Information on rank and III. We have

$$\text{Sel}^{(2)}(\text{Jac}_C / \mathbb{Q}) = L'(\mathbb{Q}, 2; S) \cap \bigcap_{v \in S} \rho_v^{-1} \gamma_v(\text{Pic}^0(C/\mathbb{Q}_v)).$$

[Lemma 5.3](#) gives a condition for when the sets on the right-hand side are generated by differences of degree 1 points. For a reasonable proportion of our curves, our data allows us to compute  $\text{Sel}^{(2)}(\text{Jac}_C / \mathbb{Q})$ . We list the results in [Table 6.2](#). In the rest of this section, we only consider these examples.

With  $\text{Jac}_C[2](\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^6$ , we must have that the Selmer rank is at least 6, but as one can see, the distribution has an average significantly higher than that. Part of that is explained by the fact that  $C$ , and hence the class  $J^1 \in H^1(k, \text{Jac}_C)$  representing  $\text{Pic}^1(C/\mathbb{Q})$ , is trivial everywhere locally. Since  $C$  has quadratic points, we can pull the class back under the homomorphism

$$\text{Sel}^{(2)}(\text{Jac}_C / \mathbb{Q}) \rightarrow H^1(k, \text{Jac}_C)[2]$$

and the preimage is likely independent of the image of  $\text{Jac}_C[2](\mathbb{Q})$ .

If  $W_C^1 = \emptyset$  in [\(5-2\)](#) then it follows by [\[Cre20, Theorem 5.3\]](#) that  $J^1$  is not divisible by two in  $\text{III}(\text{Jac}_C / \mathbb{Q})$ , and therefore is nontrivial. This happens in about half the examples.

Once we take into account that we expect that

$$\dim_2 \text{Sel}^{(2)}(\text{Jac}_C / \mathbb{Q}) \geq 7,$$

we find that the distributions in [Table 6.2](#), particularly for collection B, match [\[PR12, Conjecture 1.1\]](#) rather well. This does require us to account for the fact that  $J^1$  almost always has points everywhere locally.

Generally, nonhyperelliptic curves tend to have points everywhere locally. Therefore, one actually should expect that Selmer groups of Jacobians of curves behave a little differently from those of general abelian varieties, because they tend to come equipped with an everywhere locally trivial torsor.

## Acknowledgments

We thank Michael Stoll for interesting discussions and suggestions on how to interpret the rank results in light of [\[PR12\]](#), and an anonymous referee for helpful comments.

## Appendix: Local algorithms

We use the notation from [Section 5.2](#). The algorithms here are in the spirit of [\[Bru06, §5; BS09, §4\]](#).

**Algorithm 2: HENSELBALLS**


---

**Input:**  $f \in \mathcal{O}[x, y]$ , describing a smooth curve  
**Output:** A finite set  $\{(x_t, y_t, e_t)\}_t$  of Hensel-liftable balls covering the  $\mathcal{O}$ -valued solutions of  $f(x, y) = 0$

```

1 for  $(x_0, y_0) \in \{(x_0, y_0) \in D^2 : f(x_0, y_0) \equiv 0 \pmod{\mathfrak{p}}\}$ :
2    $R \leftarrow \emptyset$ 
3   if  $\frac{\partial f}{\partial x}(x_0, y_0) \not\equiv 0 \pmod{\mathfrak{p}}$  or  $\frac{\partial f}{\partial y}(x_0, y_0) \not\equiv 0 \pmod{\mathfrak{p}}$ :
4      $R \leftarrow R \cup \{(x_0, y_0, 1)\}$ 
5   else:
6      $g \leftarrow f(x_0 + \pi x, y_0 + \pi y)$ 
7      $T \leftarrow \text{HENSELBALLS}(g/\text{content}(g))$ 
8      $R \leftarrow R \cup \{(x_0 + \pi x_1, y_0 + \pi y_1, e + 1) : (x_1, y_1, e) \in T\}$ 
9 return  $R$ 

```

---

**Algorithm 3: LOCALIMAGE**


---

**Input:**  $f \in \mathcal{O}[x, y]$  describing a smooth plane quartic, together with its bitangent forms  $\{\ell_{ij} \in \mathcal{O}[x, y] : 0 \leq i < j \leq 7\}$  and syzygetic data  $\delta_q$  as in [Definition 2.3](#)  
**Output:** Local image of  $\gamma_v$  on the given affine patch

```

1 Denote the mod-squares map by  $\mu : \mathcal{O} \setminus \{0\} \rightarrow k^\times / k^{\times 2}$ 
2  $T \leftarrow \text{HENSELBALLS}(f)$ 
3  $R \leftarrow \emptyset$ 
4 while  $T \neq \emptyset$ :
5   Take  $(x_0, y_0, e)$  from  $T$ 
6    $L \leftarrow [\ell_{ij}(x_0, y_0) : 0 \leq i < j \leq 7]$ 
7   for  $i = 1, \dots, 7$ :
8     if  $\text{ord}(L_i) < e - \text{ord}(4)$ :
9        $\gamma_i \leftarrow \mu(L_i)$ 
10    else if there is a syzygetic quadruple  $q = \{\ell_i, \ell_a, \ell_b, \ell_c\}$  such that
         $\max(\text{ord}(\ell_a(x_0, y_0)), \text{ord}(\ell_b(x_0, y_0)), \text{ord}(\ell_c(x_0, y_0))) < e - \text{ord}(4)$ :
11       $\gamma_i \leftarrow \mu(\delta_q \ell_a(x_0, y_0) \ell_b(x_0, y_0) \ell_c(x_0, y_0))$ 
12    else: /* we refine the covering */
13       $g \leftarrow f(x_0 + \pi^e x, y_0 + \pi^e y)$ 
14       $h \leftarrow g/\text{content}(g)$  /*  $h \pmod{\mathfrak{p}}$  will be linear */
15      for  $(x_1, y_1) \in \{(x_1, y_1) \in D^2 : h(x_1, y_1) \equiv 0 \pmod{\mathfrak{p}}\}$ :
16         $T \leftarrow T \cup (x_0 + \pi^e x_1, y_0 + \pi^e y_1, e + 1)$ 
17      break to while
18   Add  $(\gamma_1, \dots, \gamma_7)$  to  $R$ 
19 return  $R$ .

```

---

## References

- [BFL19] Barinder Banwait, Francesc Fité, and Daniel Loughran, *Del pezzo surfaces over finite fields and their frobenius traces*, Math. Proc. Cambridge Philos. Soc. **167** (2019), no. 1, 35–60.
- [BGW17] Manjul Bhargava, Benedict H. Gross, and Xiaoheng Wang, *A positive proportion of locally soluble hyperelliptic curves over  $\mathbb{Q}$  have no point over any odd degree extension*, J. Amer. Math. Soc. **30** (2017), no. 2, 451–493.
- [BPS16] Nils Bruin, Bjorn Poonen, and Michael Stoll, *Generalized explicit descent and its application to curves of genus 3*, Forum Math. Sigma **4** (2016), e6, 80.
- [Bru06] Nils Bruin, *Some ternary diophantine equations of signature  $(n, n, 2)$* , pp. 63–91 in *Discovering mathematics with Magma*, Algorithms Comput. Math. **19**, Springer, Berlin (2006).
- [BS09] Nils Bruin and Michael Stoll, *Two-cover descent on hyperelliptic curves*, Math. Comp. **78** (2009), no. 268, 2347–2370.
- [Cob22] Arthur B. Coble, *Associated sets of points*, Trans. Amer. Math. Soc. **24** (1922), no. 1, 1–20.
- [Cre20] Brendan Creutz, *Generalized jacobians and explicit descents*, Math. Comp. **89** (2020), no. 323, 1365–1394.
- [CW32] C. Chevalley and A. Weil, *Un théorème d’arithmétique sur les courbes algébriques*, C. R. Acad. Sci. Paris **195** (1932), 570–572.
- [Dol12] Igor V. Dolgachev, *Classical algebraic geometry: a modern view*, Cambridge University Press, Cambridge, 2012.
- [GH81] Benedict H. Gross and Joe Harris, *Real algebraic curves*, Ann. Sci. École Norm. Sup. (4) **14** (1981), no. 2, 157–182.
- [GH04] Benedict H. Gross and Joe Harris, *On some geometric constructions related to theta characteristics*, pp. 279–311 in *Contributions to automorphic forms, geometry, and number theory*, Johns Hopkins Univ. Press, Baltimore, MD, 2004.
- [GKZ08] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky, *Discriminants, resultants and multidimensional determinants*, Modern Birkhäuser Classics, Birkhäuser Boston Inc., Boston, MA, 2008, reprint of the 1994 edition.
- [Lew19] Daniel Lewis, *An implementation of two-cover descent on plane quartic curves*, M.Sc. thesis, Simon Fraser University, 2019.
- [Mil80] James S. Milne, *Étale cohomology*, Princeton Mathematical Series **33**, Princeton University Press, Princeton, N.J., 1980.
- [PR12] Bjorn Poonen and Eric Rains, *Random maximal isotropic subspaces and selmer groups*, J. Amer. Math. Soc. **25** (2012), no. 1, 245–269.
- [Tho16] Jack A. Thorne, *Arithmetic invariant theory and 2-descent for plane quartic curves*, Algebra Number Theory **10** (2016), no. 7, 1373–1413.

Received 28 Feb 2020.

NILS BRUIN: [nbruin@cecm.sfu.ca](mailto:nbruin@cecm.sfu.ca)

Department of Mathematics, Simon Fraser University, Burnaby BC, Canada

DANIEL LEWIS: [dlewis3@math.arizona.edu](mailto:dlewis3@math.arizona.edu)

Department of Mathematics, The University of Arizona, Tucson, AZ, United States





# Abelian surfaces with fixed 3-torsion

Frank Calegari, Shiva Chidambaram, and David P. Roberts

Given a genus two curve  $X : y^2 = x^5 + ax^3 + bx^2 + cx + d$ , we give an explicit parametrization of all other such curves  $Y$  with a specified symplectic isomorphism on three-torsion of Jacobians  $\text{Jac}(X)[3] \cong \text{Jac}(Y)[3]$ . It is known that under certain conditions modularity of  $X$  implies modularity of infinitely many of the  $Y$ , and we explain how our formulas render this transfer of modularity explicit. Our method centers on the invariant theory of the complex reflection group  $C_3 \times \text{Sp}_4(\mathbb{F}_3)$ . We discuss other examples where complex reflection groups are related to moduli spaces of curves, and in particular motivate our main computation with an exposition of the simpler case of the group  $\text{Sp}_2(\mathbb{F}_3) = \text{SL}_2(\mathbb{F}_3)$  and 3-torsion on elliptic curves.

## 1. Introduction

**1.1. Overview.** Consider a genus two curve  $X$  over  $\mathbb{Q}$  given by an affine equation

$$y^2 = x^5 + ax^3 + bx^2 + cx + d. \quad (1-1)$$

The representation  $\bar{\rho} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GSp}_4(\mathbb{F}_3)$  on the three-torsion  $\text{Jac}(X)[3]$  of its Jacobian is given by an explicit degree 80 polynomial with coefficients in  $\mathbb{Q}[a, b, c, d]$ . The polynomial can be extracted from [Shi91], or by following the recipe given in Section 3.1. The main theorem of this paper parametrizes all pairs  $(Y, i)$  consisting of a curve

$$Y : y^2 = x^5 + Ax^3 + Bx^2 + Cx + D \quad (1-2)$$

and a  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ -equivariant symplectic isomorphism,  $i : \text{Jac}(X)[3] \rightarrow \text{Jac}(Y)[3]$ . The curves in (1-2) all have a rational Weierstrass point at  $\infty$ . The reader may wonder why we did not instead try to parametrize pairs  $(Y, i)$  for all genus two curves  $Y$ . The answer is that the corresponding moduli space, while rational over  $\mathbb{C}$ , will not typically be rational over  $\mathbb{Q}$  (see the discussion towards the end of Section 1.2).

---

FC and SC were supported in part by NSF grant DMS-1701703; DPR was supported in part by DMS-1601350.

MSC2020: primary 11F80; secondary 11G10, 20F55.

Keywords: abelian surfaces, three torsion, Galois representations.

Analogous problems for genus one curves and their mod  $p$  representations for  $p \leq 5$  were solved by Rubin and Silverberg [RS95]. In Section 2, we explain how the mod 3 formulas of [LR96] can be reconstructed by using that  $\mathrm{Sp}_2(\mathbb{F}_3)$  has a two-dimensional complex reflection representation, summarizing the result in Theorem 1.

Section 3 contains our main result, Theorem 2. It follows Section 2 closely, using now that  $\mathrm{Sp}_4(\mathbb{F}_3)$  is the main factor in the complex reflection group  $C_3 \times \mathrm{Sp}_4(\mathbb{F}_3)$ . We write the new curves as  $Y = X(s, t, u, v)$  with  $X(1, 0, 0, 0) = X$ . The new coefficients  $A, B, C$  and  $D$  are polynomials in  $a, b, c, d, s, t, u$ , and  $v$ . While the genus one and two cases are remarkably similar theoretically, the computations in the genus two case are orders of magnitude more complicated. For example,  $A, B, C$ , and  $D$  have 14604, 112763, 515354, and 1727097 terms respectively, while the corresponding two coefficients in the genus one case have only 6 and 9 terms. We give all these coefficients and other information the reader may find helpful in *Mathematica* files in the online supplement.

Section 4 provides four independent complements. Section 4.1 sketches an alternative method for computing the above  $(A, B, C, D)$ . Section 4.2 presents a family of examples involving Richelot isogenies. Section 4.3 gives an application to modularity which was one of the motivations for this paper. Section 4.4 illustrates that much of what we do works for arbitrary complex reflection groups; in particular, it sketches direct analogs of our main result in the computationally yet more difficult settings of 2-torsion in the Jacobians of certain curves of genus 3 and 4.

**1.2. Moduli spaces.** Theorems 1 and 2 and the analogs sketched in Section 4.4 are all formulated in terms of certain *a priori* complicated moduli spaces being actually open subvarieties of projective space. To underscore this perspective, we consider a whole hierarchy of standard moduli spaces as follows.

Let  $A$  be an abelian variety over  $\mathbb{Q}$  of dimension  $g$  with a principal polarization  $\lambda$ . If  $V_A = A[p]$  is the set of  $p$ -torsion points with coefficients in  $\overline{\mathbb{Q}}$ , then  $V_A$  is a  $2g$ -dimensional vector space over  $\mathbb{F}_p$  with a symplectic form  $\wedge_A^2$  induced by the Weil pairing  $A[p] \times A[p] \rightarrow \mu_p$ . This structure is preserved by  $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ , and so gives rise to a Galois representation

$$\bar{\rho}_A : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathrm{GSp}_{2g}(\mathbb{F}_p);$$

here the similitude character  $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathbb{F}_p^\times$  is the mod- $p$  cyclotomic character.

Conversely, if  $\bar{\rho}$  is any such representation on a symplectic space  $(V, \wedge^2)$ , coming from an abelian variety or not, there exists a moduli space  $\mathcal{A}_g(\bar{\rho})$  over  $\mathbb{Q}$  parametrizing triples  $(A, \lambda, \iota)$  consisting of a principally polarized abelian variety  $A$  together with an isomorphism  $\iota : (V, \wedge^2) \simeq (V_A, \wedge_A^2)$  of symplectic representations.

Via  $(A, \lambda, \iota) \mapsto (A, \lambda)$ , one has a covering map  $\mathcal{A}_g(\bar{\rho}) \rightarrow \mathcal{A}_g$  to the moduli space of principally polarized  $g$ -dimensional abelian varieties. For the split Galois representation  $\bar{\rho}_0$ , corresponding to the torsion structure  $(\mathbb{Z}/p\mathbb{Z})^g \oplus (\mu_p)^g$  with its natural symplectic form, the cover  $\mathcal{A}_g(\bar{\rho}_0)$  is the standard “full level  $p$ ” cover  $\mathcal{A}_g(p)$  of  $\mathcal{A}_g$ . In general,  $\mathcal{A}_g(\bar{\rho})$  is a twisted version of  $\mathcal{A}_g(p)$ , meaning that the two varieties become isomorphic after base change from  $\mathbb{Q}$  to  $\overline{\mathbb{Q}}$ .

The varieties  $\mathcal{A}_g(\bar{\rho})$  become rapidly more complicated as either  $g$  or  $p$  increases. In particular, they are geometrically rational exactly for the cases  $(g, p) = (1, 2), (1, 3), (1, 5), (2, 2), (2, 3)$ , and  $(3, 2)$  [HS02, Theorem II.2.1]. In the three cases when  $g = 1$ , the curves  $\mathcal{A}_1(\bar{\rho})$  are always rational. In the main case of interest  $(2, 3)$  for this paper, the three-dimensional variety  $\mathcal{A}_2(3) = \mathcal{A}_2(\bar{\rho}_0)$  is rational [BN18]. However, for many  $\bar{\rho}$ , including all surjective representations, it is proven in [CC20] that the variety  $\mathcal{A}_2(\bar{\rho})$  is never rational. It is true, however, that there exists a degree 6 cover  $\mathcal{A}_2^w(\bar{\rho})$  which is rational [BCGP18, Lemma 10.2.4]. Thus while Theorem 1 corresponds to a parametrization of  $\mathcal{A}_1(\bar{\rho})$  for  $p = 3$ , Theorem 2 corresponds to a parametrization of  $\mathcal{A}_2^w(\bar{\rho})$ . More precisely, the Torelli map  $\mathcal{M}_2 \rightarrow \mathcal{A}_2$  is an open immersion, and the pullback of  $\mathcal{A}_2^w(\bar{\rho})$  is the moduli space  $\mathcal{M}_2^w(\bar{\rho})$  of genus two curves of the form (1-1) whose Jacobians give rise to  $\bar{\rho}$ , and it is  $\mathcal{M}_2^w(\bar{\rho})$  which we explicitly parametrize. The retreat to this cover is optimal in the sense that six is generically the minimal degree of any dominant rational map from  $\mathbb{P}_{\mathbb{Q}}^3$  to  $\mathcal{A}_2(\bar{\rho})$  [CC20]. We mention in passing that our arguments give an alternative proof of [BCGP18, Lemma 10.2.4].

There is a natural generalization of the varieties  $\mathcal{A}_g(\bar{\rho})$ . Namely, for any  $m \in \mathbb{F}_p^\times$ , one can require instead an isomorphism  $i : (V, \wedge^2) \simeq (V_A, m \wedge_A^2)$ . For  $m/m'$  a square, the corresponding varieties are canonically isomorphic, so that one gets a new moduli space only in the case of  $p$  odd. We denote this new moduli space involving “antisymplectic” isomorphisms by  $\mathcal{A}_g^*(\bar{\rho})$ . Our policy throughout this paper is to focus on  $\mathcal{A}_g(\bar{\rho})$  and be much briefer about parallel results for  $\mathcal{A}_g^*(\bar{\rho})$ .

## 2. Elliptic curves with fixed 3-torsion

In this section, as a warm up to Section 3, we rederive the formulas in [LR96] describing elliptic curves with fixed 3-torsion from the invariant theory of the group  $\mathrm{Sp}_2(\mathbb{F}_3)$  as in [Fis12]. Many of the steps in the derivation transfer with no theoretical change to our main case of abelian surfaces. We present these steps in greater detail here, because space allows us to give explicit formulas right in the text. Throughout this section and the next, we present the derivations in elementary language which stays very close to the computations involved. Only towards the end of the sections do we recast the results in the moduli language of the introduction.

**2.1. Elliptic curves and their 3-torsion.** Let  $a$  and  $b$  be rational numbers such that the polynomial discriminant  $\Delta_{\mathrm{poly}} = -4a^3 - 27b^2$  of  $x^3 + ax + b$  is nonzero and consider the elliptic curve  $X$  over  $\mathbb{Q}$  with affine equation

$$y^2 = x^3 + ax + b. \quad (2-1)$$

We emphasize the discriminant  $\Delta(a, b) = \Delta = 2^4 \Delta_{\mathrm{poly}}$  in the sequel, because it makes Section 2.7 cleaner.

By a classical division polynomial formula, the eight primitive 3-torsion points  $(x, y) \in \mathbb{C}^2$  are exactly the points satisfying both (2-1) and

$$3x^4 + 6ax^2 + 12bx - a^2 = 0. \quad (2-2)$$

Equations (2-1) and (2-2) together define an octic algebra over  $\mathbb{Q}$ . Rather than work with the two generators  $x$  and  $y$  and the two relations (2-1) and (2-2), we will work with  $z$ , the slope of a tangent line to the elliptic curve at the 3-torsion point  $(x, y)$ . Then  $z^2 = 3x$  and assuming  $a \neq 0$  to avoid inseparability issues, the algebra in question is the quotient  $K := K_{a,b}$  of  $\mathbb{Q}[z]$  coming from the equation

$$F(a, b, z) := z^8 + 18az^4 + 108bz^2 - 27a^2 = 0. \quad (2-3)$$

**2.2.  $\mathrm{Sp}_2(\mathbb{F}_3)$  and related groups.** For generic  $(a, b)$ , the Galois group of the polynomial  $F(a, b, z)$  is  $\mathrm{GSp}_2(\mathbb{F}_3) = \mathrm{GL}_2(\mathbb{F}_3)$ . The discriminant of  $F(a, b, z)$  is  $-2^8 3^{21} a^2 \Delta^4$ . Thus the splitting field  $K'_{a,b}$  of  $F(a, b, z)$  contains  $E = \mathbb{Q}(\sqrt{-3})$  for all  $a, b$ . The relative Galois group  $\mathrm{Gal}(K'_{a,b}/E)$  is  $\mathrm{Sp}_2(\mathbb{F}_3) = \mathrm{SL}_2(\mathbb{F}_3)$ . We will generally use symplectic rather than linear language in the sequel, to harmonize our notation with our main case of genus two. Also we will systematically use  $\omega = \exp(2\pi i/3) = (-1 + \sqrt{-3})/2$  as our preferred generator for  $E$ .

To describe elliptic curves with fixed 3-torsion, we use that (2-3) arises as a generic polynomial in the invariant theory of  $\mathrm{Sp}_2(\mathbb{F}_3)$ . The invariant theory is simple because  $\mathrm{Sp}_2(\mathbb{F}_3) = \langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle$  can be realized as a complex reflection group by sending the generators in order to

$$g_1 = \begin{pmatrix} \bar{\omega} & \bar{\omega} - 1 \\ 0 & 1 \end{pmatrix}, \quad g_2 = \begin{pmatrix} 1 & 0 \\ (\omega - 1)/3 & \omega \end{pmatrix}. \quad (2-4)$$

The matrices  $g_1$  and  $g_2$  are indeed complex reflections because all but one eigenvalue is 1. In our study of the image  $\mathrm{ST}4 = G = \langle g_1, g_2 \rangle$ , the subgroup  $H = \langle g_1 \rangle$  will play an important role. Here our notation  $\mathrm{ST}4$  refers to the placement of  $G$  in the Shephard–Todd classification of the thirty-seven exceptional irreducible complex reflection groups sorted roughly by increasing size [ST54, Table VII].

For both the current case of  $n = 2$  and the main case of  $n = 4$ , we are focused principally on three irreducible characters of  $\mathrm{Sp}_n(\mathbb{F}_3)$ , the unital character  $\chi_1$  and a complex conjugate pair  $\chi_{na}$  and  $\chi_{nb}$ . Here  $\chi_{na}$  corresponds to the representations (2-4) and (3-2) on  $V = E^n$ . Just as *invariant* is used for polynomials associated to  $\chi_1$ , we will use the terms *covariant* and *contravariant* for polynomials similarly associated to  $\chi_{na}$  and  $\chi_{nb}$  respectively.

The left half of Table 1 shows how the three characters 1,  $\chi_{2a}$ , and  $\chi_{2b}$  fit into the entire character theory of  $\mathrm{Sp}_2(\mathbb{F}_3)$ . For example, via  $\bar{\omega} + 1 = -\omega$  and its conjugate,  $g_1$  and  $g_2$  lie in the classes 3A and 3B respectively. While this information is clarifying, it is not strictly speaking needed for our arguments.

The right half of Table 1 gives numerical information that will guide our calculation with explicit polynomials in the next subsections. The characters are orthonormal with respect to the Hermitian inner product  $\langle f, g \rangle = |G|^{-1} \sum_C |C| f(C) \overline{g(C)}$ . Let  $\phi_k = \sum_i \langle \chi_i, \phi_k \rangle \chi_i$  be the character of the  $k$ -th symmetric power  $\mathrm{Sym}^k V$ . The multiplicities  $\langle \chi_i, \phi_k \rangle$  for  $k \leq 8$  are given in the right half of Table 1. These numbers are given for arbitrary  $k$  by  $\sum_{k=0}^{\infty} \langle \chi_i, \phi_k \rangle x^k = N_i(x)/((1-x^4)(1-x^6))$ . The character of the permutation representation of  $G$  on the coset space  $G/H$  is  $\phi_{G/H} = \chi_1 + \chi_3 + \chi_{2a} + \chi_{2b}$ . If  $W$  has character  $\chi_i$  then the dimension of the subspace  $W^H$  of  $H$ -invariants is  $\langle \chi_i, \phi_{G/H} \rangle$ . So  $\dim(W^H) = 1$  if  $i \in \{1, 2a, 2b, 3\}$  and  $\dim(W^H) = 0$  if  $i \in \{1a, 1b, 2\}$ .

$ C $	1	1	4	4	6	4	4	$\langle \chi_i, \phi_k \rangle$									$N_i(x)$
$C$	1A	2A	3A	3B	4A	6A	6B	0	1	2	3	4	5	6	7	8	
$\chi_1$	1	1		1	1	1	1	1				1		1		1	1
$\chi_{1a}$	1	1	$\bar{\omega}$	$\omega$	1	$\bar{\omega}$	$\omega$					1				1	$x^4$
$\chi_{1b}$	1	1	$\omega$	$\bar{\omega}$	1	$\omega$	$\bar{\omega}$									1	$x^8$
$\chi_2$	2	-2	-1	-1	0	1	1						1		1		$x^5 + x^7$
$\chi_{2a}$	2	-2	$-\omega$	$-\bar{\omega}$	0	$\omega$	$\bar{\omega}$	1			1		1		2		$x + x^3$
$\chi_{2b}$	2	-2	$-\bar{\omega}$	$-\omega$	0	$\bar{\omega}$	$\omega$				1		1		1		$x^3 + x^5$
$\chi_3$	3	3	0	0	-1	0	0			1		1		2		2	$x^2 + x^4 + x^6$

**Table 1.** Character table of  $\mathrm{Sp}_2(\mathbb{F}_3)$  and invariant-theoretic information

**2.3. Rings of invariants.** The group  $G$  acts on the polynomial ring  $E[u, z]$  by the formulas induced from the matrices in (2-4),

$$\begin{aligned} g_1 u &= \bar{\omega} u + (\bar{\omega} - 1)z, & g_2 u &= u, \\ g_1 z &= z, & g_2 z &= (\omega - 1)u/3 + \omega z. \end{aligned}$$

Despite the appearance of the irrationality  $\omega$  in these formulas, there is an important rationality present. Namely we have arranged in (2-4) that  $g_1^2 = \bar{g}_1$  and  $g_2^2 = \bar{g}_2$ . Accordingly  $G$  is stable under complex conjugation, a stability not present in either the original Shephard and Todd paper [ST54, Section 4] or in *Magma*'s implementation `ShephardTodd(4)`.

We can use stability under complex conjugation to interpret  $G$  and  $H$  as the  $E$ -points of group schemes  $\underline{G}$  and  $\underline{H}$  over  $\mathbb{Q}$ . Then actually  $\underline{G}$  acts on  $\mathbb{Q}[u, z]$ . All seven irreducible representations of  $\underline{G}$  are defined over  $\mathbb{Q}$ , just like all three representations of the familiar group scheme  $\underline{H} \cong \mu_3$ , are defined over  $\mathbb{Q}$ . In practice, we continue thinking almost exclusively in terms of ordinary groups; these group schemes just provide a conceptually clean way of saying that in our various choices below we can and do always take all coefficients rational.

Define

$$w = \frac{u^3}{3} + u^2 z + u z^2, \quad a = \frac{wz}{9}, \quad b = \frac{w^2 - 6wz^3 - 3z^6}{324} \quad (2-5)$$

in  $\mathbb{Q}[u, z]$ . Then the subrings of  $\underline{H}$ - and  $\underline{G}$ -invariants are respectively

$$\mathbb{Q}[u, z]^H = \mathbb{Q}[w, z], \quad \mathbb{Q}[u, z]^G = \mathbb{Q}[a, b]. \quad (2-6)$$

Giving  $u$  and  $z$  weight one, the elements  $w$ ,  $a$ , and  $b$  clearly have weights 3, 4, and 6 respectively. If one eliminates  $w$  from the last two equations of (2-5), then one gets the polynomial relation  $F(a, b, z) = 0$  of (2-3), explaining our choice of overall scale factors in (2-5). The fact that the rings on the right in (2-6) are polynomial rings, rather than more complicated rings requiring relations to describe, comes exactly from the fact that  $H$  and  $G$  are complex reflection groups, by the Chevalley–Shephard–Todd theorem [Che55].

**2.4. Covariants and contravariants.** The graded ring  $\mathbb{Q}[w, z]$  is free of rank eight over the graded ring  $\mathbb{Q}[a, b]$ . Moreover there is a homogeneous basis  $1, z^2, z^4, z^6, \alpha_1, \alpha_3, \beta_3, \beta_5$  with the following properties. The exponent or index  $d$  gives the weight, and the elements  $\alpha_d$  and  $\beta_d$  are in the isotypical piece of  $\mathbb{Q}[u, z]_d$  corresponding to  $\chi_{2a}$  and  $\chi_{2b}$  respectively.

The covariants  $\alpha_d$  and the contravariants  $\beta_d$  are each well-defined up to multiplication by a nonzero rational scalar. Explicit formulas for particular choices can be found by simultaneously imposing the  $G$ -equivariance condition and the  $H$ -invariance condition. We take

$$\alpha_1 = z, \quad \alpha_3 = \frac{w + z^3}{6}, \quad \beta_3 = \frac{w - z^3}{2}, \quad \beta_5 = \frac{5wz^2 + 3z^5}{18}. \quad (2-7)$$

Ideas from classical invariant theory are useful in finding these quantities. For example, the polynomials in  $\mathbb{Q}[u, z]_3$  which have the required  $G$ -equivariance property for contravariance are exactly the linear combinations of the partial derivatives  $\partial_u a$  and  $\partial_z a$ . The subspace fixed by  $H$  is the line spanned by  $(\partial_u - \partial_z)a$ . Thus  $\beta_3 \propto (\partial_u - \partial_z)a$  and, in the same way,  $\beta_5 \propto (\partial_u - \partial_z)b$ . Further the covariant  $\alpha_3 \propto \partial_u D$ , where  $D^3 = \Delta(a, b)$ .

**2.5. New coefficients.** While we call the unique (up to scalar) homogeneous  $H$ -invariant elements  $\alpha_1, \alpha_3$  generating the  $\chi_{2a}$  isotypical pieces as covariants, Fisher defines in [Fis12] a covariant to be a tuple defining an equivariant map  $\mathbb{Q}[u, z]_1 \rightarrow \mathbb{Q}[u, z]_d$ . For  $d = 1$ , a covariant tuple is given by  $l_1 = (u, z)$  corresponding to the identity map. For  $d = 3$ , a covariant tuple is given as  $l_3 = (\alpha_{3,1}, \alpha_{3,2})$ , where  $\alpha_{3,2} := \alpha_3$  and the first entry  $\alpha_{3,1}$  is uniquely determined because of the required  $G$ -equivariance. Following [Fis12], one can obtain new coefficients by evaluating the invariants  $a$  and  $b$  at the general covariant tuple  $(u, z) = s \cdot l_1 + t \cdot l_3 = (su + t\alpha_{3,1}, sz + t\alpha_{3,2})$ . This approach yields our answer immediately in the case of  $g = 1$ , but becomes computationally difficult for  $g = 2$ . So we continue to treat covariants as polynomials as in Section 2.4 and describe two approaches to obtain new coefficients.

The octic  $\mathbb{Q}[a, b]$ -algebra  $\mathbb{Q}[w, z]$  acts on itself by multiplication and so every element  $e$  in  $\mathbb{Q}[w, z]$  has an octic characteristic polynomial  $\phi(e, u) \in \mathbb{Q}[a, b, u]$ . One has  $\phi(z, u) = F(a, b, u)$  from (2-3). To obtain the characteristic polynomial for a general  $e$ , one can express  $e$  as an element of  $\mathbb{Q}(a, b, z)$  via (2-7) and  $w = 9a/z$ . Then one removes  $z$  by a resultant to get the desired octic relation on  $e$ . Alternatively, we could have calculated these characteristic polynomials by using 8-by-8 matrices; in Section 3.5 we use the matrix approach.

Carrying out this procedure for the general covariant and contravariant gives

$$\phi(s\alpha_1 + t\alpha_3, u) = F(A(a, b, s, t), B(a, b, s, t), u), \quad \phi(s\beta_3 + t\beta_5, u) = F(A^*(a, b, s, t), B^*(a, b, s, t), u),$$

with

$$3A(a, b, s, t) = 3as^4 + 18bs^3t - 6a^2s^2t^2 - 6abst^3 - (a^3 + 9b^2)t^4,$$

$$9B(a, b, s, t) = 9bs^6 - 12a^2s^5t - 45abs^4t^2 - 90b^2s^3t^3 + 15a^2bs^2t^4 - 2a(2a^3 + 9b^2)st^5 - 3b(a^3 + 6b^2)t^6,$$

and  $A^*$  and  $B^*$  in the [online supplement](#). As stated in the introduction,  $A$  and  $B$  when fully expanded have 6 and 9 terms respectively and agree exactly with expressions in [LR96, Section 2].

The polynomials  $A$  and  $B$  and their starred versions are respectively of degrees four and six in  $s$  and  $t$ . Also in the main case assign weights  $(4, 6, -1, -3)$  to  $(a, b, s, t)$  and in the starred case make these weights  $(4, 6, -3, -5)$  instead. Then all four polynomials are homogeneous of weight zero.

**2.6. Geometric summary.** The following theorem summarizes our calculations in terms of moduli spaces. The  $\bar{\rho}$  of the introduction is the mod 3 representation of the initial elliptic curve, so to be more explicit we write  $\mathcal{A}_{a,b}$  rather than  $\mathcal{A}_1(\bar{\rho})$ .

**Theorem 1.** *Fix an equation  $y^2 = x^3 + ax + b$  defining an elliptic curve  $X$  over  $\mathbb{Q}$ . Let  $\mathcal{A}_{a,b}$  be the moduli space of pairs  $(Y, i)$  with  $Y$  an elliptic curve and  $i : X[3] \rightarrow Y[3]$  a symplectic isomorphism. Then  $\mathcal{A}_{a,b}$  can be realized as the complement of a discriminant locus  $\mathcal{Z}_{a,b}$  in the projective line  $\text{Proj } \mathbb{Q}[s, t]$ . The natural map to the  $j$ -line  $\mathcal{A}_1 \subset \text{Proj } \mathbb{Q}[A, B]$  has degree twelve and is given by*

$$(A, B) = (A(a, b, s, t), B(a, b, s, t)). \quad (2-8)$$

The formula  $y^2 = x^3 + A(a, b, s, t)x + B(a, b, s, t)$  gives the universal elliptic curve  $X(s, t)$  over  $\mathcal{A}_{a,b}$ .

The discriminant locus  $\mathcal{Z}_{a,b}$  is given by the vanishing of the discriminant

$$\Delta(A, B) = \Delta(a, b)\delta(a, b, s, t)^3/27, \quad \delta(a, b, s, t) = 3s^4 + 6as^2t^2 + 12bst^3 - a^2t^4. \quad (2-9)$$

It thus consists of four geometric points. Comparing with (2-2), one sees that these points are permuted by  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  according to the projective mod 3 representation into  $\text{PGL}_2(\mathbb{F}_3) \cong S_4$ . [Theorem 1](#) has a direct analog for the covers  $\mathcal{A}_{a,b}^* \rightarrow \mathcal{A}_1$ .

**2.7. Finding  $(s, t)$ .** Let  $X : y^2 = x^3 + ax + b$  and  $Y : y^2 = x^3 + Ax + B$  be elliptic curves over  $\mathbb{Q}$  with isomorphic 3-torsion. Then, in contrast with the analogous situation for the genus two case described in [Section 3.7](#), it is very easy to find associated  $(s, t) \in \mathbb{Q}^2$ . Namely, (2-8) and its analog  $(A, B) = (A^*(a, b, s, t), B^*(a, b, s, t))$  each have twenty-four solutions in  $\mathbb{C}^2$ . One just extracts the rational ones, say by eliminating  $s$  and factoring the resulting degree twenty-four polynomials  $f(t)$  and  $f^*(t)$ . If the image of  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  is all of  $\text{GSp}_2(\mathbb{F}_3) = \text{GL}_2(\mathbb{F}_3)$ , then one of these polynomials factors as  $1 + 1 + 6 + 8 + 8$  and the other as  $12 + 12$ . The two 1's correspond to the desired solutions  $\pm(s, t)$ .

Discriminants are useful in distinguishing the two moduli spaces as follows. If  $Y$  has the form  $X(s, t)$  then  $\Delta_X/\Delta_Y$  is a perfect cube by (2-9). If it has the form  $X^*(s, t)$  then  $\Delta_X\Delta_Y$  is a perfect cube by the starred analog of (2-9). These implications determine a unique space on which  $Y$  represents a point unless  $\Delta_X$  and  $\Delta_Y$  are both perfect cubes. Since  $x^3 - \Delta$  is a resolvent cubic of the octic (2-3), this ambiguous case arises if and only if the image  $\Gamma$  of  $\bar{\rho}_X$  has order dividing 16.

As an example, let  $(a, b) = (-1, 0)$  so that  $X$  has conductor  $2^5$  and discriminant  $2^6$ . Let  $(A, B) = (-27, -162)$  so that  $Y$  has conductor  $2^5 3^3$  and discriminant  $-2^9 3^9$ . The octic polynomials  $F(a, b, z)$  and  $F(A, B, z)$  define the same field because under *Pari's* `polredabs` they each become  $z^8 + 6z^4 - 3$ .



This polynomial has Galois group of order 16. The procedure in the first paragraph yields solutions only in the starred case, these being  $(s, t) = \pm(-\frac{1}{2}, \frac{3}{2})$ .

An elliptic curve  $Y$  can give rise to a point on both moduli spaces constructed from  $X$  if and only if the two moduli spaces coincide. The spaces coincide exactly when there is an equivariant isomorphism  $(X[3], \wedge) \simeq (X[3], -\wedge)$  where  $\wedge$  is the Weil pairing. Such an isomorphism exists if and only if  $X[3]$  is either a twist of  $\bar{\rho}_0 = \mathbb{Z}/3\mathbb{Z} \oplus \mu_3$  or when  $X[3]$  is irreducible but not absolutely irreducible. (The latter occurs precisely when the image factors through the nonsplit Cartan subgroup  $\mathbb{F}_9^\times$  and has order  $> 2$ ; this case does not arise over  $\mathbb{Q}$ .) An instance over  $\mathbb{Q}$  is  $X = Y$  coming from  $(a, b) = (5805, -285714)$  which is the modular curve  $X_0(14)$  of genus one and discriminant  $-2^{18}3^{12}7^3$ ; here  $(s, t) = \pm(1, 0)$  in the main case and  $2^63^47^2(s, t) = \pm(435, 11)$  in the starred case.

### 3. Abelian surfaces with fixed 3-torsion

In this section, we present our main theorem on abelian surfaces with fixed 3-torsion. We are brief on parts of the derivation which closely follow steps described in the previous section, and concentrate on steps which have a new feature.

**3.1. Weierstrass curves and their 3-torsion.** By a *Weierstrass curve* in this paper we will mean a genus two curve together with a distinguished Weierstrass point. Placing this marked point at infinity and shifting the variable  $x$ , one can always present a Weierstrass curve via the affine equation (1-1), which we call a *Weierstrass equation*. Replacing  $(a, b, c, d)$  by  $(u^4a, u^6b, u^8c, u^{10}d)$  yields an isomorphic Weierstrass curve via the compensating change  $(x, y) \mapsto (u^2x, u^5y)$ . The standard discriminant of the genus two curve (1-1) is  $\Delta(a, b, c, d) = \Delta = 2^8\Delta_{\text{poly}}$ , where  $\Delta_{\text{poly}}$  is the discriminant of the quintic polynomial on the right of (1-1). It is best for our purposes to give the parameters  $a, b, c$ , and  $d$  weights 12, 18, 24, and 30. In this system,  $\Delta$  is homogeneous of weight 120. The (coarse) moduli space of Weierstrass curves  $\mathcal{M}_2^w$  is then the complement of the hypersurface  $\Delta = 0$  in the weighted projective space  $\mathbb{P}^3(12, 18, 24, 30) = \mathbb{P}^3(2, 3, 4, 5)$ . As explained at the end of Section 1.2, rather than describing moduli spaces mapping to  $\mathcal{A}_2$ , we will be describing their base changes to  $\mathcal{M}_2^w$ .

The group law in terms of effective divisors on the Jacobian of a general genus two curve  $X : y^2 = f(x)$  yields a classical  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ -equivariant bijection [CF96] from the nonzero 3-torsion points to decompositions of the form

$$f(x) = (b_4x^3 + b_3x^2 + b_2x + b_1)^2 - b_7(x^2 + b_6x + b_5)^3.$$

In the quintic case of (1-1), one has  $b_4^2 = b_7$ . The minimal polynomial of  $b_4^{-2}$  is a degree 40 polynomial  $p_{40}$  such that  $p_{40}(x^2)$  describes the 3-torsion representation of  $X$ .

In our reflection group approach, it is actually  $p_{40}(z^6)$  which appears naturally. It has 1673 terms and begins as

$$\begin{aligned} F(a, b, c, d, z) = & z^{240} + 15120az^{228} + 2620800bz^{222} - 504(70227a^2 - 831820c)z^{216} \\ & - 1965600(2529ab - 33550d)z^{210} + \dots \quad (3-1) \end{aligned}$$



The splitting field of  $F(a, b, c, d, z)$  is the compositum of the splitting fields of  $p_{40}(x^2)$  and  $x^3 - \Delta$ . In particular, having chosen a *Weierstrass equation*, the field  $E(\Delta^{1/3})$  remains constant throughout our family of Weierstrass equations, even though  $E(\Delta^{1/3})$  is *not* determined by the 3-torsion representation. On the other hand, the change of coordinates  $(x, y) \mapsto (u^2x, u^5y)$  maps  $\Delta$  to  $u^{40}\Delta$ , and so this auxiliary choice places no restrictions on the *Weierstrass curves* which can occur in the family. In contrast, when  $g = 1$ , the field  $E(\Delta^{1/3})$  also remains constant, but in this case it *is* determined by the 3-torsion representation as it is the fixed field of the 2-Sylow of the image of  $\text{Gal}(\bar{\mathbb{Q}}/E)$  in  $\text{Sp}_2(\mathbb{F}_3)$ .

**3.2.  $\text{Sp}_4(\mathbb{F}_3)$  and related groups.** Define  $g_1, g_2, g_3$ , and  $g_4$  to be

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \omega & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} \alpha & -\bar{\alpha} & -\bar{\alpha} & 0 \\ -\bar{\alpha} & \alpha & -\bar{\alpha} & 0 \\ -\bar{\alpha} & -\bar{\alpha} & \alpha & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \omega & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} \alpha & \bar{\alpha} & 0 & \bar{\alpha} \\ \bar{\alpha} & \alpha & 0 & -\bar{\alpha} \\ 0 & 0 & 1 & 0 \\ \bar{\alpha} & -\bar{\alpha} & 0 & \alpha \end{pmatrix}, \quad (3-2)$$

where  $\alpha = \omega/\sqrt{-3}$ . Define

$$H = \langle g_1, g_2, g_3 \rangle \quad \text{and} \quad G = \langle g_1, g_2, g_3, g_4 \rangle.$$

The matrices  $g_i$  are all complex reflections of order 3, and they are exactly the matrices given in [ST54, 10.5]. As with  $H = C_3$  and  $G = \text{ST } 4 = \text{Sp}_2(\mathbb{F}_3)$  of the last section, the new groups  $H = \text{ST } 25$  and  $G = \text{ST } 32$  are also complex reflection groups. The group  $G$  has the structure  $C_3 \times \text{Sp}_4(\mathbb{F}_3)$  and it is the extra  $C_3$  that is the reason that  $\Delta$  behaves differently in the two cases.

Again numeric identities guide polynomial calculations as we discussed around Table 1. For example, orders are products of degrees of fundamental invariants. Analogous to the old cases  $|C_3| = 3$  and  $|\text{Sp}_2(\mathbb{F}_3)| = 4 \cdot 6$ , the new cases are  $|H| = 6 \cdot 9 \cdot 12$  and  $|G| = 12 \cdot 18 \cdot 24 \cdot 30$ . Thus again the index  $|G|/|H| = 240$  matches the degree of the main polynomial (3-1). The character table of  $G$  has size  $102 \times 102$ , so we certainly will not present the analog of Table 1. The most important information is that the degrees in which co- and contravariants live, previously 1, 3 and 3, 5, are now 1, 7, 13, 19 and 11, 17, 23, 29 for  $G$ .

**3.3. Rings of invariants.** One has the rationality condition  $g_i^2 = \bar{g}_i$  for all four  $i$ , allowing us again to interpret  $H$  and  $G$  as  $E$ -points of group schemes  $\underline{H}$  and  $\underline{G}$  over  $\mathbb{Q}$ . The matrices  $g_i$  together give an action of  $\underline{G}$  on  $\mathbb{Q}[z_1, z_2, z_3, z_4]$ . The variable  $z = z_4$  plays a role which is different from the other  $z_i$ .

Define, following [Hun96, 4.72],

$$\begin{aligned} p &= z_1^6 + z_2^6 + z_3^6 - 10(z_2^3 z_3^3 + z_2^3 z_1^3 + z_3^3 z_1^3), \\ q &= (z_1^3 - z_2^3)(z_2^3 - z_3^3)(z_3^3 - z_1^3), \\ r &= (z_1^3 + z_2^3 + z_3^3)[(z_1^3 + z_2^3 + z_3^3)^3 + 216z_1^3 z_2^3 z_3^3]. \end{aligned}$$

Also define  $a, b, c$ , and  $d$  by taking  $(2^4 3^7 5a, 2^6 3^9 5^2 b, 2^8 3^{12} 5^3 c, 2^{10} 3^{16} 5^5 d)$  to be

$$\begin{aligned}
& (-p^2 - 5r + 1320qz^3 - 132pz^6 - 6z^{12}, \\
& p^3 - 400q^2 - 5pr - 680pqz^3 + 323p^2z^6 - 255rz^6 - 7480qz^9 + 68pz^{12} - 4z^{18}, \\
& 2p^4 - 800pq^2 - 5p^2r + 320p^2qz^3 - 3000qz^3 - 722p^3z^6 + 175200q^2z^6 + 990prz^6 + 33040pqz^9 \\
& \quad - 953p^2z^{12} + 3495rz^{12} + 15720qz^{15} + 268pz^{18} - 3z^{24}, \\
& 13p^5 - 6000p^2q^2 - 25p^3r + 21600p^3qz^3 - 9600000q^3z^3 - 45000pqrz^3 + 11790p^4z^6 - 4572000pq^2z^6 \\
& \quad - 37575p^2rz^6 + 28125r^2z^6 - 247200p^2qz^9 - 945000qz^9 + 37155p^3z^{12} + 234000q^2z^{12} \\
& \quad - 150075prz^{12} - 214200pqz^{15} + 30855p^2z^{18} - 143775rz^{18} + 354600qz^{21} + 2340pz^{24} - 12z^{30}).
\end{aligned}$$

Because  $H$  and  $G$  are complex reflection groups, the rings of invariants are freely generated, explicit formulas being

$$\mathbb{Q}[z_1, z_2, z_3, z]^H = \mathbb{Q}[p, q, r, z], \quad \mathbb{Q}[z_1, z_2, z_3, z]^G = \mathbb{Q}[a, b, c, d].$$

When one removes  $p, q, r$  from the equations defining  $a, b, c, d$ , one gets exactly the degree 240 equation (3-1) for  $z$ .

**3.4. Covariants and contravariants.** As mentioned before, group-theoretic calculations like those in Table 1 say that covariants lie in degrees 1, 7, 13, and 19. Formulas for  $H$ -invariant covariants in these degrees are

$$\begin{aligned}
\alpha_1 &= z, \quad 2^2 3^3 5 \alpha_7 = 7pz - 3z^7, \quad 2^4 3^6 \alpha_{13} = (11r - 3p^2)z + 216qz^4 + 72pz^7, \\
2^4 3^{10} \alpha_{19} &= (p^3 - pr - 468q^2)z - 24pqz^4 + (66r - 6p^2)z^7 - 288qz^{10} - 12pz^{13}.
\end{aligned}$$

Here, unlike in the genus one case, there is an ambiguity beyond multiplying by a nonzero scalar. Namely rather than working with  $\alpha_{13}$  we could work with any linear combination of  $a\alpha_1$  and  $\alpha_{13}$  that involves  $\alpha_{13}$  nontrivially. Similarly we could replace  $\alpha_{19}$  by  $c_1 b \alpha_1 + c_7 a \alpha_7 + c_{19} \alpha_{19}$  for any nonzero  $c_{19}$ . The choices involved in picking particular contravariants  $\beta_k$  mirror the choices involved in picking  $\alpha_{k-10}$ . Our choice of  $(\beta_{11}, \beta_{17}, \beta_{23}, \beta_{29})$  is given in the online supplement. Just as in Section 2.4, the contravariants  $\beta_k$  can be described in terms of partial derivatives of the invariants. To be precise, we take  $(\beta_{11}, \beta_{17}, \beta_{23}, \beta_{29}) = (\partial_z a, \partial_z b, \partial_z c, \partial_z d)$ .

**3.5. New coefficients.** Each covariant element  $\alpha_d$  is the last entry of a uniquely determined covariant tuple  $l_d$  of length 4 defining an equivariant map  $\mathbb{Q}[z_1, z_2, z_3, z]_1 \rightarrow \mathbb{Q}[z_1, z_2, z_3, z]_d$ . By evaluating the invariants  $a, b, c, d$  at the general covariant tuple i.e., by setting  $(z_1, z_2, z_3, z) = s \cdot l_1 + t \cdot l_7 + u \cdot l_{13} + v \cdot l_{19}$ , one can theoretically obtain the new coefficients. For computational reasons, we instead follow the matrix approach as stated in Section 2.5.

Our key computation takes place in the algebra  $\mathbb{Q}[p, q, r, z]$  of  $H$ -invariants viewed as a graded module over the algebra  $\mathbb{Q}[a, b, c, d]$  of  $G$ -invariants. As a graded basis we use  $p^i q^j r^k z^l$  with  $0 \leq i, j, k < 2$  and  $0 \leq l < 30$ . Repeatedly using the vector equation in Section 3.3, we expand the products

$$\alpha_e p^i q^j r^k z^l = \sum_{I, J, K, L} M(e)_{I, J, K, L}^{i, j, k, l} p^I q^J r^K z^L$$

to represent the covariants  $\alpha_e$  as 240-by-240 matrices  $M(e)$  with entries in  $\mathbb{Q}[a, b, c, d]$ . The general covariant

$$Z = s\alpha_1 + t\alpha_7 + u\alpha_{13} + v\alpha_{19} \quad (3-3)$$

satisfies the characteristic polynomial of  $M = sM(1) + tM(7) + uM(13) + vM(19)$ . In other words,  $Z$  satisfies a degree 240 polynomial equation

$$F(A, B, C, D, Z) = Z^{240} + c_2 Z^{228} + c_3 Z^{222} + c_4 Z^{216} + c_5 Z^{210} + \dots = 0$$

with  $F$  from (3-1). We need to calculate  $A, B, C, D$  in terms of the free parameters  $a, b, c, d, s, t, u$ , and  $v$ . Define normalized traces  $\tau_n$  by

$$6\tau_n = \text{Tr}(M^{6n}) = \sum_{i+j+k+l=6n} \binom{6n}{i, j, k, l} s^i t^j u^k v^l \text{Tr}(M(1)^i M(7)^j M(13)^k M(19)^l).$$

Because the first trace  $\tau_1$  is 0, standard symmetric polynomial formulas simplify, giving  $(c_2, c_3, c_4, c_5) = (-\tau_2/2, \tau_3/3, \tau_2^2/8 - \tau_4/4, \tau_2\tau_3/6 - \tau_5/5)$ . Then (3-1) yields

$$(A, B, C, D) = \left( \frac{-\tau_2}{30240}, \frac{-\tau_3}{7862400}, \frac{3667\tau_2^2 - 5600\tau_4}{9390915072000}, \frac{2521\tau_2\tau_3 - 2688\tau_5}{886312627200000} \right). \quad (3-4)$$

The matrices  $M^k$  have entries in  $\mathbb{Q}[a, b, c, d, s, t, u, v]$  and for  $k = 1, \dots, 6$  they take approximately 2, 10, 40, 125, 300, and 675 megabytes to store. The matrix  $M^6$  suffices to determine  $A$  because the evaluation of  $\text{Tr}(M^{12}) = \text{Tr}(M^6 \cdot M^6)$  does not require the full matrix multiplication on the right. However we would not be able to continue in this way to the needed  $M^{15}$ . In contrast, the  $M(e)$  have entries only in  $\mathbb{Q}[a, b, c, d]$  and take less space to store. The worst of the  $M(e)^j$  that we actually use in the above expansion is  $M(19)^{15}$ , which requires about 210 megabytes to store. By getting the terms in smaller batches and discarding matrix products when no longer needed, we can completely compute all of  $A, B, C$ , and  $D$  without memory overflow. In principle, one could repeat everything in the contravariant case, although here the initial matrix  $M^*$  takes twice as much space to store as  $M$ .

The polynomials  $A, B, C$ , and  $D$  have respectively degrees 12, 18, 24, and 30 in  $s, t, u$ , and  $v$ . Also, assign weights (12, 18, 24, 30,  $-1, -7, -13, -19$ ) to  $(a, b, c, d, s, t, u, v)$ . Then all four polynomials are homogeneous of weight zero. The bigradation allows  $A, B, C$ , and  $D$  to have 14671, 112933, 515454, and 1727921 terms respectively. With our choice of  $\alpha_{13}$  and  $\alpha_{19}$ , respectively 67, 170, 100, and 824 of these terms vanish, so  $A, B, C$ , and  $D$  have the number of terms reported in the introduction. Not only do the polynomials have many terms, but the coefficients can have moderately large numerators. The largest absolute value of all the numerators is achieved by the term

$$2^{30} \cdot 3^3 \cdot 5^{23} \cdot 1381131815224116413 \cdot a^3 b c^5 d^{10} u^{16} v^{14}$$

in  $D$ . On the another hand, denominators of the coefficients in  $A, B, C$ , and  $D$  always divide 5,  $5^2$ ,  $5^3$ , and  $5^5$  respectively.

**3.6. Geometric summary.** We now summarize our results in the following theorem. The  $\bar{\rho}$  of [Section 1.2](#) is the mod 3 representation of the initial genus two curve (1-1). So, to be more explicit, we write  $\mathcal{M}_{a,b,c,d} = \mathcal{M}_2^w(\bar{\rho})$  below.

**Theorem 2.** Fix an equation  $y^2 = x^5 + ax^3 + bx^2 + cx + d$  defining a curve  $X$  over  $\mathbb{Q}$ . Let  $\mathcal{M}_{a,b,c,d}$  be the moduli space of pairs  $(Y, i)$  with  $Y$  a Weierstrass curve and  $i : \text{Jac}(X)[3] \rightarrow \text{Jac}(Y)[3]$  a symplectic isomorphism on the 3-torsion points of their Jacobians. Then  $\mathcal{M}_{a,b,c,d}$  can be realized as the complement of a discriminant locus  $\mathcal{Z}_{a,b,c,d}$  in the projective three-space  $\text{Proj } \mathbb{Q}[s, t, u, v]$ . The covering maps to the moduli space  $\mathcal{M}_2^w \subset \text{Proj } \mathbb{Q}[A, B, C, D]$  have degree 25920 and are given by

$$(A, B, C, D) = (A(a, \dots, v), B(a, \dots, v), C(a, \dots, v), D(a, \dots, v)). \quad (3-5)$$

The formula

$$y^2 = x^5 + A(a, \dots, v)x^3 + B(a, \dots, v)x^2 + C(a, \dots, v)x + D(a, \dots, v) \quad (3-6)$$

gives the universal Weierstrass curve  $X(s, t, u, v)$  over  $\mathcal{M}_{a,b,c,d}$ .

The discriminant locus  $\mathcal{Z}_{a,b,c,d}$  is given by the vanishing of the discriminant

$$\Delta(A(a, \dots, v), \dots, D(a, \dots, v)) = \Delta(a, b, c, d)\delta(a, b, c, d, s, t, u, v)^3. \quad (3-7)$$

where  $\delta$  is homogeneous of degree 40 in  $s, t, u, v$ . Geometrically,  $\mathcal{Z}_{a,b,c,d}$  is the union of forty planes and these planes are permuted by  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  according to the roots of  $p_{40}$  from the end of [Section 3.1](#). While the fibers of  $\mathcal{M}_{a,b,c,d}$  over  $\mathcal{M}_2^w$  are projective spaces, the entire space defines a nontrivial projective bundle which can be determined explicitly from our equations in terms of  $\text{Pic}(\mathcal{M}_2^w)$  (for more details, see the blog post [\[Cal20\]](#), in particular the comments of Najmuddin Fakhruddin). In principle, [Theorem 2](#) has a direct analog for  $\mathcal{M}_{a,b,c,d}^* \rightarrow \mathcal{M}_2^w$ . The [online supplement](#) only gives the starred coefficients evaluated at  $(a, b, c, d, 1, 0, 0, 0)$ , as this is sufficient for moving from one moduli space to the other.

**3.7. Finding  $(s, t, u, v)$ .** Let  $X$  and  $Y$  be Weierstrass curves over  $\mathbb{Q}$  having isomorphic 3-torsion and given by coefficient sequences  $(a, b, c, d)$  and  $(A, B, C, D)$  respectively. Then finding associated rational  $(s, t, u, v)$  is both theoretically and computationally more complicated than in the genus one case of [Section 2.7](#).

As in the genus one case, for (3-5) to have a solution, the ratio  $\Delta_X/\Delta_Y$  must be a perfect cube by (3-7). Similarly, for the starred version of (3-5) to have a solution the product  $\Delta_X\Delta_Y$  must be a perfect cube. The theoretical complication was introduced at the end of [Section 3.1](#): the class modulo cubes of the discriminant now depends on the model via  $\Delta(u^4A, u^6B, u^8C, u^{10}D) = u^{40}\Delta(A, B, C, D)$ . So as a preparatory step one needs to adjust the model of  $Y$  to some new  $(A, B, C, D)$  before seeking solutions to (3-5), and also to some typically different  $(A^*, B^*, C^*, D^*)$  before seeking solutions to the starred analog of (3-5).

Having presented  $Y$  properly, one then encounters the computational problem. Namely both (3-5) and its starred version have 155520 solutions  $(s, t, u, v) \in \mathbb{C}^4$ , and so one cannot expect to find the rational

ones by algebraic manipulations. Working numerically instead, one gets 240 solutions  $(p, q, r, z) \in \mathbb{C}^4$  to the large vector equation in [Section 3.3](#). Eight of these solutions are in  $\mathbb{R}^4$ . These vectors yield eight vectors  $(\alpha_1, \alpha_7, \alpha_{13}, \alpha_{19}) \in \mathbb{R}^4$  from the covariants in [Section 3.4](#), and also eight vectors  $(\beta_{11}, \beta_{17}, \beta_{23}, \beta_{29}) \in \mathbb{R}^4$ . Let  $Z$  and  $Z^*$  respectively run over the eight real roots of  $F(A, B, C, D, U)$  and  $F(A^*, B^*, C^*, D^*, U)$ . Then one can apply the LLL algorithm to find low height relations of the form [\(3-3\)](#) and its starred variant

$$Z^* = s\beta_{11} + t\beta_{17} + u\beta_{23} + v\beta_{29}.$$

When the image of  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  on 3-torsion is sufficiently large then there will just be a single pair of solutions  $\pm(s, t, u, v)$  from the eight equations of one type and none from the other eight equations. The [online supplement](#) provides a *Mathematica* program `findisos` to do all steps at once. Examples are given in [Sections 4.2](#) and [4.3](#).

## 4. Complements

The four subsections of this section can be read independently.

**4.1. A matricial identity.** The polynomials  $A, B, C$ , and  $D$  in [Theorem 2](#) satisfy the matricial identity

$$\mathcal{E}(A(a, \dots, v), B(a, \dots, v), C(a, \dots, v), D(a, \dots, v), S, T, U, V) = \mathcal{E}(a, b, c, d, M(S, T, U, V)^t),$$

where  $\mathcal{E}$  can be any one of  $A, B, C, D$ , and  $M$  is a  $4 \times 4$  matrix with entries in  $\mathbb{Q}[a, b, c, d, s, t, u, v]$  whose first column is  $(s, t, u, v)^t$ . The columns of  $M$  are homogeneous of degrees 1, 7, 13, 19 in  $s, t, u, v$ , and the rows are homogeneous of degrees  $-1, -7, -13, -19$  with respect to the weights assigned in [Section 3.5](#).

The situation in the  $g = 1$  case is analogous but enormously simpler:

$$\begin{aligned} A(A(a, b, s, t), B(a, b, s, t), S, T) &= A(a, b, M(S, T)^t), \\ B(A(a, b, s, t), B(a, b, s, t), S, T) &= B(a, b, M(S, T)^t), \end{aligned} \quad M = \begin{pmatrix} s & -as^2t - 3bst^2 + a^2t^3/3 \\ t & s^3 + ast^2 + bt^3 \end{pmatrix}$$

Here, as is visible, columns of  $M$  have degrees 1 and 3 in  $s, t$ , while rows have weights  $-1$  and  $-3$  with respect to the weights assigned in [Section 2.5](#). The second column is in fact proportional to  $[-\partial_t \delta, \partial_s \delta]^t$ , where  $\delta$  is as in [\(2-9\)](#). Hence  $M$  is the matrix found in Lemma 8.4 of [\[Fis12\]](#), up to rescaling of the columns.

The identities say that changing the initial Weierstrass curve to a different one in  $\mathcal{M}_{a,b,c,d}$  has the effect of changing the parametrization of the family through a linear transformation  $M$  of the covariants. In fact, our first method of calculating the quantities  $\mathcal{E}(a, \dots, v)$  exploited this ansatz. Starting from a few curves with  $a = b = 0$ , computing covariants numerically, and changing bases so as to meet the bigradation conditions of [Section 3.5](#), we obtained the polynomials  $\mathcal{E}(0, 0, c, d, s, t, u, v)$ . We then examined the matricial identity with  $a = b = 0$ . Comparing certain monomial coefficients, we determined the second column of  $M$  precisely, the third column up to one free parameter, and the fourth column up to two free parameters. This corresponds to the ambiguity in the covariants in degrees 13 and 19

described in [Section 3.4](#). Once a choice of  $M$  was made, comparing coefficients again and solving the resulting linear equations determined the polynomials  $\mathcal{E}(a, \dots, v)$  completely.

**4.2. Examples involving Richelot isogenies.** Let  $X$  and  $Y$  be Weierstrass curves and let  $I : \text{Jac}(X) \rightarrow \text{Jac}(Y)$  be an isogeny with isotropic kernel of type  $(m, m)$  with  $m$  prime to 3. Then  $I$  induces an isomorphism  $\iota : \text{Jac}(X)[3] \rightarrow \text{Jac}(Y)[3]$  which is symplectic if  $m \equiv 1(3)$  and antisymplectic if  $m \equiv 2(3)$ . In the following examples,  $m = 2$ .

Let  $X_{e,f,g}$  be defined by (1-1) with

$$(a, b, c, d) = (-5(7e^2 - 2f), -10e(3e^2 - 2f), 5(32e^4 - 39e^2f + g), -4e(24e^4 + 115e^2f - 5g)).$$

The discriminant of  $X_{e,f,g}$  is

$$\Delta_X = -2^{12}5^5(125e^4 + 20f^2 - 4g)^2(25e^2f - g)(25e^2f + g)^2.$$

Define  $Y_{e,f,g}$  to be the quadratic twist by 2 of  $X_{e,-f,g}$ . The form of  $(a, b, c, d)$  has been chosen so that there is a Richelot isogeny from  $\text{Jac}(X_{e,f,g})$  to  $\text{Jac}(Y_{e,f,g})$ .

Let  $\bar{\cdot}$  be the involution of  $\mathbb{Q}[e, f, g]$  given by  $(\bar{e}, \bar{f}, \bar{g}) = (e, -f, g)$ . To make  $\Delta_X \Delta_Y$  a cube and avoid denominators in  $(s, t, u, v)$ , present  $Y_{e,f,g}$  via

$$(A, B, C, D) = (\bar{a}z^2, \bar{b}z^3, \bar{c}z^4, \bar{d}z^5)$$

with

$$z = 2^35^4(125e^4 + 20f^2 - 4g)^4(25e^2f + g)^6.$$

Applying the numeric method of [Section 3.7](#) and interpolating strongly suggests

$$(s, t, u, v) = \pm(-4e(80e^4 + 7e^2f - g), 2(40e^4 - 9e^2f - g), -4e(5e^2 + 2f), 5e^2 + 2f).$$

Specializing the contravariant matrix  $M(a, b, c, d, s, t, u, v)^*$  of [Section 3.5](#) to  $M(e, f, g)^*$  allows direct computation of its powers up through the needed fifteenth power. Applying (3-4) indeed recovers  $(A, B, C, D)$  so that the interpolation was correct.

The examples of this subsection are already much simpler than the general case with its millions of terms. For a smaller family of even simpler examples, now with all mod 3 representations nonsurjective, one can set  $e = 0$ . Then  $b, d, B, D, s$ , and  $u$  are all 0, while  $a, c, A, C, t$ , and  $v$  are given by tiny formulas.

**4.3. Explicit families of modular abelian surfaces.** Our main theorem gives a process by which modularity of a genus two curve can be transferred to modularity of infinitely many other genus two curves.

**Corollary 3.** *Suppose the genus two curve  $X : y^2 = x^5 + ax^3 + bx^2 + cx + d$  has good reduction at 3, and assume that  $A = \text{Jac}(X)$  satisfies all the conditions of [BCGP18, Propositions 10.1.1 and 10.1.3], so that  $X$  is modular. Then all the curves  $X(s, t, u, v)$  or  $X^*(s, t, u, v)$  having good reduction at 3 are also modular.*

The conclusion follows simply because the hypotheses imply that the new Jacobians also satisfy the conditions of [BCGP18, Propositions 10.1.1, and 10.1.3] and are thus modular. In particular, for any  $(s, t, u, v) \in \mathbb{P}^3(\mathbb{Q})$  reducing to  $(1, 0, 0, 0) \in \mathbb{P}^3(\mathbb{F}_3)$ , the curves  $X$  and  $X(s, t, u, v)$  are identical modulo 3 and therefore  $X(s, t, u, v)$  is modular.

The hypotheses of [BCGP18, Propositions 10.1.1 and 10.1.3] include that the mod 3 representation  $\bar{\rho}$  is not surjective. The easiest way to satisfy the hypotheses is to look among  $X$  for which the geometric endomorphism ring of  $\text{Jac}(X)$  is larger than  $\mathbb{Z}$ . One such  $X$ , appearing in [CCG20, Example 3.3], is given by

$$(a, b, c, d) = \left( \frac{12}{5}, \frac{12}{5^2}, \frac{292}{5^3}, -\frac{3672}{5^5} \right),$$

having arisen from the simple equation  $y^2 = (x^2 + 2x + 2)(x^2 + 2)x$ . This curve has conductor  $2^{15}$  and discriminant  $\Delta_X = 2^{23}$ . Applying the corollary, one gets infinitely many modular genus two curves  $X(s, t, u, v)$ . For generic parameters, the geometric endomorphism ring of  $\text{Jac}(X(s, t, u, v))$  is just  $\mathbb{Z}$ .

It is much harder to directly find curves  $Y$  satisfying the hypotheses of [BCGP18, Propositions 10.1.1 and 10.1.3] and also satisfying  $\text{End}_{\bar{\mathbb{Q}}}(\text{Jac}(Y)) = \mathbb{Z}$ . A short list was found in [CCG20]. The curve  $Y$  in Example 3.3 there has

$$(A, B, C, D) = \left( \frac{2^7}{5}, \frac{2^{11} \cdot 57}{5^2}, -\frac{2^{12} \cdot 503}{5^3}, \frac{2^{17} \cdot 17943}{5^5} \right)$$

and comes from the simple equation  $y^2 = (2x^4 + 2x^2 + 1)(2x + 3)$ . It has conductor  $2^{15}5$  and Example 3.3 also observes that its 3-torsion is isomorphic to that of  $X$ .

While  $Y$  was found in [CCG20] via an *ad hoc* search, it now appears as just one point in an infinite family. To see this explicitly, note that  $\Delta_Y = 2^{83}5^6$  so that  $\Delta_Y/\Delta_X$  is a perfect cube. Numerical computation as in Section 3.7 followed by algebraic verification yields

$$Y = X\left(\frac{129}{125}, \frac{11}{25}, \frac{3}{100}, \frac{1}{20}\right).$$

If this procedure had failed, we would have found the proper  $X^*(s, t, u, v)$  by dividing  $(A, B, C, D)$  by  $(2^4, 2^6, 2^8, 2^{10})$  to make  $\Delta_X \Delta_Y$  a cube.

**4.4. Analogs for  $p = 2$ .** Complex reflection groups also let one respond to the problem of the introduction for residual prime  $p = 2$  and dimensions  $g = 2, 3$ , and 4 via descriptions of moduli spaces related to  $\mathcal{A}_g(\bar{\rho})$ . A conceptual simplification is that since  $p = 2$  one does not have the second collection of spaces  $\mathcal{A}_g^*(\bar{\rho})$ . Correspondingly, the relevant groups are actually reflection groups defined over  $\mathbb{Q}$ , so that covariants and contravariants coincide. The cases of dimension  $g = 3, 4$  make fundamental use of work of Shioda [Shi91].

We begin with the easiest case  $g = 2$ , because it shows clearly that our approach has classical roots in Tschirnhausen transformations. Greater generality would be possible by using the symmetric group  $S_6$ , but we describe things instead using  $S_5$  to stay in the uniform context of Weierstrass curves. Let  $\alpha_1$  be a



companion matrix of  $x^5 + ax^3 + bx^2 + cx + d$ . For  $j = 2, 3, 4$ , let  $\alpha_j = \alpha_1^j - k_j I$  where  $k_j$  is chosen to make  $\alpha_j$  traceless. Then the curve

$$y^2 = \det(xI - s\alpha_1 - t\alpha_2 - u\alpha_3 - v\alpha_4)$$

has the same 2-torsion as the original curve. From this fact follows a very direct analog of [Theorem 2](#), with the new  $\mathcal{M}_{a,b,c,d} \subset \text{Proj } \mathbb{Q}[s, t, u, v]$  now mapping to the same  $\mathcal{M}_2^w \subset \text{Proj } \mathbb{Q}[A, B, C, D]$  with degree 120. Carrying out this easy computation, the elements  $A, B, C$ , and  $D$  of  $\mathbb{Q}[a, b, c, d, s, t, u, v]$  respectively have 24, 86, 235, and 535 terms. Of course there is nothing special about degree 5, and the analogous computations in degrees  $2g + 1$  and  $2g + 2$  give statements about genus  $g$  hyperelliptic curves with fixed 2-torsion.

For  $g = 3$ , we work with the moduli space  $\mathcal{M}_3^q$  of smooth plane quartics which maps isomorphically to an open subvariety of  $\mathcal{A}_3$ . From the analog addressed in [\[CC20\]](#), we suspect that the varieties  $\mathcal{A}_3(\bar{\rho})$  are in general not rational. To place ourselves in a clearly rational setting, we work with the moduli space  $\mathcal{M}_3^f$  of smooth plane quartics with a rational flex. This change is analogous to imposing a rational Weierstrass point on a genus two curve, although now the resulting cover  $\mathcal{M}_3^f \rightarrow \mathcal{M}_3^q$  has degree twenty four. A quartic curve with a rational flex can always be given in affine coordinates by

$$y^3 + (x^3 + a_8x + a_{12})y + (a_2x^4 + a_6x^3 + a_{10}x^2 + a_{14}x + a_{18}) = 0. \quad (4-1)$$

Here the flex in homogeneous coordinates is at  $(x, y, z) = (0, 1, 0)$  and its tangent line is the line at infinity  $z = 0$ . Changing  $a_d$  to  $u^d a_d$  gives an isomorphic curve via  $(x, y) \mapsto (u^4 x, u^6 y)$ . The variety  $\mathcal{M}_3^f$  is the complement of a discriminant locus in the weighted projective space  $\text{Proj } \mathbb{Q}[a_2, \dots, a_{18}] = \mathbb{P}^6(2, \dots, 18)$ . The invariant theory of the reflection group  $\text{ST } 36 = W(E_7) = C_2 \times \text{Sp}_6(\mathbb{F}_2)$  gives polynomials  $A_i(a_2, \dots, a_{18}, s_{-1}, \dots, s_{-17})$  of degree  $i$  in the  $s_{-j}$  and total weight 0. Following the template of the previous cases, for fixed  $(a_2, \dots, a_{18})$  one has a six-dimensional variety  $\mathcal{M}_{a_2, \dots, a_{18}} \subset \text{Proj } \mathbb{Q}[s_{-1}, \dots, s_{-17}]$  parametrizing genus three curves with a rational flex and 2-torsion identified with that of [\(4-1\)](#). The covering maps  $\mathcal{M}_{a_2, \dots, a_{18}} \rightarrow \mathcal{M}_3^f$  now have degree  $|\text{Sp}_6(\mathbb{F}_2)| = 1451520$ . The number of terms allowed in  $A_i(a_2, \dots, a_{18}, s_{-1}, \dots, s_{-17})$  by the bigradation is the coefficient of  $x^i t^{19i}$  in

$$\prod_{d \in \{2, 6, 8, 10, 12, 14, 18\}} \frac{1}{(1 - t^d)(1 - x t^d)}. \quad (4-2)$$

For  $i = 18$ , this number is 11, 617, 543, 745, so complete computations in the style of this paper seem infeasible.

For  $g = 4$ , one needs to go quite far away from the 10-dimensional variety  $\mathcal{A}_4$  to obtain a statement parallel to the previous ones. Even the nine-dimensional variety  $\mathcal{M}_4$  is too large because for a generic genus four curve  $X$  corresponding to a point in  $\mathcal{M}_4$ , the image of  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  in its action on  $\text{Jac}(X)[2]$  is  $\text{Sp}_8(\mathbb{F}_2)$ , and this group is not a complex reflection group. However, one can work with the smooth curves

$$y^3 + (a_2x^3 + a_8x^2 + a_{14}x + a_{20})y + (x^5 + a_{12}x^3 + a_{18}x^2 + a_{24}x + a_{30}) = 0 \quad (4-3)$$



and a corresponding seven-dimensional moduli space  $\mathcal{M}_4^s \subset \mathbb{P}^7(2, \dots, 30)$ . For a generic curve in (4-3), the image of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  is the index 136 subgroup  $\text{O}_8^+(\mathbb{F}_2) : 2$  of  $\text{Sp}_8(\mathbb{F}_2)$ . Now from the invariant theory of the largest Shephard–Todd group  $\text{ST } 37 = W(E_8) = 2 \cdot \text{O}_8^+(\mathbb{F}_2) : 2$ , one gets polynomials  $A_i(a_2, \dots, a_{30}, s_{-1}, \dots, s_{-29})$  and covering maps  $\mathcal{M}_{a_2, \dots, a_{30}} \rightarrow \mathcal{M}_4^s$  of degree  $|\text{O}_8^+(\mathbb{F}_2) : 2| = 348, 364, 800$ . Aspects of this situation are within computational reach; for example Shioda computed the degree 240 polynomial  $F(a_2, \dots, a_{30}, z)$  analogous to (2-3) and (3-1). However the number of allowed terms in  $A_i(a_2, \dots, a_{30}, s_{-1}, \dots, s_{-29})$  is even larger than in the previous  $g = 3$  case, being the coefficient of  $x^i t^{31i}$  in the analog of (4-2) where  $d$  runs over  $\{2, 8, 12, 14, 18, 20, 24, 30\}$ . For  $i = 30$ , this number is 100, 315, 853, 630, 512. We close the paper with this  $W(E_8)$  case because it is here that the paper actually began: the polynomial (3-1) for our main case  $C_3 \times \text{Sp}_4(\mathbb{F}_3)$  is also the specialization  $F(0, 0, a_{12}, 0, a_{18}, 0, a_{24}, a_{30}, z)$  of Shioda’s polynomial.

### Acknowledgements

We thank Tom Fisher and the anonymous referees for corrections and other improvements.

### References

- [BCGP18] George Boxer, Frank Calegari, Toby Gee, and Vincent Pilloni, *Abelian Surfaces over totally real fields are potentially modular*, preprint, 2018. [arXiv 1812.09269](#)
- [BN18] Nils Bruin and Brett Nasserden, *Arithmetic aspects of the Burkhardt quartic threefold*, J. Lond. Math. Soc. (2) **98** (2018), no. 3, 536–556. [MR 3893190](#)
- [Cal20] Frank Calegari, *Picard groups of moduli stacks*, blog post (and comments), 2020, <https://tinyurl.com/FCalegariBlog>.
- [CC20] Frank Calegari and Shiva Chidambaram, *Rationality of twists of  $\mathcal{A}_2(3)$* , preprint, 2020. [arXiv 2009.00194](#)
- [CCG20] Frank Calegari, Shiva Chidambaram, and Alexandru Ghitza, *Some modular abelian surfaces*, Math. Comp. **89** (2020), no. 321, 387–394. [MR 4011548](#)
- [CF96] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2*, LMS Lecture Note Series, Cambridge University Press, 1996.
- [Che55] Claude Chevalley, *Invariants of finite groups generated by reflections*, Amer. J. Math. **77** (1955), 778–782. [MR 72877](#)
- [Fis12] Tom Fisher, *The Hessian of a genus one curve*, Proceedings of the London Mathematical Society **104** (2012), no. 3, 613–648.
- [HS02] Klaus Hulek and G. K. Sankaran, *The geometry of Siegel modular varieties*, Higher dimensional birational geometry (Kyoto, 1997), Adv. Stud. Pure Math., vol. 35, Math. Soc. Japan, Tokyo, 2002, pp. 89–156. [MR 1929793](#)
- [Hun96] Bruce Hunt, *The geometry of some special arithmetic quotients*, Lecture Notes in Mathematics, vol. 1637, Springer-Verlag, Berlin, 1996. [MR 1438547](#)
- [LR96] Joan-C. Lario and Anna Rio, *Elliptic modularity for octahedral Galois representations*, Math. Res. Lett. **3** (1996), no. 3, 329–342. [MR 1397682](#)
- [RS95] K. Rubin and A. Silverberg, *Families of elliptic curves with constant mod  $p$  representations*, Elliptic curves, modular forms, & Fermat’s last theorem (Hong Kong, 1993), Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995, pp. 148–161. [MR 1363500](#)
- [Shi91] Tetsuji Shioda, *Construction of elliptic curves with high rank via the invariants of the Weyl groups*, J. Math. Soc. Japan **43** (1991), no. 4, 673–719. [MR 1126145](#)
- [ST54] G. C. Shephard and J. A. Todd, *Finite unitary reflection groups*, Canad. J. Math. **6** (1954), 274–304. [MR 59914](#)

Received 23 Feb 2020. Revised 1 Sep 2020.

FRANK CALEGARI: [fcale@math.uchicago.edu](mailto:fcale@math.uchicago.edu)

*Department of Mathematics, The University of Chicago, Chicago, IL, United States*

SHIVA CHIDAMBARAM: [shivac@math.uchicago.edu](mailto:shivac@math.uchicago.edu)

*Department of Mathematics, The University of Chicago, Chicago, IL, United States*

DAVID P. ROBERTS: [roberts@morris.umn.edu](mailto:roberts@morris.umn.edu)

*Division of Science and Mathematics, University of Minnesota, Morris, MN, United States*

# Lifting low-gonal curves for use in Tuitman's algorithm

Wouter Castryck and Floris Vermeulen

Consider a smooth projective curve  $\bar{C}$  over a finite field  $\mathbb{F}_q$ , equipped with a simply branched morphism  $\bar{C} \rightarrow \mathbb{P}^1$  of degree  $d \leq 5$ . Assume  $\text{char } \mathbb{F}_q > 2$  if  $d \leq 4$ , and  $\text{char } \mathbb{F}_q > 3$  if  $d = 5$ . In this paper we describe how to efficiently compute a lift of  $\bar{C}$  to characteristic zero, such that it can be fed as input to Tuitman's algorithm for computing the Hasse–Weil zeta function of  $\bar{C}/\mathbb{F}_q$ . Our method relies on the parametrizations of low rank rings due to Delone and Faddeev, and Bhargava.

## 1. Introduction

About 20 years ago, Kedlaya published an influential paper [22], showing how one can employ Monsky–Washnitzer cohomology to efficiently compute Hasse–Weil zeta functions of hyperelliptic curves over finite fields having small odd characteristic. Its many follow-up works include several generalizations to geometrically larger classes of curves, first to superelliptic curves [18], then to  $C_{ab}$  curves [13] and then further to nondegenerate curves [6], i.e., smooth curves in toric surfaces. A more significant step was taken in 2016, when Tuitman [28; 29] published a Kedlaya-style algorithm that potentially covers arbitrary curves, and at the same time beats the methods from [6; 13] in terms of efficiency. Unfortunately, the user of Tuitman's algorithm is expected to provide a lift of the input curve to characteristic zero that meets the technical requirements from [29, Assumption 1]. Beyond nondegenerate curves, this is a nontrivial task. As a result, the exact range of applicability of Tuitman's method remains unclear.

A partial approach to lifting curves having gonality at most four was sketched in [7], with concrete details being limited to curves of genus five. In the current paper we present a different method, which is faster, works for curves of gonality at most five, and is much easier to implement. Concretely, we assume that we are given an absolutely irreducible curve over a finite field  $\mathbb{F}_q$  of characteristic  $p > 2$ , defined by a polynomial of the form

$$\bar{f}_d(x)y^d + \bar{f}_{d-1}(x)y^{d-1} + \cdots + \bar{f}_0(x) \in \mathbb{F}_q[x, y] \quad (1)$$

for some  $d \leq 5$ . Moreover, the morphism  $\bar{\varphi}$  from its nonsingular projective model  $\bar{C}$  to the projective line, induced by  $(x, y) \mapsto x$ , is assumed to be simply branched of degree  $d$ ; in other words, all fibers of

*MSC2010:* 11G20, 11Y99, 14Q05.

*Keywords:* point counting, Tuitman's algorithm, Delone–Faddeev correspondence, Bhargava correspondence.

$\bar{\varphi}$  should consist of either  $d - 1$  or  $d$  geometric points. Finally, if  $d = 5$  then it is assumed that  $p > 3$ . Then our method efficiently produces a lift satisfying the main requirement from [29, Assumption 1], which therefore can be fed as input to Tuitman’s algorithm, modulo [Heuristic H](#) discussed below.

In terms of moduli, the locus of genus  $g$  curves admitting a simply branched morphism to  $\mathbb{P}^1$  of degree at most 5 has dimension  $\min\{2g + 5, 3g - 3\}$  by a result of Segre [27]. For  $g = 6$  and  $g \geq 8$  this exceeds the locus of nondegenerate curves (and hence the locus of curves for which point counting was previously feasible) by four dimensions; see [10]. In particular, our lifting procedure applies to all sufficiently general curves of genus  $g \leq 8$ .

**Remark 1.1.** Expecting our curve to be given in the form (1) is essentially equivalent to assuming *knowledge* of an  $\mathbb{F}_q$ -rational degree  $d$  morphism  $\bar{C} \rightarrow \mathbb{P}^1$  that is simply branched, in contrast with the assumptions from [7]. If such a morphism to  $\mathbb{P}^1$  exists but is not known, then one can try to resort to methods due to Schicho, Schreyer and Weimann [24] or Derickx [14, Section 2.3] for finding one.

**Lifting strategy.** Write  $q = p^n$  and fix a degree  $n$  number field  $K$  in which  $p$  is inert. Let  $\mathcal{O}_K$  denote its ring of integers and identify  $\mathbb{F}_q$  with  $\mathcal{O}_K/(p)$ . To *lift* the curve  $\bar{C}$  means to produce a nonsingular projective curve  $C/K$  whose reduction mod  $p$  is isomorphic to  $\bar{C}/\mathbb{F}_q$ ; necessarily, the genus of  $C$  should be equal to that of  $\bar{C}$ . Our actual goal is to lift the morphism  $\bar{\varphi}$ , which means that we want to equip  $C$  with a morphism  $\varphi : C \rightarrow \mathbb{P}^1$  reducing to  $\bar{\varphi} : \bar{C} \rightarrow \mathbb{P}^1$  mod  $p$ , up to isomorphism. Our approach to solving this problem is based on the parametrization of low rank rings by Delone and Faddeev [17, Proposition 4.2], and Bhargava [2; 3], in combination with algorithms due to Hess for computing reduced bases [21]. In doing so, we will find concrete, typically nonplanar equations for  $\bar{C}$  over  $\mathbb{F}_q$  that have “free coefficients”, which can be lifted to  $\mathcal{O}_K$  naively,<sup>1</sup> in order to obtain a nonsingular projective curve  $C/K$  along with a morphism  $\varphi : C \rightarrow \mathbb{P}^1$  of the said kind. We refer to [Section 2](#) for a more elaborate discussion.

**Remark 1.2.** In general, the polynomial (1), which defines a plane curve that is birationally equivalent with  $\bar{C}$ , is not liftable directly: there may be many singularities, which typically disappear when lifting the coefficients of (1) naively to  $\mathcal{O}_K$ , causing an increase of the genus.

**Remark 1.3.** In Kedlaya’s original algorithm, corresponding to the case  $d = 2$ , an implicit first step is to rewrite (1) into Weierstrass form. Indeed, Weierstrass models have “free coefficients” that can be lifted naively to  $\mathcal{O}_K$ , always resulting in a hyperelliptic curve over  $K$  having the same genus. From now on we assume  $d \geq 3$ .

Through elimination of variables (i.e., projection) we then obtain a planar model of the form  $f_d(x)y^d + f_{d-1}(x)y^{d-1} + \cdots + f_0(x) = 0$ , for polynomials  $f_i \in \mathcal{O}_K[x]$  which, in general, do not reduce to  $\bar{f}_i$  mod  $p$ ; here, the lifted morphism  $\varphi$  again corresponds to  $(x, y) \mapsto x$ . The change of variables  $y \leftarrow y/f_d(x)$  yields a monic defining equation

$$Q(x, y) = y^d + f_{d-1}(x)y^{d-1} + \cdots + f_0(x)f_d(x)^{d-1}, \quad (2)$$

<sup>1</sup>Lifting  $\bar{a} \in \mathbb{F}_q \setminus \{0\}$  naively to  $\mathcal{O}_K$  means producing an element  $a \in \mathcal{O}_K$  such that  $a \bmod p = \bar{a}$ .

having the right shape to serve as input for Tuitman's algorithm. All subsequent arithmetic in Tuitman's algorithm is done in the  $p$ -adic completion  $\mathbb{Z}_q$  of  $\mathcal{O}_K$  (or rather its fraction field  $\mathbb{Q}_q$ ), up to some finite  $p$ -adic precision. But for the lifting step it suffices to work over  $\mathcal{O}_K$ , and this has some implementation-technical advantages [7, Remark 2].

**On Tuitman's assumption.** Let us discuss the specific requirements from [29, Assumption 1] in more detail. A first assumption concerns the polynomial  $r(x) = \Delta / \gcd(\Delta, d\Delta/dx)$  with  $\Delta$  the discriminant of (2), when viewed as a polynomial in  $y$  over  $\mathcal{O}_K[x]$ :

- (a) The discriminant of  $r(x)$  is a unit in  $\mathbb{Z}_q$ .

Next, consider the ring  $\mathcal{R} = \mathbb{Z}_q[x, 1/r, y]/(Q)$  and write  $\mathbb{Q}_q(x, y)$  for the field of fractions of  $\mathcal{R} \otimes \mathbb{Q}_q$  and  $\mathbb{F}_q(x, y)$  for the field of fractions of  $\mathcal{R} \otimes \mathbb{F}_q$ . A second assumption is that we know explicit matrices

$$W_0 \in \mathrm{GL}_d(\mathbb{Z}_q[x, 1/r]) \quad \text{and} \quad W_\infty \in \mathrm{GL}_d(\mathbb{Z}_q[x^{\pm 1}, 1/r])$$

such that, if we write  $b_{j,0} = \sum_{i=0}^{d-1} (W_0)_{i+1,j+1} y^i$  and  $b_{j,\infty} = \sum_{i=0}^{d-1} (W_\infty)_{i+1,j+1} y^i$ , then:

- (b)  $\{b_{0,0}, \dots, b_{d-1,0}\}$  is an integral basis for  $\mathbb{Q}_q(x, y)$  over  $\mathbb{Q}_q[x]$  and its reduction mod  $p$  is an integral basis for  $\mathbb{F}_q(x, y)$  over  $\mathbb{F}_q[x]$ ,  
(c)  $\{b_{0,\infty}, \dots, b_{d-1,\infty}\}$  is an integral basis for  $\mathbb{Q}_q(x, y)$  over  $\mathbb{Q}_q[x^{-1}]$  and its reduction mod  $p$  is an integral basis for  $\mathbb{F}_q(x, y)$  over  $\mathbb{F}_q[x^{-1}]$ .

Finally, writing

$$\mathcal{R}_0 = \mathbb{Z}_q[x]b_{0,0} + \dots + \mathbb{Z}_q[x]b_{d-1,0} \quad \text{and} \quad \mathcal{R}_\infty = \mathbb{Z}_q[x^{-1}]b_{0,\infty} + \dots + \mathbb{Z}_q[x^{-1}]b_{d-1,\infty},$$

it is assumed that

- (d) the discriminants of the finite  $\mathbb{Z}_q$ -algebras  $(\mathcal{R}_0/(r))_{\mathrm{red}}$  and  $(\mathcal{R}_\infty/(1/x))_{\mathrm{red}}$  are units.

Here the subscript “red” means that we consider the reduced ring obtained by quotienting out the nilradical.<sup>2</sup>

The geometric meaning of assumptions (a) and (d) is discussed in [29, Proposition 2.3]; see also [28, Remark 2.3]. They express that all branch points of  $\varphi : C \rightarrow \mathbb{P}^1$ , as well as all points lying over these branch points, should be distinct mod  $p$ . In our context, these properties are automatic. Indeed, since  $p > 2$  and  $\bar{\varphi} : \bar{C} \rightarrow \mathbb{P}^1$  is simply branched, there is no wild ramification, hence the ramification divisor of  $\varphi$  reduces mod  $p$  to that of  $\bar{\varphi}$ . Thus, again because  $\bar{\varphi}$  is simply branched, we see that the ramification points of  $\varphi$  must reduce to  $2g + 2d - 2$  distinct points that take distinct images under  $\bar{\varphi}$ , as wanted; here  $g$  denotes the genus of  $\bar{C}$ . We also see that  $\varphi$  is simply branched as well.

Assumptions (b) and (c), on the other hand, ask for an explicit description of our lift  $\varphi : C \rightarrow \mathbb{P}^1$  in terms of two affine patches  $\varphi^{-1}(\mathbb{P}^1 \setminus \{\infty\})$  and  $\varphi^{-1}(\mathbb{P}^1 \setminus \{0\})$ , glued together using  $W = W_0^{-1}W_\infty$ , that is compatible with reduction mod  $p$ . In Tuitman's own pcc\_p and pcc\_q code,<sup>3</sup> the matrices  $W_0$

<sup>2</sup>This takes into account the erratum pointed out in <https://juitman.github.io/erratum.pdf>.

<sup>3</sup><https://github.com/juitman/pcc>, see `mat_W0()` and `mat_Winf()` in `coho_p.m` and `coho_q.m`.

and  $W_\infty$  are found by computing integral bases for the function field extension  $K(x) \subseteq K(C)$  defined by (2), using the Magma intrinsic `MaximalOrderFinite()`, and hoping that these have good reduction mod  $p$ . There is a nonzero probability that this approach fails, in which case Tuitman’s code outputs “bad model for curve”, but in practice this probability become negligible very rapidly as  $q$  grows; see the tables in [7]. We therefore content ourselves with relying on the same bet, which we call **Heuristic H**:

**Definition 1.4** (informal). The output (2) satisfies *Heuristic H* if the associated integral bases of  $K(C)$  over  $K[x]$  and  $K[x^{-1}]$ , computed using Magma as in Tuitman’s implementation, meet the requirements from [29, Assumption 1].

Of course, if through some other method one manages to find integral bases with good reduction, then this would bypass **Heuristic H**. In particular, if  $d = 3$  then, as explained in **Remark 3.4**, such integral bases can be extracted as by-products of our lifting procedure.

**Combined runtime.** The running time of our lifting procedure is strongly dominated by that of Tuitman’s algorithm, as should be clear from the discussions in Sections 3, 4 and 5 below. We will therefore omit a detailed analysis, although it is crucial to note that lifting does not inflate the input size too badly. Concretely, if we let  $\delta = \max_{0 \leq i \leq d} \deg \bar{f}_i$ , then:

- The reader can check that all  $f_i$  are of degree  $O(g)$ , which in turn is  $O(\delta)$  thanks to Baker’s bound [1, Theorem 2.4].
- When lifting coefficients from  $\mathbb{F}_q$  to  $\mathcal{O}_K$  naively, we can choose them to be of bit size  $O(n \log q)$ , and as a result the same asymptotic estimate applies to the size of the coefficients of the  $f_i$ .
- As discussed in [29, pages 313–314], the matrices  $W_0, W_\infty$  produced by the Magma intrinsic, as well as their inverses, involve  $K(x)$ -coefficients whose pole orders are in  $O(\delta)$ , as required by [29, Assumption 2]; for  $d = 3$ , the reader can check that the same bound applies to the integral bases from **Remark 3.4**.

From [29, Theorem 4.10] it follows that  $\tilde{O}(p\delta^4 n^3)$  bit operations suffice for computing the Hasse–Weil zeta function of any curve  $\bar{C}/\mathbb{F}_q$  of the form (1), where we recall our dependence on **Heuristic H** if  $d = 4, 5$ .

**Practical performance.** This paper comes with an implementation of our lifting procedure in Magma [4], which can be found in the [online supplement](#). The arxiv version [8] of our paper contains an appendix reporting on how the code performs in combination with Tuitman’s implementation for computing Hasse–Weil zeta functions. As discussed there, this gives satisfactory results for  $d = 3$  and  $d = 4$ , leading to a substantial enlargement of the class of curves admitting fast computation of their zeta function (over finite fields with small odd characteristic). In degree  $d = 5$  the combined code is considerably slower. This is almost entirely due to the seemingly harmless “elimination of variables” step, which is needed to put the lifted curve  $C/K$  in the form (2) and which produces large hidden constants in the above  $O(g)$  and  $O(n \log q)$  estimates. Nevertheless, here too, it is practically feasible to compute zeta functions in a nontrivial range.

**Tracks for future work.** Besides mitigating the effect of variable elimination and getting rid of [Heuristic H](#), a challenging goal is to dispose of the conditions on  $p$  and of the condition that  $\bar{\varphi}$  is simply branched. This seems to require changes to Tuitman's algorithm that are similar to how Denef and Vercauteren managed to make Kedlaya's algorithm work in even characteristic [12]. Also, as explained in [Section 2](#), our naive lifting strategy using “free coefficients” is closely related to Schreyer's proof [25, Corollary 6.8] of the unirationality of  $\mathcal{H}_{g,d}$ , the moduli space of simply branched degree  $d$  covers of  $\mathbb{P}^1$  by curves of genus  $g$ , for  $d \leq 5$ . Such unirationality results are known to be false for  $d \geq 7$ , where there is no hope for our strategy to work. This leaves  $d = 6$  as an interesting open case, on which several partial (positive) results have been proved by Geiss [20]; see [26, Figure 1] for an overview. It seems worth investigating how Geiss' results combine with our approach.

## 2. Preliminaries

**Reduced bases and Maroni invariants.** Let  $k$  be any field, which in the next sections will be specialized to  $k = \mathbb{F}_q$  and/or  $k = K$ . Consider a nonsingular projective curve  $C/k$  of genus  $g$ , along with a  $k$ -rational degree  $d$  morphism  $\varphi : C \rightarrow \mathbb{P}^1$ . Consider the inclusion of function fields  $k(x) \subseteq k(C)$  corresponding to  $\varphi$ . Let  $k[C]_0$  and  $k[C]_\infty$ , denote the integral closure of  $k[x]$  and  $k[1/x]$  inside  $k(C)$ , respectively.

**Theorem 2.1.** *There exist unique negative integers  $r_1 \geq r_2 \geq \dots \geq r_{d-1}$  for which there is a basis  $1, \alpha_1, \dots, \alpha_{d-1}$  of  $k[C]_0$  over  $k[x]$  such that  $1, x^{r_1}\alpha_1, \dots, x^{r_{d-1}}\alpha_{d-1}$  is a basis of  $k[C]_\infty$  over  $k[1/x]$ .*

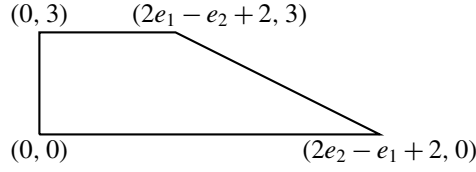
See [21] for a proof; it is standard to call  $e_i = -r_i - 2$  the *Maroni invariants* of  $C$  with respect to  $\varphi$  (e.g., if  $\varphi$  is a degree 2 cover, then there is just one Maroni invariant, namely  $g - 1$ ). A corresponding basis  $1, \alpha_1, \dots, \alpha_{d-1}$  is called a *reduced basis*. In our cases of interest, the integers  $r_i$  and an accompanying reduced basis can be computed efficiently: if  $k$  is a finite field or a number field, then the Magma command `ShortBasis()` takes care of this.

**Remark 2.2.** In more geometric language, the integers  $r_i$  are characterized by the sheaf decomposition  $\varphi_* \mathcal{O}_C \cong \mathcal{O}_{\mathbb{P}^1} \oplus \mathcal{O}_{\mathbb{P}^1}(r_1) \oplus \mathcal{O}_{\mathbb{P}^1}(r_2) \oplus \dots \oplus \mathcal{O}_{\mathbb{P}^1}(r_{d-1})$  which, according to a theorem due to Grothendieck, is indeed unique. As a consequence to the Riemann–Roch theorem, the Maroni invariants satisfy the following basic properties:

- (i)  $-1 \leq e_1 \leq e_2 \leq \dots \leq e_{d-1}$ ,
- (ii)  $e_1 + e_2 + \dots + e_{d-1} = g - d + 1$ ,
- (iii)  $e_{d-1} \leq (2g - 2)/d$ .

**Models with “free coefficients”.** As mentioned in the introduction, every cover  $\varphi : C \rightarrow \mathbb{P}^1$  of degree  $3 \leq d \leq 5$  admits a nonsingular projective model with “free coefficients” that can be lifted naively from  $\mathbb{F}_q$  to  $\mathcal{O}_K$ . This follows from Schreyer's proof [25, Corollary 6.8] of the unirationality of  $\mathcal{H}_{g,d}$  for  $d \leq 5$ . The natural ambient space for this model is a *rational normal scroll*, which can be obtained by gluing together

$$(\mathbb{P}^1 \setminus \{\infty\}) \times \mathbb{P}^{d-2} \quad \text{and} \quad (\mathbb{P}^1 \setminus \{0\}) \times \mathbb{P}^{d-2}$$



**Figure 1.** Polygon describing covers of degree 3.

in a nonstandard way; the gluing depends on the Maroni invariants  $e_1, \dots, e_{d-1}$  of  $C$  with respect to  $\varphi$ . We refer to [15; 25] for more details on this construction, as well as on the claims below. For the sake of conciseness we only describe what the model looks like on the left copy  $\mathbb{A}^1 \times \mathbb{P}^{d-2}$ , which we equip with coordinates  $x, Y_1, \dots, Y_{d-1}$ .

First assume that  $d = 3$ . Then  $C$  admits a defining equation of the form

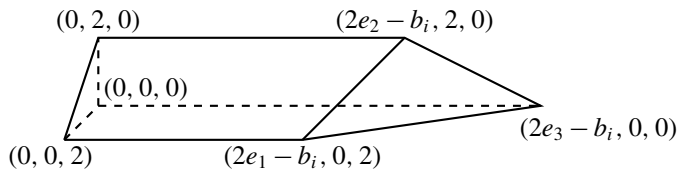
$$\sum_{l_1+l_2=3} f_{l_1,l_2}(x) Y_1^{l_1} Y_2^{l_2} = 0 \quad (3)$$

with  $\deg f_{l_1,l_2} \leq l_1 e_1 + l_2 e_2 + 4 - g$ , such that  $\varphi$  corresponds to projection on the  $x$ -coordinate. Conversely, every irreducible polynomial of the form (3) defines a curve having genus at most  $g$ ; this can also be seen using Baker's bound [1, Theorem 2.4], because the dehomogenization with respect to  $Y_2$  is supported on the polygon from Figure 1. If equality holds then this polynomial defines a nonsingular projective curve (on the entire rational normal scroll) and projection on the  $x$ -coordinate yields a degree 3 morphism to  $\mathbb{P}^1$  whose associated Maroni invariants are  $e_1, e_2$ .

Next, assume that  $d = 4$ . Then  $C$  arises as the intersection of two surfaces defined by

$$\sum_{l_1+l_2+l_3=2} f_{i,l_1,l_2,l_3}(x) Y_1^{l_1} Y_2^{l_2} Y_3^{l_3} = 0 \quad (4)$$

for  $i = 1, 2$ , where  $\deg f_{i,l_1,l_2,l_3} \leq l_1 e_1 + l_2 e_2 + l_3 e_3 - b_i$  for unique integers  $-1 \leq b_1 \leq b_2$  with  $b_1 + b_2 = g - 5$ , called the Schreyer invariants of  $C$  with respect to  $\varphi$ . Conversely, every irreducible such intersection defines a curve of genus at most  $g$ ; this too can be seen using (a three-dimensional version of) Baker's bound [23, Theorem 1], by noting that the dehomogenizations with respect to  $Y_3$  are supported on the polytopes from Figure 2. If equality holds then it concerns a nonsingular projective curve, and projection



**Figure 2.** Polytope describing covers of degree 4.



on the  $x$ -coordinate defines a degree 4 morphism to  $\mathbb{P}^1$  with associated Maroni invariants  $e_1, e_2, e_3$  and Schreyer invariants  $b_1, b_2$ .

Finally, assume  $d = 5$ , which comes with five Schreyer invariants  $b_1 \leq \dots \leq b_5$  summing up to  $2g - 12$ . In this case  $C$  can be viewed as the intersection of five hypersurfaces, which are all obtained from a single  $5 \times 5$  skew-symmetric matrix  $M$  over  $k[x][Y_1, Y_2, Y_3, Y_4]$  whose  $(i, j)$ -th entry is of the form

$$M_{1,i,j}(x)Y_1 + M_{2,i,j}(x)Y_2 + M_{3,i,j}(x)Y_3 + M_{4,i,j}(x)Y_4 \quad (5)$$

with  $M_{r,i,j}(x) \in k[x]$  of degree at most  $e_r + b_i + b_j + 6 - g$ . More precisely, our hypersurfaces are cut out by the five  $4 \times 4$  sub-Pfaffians of  $M$ .<sup>4</sup> Conversely, whenever the  $4 \times 4$  sub-Pfaffians of such a matrix define an irreducible curve, it has genus at most  $g$ . If equality holds then it concerns a nonsingular projective curve, and projection on the  $x$ -coordinate defines a degree 5 morphism to  $\mathbb{P}^1$  with Maroni invariants  $e_1, e_2, e_3, e_4$  and Schreyer invariants  $b_1, b_2, b_3, b_4, b_5$ .

**Lifting strategy revisited.** In the next sections we show how results on ring parametrizations due to Delone and Faddeev [17, Proposition 2.4] and Bhargava [2; 3] can be used to efficiently produce such a “free coefficient” model for our input curve  $\bar{C}/\mathbb{F}_q$ . Then, by the above discussion, and using that the genus cannot increase under reduction mod  $p$ , any naive coefficient-wise lift of this model to  $\mathcal{O}_K$  will define a nonsingular projective curve  $C/K$  along with a morphism  $\varphi : C \rightarrow \mathbb{P}^1$  lifting  $\bar{C}$  and  $\bar{\varphi}$ .

**Remark 2.3.** From a nonalgorithmic viewpoint, the fact that the Delone–Faddeev and Bhargava correspondences produce nonsingular curves in rational normal scrolls might have been known to some specialists (e.g., for  $d = 3$  this can be read in Zhao’s Ph.D. thesis [31]).

### 3. Lifting curves in degree $d = 3$

For  $R$  a PID, we recall that a *ring of rank  $d$*  over  $R$  is a commutative  $R$ -algebra which is free of rank  $d$  as a module over  $R$ . Every ring  $S$  of rank  $d$  over  $R$  admits an  $R$ -basis of the form  $1, \alpha_1, \dots, \alpha_{d-1}$ . This can be seen by applying the structure theorem for finitely generated free modules over PIDs to the submodule  $R \cdot 1$  of  $S$ .

**Parametrizing cubic rings.** Let  $R$  be a PID. Cubic rings over  $R$  admit a parametrization using binary cubic forms over  $R$ , considered modulo a natural action by  $\mathrm{GL}_2(R)$ : for an element

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(R),$$

and  $f = f_3Y_1^3 + f_2Y_1^2Y_2 + f_1Y_1Y_2^2 + f_0Y_2^3$  a cubic form over  $R$ , we let

$$A * f(Y_1, Y_2) = \frac{1}{\det A} f(aY_1 + cY_2, bY_1 + dY_2).$$

<sup>4</sup>The square roots of the determinants of the five  $4 \times 4$  skew-symmetric submatrices.

**Theorem 3.1** (Delone–Faddeev). *There is a canonical bijection between the set of cubic  $R$ -rings up to isomorphism and binary cubic forms over  $R$ , modulo the action of  $\mathrm{GL}_2(R)$ .*

For a proof see e.g., [17, Proposition 4.2]. For use below we briefly describe how this bijection is constructed. Let  $S$  be a cubic  $R$ -ring with basis  $1, \alpha_1, \alpha_2$ . By adding elements of  $1 \cdot R$  to  $\alpha_1$  and  $\alpha_2$  we can assume that  $\alpha_1\alpha_2$  is in  $R$ . We call such bases *normal*. Now write out the multiplication table of  $S$ :

$$\begin{aligned}\alpha_1\alpha_2 &= -g_0, \\ \alpha_1^2 &= -g_1 + f_2\alpha_1 - f_3\alpha_2, \\ \alpha_2^2 &= -g_2 + f_0\alpha_1 - f_1\alpha_2.\end{aligned}\tag{6}$$

By associativity of  $S$  we have  $\alpha_1^2 \cdot \alpha_2 = \alpha_1 \cdot (\alpha_1\alpha_2)$  and  $\alpha_1 \cdot \alpha_2^2 = (\alpha_1\alpha_2) \cdot \alpha_2$ . This gives

$$\begin{aligned}g_0 &= f_0f_3, \\ g_1 &= f_1f_3, \\ g_2 &= f_0f_2,\end{aligned}\tag{7}$$

so the  $g_i$  are determined by the  $f_i$ . One then associates to  $S$  the cubic form  $f = f_3Y_1^3 + f_2Y_1^2Y_2 + f_1Y_1Y_2^2 + f_0Y_2^3$ . Conversely, given such a form  $f$ , associate to this the cubic ring, formally equipped with basis  $1, \alpha_1, \alpha_2$  and multiplication defined by (6) and (7). The  $\mathrm{GL}_2(R)$ -action on cubic forms corresponds precisely to changing one normal basis to another on the level of cubic rings.

**Remark 3.2.** A cubic form  $f = f_3Y_1^3 + f_2Y_1^2Y_2 + f_1Y_1Y_2^2 + f_0Y_2^3$  is irreducible if and only if its associated cubic  $R$ -ring is a domain. In this case, we may describe it as the subring of

$$\mathrm{Frac}\left(\frac{R[y]}{(f_3y^3 + f_2y^2 + f_1y + f_0)}\right)$$

generated by  $1, \alpha_1 = f_3y, \alpha_2 = -f_0y^{-1} = f_3y^2 + f_2y + f_1$ . This point of view is especially nice when  $R = k[x]$  for some field  $k$ . Indeed, then  $f(y, 1) = 0$  defines a curve in  $\mathbb{A}^2$  over  $k$  and the cubic ring associated to  $f$  has as its field of fractions the function field of this curve.

**Lifting degree 3 covers.** Consider the function field

$$\mathbb{F}_q(\bar{C}) = \mathrm{Frac}\left(\frac{\mathbb{F}_q[x, y]}{(\bar{f}_3y^3 + \bar{f}_2y^2 + \bar{f}_1y + \bar{f}_0)}\right)$$

defined by our input polynomial, and consider the integral closure  $\mathbb{F}_q[\bar{C}]_0$  of  $\mathbb{F}_q[x]$  inside it; this is a cubic  $\mathbb{F}_q[x]$ -ring. Let  $e_1, e_2$  be the Maroni invariants of  $\bar{C}$  with respect to  $\bar{\varphi}$  and let  $1, \alpha_1, \alpha_2$  be a corresponding reduced basis. After adding to  $\alpha_1$  and  $\alpha_2$  elements of  $\mathbb{F}_q[x]$  we may assume that this basis is normal. In more detail, if  $\alpha_1\alpha_2 = a\alpha_1 + b\alpha_2 + c$ , for  $a, b, c \in \mathbb{F}_q[x]$ , then we replace  $\alpha_1$  by  $\alpha_1 - b$  and  $\alpha_2$  by  $\alpha_2 - a$ . This operation will not change the fact that the basis is reduced. Applying the Delone–Faddeev correspondence to this basis produces a new cubic form

$$\bar{f}(Y_1, Y_2) = \bar{f}_3Y_1^3 + \bar{f}_2Y_1^2Y_2 + \bar{f}_1Y_1Y_2^2 + \bar{f}_0Y_2^3$$

whose coefficients we, abusingly, again denote by  $\bar{f}_i$ .

**Lemma 3.3.** *Let  $\bar{f}$  be obtained through the Delone–Faddeev correspondence as above. Then this is a model for  $\bar{C}$  of the form (3).*

*Proof.* Note that the curve  $\bar{f}(y, 1) = 0$  is indeed birationally equivalent with  $\bar{C}$ , in view of Remark 3.2. Denote by  $e_1, e_2$  the Maroni invariants of  $\bar{C}$ . Since  $1, \alpha_1, \alpha_2$  is a reduced basis, the elements  $1, x^{-e_1-2}\alpha_1, x^{-e_2-2}\alpha_2$  form a basis for  $\mathbb{F}_q[\bar{C}]_\infty$ , the integral closure of  $\mathbb{F}_q[x^{-1}]$  inside  $\mathbb{F}_q(\bar{C})$ . Writing out the multiplication for this ring gives

$$\begin{aligned} x^{-e_1-e_2-4}\alpha_1\alpha_2 &= -x^{-e_1-e_2-4}\bar{f}_0\bar{f}_3, \\ x^{-2e_1-4}\alpha_1^2 &= -x^{-2e_1-4}\bar{f}_1\bar{f}_3 + x^{-e_1-2}\bar{f}_2x^{-e_1-2}\alpha_1 - x^{-2e_1+e_2-2}\bar{f}_3x^{-e_2-2}\alpha_2, \\ x^{-2e_2-4}\alpha_2^2 &= -x^{-2e_2-4}\bar{f}_0\bar{f}_2 + x^{-2e_2+e_1-2}\bar{f}_0x^{-e_1-2}\alpha_1 - x^{-e_2-2}\bar{f}_1x^{-e_2-2}\alpha_2. \end{aligned}$$

Since the coefficients of this table must be elements of  $\mathbb{F}_q[x^{-1}]$  we see that  $\deg \bar{f}_i \leq (i-1)e_1 + (2-i)e_2 + 2$  for  $i = 1, 2$ , hence  $\bar{f}(y, 1)$  is supported on the polygon from Figure 1.  $\square$

Thus we can proceed as follows. We compute a reduced basis for the function field  $\mathbb{F}_q(\bar{C})$  over  $\mathbb{F}_q[x]$ , make it normal if needed, and apply the Delone–Faddeev correspondence to it to obtain a model  $\bar{f} = 0$  of the form (3). As discussed in Section 2, any naive coefficient-wise lift of the polynomial  $\bar{f}(y, 1)$  to a polynomial  $f = f_3y^3 + f_2y^2 + f_1y + f_0 \in \mathcal{O}_K[x]$  defines a good lift. After making the polynomial  $f$  monic as in (2), it can be fed to Tuitman's algorithm to compute the zeta function of  $\bar{C}$  over  $\mathbb{F}_q$ .

**Remark 3.4.** Our discussion also shows that  $1, f_3y, f_0y^{-1} = f_3y^2 + f_2y + f_1$  is an integral basis of  $K(C)$  over  $K[x]$  that reduces to an integral basis of  $\mathbb{F}_q[\bar{C}]$  over  $\mathbb{F}_q[x]$ . Using the variable change  $x = x^{-1}$  and  $y = y/x^{e_2-e_1}$  we find the patch

$$f_3^{\text{recipr.}}(x)y^3 + f_2^{\text{recipr.}}(x)y^2 + f_1^{\text{recipr.}}(x)y + f_0^{\text{recipr.}}(x)$$

above infinity, which admits an analogous integral basis. Here  $f_i^{\text{recipr.}}$  denotes the degree  $(i-1)e_1 + (2-i)e_2 + 2$  reciprocal of  $f_i$ . We can supply these bases as additional input to Tuitman's algorithm, thereby bypassing Heuristic H.

#### 4. Lifting curves in degree $d = 4$

**Parametrizing quartic rings.** The parametrization of quartic  $R$ -rings  $S$  is due to Bhargava [2]. This time, the objects involved are pairs of ternary quadratic forms, up to an action of  $\text{GL}_3(R) \times \text{GL}_2(R)$ . For an element

$$(A, B) \in \text{GL}_3(R) \times \text{GL}_2(R),$$

and a pair of ternary quadratic forms  $(Q_1, Q_2)$  over  $R$  represented as  $3 \times 3$  matrices, the action is defined by

$$(A, B) * (Q_1, Q_2) = B \cdot \begin{pmatrix} A Q_1 A^T \\ A Q_2 A^T \end{pmatrix}.$$

Concretely, the quadratic forms associated with a quartic ring are obtained by specifying a *cubic resolvent* (the next paragraph provides more details).

**Theorem 4.1** (Bhargava). *There is a canonical bijection between pairs  $(S, S')$  where  $S$  is a quartic ring over  $R$  and  $S'$  is a cubic resolvent for  $S$ , considered up to isomorphism, and pairs of ternary quadratic forms over  $R$ , up to the action of  $\mathrm{GL}_3(R) \times \mathrm{GL}_2(R)$ .*

See [2, Theorem 1], although we will not explicitly rely on this theorem. But we will recycle its central map  $\phi$ , whose construction we briefly recall, while zooming in on our main case of interest, namely where  $S$  is a domain, say with field of fractions  $F$ . We assume moreover that  $F$  is a separable  $S_4$ -extension of  $K = \mathrm{Frac} R$ , i.e., its Galois closure  $E/K$  has as Galois group the full symmetric group  $S_4$ . Then a cubic resolvent for  $S$  is a certain full-rank subring  $S' \subseteq E^{D_4} =: F^{\mathrm{res}}$ , where  $D_4 = \langle (12), (1324) \rangle$ ; see [2, Definition 8] for a precise definition. In general, there might be more than one cubic resolvent ring, but for maximal rings it is unique [2, Corollary 5]. Note that if  $F = K[y]/(f)$  with

$$f = (y - r_1)(y - r_2)(y - r_3)(y - r_4) = y^4 + ay^3 + by^2 + cy + d$$

then  $F^{\mathrm{res}} = K[y]/(\mathrm{res} f)$  with

$$\begin{aligned} \mathrm{res} f &= (y - r_1r_2 - r_3r_4)(y - r_1r_3 - r_2r_4)(y - r_1r_4 - r_2r_3) \\ &= y^3 - by^2 + (ac - 4d)y - (a^2d + c^2 - 4bd). \end{aligned}$$

This polynomial is famously known as *Lagrange's cubic resolvent*. The most important feature of the Bhargava correspondence is the natural quadratic map

$$\tilde{\phi} : F \rightarrow F^{\mathrm{res}} : \alpha \mapsto \alpha^{(1)}\alpha^{(2)} + \alpha^{(3)}\alpha^{(4)},$$

where the  $\alpha^{(i)}$  denote the conjugates of  $\alpha$  inside  $E$  (numbered compatibly with the roots  $r_i$ ). This map turns out to descend to a quadratic map of  $R$ -modules

$$\phi : \frac{S}{R} \rightarrow \frac{S'}{R}.$$

Upon taking bases for  $S/R$  and  $S'/R$  we obtain our two ternary quadratic forms over  $R$ . Changing bases of these modules then corresponds to an element of  $\mathrm{GL}_3(R) \times \mathrm{GL}_2(R)$ .

**Lifting degree 4 covers.** We can assume that  $\bar{f}_4 = 1$ , i.e., our input polynomial (1) is monic. Let  $\mathbb{F}_q(\bar{C})$  denote the function field it defines, which is a separable  $S_4$ -extension of  $\mathbb{F}_q(x)$  because  $\bar{\varphi}$  is simply branched [16, Lemma 6.10]. Similarly, consider the cubic resolvent

$$y^3 - \bar{f}_2y^2 + (\bar{f}_1\bar{f}_3 - 4\bar{f}_0)y - (\bar{f}_0\bar{f}_3^2 + \bar{f}_1^2 - 4\bar{f}_0\bar{f}_2) \quad (8)$$

defining  $\mathbb{F}_q(\bar{C}^{\mathrm{res}}) := \mathbb{F}_q(\bar{C})^{\mathrm{res}}$ . We let  $\mathbb{F}_q[\bar{C}]_0$  and  $\mathbb{F}_q[\bar{C}^{\mathrm{res}}]_0$  be the respective integral closures of  $R = \mathbb{F}_q[x]$  inside these fields. It can be argued that  $\mathbb{F}_q[\bar{C}^{\mathrm{res}}]_0$  is the unique cubic resolvent ring  $S'$  for  $S = \mathbb{F}_q[\bar{C}]_0$ , but for our needs it suffices to know that  $S' \subseteq \mathbb{F}_q[\bar{C}^{\mathrm{res}}]_0$ , which is immediate since  $\mathbb{F}_q[\bar{C}^{\mathrm{res}}]_0$  is maximal.

Let  $e_1, e_2, e_3$  be the Maroni invariants of  $\bar{C}$  with respect to  $\bar{\varphi}$ , and let  $b_1, b_2$  be its Schreyer invariants. Take reduced  $\mathbb{F}_q[x]$ -bases  $1, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_q[\bar{C}]_0$  and  $1, \beta_1, \beta_2 \in \mathbb{F}_q[\bar{C}^{\text{res}}]_0$ . With respect to these bases, the map  $\phi$  above gives us two ternary quadratic forms  $\bar{Q}_1, \bar{Q}_2 \in \mathbb{F}_q[x][Y_1, Y_2, Y_3]$ . To properly bound the degrees of their coefficients, we have to understand how the Maroni invariants of the resolvent curve  $\bar{C}^{\text{res}}$  relate to data associated with  $\bar{C}$ . Surprisingly, up to a small shift, these turn out to be the Schreyer invariants of  $\bar{C}$  with respect to  $\bar{\varphi}$ .

**Theorem 4.2.** *Let  $k$  be a field of characteristic  $\neq 2$  and consider a smooth projective curve over  $k$  equipped with a simply branched degree 4 morphism to  $\mathbb{P}^1$ , say with Schreyer invariants  $b_1, b_2$ . Then the Maroni invariants of its cubic resolvent are  $b_1 + 2, b_2 + 2$ .*

*Proof.* This result is due to Casnati [5, Definition 6.4], although he formulated it in terms of Recillas' trigonal construction, which is the geometric counterpart of Lagrange's cubic resolvent, as pointed out in [19, Section 8.6].  $\square$

**Lemma 4.3.** *The quadratic forms  $\bar{Q}_1, \bar{Q}_2$  obtained through Bhargava's correspondence as above are a model of  $\bar{C}$  of the form (4).*

*Proof.* Note that the polynomials indeed cut out a curve that is birationally equivalent with  $\bar{C}$ , in view of [3, Section 2].<sup>5</sup> Since  $1, \alpha_1, \alpha_2, \alpha_3$  and  $1, \beta_1, \beta_2$  are reduced bases, by Theorem 4.2 we have that

$$1, x^{-e_1-2}\alpha_1, x^{-e_2-2}\alpha_2, x^{-e_3-2}\alpha_3 \quad \text{and} \quad 1, x^{-b_1-4}\beta_1, x^{-b_2-4}\beta_2$$

are bases of  $\mathbb{F}_q[\bar{C}]_\infty$  and  $\mathbb{F}_q[\bar{C}^{\text{res}}]_\infty$ , the integral closures of  $\mathbb{F}_q[x^{-1}]$  in  $\mathbb{F}_q(\bar{C})$  and  $\mathbb{F}_q(\bar{C}^{\text{res}})$ , respectively. Now the quadratic map

$$\tilde{\phi} : \mathbb{F}_q(\bar{C}) \rightarrow \mathbb{F}_q(\bar{C}^{\text{res}})$$

from above also descends to a quadratic map of  $\mathbb{F}_q[x^{-1}]$ -modules

$$\phi' : \frac{\mathbb{F}_q[\bar{C}]_\infty}{\mathbb{F}_q[x^{-1}]} \rightarrow \frac{\mathbb{F}_q[\bar{C}^{\text{res}}]_\infty}{\mathbb{F}_q[x^{-1}]}.$$

With respect to the above bases,  $\phi'$  is defined by two quadratic forms over  $\mathbb{F}_q[x^{-1}]$ , which are necessarily obtained from  $\bar{Q}_1$  and  $\bar{Q}_2$  by applying the corresponding (diagonal) change of basis matrices. In other words,  $\phi'$  is represented by the quadratic forms

$$x^{b_1+4}\bar{Q}_1(x^{-e_1-2}Y_1, x^{-e_2-2}Y_2, x^{-e_3-2}Y_3), \quad x^{b_2+4}\bar{Q}_2(x^{-e_1-2}Y_1, x^{-e_2-2}Y_2, x^{-e_3-2}Y_3).$$

But these have coefficients in  $\mathbb{F}_q[x^{-1}]$ . Hence the degree of the  $Y_i Y_j$ -coefficient in  $\bar{Q}_1$  can be at most  $e_i + e_j - b_1$ , and similarly for  $\bar{Q}_2$ . In other words, the dehomogenized polynomials  $\bar{Q}_1(y_1, y_2, 1)$  and  $\bar{Q}_2(y_1, y_2, 1)$  are supported on the polytopes from Figure 2.  $\square$

<sup>5</sup>Alternatively, the reader can check that  $\text{res}_{y_2}(\bar{Q}'_1(y_1, y_2, 1), \bar{Q}'_2(y_1, y_2, 1)) = y_1^4 + \bar{f}_3 y_1^3 + \bar{f}_2 y_1^2 + \bar{f}_1 y_1 + \bar{f}_0$ , where  $\bar{Q}'_1$  and  $\bar{Q}'_2$  are the quadratic forms from below.

To compute these liftable quadrics  $\bar{Q}_1, \bar{Q}_2$  in practice we will not directly compute the resolvent map  $\phi$  with respect to reduced bases for  $\mathbb{F}_q(\bar{C})$  and  $\mathbb{F}_q(\bar{C}^{\text{res}})$ . Instead, we compute the map  $\phi$  with respect to certain *naive bases* for  $\mathbb{F}_q(\bar{C})$  and  $\mathbb{F}_q(\bar{C}^{\text{res}})$  and then apply change of basis to a reduced basis. In more detail, denoting by  $\bar{f}'_i$  the coefficients of the cubic resolvent polynomial of  $\bar{f}$  as in (8), we consider the bases

$$1, -\bar{f}'_0 y^{-1}, y, y^2 \text{ for } \mathbb{F}_q(\bar{C}) \quad \text{and} \quad 1, y, -\bar{f}'_0 y^{-1} \text{ for } \mathbb{F}_q(\bar{C}^{\text{res}}). \quad (9)$$

Computing the representation of the resolvent map  $\phi$  with respect to these bases can be done symbolically by means of Vieta's formulas, yielding the quadrics

$$\bar{Q}'_1 = \begin{pmatrix} \bar{f}'_0 & 0 & \bar{f}'_1/2 \\ 0 & 1 & -\bar{f}'_3/2 \\ \bar{f}'_1/2 & -\bar{f}'_3/2 & \bar{f}'_2 \end{pmatrix}, \quad \bar{Q}'_2 = \begin{pmatrix} 0 & -1/2 & \bar{f}'_3/2 \\ -1/2 & 0 & 0 \\ \bar{f}'_3/2 & 0 & 1 \end{pmatrix}. \quad (10)$$

Now let  $1, \alpha_1, \alpha_2, \alpha_3$  and  $1, \beta_1, \beta_2$  be reduced bases for  $\mathbb{F}_q[\bar{C}]_0$  and  $\mathbb{F}_q[\bar{C}^{\text{res}}]_0$ , respectively, as above. To compute the cubic resolvent map with respect to these bases, we simply apply the change of basis action from the naive bases in (9) to these reduced bases. We note that this involves elements of  $\text{GL}_3(\mathbb{F}_q(x)) \times \text{GL}_2(\mathbb{F}_q(x))$  rather than  $\text{GL}_3(\mathbb{F}_q[x]) \times \text{GL}_2(\mathbb{F}_q[x])$ . The resulting quadrics  $\bar{Q}_1, \bar{Q}_2$  will be our model of the form (4). Then, as explained in Section 2, we can take any  $Q_1, Q_2 \in \mathcal{O}_K[x][y_1, y_2]$  lifting the  $\bar{Q}_i(y_1, y_2, 1)$  in a support-preserving way. In order to find a plane model, we can compute the resultant  $\text{res}_{y_2}(Q_1, Q_2)$ , which is indeed of degree 4 in  $y = y_1$ . After making it monic, it can be fed as input to Tuitman's algorithm.

## 5. Lifting curves in degree $d = 5$

**Parametrizing quintic rings.** The parametrization of quintic  $R$ -rings  $S$  is also due to Bhargava [3]. We assume that  $\text{char } R \neq 2, 3$ . The objects involved in the parametrization are now quadruples of  $5 \times 5$  skew-symmetric matrices over  $R$ . There is a natural action of  $\text{GL}_5(R) \times \text{GL}_4(R)$  on such objects, given by

$$(A, B) * M = B \cdot \begin{pmatrix} AM_1A^T \\ AM_2A^T \\ AM_3A^T \\ AM_4A^T \end{pmatrix},$$

with  $M = (M_1, M_2, M_3, M_4)$  a quadruple of  $5 \times 5$  skew-symmetric matrices and  $(A, B) \in \text{GL}_5(R) \times \text{GL}_4(R)$ . Here the parametrization requires us to specify a *sextic resolvent* (see the next paragraph for details).

**Theorem 5.1** (Bhargava). *There is a canonical bijection between pairs  $(S, S')$  where  $S$  is a quintic ring and  $S'$  is a sextic resolvent for  $S$ , considered up to isomorphism, and quadruples of  $5 \times 5$  skew-symmetric matrices over  $R$ , up to the action of  $\text{GL}_5(R) \times \text{GL}_4(R)$ .*

See [3]; although as in the previous sections, we will not explicitly rely on this theorem. But we will need the fundamental resolvent map (11) below. Let us again focus on the setting where  $S$  is a domain with field of fractions  $F$ , and let  $K = \text{Frac } R$ . We assume that  $F$  is a separable  $S_5$ -extension of  $K$ , i.e., its Galois closure  $E/K$  has as Galois group the whole of  $S_5$ . Consider the order 20 subgroup  $H = H^{(1)} = \text{AGL}_1(\mathbb{F}_5) = \langle (12345), (1243) \rangle \subseteq S_5$ . Then a sextic resolvent for  $S$  is a certain full-rank subring  $S' \subseteq E^H =: F^{\text{res}}$ ; for a precise definition we refer to [3, Definition 5]. In general, such a sextic resolvent ring is not unique, but for maximal quintic rings it is [3, Corollary 19]. If  $F = K[y]/(f)$  with

$$f = (y - r_1)(y - r_2)(y - r_3)(y - r_4)(y - r_5) = y^5 + ay^4 + by^3 + cy^2 + dy + e,$$

then  $F^{\text{res}} = K[y]/(\text{res } f)$  with  $\text{res } f = (y - \rho_1)(y - \rho_2)(y - \rho_3)(y - \rho_4)(y - \rho_5)(y - \rho_6)$ , where

$$\rho_1 = (r_1r_2 + r_2r_3 + r_3r_4 + r_4r_5 + r_5r_1 - r_1r_3 - r_3r_5 - r_5r_2 - r_2r_4 - r_4r_1)^2$$

and  $\{\rho_1, \rho_2, \dots, \rho_6\}$  is the orbit of  $\rho_1$  under the natural  $S_5$ -action permuting the  $r_i$ . Note that  $\rho_1$  is stabilized by  $H^{(1)}$ . We choose  $\rho_{2+i}$  to be stabilized by the conjugate subgroup

$$H^{(2+i)} = (12345)^{-i} \langle (13254), (3245) \rangle (12345)^i, \text{ for } 0 \leq i \leq 4.$$

The polynomial  $\text{res } f$  is known as *Cayley's sextic resolvent*; concrete expressions for its coefficients in terms of  $a, b, c, d, e$  can be found in [11, Proof of Proposition 13.2.5].<sup>6</sup>

For an element  $\alpha \in F^{\text{res}}$  we denote by  $\alpha^{(i)}$  the conjugates of  $\alpha$  inside  $E$ , labeled so that  $\alpha^{(i)}$  is fixed by  $H^{(i)}$ . Consider bases  $\alpha_0 = 1, \alpha_1, \dots, \alpha_4$  for  $S/R$  and  $\beta_0 = 1, \beta_1, \dots, \beta_5$  for  $S'/R$ , and define

$$\sqrt{\text{disc } S} = \begin{vmatrix} 1 & 1 & \dots & 1 \\ \alpha_1^{(1)} & \alpha_1^{(2)} & \dots & \alpha_1^{(5)} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_4^{(1)} & \alpha_4^{(2)} & \dots & \alpha_4^{(5)} \end{vmatrix}.$$

The central tool in Bhargava's correspondence is the *fundamental resolvent map*, which is the bilinear alternating form

$$g : F^{\text{res}} \times F^{\text{res}} \rightarrow F : (\alpha, \beta) \mapsto \sqrt{\text{disc } S} \cdot \begin{vmatrix} 1 & 1 & 1 \\ \alpha^{(1)} + \alpha^{(2)} & \alpha^{(3)} + \alpha^{(6)} & \alpha^{(4)} + \alpha^{(5)} \\ \beta^{(1)} + \beta^{(2)} & \beta^{(3)} + \beta^{(6)} & \beta^{(4)} + \beta^{(5)} \end{vmatrix}. \quad (11)$$

This turns out to descend to a well-defined map  $\tilde{S}' \times \tilde{S}' \rightarrow \tilde{S}$ , where

$$\tilde{S} = R\alpha_1^* + R\alpha_2^* + R\alpha_3^* + R\alpha_4^* \subseteq F, \quad \tilde{S}' = R\beta_1^* + R\beta_2^* + R\beta_3^* + R\beta_4^* + R\beta_5^* \subseteq F^{\text{res}}$$

are defined in terms of the dual bases  $\alpha_0^*, \dots, \alpha_4^*$  and  $\beta_0^*, \dots, \beta_5^*$  with respect to the trace pairing, i.e.,  $\text{Tr}_{F/K}(\alpha_i \alpha_j^*) = \delta_{ij}$  (with  $\delta_{ij}$  the Kronecker delta), and similarly for  $\beta_j^*$ . Note that the extensions  $F/K$  and  $F^{\text{res}}/K$  are both separable and so their trace pairings are nondegenerate. With respect to the bases  $\{\beta_i^*\}_i$

<sup>6</sup>Or they can be found hard-coded in our accompanying Magma file `precomputed_5.m`.

and  $\{\alpha_i^*\}_i$ , the map  $g$  is represented by a quadruple  $M = (M_1, M_2, M_3, M_4)$  of  $5 \times 5$  skew-symmetric matrices. Changing bases of  $\tilde{S}'$  and  $\tilde{S}$  then corresponds to an element of  $\mathrm{GL}_5(R) \times \mathrm{GL}_4(R)$ .

**Remark 5.2.** Our fundamental resolvent map differs from Bhargava's original map by a factor  $\frac{4}{3}$ , which is not an issue in view of our restrictions on the field characteristic.

**Lifting degree 5 covers.** As in the  $d = 4$  case, we assume that our input polynomial  $\bar{f}$  from (1) is monic (i.e.,  $\bar{f}_5 = 1$ ). Let  $\mathbb{F}_q(\bar{C})$  be the corresponding function field; this is a separable  $S_5$ -extension of  $\mathbb{F}_q(x)$  because  $\bar{\varphi}$  is simply branched [16, Lemma 6.10]. We also consider Cayley's sextic resolvent associated with our input polynomial, defining  $\mathbb{F}_q(\bar{C}^{\mathrm{res}}) := \mathbb{F}_q(\bar{C})^{\mathrm{res}}$ . Let  $\mathbb{F}_q[\bar{C}]_0$  and  $\mathbb{F}_q[\bar{C}^{\mathrm{res}}]_0$  be the respective integral closures of  $R = \mathbb{F}_q[x]$  inside these two function fields; it can be argued that  $\mathbb{F}_q[\bar{C}^{\mathrm{res}}]_0$  is the unique sextic resolvent ring  $S'$  for  $S = \mathbb{F}_q[\bar{C}]_0$ , but as in the  $d = 4$  case it suffices to observe that  $S' \subseteq \mathbb{F}_q[\bar{C}^{\mathrm{res}}]_0$ .

Let  $e_1, e_2, e_3, e_4$  be the Maroni invariants of  $\bar{C}$  with respect to  $\bar{\varphi}$ , and let  $b_1, b_2, b_3, b_4, b_5$  be its Schreyer invariants. Take reduced  $\mathbb{F}_q[x]$ -bases  $1, \alpha_1, \dots, \alpha_4 \in \mathbb{F}_q[\bar{C}]_0$  and  $1, \beta_1, \dots, \beta_5 \in \mathbb{F}_q[\bar{C}^{\mathrm{res}}]_0$  and consider the quadruple  $(\bar{M}_1, \bar{M}_2, \bar{M}_3, \bar{M}_4)$  of  $5 \times 5$  skew-symmetric matrices over  $\mathbb{F}_q[x]$  arising along the above construction. We represent this by the single matrix

$$\bar{M} = \bar{M}_1 Y_1 + \bar{M}_2 Y_2 + \bar{M}_3 Y_3 + \bar{M}_4 Y_4 \in k[x][Y_1, Y_2, Y_3, Y_4]$$

whose entries are now linear and homogeneous in the  $Y_i$ . To get a handle on the degrees of their coefficients, we should again express the Maroni invariants of the resolvent curve  $\bar{C}^{\mathrm{res}}$  in terms of data associated with  $\bar{C}$ . As in the case of the cubic resolvent, this can be done in a surprisingly explicit way.

**Theorem 5.3.** *Let  $k$  be a field of characteristic  $\neq 2$  and consider a smooth projective curve over  $k$  equipped with a simply branched degree 5 morphism to  $\mathbb{P}^1$ , say with Schreyer invariants  $b_1, \dots, b_5$ . Then the Maroni invariants of its sextic resolvent are  $g - 2 - b_5, \dots, g - 2 - b_1$ .*

*Proof.* This theorem seems new and is part of a generalization of Theorem 4.2, which is currently being elaborated in collaboration with Yongqiang Zhao [9]. In the meantime, a proof of Theorem 5.3 can be found in the master thesis of the second listed author [30].  $\square$

**Lemma 5.4.** *Denote by  $\bar{M}_{r,i,j}$  the  $(i, j)$ -th entry of the matrix  $\bar{M}_r$  constructed through Bhargava's correspondence as above. Then  $\deg \bar{M}_{r,i,j} \leq e_r + b_i + b_j + 6 - g$ . In particular, this defines a model for  $\bar{C}$  of the form (5).*

*Proof.* The fact that the sub-Pfaffians of  $\bar{M}$  cut out a curve birational to  $\bar{C}$  follows again from [3, Section 2]. As for the claim on the degrees, we apply the same proof strategy as in the degree 4 case. Denote by  $\mathbb{F}_q[\bar{C}]_\infty$  the integral closure of  $\mathbb{F}_q[x^{-1}]$  in  $\mathbb{F}_q(\bar{C})$ . Let  $g_0$  be the fundamental resolvent form attached to the basis  $1, \alpha_1, \dots, \alpha_4$  of  $\mathbb{F}_q[\bar{C}]_0$  over  $\mathbb{F}_q[x]$ , and let  $g_\infty$  be the fundamental resolvent form attached to the basis  $1, x^{-e_1-2}\alpha_1, \dots, x^{-e_4-2}\alpha_4$  of  $\mathbb{F}_q[\bar{C}]_\infty$  over  $\mathbb{F}_q[x^{-1}]$ . We have that, for all  $u, v \in \mathbb{F}_q(\bar{C}^{\mathrm{res}})$ ,

$$g_0(u, v) = \frac{\sqrt{\mathrm{disc} \mathbb{F}_q[\bar{C}]_0}}{\sqrt{\mathrm{disc} \mathbb{F}_q[\bar{C}]_\infty}} g_\infty(u, v) = x^{g+4} g_\infty(u, v).$$



Let  $\alpha_0^*, \dots, \alpha_4^*$  and  $\beta_0^*, \dots, \beta_5^*$  be dual bases for  $1, \alpha_1, \dots, \alpha_4$  and  $1, \beta_1, \dots, \beta_5$ , respectively. Then the corresponding dual bases for the rings  $\mathbb{F}_q[\bar{C}]_\infty$  and  $\mathbb{F}_q[\bar{C}^{\text{res}}]_\infty$  are

$$\alpha_0^*, x^{e_1+2}\alpha_1^*, \dots, x^{e_4+2}\alpha_4^* \text{ for } \mathbb{F}_q[\bar{C}]_\infty \quad \text{and} \quad \beta_0^*, x^{e'_1+2}\beta_1^*, \dots, x^{e'_5+2}\beta_5^* \text{ for } \mathbb{F}_q[\bar{C}^{\text{res}}]_\infty,$$

where the  $e'_i$  are the Maroni invariants of the resolvent. We now compute, for  $i, j > 0$ ,

$$g_\infty(x^{e'_i+2}\beta_i^*, x^{e'_j+2}\beta_j^*) = x^{e'_i+e'_j+4}x^{-g-4}g_0(\beta_i^*, \beta_j^*) \quad (12)$$

$$= \sum_{l=1}^4 x^{-e_l-g-2+e'_i+e'_j}(\bar{M}_l)_{ij}(x^{e_l+2}\alpha_l^*). \quad (13)$$

It follows that  $g_\infty$  is represented by the matrix whose entries have coefficients

$$x^{-e_l-g-2+e'_i+e'_j}(\bar{M}_l)_{ij}, \quad i, j = 1, \dots, 5, \quad l = 1, \dots, 4.$$

But these coefficients belong to  $\mathbb{F}_q[x^{-1}]$ . Hence we find that  $\deg(\bar{M}_l)_{ij} \leq e_l + b_i + b_j + 6 - g$  by [Theorem 5.3](#), as wanted.  $\square$

To compute such a liftable matrix in practice, we follow a similar approach as in the case of degree 4 covers. Namely, we will not be computing the fundamental resolvent map with respect to our reduced bases directly, but rather compute this for certain naive bases and apply change of basis. Concretely, consider the naive bases

$$1, y, y^2, y^3, y^4 \text{ for } \mathbb{F}_q(\bar{C}) \quad \text{and} \quad 1, y, y^2, y^3, y^4, y^5 \text{ for } \mathbb{F}_q(\bar{C}^{\text{res}}),$$

along with the slightly altered fundamental resolvent map

$$g' : \mathbb{F}_q(\bar{C}^{\text{res}}) \times \mathbb{F}_q(\bar{C}^{\text{res}}) \rightarrow \mathbb{F}_q(\bar{C}) : (\alpha, \beta) \mapsto \sqrt{\text{disc } \bar{f}} \cdot \begin{vmatrix} 1 & 1 & 1 \\ \alpha^{(1)} + \alpha^{(2)} & \alpha^{(3)} + \alpha^{(6)} & \alpha^{(4)} + \alpha^{(5)} \\ \beta^{(1)} + \beta^{(2)} & \beta^{(3)} + \beta^{(6)} & \beta^{(4)} + \beta^{(5)} \end{vmatrix}$$

where  $\sqrt{\text{disc } \bar{f}} = \det((y^i)^{(j)})_{0 \leq i \leq 4, 1 \leq j \leq 5}$ . We compute the  $\bar{M}'_{ij}{}^{(r)} \in \mathbb{F}_q[x]$  for which

$$g'(y^i, y^j) = \sum_{r=0}^4 \bar{M}'_{ij}{}^{(r)} y^r,$$

giving five  $5 \times 5$  skew-symmetric matrices  $\bar{M}'^{(0)}, \dots, \bar{M}'^{(4)}$ ; here we used that  $\bar{M}'_{ij}{}^{(r)} = 0$  as soon as  $i$  or  $j$  is zero, allowing us to disregard these terms. We call this the *naive model*.

**Remark 5.5.** It is important to note that these expressions can be computed symbolically in terms of the coefficients  $\bar{f}_i$  of  $\bar{f}$ , by means of Vieta's formulas. Therefore this computation only has to be done once for all curves. This is in complete analogy with the degree 4 case, see [\(10\)](#). However, there the naive model was very simple, whereas this time the expressions involved are rather long. However, a computer has no trouble with these computations.

Now compute reduced bases  $1, \alpha_1, \dots, \alpha_4$  for  $\mathbb{F}_q[\bar{C}]_0$  and  $1, \beta_1, \dots, \beta_5$  for  $\mathbb{F}_q[\bar{C}^{\text{res}}]_0$  along with their corresponding dual bases. Acting on the naive model with a change of basis from the naive bases to the duals of these reduced bases, yields the altered resolvent map  $g'$  with respect to these dual reduced bases. Note that this action will be by an element of  $\text{GL}_5(\mathbb{F}_q(x)) \times \text{GL}_4(\mathbb{F}_q(x))$  rather than  $\text{GL}_5(\mathbb{F}_q[x]) \times \text{GL}_4(\mathbb{F}_q[x])$ . To obtain instead the resolvent map  $g$  we have to multiply by

$$\frac{\sqrt{\text{disc } \mathbb{F}_q[\bar{C}]_0}}{\sqrt{\text{disc } \bar{f}}}.$$

Since we already have the reduced bases at hand, this factor is easiest to compute as the determinant of the change of basis matrix from the naive basis for  $\mathbb{F}_q(\bar{C})$  to the reduced basis  $1, \alpha_1, \dots, \alpha_4$ .

At this point, we have a representation of the fundamental resolvent map  $g$  with respect to the duals of the reduced bases for  $\mathbb{F}_q[\bar{C}]_0$  and  $\mathbb{F}_q[\bar{C}^{\text{res}}]_0$  as a  $5 \times 5$  skew-symmetric matrix  $\bar{M}$  with entries in  $k[x][Y_1, Y_2, Y_3, Y_4]$ , linear and homogeneous in the  $Y_i$ . This is the desired model, which we can lift naively, in a skew-symmetry preserving way, to a matrix having entries in  $\mathcal{O}_K[x][Y_1, Y_2, Y_3, Y_4]$ . Computing its five  $4 \times 4$  sub-Pfaffians, dehomogenizing, and then eliminating variables finally returns our output (2), ready to be fed as input to Tuitman's algorithm.

### Acknowledgements

We thank Jan Tuitman and Yongqiang Zhao for several inspiring conversations, and the anonymous reviewers for their many helpful comments. This work is supported by CyberSecurity Research Flanders with reference VR20192203 and by KU Leuven with references C14/17/083 and C14/18/067.

### References

- [1] P. Beelen, *A generalization of Baker's theorem*, Finite Fields and Their Applications **15**(5), pp. 558–568 (2009).
- [2] M. Bhargava, *Higher composition laws III: The parametrization of quartic rings*, Annals of Mathematics **159**(3), pp. 1329–1360 (2004).
- [3] M. Bhargava, *Higher composition laws IV: The parametrization of quintic rings*, Annals of Mathematics **167**(1), pp. 53–98 (2008).
- [4] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, Journal of Symbolic Computation **24**(3–4), pp. 235–265 (1997).
- [5] G. Casnati, *Covers of algebraic varieties III. The discriminant of a cover of degree 4 and the trigonal construction*, Transactions of the American Mathematical Society **350**(4), pp. 1359–1378 (1998).
- [6] W. Castryck, J. Denef, F. Vercauteren, *Computing zeta functions of nondegenerate curves*, International Mathematics Research Papers **2006**, pp. 1–57 (2006).
- [7] W. Castryck, J. Tuitman, *Point counting on curves using a gonality preserving lift*, The Quarterly Journal of Mathematics **69**(1), pp. 33–74 (2018).
- [8] W. Castryck, F. Vermeulen, *Lifting low-gonal curves for use in Tuitman's algorithm*, preprint, [arxiv](https://arxiv.org/abs/2007.00000) (2020).
- [9] W. Castryck, F. Vermeulen, Y. Zhao, *Szygies, Galois representations and the geometry of function fields*, in preparation (2020).
- [10] W. Castryck, J. Voight, *On nondegeneracy of curves*, Algebra & Number Theory **3**(3), pp. 255–281 (2009).

- [11] D. A. Cox, *Galois theory*, 2<sup>nd</sup> edition, John Wiley & Sons (2012).
- [12] J. Denef, F. Vercauteren, *Computing zeta functions of hyperelliptic curves over finite fields of characteristic 2*, Advances in Cryptology – CRYPTO 2002, Lecture Notes in Computer Science **2442**, pp. 369–384 (2002).
- [13] J. Denef, F. Vercauteren, *Counting points on  $C_{ab}$  curves using Monsky–Washnitzer cohomology*, Finite Fields and Their Applications **12**(1), pp. 78–102 (2006).
- [14] M. Derickx, *Torsion points on elliptic curves and gonality of modular curves*, Master thesis, Universiteit Leiden (2012).
- [15] D. Eisenbud, J. Harris, *On varieties of minimal degree (a centennial account)*, Proceedings of Symposia in Pure Mathematics **46**, pp. 3–13 (1987).
- [16] W. Fulton, *Hurwitz schemes and irreducibility of moduli of algebraic curves*, Annals of Mathematics **90**(3), pp. 542–575 (1969).
- [17] W.-T. Gan, B. Gross, G. Savin, *Fourier coefficients of modular forms on  $G_2$* , Duke Mathematical Journal **115**(1), pp. 105–169 (2002).
- [18] P. Gaudry, N. Gürel, *An extension of Kedlaya's point-counting algorithm to superelliptic curves*, Advances in Cryptology – ASIACRYPT 2001, Lecture Notes in Computer Science **2248**, pp. 480–494 (2001).
- [19] B. van Geemen, *Some remarks on Brauer groups of K3 surfaces*, Advances in Mathematics **197**, pp. 222–247 (2005).
- [20] F. Geiss, *The unirationality of Hurwitz spaces of 6-gonal curves of small genus*, Documenta Mathematica **17**, pp. 627–640 (2012).
- [21] F. Hess, *Computing Riemann–Roch spaces in algebraic function fields and related topics*, Journal of Symbolic Computation **33**(4), pp. 425–445 (2002).
- [22] K. S. Kedlaya, *Counting points on hyperelliptic curves using Monsky–Washnitzer cohomology*, Journal of the Ramanujan Mathematical Society **16**(4), pp. 323–338 (2001).
- [23] A. Khovanskii, *Newton polyhedra and the genus of complete intersections*, Functional Analysis and its Applications **12**(1), pp. 38–46 (1978).
- [24] J. Schicho, F.-O. Schreyer, M. Weimann, *Computational aspects of gonal maps and radical parametrization of curves*, Applicable Algebra in Engineering, Communication and Computing **24**(5), pp. 313–341 (2013).
- [25] F.-O. Schreyer, *Syzygies of canonical curves and special linear series*, Mathematische Annalen **275**(1), pp. 105–137 (1986).
- [26] F.-O. Schreyer, F. Tanturri, *Matrix factorizations and curves in  $\mathbb{P}^4$* , Documenta Mathematica **23**, pp. 1895–1924 (2018).
- [27] B. Segre, *Sui moduli delle curve poligonale, e sopra un complemento al teorema di esistenza di Riemann*, Mathematische Annalen **100**, pp. 537–551 (1928).
- [28] J. Tuitman, *Counting points on curves using a map to  $\mathbb{P}^1$* , Mathematics of Computation **85**(298), pp. 961–981 (2016).
- [29] J. Tuitman, *Counting points on curves using a map to  $\mathbb{P}^1$ , II*, Finite Fields and Their Applications **45**, pp. 301–322 (2017).
- [30] F. Vermeulen, *Lifting curves of low gonality*, Master thesis, KU Leuven (2019), available at <https://sites.google.com/view/floris-vermeulen/>.
- [31] Y. Zhao, *On sieve methods for varieties over finite fields*, Ph.D. thesis, University of Wisconsin Madison (2013).

Received 23 Feb 2020. Revised 19 Jul 2020.

WOUTER CASTRYCK: [wouter.castrycck@kuleuven.be](mailto:wouter.castrycck@kuleuven.be)  
 Department ESAT, imec-COSIC, KU Leuven, Leuven, Belgium  
 and

Department of Mathematics: Algebra and Geometry, Ghent University, Belgium

FLORIS VERMEULEN: [floris.vermeulen@kuleuven.be](mailto:floris.vermeulen@kuleuven.be)  
 Department of Mathematics, KU Leuven, Leuven, Belgium



# Simultaneous diagonalization of incomplete matrices and applications

Jean-Sébastien Coron, Luca Notarnicola, and Gabor Wiese

We consider the problem of recovering the entries of diagonal matrices  $\{U_a\}_a$  for  $a = 1, \dots, t$  from multiple “incomplete” samples  $\{W_a\}_a$  of the form  $W_a = PU_aQ$ , where  $P$  and  $Q$  are unknown matrices of low rank. We devise practical algorithms for this problem depending on the ranks of  $P$  and  $Q$ . This problem finds its motivation in cryptanalysis: we show how to significantly improve previous algorithms for solving the approximate common divisor problem and breaking CLT13 cryptographic multilinear maps.

## 1. Introduction

**1A. Problem statement.** This work considers the following computational problem from linear algebra.

**Definition 1.1** (Problems  $\mathbb{A}$ ,  $\mathbb{B}$ ,  $\mathbb{C}$ ,  $\mathbb{D}$ ). Let  $n \geq 2, t \geq 2$  and  $2 \leq p, q \leq n$  be integers. Let  $\{U_a : 1 \leq a \leq t\}$  be diagonal matrices in  $\mathbb{Q}^{n \times n}$ . Let  $\{W_a : 1 \leq a \leq t\}$  be matrices in  $\mathbb{Q}^{p \times q}$  and  $W_0 \in \mathbb{Q}^{p \times q}$  such that  $W_0$  has full rank and there exist matrices  $P \in \mathbb{Q}^{p \times n}$  of full rank  $p$  and  $Q \in \mathbb{Q}^{n \times q}$  of full rank  $q$ , such that  $W_0 = P \cdot Q$  and  $W_a = P \cdot U_a \cdot Q$  for  $1 \leq a \leq t$ . We distinguish the following cases:

- |                  |                       |                  |                       |
|------------------|-----------------------|------------------|-----------------------|
| ( $\mathbb{A}$ ) | $p = n$ and $q = n$ , | ( $\mathbb{B}$ ) | $p = n$ and $q < n$ , |
| ( $\mathbb{C}$ ) | $p < n$ and $q = n$ , | ( $\mathbb{D}$ ) | $p < n$ and $q = p$ . |

In each of the four cases, the problem is stated as follows:

- (1) Given the matrices  $\{W_a : 0 \leq a \leq t\}$ , compute  $\{(u_{1,i}, \dots, u_{t,i}) : 1 \leq i \leq n\}$ , where for  $1 \leq a \leq t$ ,  $u_{a,1}, \dots, u_{a,n} \in \mathbb{Q}$  are the diagonal entries of matrices  $\{U_a : 1 \leq a \leq t\}$  as above.
- (2) Determine whether the solution is unique.

Problem  $\mathbb{A}$  is straightforward for any  $t \geq 1$  by simultaneous diagonalization of  $W_0^{-1}W_a = Q^{-1}U_aQ$  for every  $a$ . Problems  $\mathbb{B}$  and  $\mathbb{C}$  are equivalent in view of their symmetry in  $p$  and  $q$ , and any algorithm for one solves the other upon transposing. Therefore, we shall devise algorithms for  $\mathbb{C}$  and  $\mathbb{D}$  only. We

MSC2010: 15A06, 94A60.

**Keywords:** simultaneous diagonalization, cryptanalysis, linear algebra, multilinear maps in cryptography, approximate common divisor problem.

refer to the matrices  $\{W_a\}_a$  as “incomplete”, as the low rank matrices  $P$  and/or  $Q$  “steal” information. Of interest is the case when  $p$  is much smaller than  $n$ . We remark that Problem  $\mathbb{A}$  is an underlying problem in previous works [CP19; CHL<sup>+</sup>15] in cryptanalysis.

**1B. Our contributions.** Mainly, we provide efficient algorithms for Problems  $\mathbb{C}$  and  $\mathbb{D}$  of Definition 1.1, and show how to minimize the parameters  $p$  and  $t$  with respect to  $n$ . We further propose two concrete applications of our algorithms in cryptography. We believe that our algorithms are of independent interest and hope that more applications are to be found.

*Algorithms for Problems  $\mathbb{C}$  and  $\mathbb{D}$ .* Our approach to Problem  $\mathbb{C}$  is to use the invertibility of  $Q$  and write  $W_a = P U_a Q = P Q Q^{-1} U_a Q = W_0 Z_a$  with  $Z_a = Q^{-1} U_a Q$ , for every  $1 \leq a \leq t$ . As  $W_0$  is not invertible, we cannot recover  $Z_a$  directly. However we interpret this as a system of linear equations to solve for  $\{Z_a\}_a$ . This system is, in general, underdetermined and does not yield the matrices  $\{Z_a\}_a$  uniquely. However, exploiting the special feature that  $\{Z_a\}_a$  commute among each other leads to additional linear equations. This enables us to recover  $\{Z_a\}_a$  uniquely, and simultaneous diagonalization eventually yields the diagonal entries of  $\{U_a\}_a$ . We determine exact bounds on the parameters to ensure that we have at least as many linear equations as variables; we obtain that  $p$  and  $t$  can be set as  $\mathcal{O}(\sqrt{n})$ . Our algorithm is heuristic only, but performs well in practice.

We reduce Problem  $\mathbb{D}$  to Problem  $\mathbb{C}$  by “augmenting”  $Q$  with extra columns so that it becomes invertible. In this case, we show that  $p$  can be close to  $2n/3$ . We refer to Sections 3 and 4 for a complete description of our algorithms and provide the results of practical experiments in Section 6.

*Improved algorithm for an approximate common divisor problem.* Approximate common divisor problems have gained a lot of interest and different variants have been investigated. In [CH13], Cohn and Heninger study generalizations of the approximate common divisor problem via lattices. A simple version including only a single prime number is studied in [GGM16]. A lattice cryptanalysis of the single-prime version is described in [vDGHV10]. In this work we consider the multi-prime version (CRT-ACD Problem) from [CP19], which is a factorization problem with constraints based on Chinese remaindering.

We improve the two-step algorithm by [CP19]. Namely, we remark that [CP19] relies on solving a certain instance of Problem  $\mathbb{A}$ . By solving an appropriate instance of Problem  $\mathbb{C}$  instead, we obtain a quadratic improvement in the number of input samples. Namely, letting  $n$  be the number of secret primes in the public modulus  $M$ , we can factor  $M$  given only  $\mathcal{O}(\sqrt{n})$  input samples, whereas [CP19] uses  $\mathcal{O}(n)$ . We therefore achieve complete factorization of the public modulus while limiting the input size drastically.

*Improved cryptanalysis of CLT13 multilinear maps.* In 2013, [GGH13] described the first construction of cryptographic multilinear maps, and since then, many important applications in cryptography have been found. A similar construction over the integers was described in [CLT13] and a third construction based on the LWE Problem was proposed [GGH15]. In the recent years, many attacks against these constructions appeared. The most devastating is the so-called “zeroizing attack”, exploiting the availability

of low-level encodings of zero. The algorithm [CHL<sup>+</sup>15] recovers all secret parameters of [CLT13] in the multiparty Diffie–Hellman key exchange. Similar attacks have been described against GGH13 and GGH15; see [HJ16; CLLT16].

Our third contribution is therefore to improve the cryptanalysis of Cheon et al. [CHL<sup>+</sup>15] against CLT13 when fewer encodings are public. Namely, [CHL<sup>+</sup>15] relies on solving some instance of Problem A. By solving instances of Problems C or D instead, we can lower the number of public encodings required for the cryptanalysis. Specifically, for a composite modulus  $x_0$  of  $n$  primes, we obtain improved algorithms using only  $\mathcal{O}(\sqrt{n})$  encodings of zero (compared to  $n$  in [CHL<sup>+</sup>15]), or in total  $4n/3$  encodings (compared to  $2n + 2$  in [CHL<sup>+</sup>15]). We confirm our results with practical experiments in Section 6.

## 2. Notations and preliminary remarks

**2A. Notation.** For  $n \in \mathbb{Z}_{\geq 1}$ , let  $[n]$  be the set  $\{1, \dots, n\}$ . For a set  $R$  and  $r, s \in \mathbb{Z}_{\geq 1}$ , we let  $R^{r \times s}$  be the set of  $r \times s$  matrices with entries in  $R$ . For  $A \in R^{r \times s}$  and  $B \in R^{r \times s'}$ ,  $[A|B] \in R^{r \times (s+s')}$  is the matrix obtained by concatenating the columns of  $A$  and  $B$ . We let  $1_n$  be the identity matrix in dimension  $n \in \mathbb{Z}_{\geq 1}$ . For a set  $S$ , its cardinality is denoted by  $\#S$ .

**2B. Remarks about Definition 1.1.** (i) Let  $\{W_a\}_a$  be as in Definition 1.1,  $\pi \in \mathfrak{S}_n$  be a permutation with associated matrix  $A_\pi \in \{0, 1\}^{n \times n}$  and  $D$  be any invertible diagonal  $n \times n$  matrix. Then  $P' = PDA_\pi$  and  $Q' = A_\pi^{-1}D^{-1}Q$  satisfy  $W_0 = P'Q'$  and  $W_a = P'U'_aQ'$  for all  $a \in [t]$ , where  $U'_a = A_\pi^{-1}U_aA_\pi$  is obtained from  $U_a$  by permuting its diagonal entries via  $\pi$ . Thus,  $P'$ ,  $\{U'_a\}_a$  and  $Q'$  satisfy the same problem. For this reason, we only ask to recover the set  $\{(u_{1,i}, \dots, u_{t,i}) : 1 \leq i \leq n\}$  in Definition 1.1.

(ii) If  $t = 1$  in Problem C, then the problem is not solvable because its solution is not unique. Namely, we write  $W_1 = W_0Z_1$ , where  $Z_1 = Q^{-1}U_1Q$  is diagonalizable with eigenvalues the diagonal entries of  $U_1$ . But also, for every  $v \in \ker(W_0)$  one has  $W_1 = W_0(Z_1 + vw_1^T)$  for some  $w_1 \in \mathbb{Q}^n$ . Now,  $Z_1$  and  $Z_1 + vw_1^T$  likely have different eigenvalues which means that the solution is not unique.

(iii) There are cases when the problem is clearly not solvable for  $p < n$ . For example, if  $P = [1_p | 0_{p \times (n-p)}]$  then for all  $a$  the matrix  $PU_a$  only involves the first  $p$  diagonal entries of  $U_a$  and the information on the remaining  $n - p$  is lost. These cases will not occur for “generic” or “random” instances of the problem.

(iv) If a matrix  $W_0 = PQ$  is not available as input (we call it a “special input” here), then one can recover ratios of diagonal entries of the matrices  $\{U_a\}_a$ , if  $t \geq 3$ . Namely, defining  $P' = PU_1$  and assuming that  $U_1$  is invertible, one obtains  $W'_0 := P'Q = W_1$  and for  $2 \leq a \leq t$ ,  $W'_a := P'(U_aU_1^{-1})Q = W_a$ . Running the algorithm on input  $\{W'_a : 0 \leq a \leq t - 1\}$  reveals the tuples of diagonal entries of the matrices  $U_aU_1^{-1}$  for  $1 \leq a \leq t - 1$ . We will use this approach in Section 5B3 to improve the (CLT13) multilinear map cryptanalysis.

(v) For simplicity, we have stated Definition 1.1 over  $\mathbb{Q}$ . More generally, we can consider matrices over a field  $\mathbb{K}$  with exact linear algebra (e.g., solving linear systems, diagonalizing matrices, etc.). Our algorithms apply to that case.

### 3. An algorithm for Problem $\mathbb{C}$

We describe an algorithm to solve Problem  $\mathbb{C}$  of Definition 1.1.

**3A. Description.** Consider integers  $n, t \geq 2$  and  $2 \leq p < n$  and an instance of Problem  $\mathbb{C}$ . We remark that it is enough to solve the following problem.

**Definition 3.1** (Problem  $\mathbb{C}'$ ). Let integers  $n, t \geq 2$  and  $2 \leq p < n$ . Given

- a matrix  $V \in \mathbb{Q}^{p \times n}$  of rank  $p$  and a basis matrix  $E \in \mathbb{Q}^{n \times (n-p)}$  of  $\ker(V)$ ,
- a set of matrices  $\{Y_a : a \in [t]\} \subseteq \mathbb{Q}^{n \times n}$ ,

compute matrices  $\{X_a : a \in [t]\} \subseteq \mathbb{Q}^{(n-p) \times n}$ , such that the matrices  $Y_a + EX_a$  for  $a \in [t]$  commute with each other.

**Proposition 3.2.** Let  $\{W_a : 0 \leq a \leq t\}$  as in Problem  $\mathbb{C}$ . Let  $E \in \mathbb{Q}^{n \times (n-p)}$  be a basis matrix of the kernel of  $W_0$ . Let  $W_0^+$  be a right-inverse<sup>1</sup> of  $W_0$ . Define  $V = W_0$  and  $Y_a = W_0^+ W_a$  for  $a \in [t]$ . Assume that Problem  $\mathbb{C}'$  is uniquely solvable for the input matrices  $V, E$  and  $\{Y_a : a \in [t]\}$ .

Then Problem  $\mathbb{C}$  is uniquely solvable for the input matrices  $\{W_a : 0 \leq a \leq t\}$ . Moreover, the matrix  $Q$  in the assumption of Problem  $\mathbb{C}$  is unique up to multiplication by a permutation matrix and an invertible diagonal matrix if at least one of the matrices  $\{U_a\}_a$  has pairwise distinct diagonal entries.

*Proof.* Write  $W_0 = PQ$  and  $W_a = PU_aQ$  as in Problem  $\mathbb{C}$ . For all  $a \in [t]$ , we will write  $W_a = (PQ)(Q^{-1}U_aQ) = W_0Z_a$ , where  $Z_a := Q^{-1}U_aQ$ . The matrices  $\{Z_a : a \in [t]\}$  commute and are simultaneously diagonalizable. For every  $a \in [t]$ ,  $Z_a$  can be written as  $Z_a = Y_a + EX_a$  for some  $X_a \in \mathbb{Q}^{(n-p) \times n}$  since  $W_0Y_a = W_a$ . Since the matrices  $\{Z_a\}_a$  commute,  $V, E$  and  $\{Y_a\}_a$  define a valid input for Problem  $\mathbb{C}'$ . By assumption, we can compute the matrices  $\{X_a\}_a$  by solving Problem  $\mathbb{C}'$  and these are unique. From the knowledge of  $\{X_a\}_a$ , we compute  $Z_a = Y_a + EX_a$  for  $a \in [t]$ . Then these matrices are also unique. Thus the set of tuples of eigenvalues

$$\{(u_{1,i}, \dots, u_{t,i}) : 1 \leq i \leq n\}$$

is unique and can be computed by simultaneous diagonalization.

For the last part of the statement, assume that we have matrices  $P', Q'$ , diagonal matrices  $\{U'_a\}_a$ , which are necessarily of the form  $U'_a = A^{-1}U_aA$  for a permutation matrix  $A$ , such that  $W_0 = P'Q'$  and  $W'_a = P'U'_aQ'$  for every  $a$ . By uniqueness of the matrices  $\{Z_a\}_a$ , we have

$$Z_a = Q^{-1}U_aQ = Q'^{-1}U'_aQ' = Q'^{-1}A^{-1}U_aAQ', \quad a \in [t]$$

or, equivalently  $U_a(QQ'^{-1}A^{-1}) = (QQ'^{-1}A^{-1})U_a$  for  $a \in [t]$ . Thus,  $D := QQ'^{-1}A^{-1}$  commutes with the matrices  $\{U_a\}_a$  and so is diagonal itself, as one of  $\{U_a\}_a$  has pairwise distinct entries. This gives  $Q = DAQ'$  and proves the statement.  $\square$

<sup>1</sup>If  $W_0$  (of full rank  $p$ ) is defined over the complex numbers, one can take  $W_0^+ = W_0^*(W_0W_0^*)^{-1}$  where  $W_0^*$  is the conjugate transpose of  $W_0$ , and  $W_0^* = W_0^T$  over the real numbers.



**3A1. Solving problem  $\mathbb{C}'$ .** We consider matrices  $V, E, \{Y_a\}_a$  as in Problem  $\mathbb{C}'$ . We want to compute matrices  $\{X_a\}_a$  such that the matrices  $Z_a = Y_a + EX_a$  commute for all  $a \in [t]$ , that is, the Jacobi bracket  $[Z_a, Z_b] = Z_a Z_b - Z_b Z_a$  is the zero matrix for all  $a < b$ . Using  $Z_a = Y_a + EX_a$ , this is equivalent to

$$0 = Y_a Y_b - Y_b Y_a + E \cdot S_{ab} + Y_a E X_b - Y_b E X_a, \quad (3-1)$$

where  $S_{ab} := X_a Y_b + X_a E X_b - X_b Y_a - X_b E X_a$ . Left multiplication by  $V$  and  $VE = 0$  implies

$$V Y_a Y_b - V Y_b Y_a + V Y_a E X_b - V Y_b E X_a = 0,$$

which is equivalent to

$$\Delta_{ab} = V Y_b E X_a - V Y_a E X_b, \quad 1 \leq a < b \leq t, \quad (3-2)$$

where  $\Delta_{ab} := V Y_a Y_b - V Y_b Y_a$  is completely explicit in terms of the input matrices. Equation (3-2) describes a system of linear equations over  $\mathbb{Q}$  in the variables given by the entries of  $X_a$  and  $X_b$ . Since  $\Delta_{ab}$  has size  $p \times n$ , this gives a system of  $np$  linear equations in the  $2(n-p)n$  variables given by the entries of  $X_a$  and  $X_b$ . Writing (3-2) for every  $(a, b) \in [t]^2$  with  $a < b$  we obtain a system of  $t(t-1)/2np$  linear equations and  $t(n-p)n$  variables given by the entries of the matrices  $\{X_a : a \in [t]\}$ .

From this and Proposition 3.2, we deduce the following result.

**Proposition 3.3.** *A unique solution to Problem  $\mathbb{C}$  is implied by the existence of a unique solution to the explicit system of linear equations given in (3-2), which is a system of  $\frac{1}{2}t(t-1)np$  linear equations in  $t(n-p)n$  variables. There are at least as many equations as variables as soon as*

$$\frac{p}{n} \geq \frac{2}{t+1}. \quad (3-3)$$

Since there is no obvious linear dependence in the equations of the system, we heuristically expect, in the generic case, to find a unique solution  $\{X_a : a \in [t]\}$  under (3-3). This solves Problem  $\mathbb{C}'$ , and therefore Problem  $\mathbb{C}$ .

**3B. Algorithm.** We refer to this algorithm as Algorithm  $\mathcal{A}_{\mathbb{C}}$  in the sequel.

*Input:* A valid input for Problem  $\mathbb{C}$ .

*Output:* “Success” or “Fail”. In case of “Success”, also output a solution. “Success” means uniqueness of the solution; “Fail” means that no solution was found.

1. Compute a basis matrix  $E$  of  $\ker(W_0)$ .
2. Define  $W_0^+ = W_0^T(W_0 W_0^T)^{-1}$  and for  $(a, b) \in [t]^2$  with  $a < b$ , compute the matrices  $\Delta_{ab} = W_a W_0^+ W_b - W_b W_0^+ W_a$ .
3. Solve the system of linear equations described in (3-2).
  - 3.1. If the solution is not unique, output “Fail” and break.
  - 3.2. Otherwise, denote by  $\{X_a : a \in [t]\}$  the unique solution.
4. Perform simultaneous diagonalization of  $Z_a = W_0^+ W_a + E X_a$  for  $a \in [t]$ .
5. Output “Success” with the tuples of eigenvalues of the matrices  $\{Z_a\}_a$ .

**3C. Optimization of the parameters.** We find minimal possible (with respect to  $n$ ) values for  $t$  and  $p$ . In our applications in [Section 5](#) we are led to minimize  $p + t$  as a function of  $n$ . Following [Proposition 3.3](#), we set  $F_n(t) = p_n(t) + t = \frac{2n}{t+1} + t$  with  $t \in \mathbb{R}_{>0}$  and  $n \in \mathbb{Z}_{\geq 2}$ . It is easy to see that  $F_n$  has a minimum at  $t_0 = \sqrt{2n} - 1$  which gives  $p = p_n(t_0) = \sqrt{2n}$ . This shows that minimal values for  $p$  and  $t$  are  $\mathcal{O}(\sqrt{n})$ . This is confirmed practically in [Section 6](#).

#### 4. An algorithm for problem $\mathbb{D}$

We now present an algorithm to solve Problem  $\mathbb{D}$  of [Definition 1.1](#).

**4A. Description.** Consider integers  $n, t \geq 2$  and  $2 \leq p < n$  and an instance of Problem  $\mathbb{D}$ . The main idea of our algorithm is a reduction to Problem  $\mathbb{C}$  which can be solved using Algorithm  $\mathcal{A}_C$ . More precisely, we exhibit matrices (that are augmentations of  $\{W_a\}_a$ )  $W'_0 = PQ'$  and  $W'_a = PU_aQ'$  for  $a \in [t]$ , for the same diagonal matrices  $\{U_a\}_a$  and for some  $n \times n$  invertible matrix  $Q'$ .

**4A1. Reducing problem  $\mathbb{D}$  to problem  $\mathbb{C}$ .** For  $1 \leq a, b \leq t$ , we define the matrices

$$\Delta_{ab} = W_a W_0^{-1} W_b - W_b W_0^{-1} W_a. \quad (4-1)$$

Note that  $\Delta_{ab} = -\Delta_{ba}$ . We have the following lemma.

**Lemma 4.1.** *Let  $W_0 = PQ$  and  $W_a = PU_aQ$  for  $a \in [t]$  as in Problem  $\mathbb{D}$ . Let  $B = QW_0^{-1}P - 1_n \in \mathbb{Q}^{n \times n}$  and let  $r$  denote its rank. Then:*

- (i)  $r = n - p$ .
- (ii) *There exist matrices  $V_a \in \mathbb{Q}^{p \times r}$  and  $G_a \in \mathbb{Q}^{r \times p}$  for  $a \in [t]$  such that for all  $1 \leq a < b \leq t$ , one has  $\Delta_{ab} = V_a G_b - V_b G_a$ .*

*Proof.* (i) Let  $C = QW_0^{-1}P$ . Then  $CQ = Q$  and the column-image of  $Q$  is contained in the eigenspace, say  $\mathcal{E}$ , of  $C$  for eigenvalue 1. So,  $\mathcal{E}$  has dimension at least  $p$ . However, the rank of  $C$  is bounded above by the rank of  $Q$ , i.e., by  $p$ . Finally,  $\mathcal{E}$  has dimension exactly  $p$  and the rank  $r$  of  $B = C - 1_n$  equals  $n - p$ .

(ii) For every  $1 \leq a, b \leq t$ , we can write

$$\Delta_{ab} = PU_a(QW_0^{-1}P - 1_n)U_bQ - PU_b(QW_0^{-1}P - 1_n)U_aQ = PU_aBU_bQ - PU_bBU_aQ \quad (4-2)$$

since  $U_a$  and  $U_b$  commute. Since  $B$  has rank  $r$ , there exist matrices  $B_1 \in \mathbb{Q}^{n \times r}$ ,  $B_2 \in \mathbb{Q}^{r \times n}$  with  $B = B_1 B_2$ . Setting  $V_a = PU_a B_1$  and  $G_a = B_2 U_a Q$  gives the claim.  $\square$

The following properties of the matrix  $B$  defined in [Lemma 4.1](#) are useful.

**Lemma 4.2.** *Let  $W_0 = PQ$  and  $W_a = PU_aQ$  for  $a \in [t]$  as in Problem  $\mathbb{D}$ . Let  $B \in \mathbb{Q}^{n \times n}$  be the matrix of [Lemma 4.1](#) with respect to  $P$  and  $Q$  and let  $r = n - p$ . Let  $B_1 \in \mathbb{Q}^{n \times r}$  and  $B_2 \in \mathbb{Q}^{r \times n}$  be such that  $B = B_1 B_2$ . Then:*

- (i)  $PB_1 = 0_{p \times r}$ .
- (ii) *The matrix  $Q' := [Q|B_1]$  is an  $n \times n$  invertible matrix.*

*Proof.* (i) The matrix  $B_2$  defines a surjection  $B_2 : \mathbb{Q}^n \rightarrow \mathbb{Q}^r$ . Thus for every  $x \in \mathbb{Q}^r$ , we write  $x = B_2 y$  for some  $y \in \mathbb{Q}^n$  and obtain  $P B_1 x = P B_1 (B_2 y) = (P B) y = 0$ .

(ii) Since  $r = n - p$ ,  $\mathbb{Q}^r$  has size  $n \times n$ . To show its invertibility, we show that  $\text{im}(Q) \cap \text{im}(B_1) = \{0\}$ . Since  $B_2$  is surjective, the images of  $B_1$  and  $B_1 B_2 = B$  coincide. Let  $Qx = By \in \text{im}(Q) \cap \text{im}(B_1)$ , with  $x \in \mathbb{Q}^p$  and  $y \in \mathbb{Q}^n$ . This gives  $Qx = (QW_0^{-1}P - 1_n)y = QW_0^{-1}Py - y$ . Thus  $y = QW_0^{-1}Py - Qx = Qz$  with  $z = W_0^{-1}Py - x$ . Therefore,  $Qx = By = B(Qz) = 0$  because  $BQ = 0$ .  $\square$

We now show that finding matrices  $\{V_a\}_a$  such that there exist  $\{G_a\}_a$  satisfying  $\Delta_{ab} = V_a G_b - V_b G_a$  for every  $a, b$  is sufficient to solve Problem  $\mathbb{D}$ . We view these matrices as being complementary to  $\{W_a\}_a$  because they define themselves an instance of Problem  $\mathbb{D}$  with the same solution as  $\{W_a\}_a$  (see the proof of Lemma 4.1). This allows us to increase the rank of  $Q$ . We thus now formulate Problem  $\mathbb{D}'$ .

**Definition 4.3** (Problem  $\mathbb{D}'$ ). Let  $n, t \geq 2$  and  $2 \leq p < n$  be integers. For every  $1 \leq a, b \leq t$ , let  $\Delta_{ab} \in \mathbb{Q}^{p \times p}$  be such that  $\Delta_{ab} = V_a G_b - V_b G_a$  for  $V_a \in \mathbb{Q}^{p \times (n-p)}$  of rank  $n - p$  and  $G_a \in \mathbb{Q}^{(n-p) \times p}$ . The problem is as follows: Given the matrices  $\Delta_{ab}$  for all  $1 \leq a, b \leq t$ , compute such matrices  $V_a$  for  $a \in [t]$ .

The following proposition links Problem  $\mathbb{D}$  and Problem  $\mathbb{C}$ .

**Proposition 4.4.** Let  $W_0 = PQ$  and  $W_a = PU_a Q$  for  $a \in [t]$  be as in Problem  $\mathbb{D}$ . For  $1 \leq a, b \leq t$ , let  $\Delta_{ab}$  be the matrices defined in (4-1). Moreover, assume that:

- (i) Problem  $\mathbb{D}'$  is uniquely solvable for the input matrices  $\{\Delta_{ab} : 1 \leq a < b \leq t\}$  and denote the unique solution by  $\{V_a : a \in [t]\}$ .
- (ii) Problem  $\mathbb{C}$  is uniquely solvable for the input matrices  $W'_0 = [W_0 | 0_{p \times (n-p)}] \in \mathbb{Q}^{p \times n}$  and  $W'_a = [W_a | V_a] \in \mathbb{Q}^{p \times n}$  for  $a \in [t]$ .

Then Problem  $\mathbb{D}$  is uniquely solvable on input  $\{W_a : 0 \leq a \leq t\}$  and the unique solution is given by the unique solution to Problem  $\mathbb{C}$  on input  $\{W'_a : 0 \leq a \leq t\}$ .

*Proof.* By Lemma 4.1 there exist  $V_a \in \mathbb{Q}^{p \times r}$  and  $G_a \in \mathbb{Q}^{r \times p}$  for  $a \in [t]$  such that  $\Delta_{ab} = V_a G_b - V_b G_a$  for all  $1 \leq a < b \leq t$ . Therefore the matrices  $\{\Delta_{ab}\}_{a,b}$  define an instance of Problem  $\mathbb{D}'$ . By Proposition 4.4(i), we compute the unique solution  $\{V_a\}_a$  for this problem.

Now, let  $W'_0 = [W_0 | 0_{p \times (n-p)}] \in \mathbb{Q}^{p \times n}$  and  $W'_a = [W_a | V_a] \in \mathbb{Q}^{p \times n}$  for  $a \in [t]$ . Let  $B = QW_0^{-1}P - 1_n$  as in Lemma 4.1 of rank  $r = n - p$ . Let  $B_1 \in \mathbb{Q}^{n \times r}$  and  $B_2 \in \mathbb{Q}^{r \times n}$  be a rank factorization of  $B$ ; i.e.,  $B = B_1 B_2$ . Letting  $Q' := [Q | B_1] \in \mathbb{Q}^{n \times n}$ , we have  $PQ' = P[Q | B_1] = [W_0 | 0_{p \times r}] = W'_0$  and, by uniqueness of  $\{V_a\}_a$  (see proof of Lemma 4.1),

$$PU_a Q' = PU_a [Q | B_1] = [W_a | V_a] = W'_a$$

for  $a \in [t]$ , as  $PB_1 = 0_{n \times r}$  by Lemma 4.2(i). The matrix  $Q'$  is invertible by Lemma 4.2(ii). Therefore,  $W'_0$  and  $\{W'_a\}_a$  define a valid input for Problem  $\mathbb{C}$ . By Proposition 4.4(ii), this problem is uniquely solvable and the solution must be the tuples of diagonal entries of the matrices  $\{U_a\}_a$ . This is also a solution to Problem  $\mathbb{D}$  since the matrices  $\{U_a\}_a$  are the same for the input matrices  $\{W_a\}_a$  for Problem  $\mathbb{D}$  and  $\{W'_a\}_a$  for Problem  $\mathbb{C}$ .  $\square$

**4A2. Solving problem  $\mathbb{D}'$ .** In view of [Proposition 4.4](#), it remains to compute matrices  $\{V_a\}_a$  from  $\{\Delta_{ab}\}_{a,b}$ . We achieve this by standard linear algebra, and combining with Algorithm  $\mathcal{A}_{\mathbb{C}}$  describes a full algorithm for Problem  $\mathbb{D}$ .

From now on we assume  $t \geq 3$ . Let  $\Delta_{ab} = V_a G_b - V_b G_a$  for  $1 \leq a, b \leq t$  as in Problem  $\mathbb{D}'$ . Let  $r = n - p$  and  $r_{ab}$  be the rank of  $\Delta_{ab}$ ; clearly,  $r_{ab} \leq \min(2r, p)$ . We further assume  $p > 2n/3$  (equivalently,  $2r < p$ ), which is a necessary condition as otherwise the matrices  $\Delta_{ab}$  likely have full rank and thus cannot reveal any information. We define  $\mathcal{K}_{ab} := \text{im}(\Delta_{ab}) = \mathcal{K}_{ba} \subseteq \mathbb{Q}^p$  and

$$\mathcal{K}_a = \bigcap_{b \in [t], b \neq a} \mathcal{K}_{ab}, a \in [t].$$

Let  $\mathcal{V}_a$  be the image of the matrix  $V_a$  for  $a \in [t]$ . We first argue that, heuristically,  $\mathcal{V}_a \subseteq \mathcal{K}_{ab}$  for every  $b \neq a$ . Let  $v \in \mathcal{V}_a$ . If there exists  $x \in \mathbb{Q}^p$  such that  $v = V_a G_b x$  and  $V_b G_a x = 0$  then  $v = \Delta_{ab} x$ , i.e.,  $v \in \mathcal{K}_{ab}$ . Such an element  $x$  must therefore lie in  $(x_0 + \ker(V_a G_b)) \cap \ker(V_b G_a)$ , where  $x_0 \in \mathbb{Q}^p$  is any vector such that  $v = V_a G_b x_0$ . It is easy to see that this intersection is nonempty if  $\ker(V_a G_b) + \ker(V_b G_a) = \mathbb{Q}^p$ . Heuristically, as  $\{V_a\}_a$  have rank  $r$ ,  $\ker(V_a G_b) + \ker(V_b G_a)$  has dimension at least  $2(p - r)$ ; accordingly we can heuristically expect that  $\ker(V_a G_b) + \ker(V_b G_a) = \mathbb{Q}^p$  as soon as  $2(p - r) > p$ , i.e.,  $p > 2n/3$ .

We now justify that, heuristically under a suitable parameter selection,  $\mathcal{K}_a = \mathcal{V}_a$  for every  $a \in [t]$ . For fixed  $a \in [t]$ , we compute  $\mathcal{K}_a$  modulo  $\mathcal{V}_a$  and consider  $\overline{\mathcal{K}_{ab}} := \mathcal{K}_{ab}/\mathcal{V}_a \subseteq \mathbb{Q}^{p-r}$  for  $b \neq a$ . Then  $\mathcal{K}_a = \mathcal{V}_a$  if and only if  $\overline{\mathcal{K}_a} := \bigcap_{b \neq a} \overline{\mathcal{K}_{ab}} = \{0\}$ . Since  $\mathcal{V}_a$  has dimension  $r$ ,  $\overline{\mathcal{K}_{ab}}$  has dimension  $r_{ab} - r$ . For every  $b \neq a$ , we view  $\overline{\mathcal{K}_{ab}}$  as the kernel of  $\mathbb{Q}^{p-r} \rightarrow \mathbb{Q}^{p-r}/\overline{\mathcal{K}_{ab}}$ , represented by a matrix  $A_{ab} \in \mathbb{Q}^{(p-r_{ab}) \times (p-r)}$ . Therefore  $\overline{\mathcal{K}_a}$  is represented by an augmented matrix  $A_a = [A_{a1} | \cdots | A_{a,a-1} | A_{a,a+1} | \cdots | A_{at}]$  describing the kernel of  $\mathbb{Q}^{p-r} \rightarrow \bigoplus_{b \neq a} \mathbb{Q}^{p-r}/\overline{\mathcal{K}_{ab}}$ . The matrix  $A_a$  has  $\sum_{b \in [t], b \neq a} (p - r_{ab})$  rows and  $p - r$  columns. Now,  $\mathcal{K}_a = \mathcal{V}_a$  if and only if  $A_a$  has full rank; and heuristically, we expect this to be the case as soon as  $\sum_{b \in [t], b \neq a} (p - r_{ab}) \geq p - r$ .

**Remark 4.5.** (i) In fact, we expect that  $r_{ab} = 2r$  for every  $a, b$ . Then, from what precedes, we expect, heuristically that  $\mathcal{K}_a = \mathcal{V}_a$  for every  $a$ , if  $(t - 1)(p - 2r) \geq p - r$ , i.e.,

$$\frac{p}{n} \geq \frac{2t - 3}{3t - 5} \quad \text{or, equivalently,} \quad t \geq \frac{2p - n}{3p - 2n} + 1. \quad (4-3)$$

(ii) We assumed  $t \geq 3$  so that the intersections  $\{\mathcal{K}_a\}_a$  are well-defined. If  $t = 2$ ,  $\mathcal{K}_1$  coincides with the image of  $\Delta_{12}$ , which will not reveal  $V_1$  and  $V_2$ .

We compute bases of  $\{\mathcal{K}_a\}_a$  by standard linear algebra. For the rest of this section, assume  $\mathcal{K}_a = \mathcal{V}_a$  for every  $a$ , and let  $C_a$  be a basis matrix for  $\mathcal{K}_a$ . Thus, there exists  $M_a \in \text{GL}_r(\mathbb{Q})$  such that  $V_a = C_a M_a$ . This gives for  $a < b$ :

$$\Delta_{ab} = V_a G_b - V_b G_a = C_a (M_a G_b) - C_b (M_b G_a) = C_a N_{ab} - C_b N_{ba} \quad (4-4)$$

with  $N_{ab} = M_a G_b$ . In (4-4),  $\Delta_{ab}$  and  $C_a, C_b$  are known, which allows us to compute  $N^{(ab)} = [N_{ab} | N_{ba}]^T$  as a solution to  $\Delta_{ab} = [C_a | -C_b] \cdot N^{(ab)}$ . Once the  $\{N_{ab}\}_{a,b}$  are computed, we obtain a system of linear

equations over  $\mathbb{Q}$ , given by

$$M_a^{-1} \cdot N_{ab} = G_b, \quad 1 \leq a < b \leq t. \quad (4-5)$$

It has  $\frac{1}{2}t(t-1)rp$  equations (there are  $\frac{1}{2}t(t-1)$  choices for pairs  $(a, b)$  and for each pair the matrix equality gives  $rp$  equations) and  $tr^2 + trp = trn$  variables, given by the  $tr^2$  entries of the matrices  $\{M_a^{-1} : a \in [t]\}$  and the  $trp$  entries of the matrices  $\{G_b : b \in [t]\}$ . Heuristically, if  $trn \leq \frac{1}{2}t(t-1)rp$ , i.e.,  $2n \leq (t-1)p$ , the system is expected to have a unique solution. This bound is automatically satisfied if (4-3) holds. This reveals  $\{M_a : a \in [t]\}$  and thus  $\{V_a : a \in [t]\}$  by computing  $V_a = C_a M_a$ .

**Proposition 4.6.** *Assume that  $\mathcal{K}_a = \mathcal{V}_a$  for every  $a \in [t]$  (see Remark 4.5(i)). Then, a unique solution to Problem  $\mathbb{D}'$  is implied by the existence of a unique solution to the explicit system of linear equations given in (4-5), which is a system of  $\frac{1}{2}t(t-1)(n-p)p$  linear equations in  $t(n-p)n$  variables. There are at least as many equations as variables as soon as  $p(t-1) \geq 2n$ .*

**4B. Algorithm.** We refer to this algorithm as Algorithm  $\mathcal{A}_{\mathbb{D}}$  in the sequel.

*Input:* A valid input for Problem  $\mathbb{D}$ .

*Output:* “Success” or “Fail”, and in case of “Success”, additionally output a solution. “Success” means that the computed solution is unique; “Fail” means that a solution was not found.

1. Compute  $\Delta_{ab} = W_a W_0^{-1} W_b - W_b W_0^{-1} W_a$  for  $1 \leq a \neq b \leq t$ .
2. For  $a \in [t]$ , compute a basis matrix  $C_a$  of  $\mathcal{K}_a := \bigcap_{b \in [t], b \neq a} \text{im}(\Delta_{ab})$ .
3. Check whether  $\dim(\mathcal{K}_a) \neq n - p$  for all  $a \in [t]$ .
  - 3.1 If true, output “Fail” and break.
  - 3.2 Otherwise, for every  $a < b$  compute  $N_{ab}$  as solutions to  $\Delta_{ab} = [C_a | -C_b] \cdot [N_{ab} | N_{ba}]^T$ .
4. Solve for  $\{M_a\}_a$  the system of linear equations  $M_a^{-1} N_{ab} = G_b$  for  $(a, b) \in [t]^2, a < b$ .
  - 4.1. If a unique solution is not found, output “Fail” and break.
5. Compute the matrices  $\{V_a : a \in [t]\}$  as  $V_a = C_a \cdot M_a$ .
6. Run Algorithm  $\mathcal{A}_{\mathbb{C}}$  on the matrices  $W'_0 = [W_0 | 0]$  and  $W'_a = [W_a | V_a]$  for  $a \in [t]$  and return its output.

**Remark 4.7.** Problem  $\mathbb{D}$  of Definition 1.1 is symmetric in the sense that  $P$  and  $Q$  have the same rank. An asymmetric variant consists in having  $P$  and  $Q$  of ranks  $p \neq q$ . Our algorithm adapts to that case: if  $p < q$ , then “cutting” the last  $q - p$  columns of  $\{W_a\}_a$  means “cutting” the last  $q - p$  columns of  $Q$ , which reduces to the symmetric case. This approach is however not very genuine, as it “cuts” information instead of possibly exploiting it. We leave it open to find a better algorithm.

**4C. Optimization of the parameters.** We find minimal possible values for  $t$  and  $p$  with respect to a given  $n$ . In Section 5B1 we will see that it is of interest to minimize  $2p + t$  in order to minimize the number of public encodings in [CLT13]. According to (4-3), the main (heuristic) condition to be ensured is  $p \geq \frac{2t-3}{3t-5}n$ . We set  $F_n(t) = 2p_n(t) + t = \frac{2t-3}{3t-5}n + t$  for  $t \in \mathbb{R}_{>0} \setminus \{\frac{5}{3}\}$  and  $n \geq 2$ . Then  $F_n$  has a minimum

at  $t_0 = \frac{1}{3}(\sqrt{2n} + 5)$ , with  $p_n(t_0) = \frac{2}{3}n + \frac{1}{3\sqrt{2}}\sqrt{n}$  and  $F_n(t_0) = \frac{4}{3}n + \frac{2}{3}\sqrt{2n} + \frac{5}{3}$ . In conclusion, we expect Algorithm  $\mathcal{A}_{\mathbb{D}}$  to succeed for  $p = \lceil p_n(t_0) \rceil$  and  $t = \lceil t_0 \rceil$ .

## 5. Applications

We describe two applications for our algorithms and obtain significant improvements on previous works.

**5A. Improved algorithm for the CRT-ACD Problem.** We consider the following “multi-prime” version of the approximate common divisor problem [CP19] based on Chinese remaindering:

**Definition 5.1** (CRT-ACD problem). Let  $n, \eta, \rho \in \mathbb{Z}_{\geq 1}$ . Let  $p_1, \dots, p_n$  be distinct  $\eta$ -bit prime numbers and  $M = \prod_{i=1}^n p_i$ . Consider a nonempty finite set  $\mathcal{S}$  of integers in  $\mathbb{Z} \cap [0, M)$  such that for every  $x \in \mathcal{S}$ ,

$$x \equiv x_i \pmod{p_i}, \quad 1 \leq i \leq n,$$

for uniformly distributed integers  $x_i \in \mathbb{Z}$  satisfying  $|x_i| \leq 2^\rho$ .

The CRT-ACD problem is stated as follows: given the set  $\mathcal{S}$ , the integers  $\eta, \rho$  and  $M$  factor  $M$  completely (i.e., find the prime numbers  $p_1, \dots, p_n$ ).

Clearly, the larger the set  $\mathcal{S}$ , the more information one can exploit to factor  $M$ . Our interest is therefore to minimize the cardinality of the set  $\mathcal{S}$  with respect to  $n$ .

**5A1. The algorithm of [CP19].** Coron and Pereira propose an algorithm for the case  $\#\mathcal{S} = n + 1$ . They proceed in two steps called the “orthogonal lattice attack” following [NS99] and the “algebraic attack” following [CHL<sup>+</sup>15]. We briefly review their algorithm; for a complete description we refer to [CP19, Section 4.3].

Let  $\mathcal{S} = \{x_1, \dots, x_n, y\}$  and  $x = (x_1, \dots, x_n) \in \mathcal{S}^n$ . Then, the vector  $b = (x, y \cdot x) \in \mathbb{Z}^{2n}$  is public, and by the Chinese remainder theorem, letting  $x \equiv x^{(i)} \pmod{p_i}$  and  $y \equiv y^{(i)} \pmod{p_i}$  for all  $i \in [n]$ , one has  $b \equiv \sum_{i=1}^n c_i(x^{(i)}, y^{(i)}x^{(i)}) =: \sum_{i=1}^n c_i b^{(i)} \pmod{M}$ , for some integers  $c_1, \dots, c_n$ . If the vectors  $\{x^{(i)}\}_i$  are  $\mathbb{R}$ -linearly independent, then so are  $\{b^{(i)}\}_i$  and they generate a  $2n$ -dimensional lattice  $\mathcal{L}$  of rank  $n$ . Importantly, by Definition 5.1, the vectors  $\{b^{(i)}\}_i$  are reasonably short vectors (of  $\ell_2$ -norm approximately  $2^{2\rho}$ ; and  $\rho$  is considered much smaller than  $\eta$ ).

The “orthogonal lattice attack” is an algorithm, which on input  $b$ , outputs a basis of the completion  $\bar{\mathcal{L}} = \mathcal{L} \otimes_{\mathbb{Z}} \mathbb{Q}$  of  $\mathcal{L}$ , performing lattice reduction on the lattice  $\langle b \rangle^{\perp_M}$  of vectors  $v \in \mathbb{Z}^m$  such that  $\langle v, b \rangle \equiv 0 \pmod{M}$ . The parameters are chosen accordingly, and one essentially requires  $2\rho < \eta$ .

Upon finding a basis  $\{b'^{(i)}\}_i$  of  $\bar{\mathcal{L}}$ , Coron and Pereira proceed with the “algebraic attack”. The bases  $\{b'^{(i)}\}_i$  of  $\bar{\mathcal{L}}$  and  $\{b^{(i)}\}_i$  of  $\mathcal{L}$  are related via an unknown invertible base change matrix  $Q \in \mathbb{Q}^{n \times n}$ . Letting  $P = [x^{(1)} | \dots | x^{(n)}] \in \mathbb{Z}^{n \times n}$  with columns  $\{x^{(i)}\}_i$ , one obtains matrix relations

$$W_0 = P \cdot Q, \quad W_1 = P \cdot U_1 \cdot Q, \tag{5-1}$$

where  $U_1$  is  $n \times n$  diagonal with entries  $\{y^{(i)}\}_i$ . The matrix  $W_0$  is invertible (over  $\mathbb{Q}$ ) and one computes the eigenvalues  $\{y^{(i)}\}_i$  of  $W_1 W_0^{-1} = P U_1 P^{-1}$ . Using  $y \equiv y^{(i)} \pmod{p_i}$ , one factors  $M$  by computing greatest common divisors.

**5A2. A naive improvement.** There is a naive generalization of [CP19] using only  $\mathcal{O}(\sqrt{n})$  public instances in  $\mathcal{S}$ . However, we argue that this approach gives a worse range of parameters when combined with [CP19].

For integers  $p \geq 2$  and  $t \geq 1$  of size  $\mathcal{O}(\sqrt{n})$ , let  $x = (y_1 \cdot z, \dots, y_t \cdot z) \in \mathbb{Z}^{tp}$  of dimension  $\mathcal{O}(n)$  for  $y_1, \dots, y_t \in \mathcal{S}$  and  $z \in \mathcal{S}^p$ . This variant reduces  $\#\mathcal{S}$  considerably, as  $\#\mathcal{S} = p + t = \mathcal{O}(\sqrt{n})$ . However, [CP19] requires one to construct the vector  $b = (x, y \cdot x)$  for  $y \in \mathcal{S}$ . This gives rise to residue vectors  $\{b^{(i)}\}_i$  of approximate  $\ell_2$ -norm  $2^{3\rho}$  instead of  $2^{2\rho}$  as in [CP19]. Therefore the stronger condition  $3\rho < \eta$  will be required for the orthogonal lattice attack to succeed. In our improvement, we would like to lower  $\#\mathcal{S}$  while continuing to use  $2\rho < \eta$ , as in [CP19].

**5A3. Our improved algorithm.** We recognize that (5-1) defines an instance of Problem  $\mathbb{A}$  of Definition 1.1 with  $t = 1$  because  $P$  and  $Q$  have rank  $n$ . Our improvement lies in generalizing the vector  $b$  to obtain an instance of Problem  $\mathbb{C}$ .

We consider  $\#\mathcal{S} < n + 1$  and write for convenience  $\mathcal{S} = \{x_1, \dots, x_p, y_1, \dots, y_t\}$  with integers  $2 \leq p < n$  and  $2 \leq t < n$  satisfying  $2n \leq (t+1)p$ . We let  $x = (x_1, \dots, x_p) \in \mathcal{S}^p$  and  $b = (x, y_1 \cdot x, \dots, y_t \cdot x) \in \mathbb{Z}^{(t+1)p}$ . As before, let  $\{b^{(i)}\}_i$  denote the short residue vectors modulo the primes  $\{p_i\}_i$  and  $x \equiv x^{(i)} \pmod{p_i}$ ,  $y_a \equiv y_a^{(i)} \pmod{p_i}$  for  $a \in [t]$  and  $i \in [n]$ . By the Chinese remainder theorem, we observe that  $b$  lies in the lattice  $\mathcal{L} = \bigoplus_{i=1}^n \mathbb{Z}b^{(i)}$  modulo  $M$ . Namely, there are integers  $c_1, \dots, c_n$  such that

$$b \equiv \sum_{i=1}^n c_i \begin{bmatrix} x^{(i)} \\ y_1^{(i)} \cdot x^{(i)} \\ \vdots \\ y_t^{(i)} \cdot x^{(i)} \end{bmatrix} =: \sum_{i=1}^n c_i b^{(i)} \pmod{M}.$$

As in [CP19], the orthogonal lattice algorithm reveals a basis  $\{b^{(i)}\}_i$  of  $\overline{\mathcal{L}}$  and the  $\ell_2$ -norm of  $\{b^{(i)}\}_i$  is still approximately  $2\rho$ .

Contrary to (5-1), we now derive matrix equations

$$W_0 = P \cdot Q, W_a = P \cdot U_a \cdot Q, a \in [t], \quad (5-2)$$

where  $P \in \mathbb{Z}^{p \times n}$  has columns  $\{x^{(i)}\}_i$  and  $\{U_a\}_a$  are  $n \times n$  diagonal with entries  $\{y_a^{(i)}\}_{a,i}$ . The matrix  $Q$  is a base change matrix from  $\{b^{(i)}\}_i$  to  $\{b^{(i)}\}_i$ . If  $W_0$  has rank  $p$ , (5-2) now defines a valid input for Problem  $\mathbb{C}$  of Definition 1.1 and Algorithm  $\mathcal{A}_{\mathbb{C}}$  from Section 3 reveals the diagonal entries  $\{y_a^{(i)}\}_{a,i}$  of the matrices  $\{U_a\}_a$ . One can then factor  $M$  by computing  $\gcd(y_a - y_a^{(i)}, M)$ .

From Section 3C we see that  $\#\mathcal{S} = p + t$  is minimized for  $p = \lceil \sqrt{2n} \rceil$  and  $t + 1 = \lceil \sqrt{2n} \rceil$ . Thus,  $\#\mathcal{S} = 2\lceil \sqrt{2n} \rceil = \mathcal{O}(\sqrt{n})$ . In summary, letting  $n$  be the number of secret primes in the public modulus  $M$ , we can factor  $M$  given only  $\mathcal{O}(\sqrt{n})$  input samples, whereas [CP19] uses  $\mathcal{O}(n)$ .

**Remark 5.2.** We remark that we do not impact the security of the key-exchange from [CP19], as it uses certain encodings of matrices. However, the product of matrices does not commute, so our techniques do not apply to that case.



**5B. Improved cryptanalysis of CLT13 multilinear maps.** We consider now the CLT13 multilinear map scheme by Coron et al., [CLT13]. Cheon et al. [CHL<sup>+</sup>15] described a polynomial-time attack against the Diffie–Hellman key exchange based on CLT13 when enough encodings of zero are public. Such encodings are for instance public in the rerandomization procedure. It is of interest to investigate this cryptanalysis when only a limited number of such encodings is available. Namely, not every CLT13-based construction necessarily reveals enough such encodings and the attack of Cheon et al. is prevented.

**5B1. CLT13 multilinear maps.** The CLT13 multilinear map is a construction over the integers based on the notion of graded encoding scheme [GGH13]. Its hardness relies on Chinese remainder representations and factorization. We fix an integer  $n \geq 2$ , thought of as a dimension for CLT13. The message space is  $\bigoplus_{i=1}^n \mathbb{Z}/g_i\mathbb{Z}$  for some small secret primes  $\{g_i\}_i$ . The encoding space has a graded structure and supports homomorphic addition and multiplication. It is defined over  $\bigoplus_{i=1}^n \mathbb{Z}/p_i\mathbb{Z}$  for large secret primes  $\{p_i\}_i$  with public product  $x_0 = \prod_i p_i$ . More precisely, an encoding of a message  $m = (m_i)_i \in \bigoplus_{i=1}^n \mathbb{Z}/g_i\mathbb{Z}$  at level  $k \in [\kappa]$  (where  $\kappa$  denotes the multilinearity degree) is an integer  $c$  such that

$$c \equiv (r_i g_i + m_i) \cdot z^{-k} \pmod{p_i}$$

for all  $i \in [n]$  where  $z \in (\mathbb{Z}/x_0\mathbb{Z})^\times$  and  $r_i$  is a random “small” noise. By the Chinese remainder theorem,  $c$  is computed modulo  $x_0$ . For encodings  $c$  at the last level  $\kappa$ , a public zero-testing procedure allows one to test if  $c$  encodes zero. This procedure works by computing  $\omega(c) := p_{zt} \cdot c$  for a public parameter  $p_{zt} \in \mathbb{Z}/x_0\mathbb{Z}$ . Then  $c$  encodes the zero message if  $\omega$  is “small” compared to  $x_0$ . In [CLT13], one actually defines a vector of  $n$  zero-test parameters  $\{p_{zt,i} : i \in [n]\}$  to define a proper zero-testing. For the precise parameter setting, we refer to [CLT13, Section 3.1].

**5B2. Cryptanalysis.** The algorithm from [CHL<sup>+</sup>15] reveals all secret parameters given sufficiently many encodings of zero. We briefly recall the attack here, and for simplicity of exposition, assume  $\kappa = 3$ . Consider sets  $\mathcal{A} = \{\alpha_j : j \in [n]\}$ ,  $\mathcal{B} = \{\beta_1, \beta_2\}$  and  $\mathcal{C} = \{\gamma_k : k \in [n]\}$  of encodings at level 1 and where all encodings in  $\mathcal{A}$  encode zero. Therefore, there are  $\#\mathcal{A} = n$  public encodings of zero and  $\#(\mathcal{A} \cup \mathcal{B} \cup \mathcal{C}) = 2n + 2$  encodings in total. In the previous notation, we write  $\alpha_j \equiv \alpha_{ji}/z \pmod{p_i}$ ,  $\beta_a \equiv \beta_{ai}/z \pmod{p_i}$  and  $\gamma_k \equiv \gamma_{ki}/z \pmod{p_i}$  for all  $i, j, k \in [n]$  and  $a \in [2]$ . Because the products  $\alpha_j \beta_a \gamma_k$  encode zero at level 3, correct zero-testing ensures that the zero-test equations  $\omega_{jk}^{(a)} = p_{zt}(\alpha_j \beta_a \gamma_k)$ , given by

$$\omega_{jk}^{(a)} = \sum_{i=1}^n p_{zt,i} \alpha_{ji} \beta_{ai} \gamma_{ki} = [\alpha_{j1} \cdots \alpha_{jn}] \begin{bmatrix} \beta_{a1} p_{zt,1} & & \\ & \ddots & \\ & & \beta_{an} p_{zt,n} \end{bmatrix} \begin{bmatrix} \gamma_{k1} \\ \vdots \\ \gamma_{kn} \end{bmatrix}$$

for certain explicit integers  $p_{zt,i}$  for  $i \in [n]$  defining the zero-test parameter, hold over  $\mathbb{Z}$  instead of  $\mathbb{Z}/x_0\mathbb{Z}$ . Writing these relations out for all indices  $(j, k) \in [n]^2$ , the  $n \times n$  matrices  $W_a := (\omega_{jk}^{(a)})_{j,k \in [n]}$  for  $a = 1, 2$  satisfy

$$W_a = P \cdot U_a \cdot Q \tag{5-3}$$

for secret matrices  $P, Q$  of full rank  $n$  (corresponding to encodings of  $\mathcal{A}$  and  $\mathcal{C}$ , respectively) and diagonal



matrices  $\{U_a\}_a$  containing the elements  $\{\beta_{ai} : i \in [n]\}$ . If at least one of  $W_1, W_2$  is invertible over  $\mathbb{Q}$  (say,  $W_2$ ), the attacker computes the eigenvalues  $\{\beta_{1i}/\beta_{2i} : i \in [n]\}$  of  $W_1 W_2^{-1}$ . These ratios are enough to factor  $x_0$ . Indeed, letting  $\beta_{1i}/\beta_{2i} = x_i/y_i$  for coprime integers  $x_i, y_i$  and using  $\beta_a \equiv \beta_{ai}/z \pmod{p_i}$ , we deduce  $x_i \beta_2 - y_i \beta_1 \equiv (x_i \beta_{2i} - y_i \beta_{1i})/z \equiv 0 \pmod{p_i}$  for  $i \in [n]$  and therefore  $\gcd(x_i \beta_2 - y_i \beta_1, x_0) = p_i$  with high probability.

In summary, the Cheon et al. attack recovers all secret primes  $\{p_i\}_i$  in polynomial time given the set  $\mathcal{A}$  of level-one encodings of zero and the sets  $\mathcal{B}$  and  $\mathcal{C}$ .

**5B3. Attacking CLT13 with fewer encodings.** We consider the following CLT13-based problem.

**Definition 5.3** (CLT13 problem). Let  $n \geq 2$  be the dimension of CLT13 and  $x_0 = \prod_{i=1}^n p_i$ . Let  $\mathcal{E}$  be a finite nonempty set of encodings at level 1 and  $\mathcal{E}_0 \subseteq \mathcal{E}$  a nonempty subset such that every element of  $\mathcal{E}_0$  is an encoding of zero. The CLT13 problem is as follows: Given the sets  $\mathcal{E}$  and  $\mathcal{E}_0$ , factor  $x_0$ .

We refer to  $\mathcal{E}$  and  $\mathcal{E}_0$  as the sets of “available encodings” and “available encodings of zero”, respectively. It is not a loss of generality to consider level-one encodings. As in [CHL<sup>+</sup>15], we write  $\mathcal{E} = \mathcal{A} \cup \mathcal{B} \cup \mathcal{C}$  with  $\mathcal{A} \subseteq \mathcal{E}_0$ . As recalled above, [CHL<sup>+</sup>15] requires  $\#\mathcal{E}_0 \geq n$  to factor  $x_0$ , and a total number of public encodings  $\#\mathcal{E} = 2n + 2$ .

We aim at reducing the number of encodings needed for the factorization of  $x_0$  and treat the following questions independently:

- (i) Factor  $x_0$  with fewer available encodings of zero, i.e.,  $\#\mathcal{E}_0 < n$ .
- (ii) Factor  $x_0$  with fewer available encodings, i.e.,  $\#\mathcal{E} < 2n + 2$ .

*A naive improvement.* As for the CRT-ACD problem, there is a naive improvement using fewer encodings, but assuming  $\kappa = 4$ . One can form product encodings  $\alpha_j \beta_a \gamma_k \delta_\ell$  at level 4, where every encoding is at level 1. These can be partitioned into sets  $\mathcal{A}, \mathcal{B}$  and  $\mathcal{C}$  such that  $\mathcal{A}$  corresponds to encodings of zero with  $\#\mathcal{A} = \mathcal{O}(\sqrt{n})$ . However, this approach has the inconvenience of using  $\kappa = 4$  and our improved attack aims at lowering the number of public encodings while  $\kappa = 3$ .

*Minimizing the number of encodings of zero.* We explain how to use Algorithm  $\mathcal{A}_\mathbb{C}$  to factor  $x_0$  using only  $\#\mathcal{E}_0 = \mathcal{O}(\sqrt{n})$  level-one encodings of zero.

We fix integers  $2 \leq p < n$  and  $3 \leq t < n$  and assume again  $\kappa = 3$ . As in [CHL<sup>+</sup>15], we write  $\mathcal{E} = \mathcal{A} \cup \mathcal{B} \cup \mathcal{C}$  with  $\mathcal{A} \subseteq \mathcal{E}_0$ . We let  $\#\mathcal{A} = p$ ,  $\#\mathcal{B} = t$  and  $\#\mathcal{C} = n$ ; and claim  $p = \mathcal{O}(\sqrt{n})$ .

Every product encoding  $c = \alpha_j \beta_a \gamma_k$  with  $(\alpha_j, \beta_a, \gamma_k) \in \mathcal{A} \times \mathcal{B} \times \mathcal{C}$  is an encoding of zero and by correct zero-testing we obtain integer matrix relations

$$W_a = P \cdot U_a \cdot Q, \quad a \in [t], \quad (5-4)$$

for  $P \in \mathbb{Z}^{p \times n}$ ,  $Q \in \mathbb{Z}^{n \times n}$  corresponding to encodings in  $\mathcal{A}$  and  $\mathcal{C}$ , respectively, and diagonal matrices  $\{U_a\}_a$  corresponding to  $\mathcal{B}$ . Exactly as in [CHL<sup>+</sup>15], the matrices  $\{U_a\}_a$  contain integers  $\beta_{ai}$  such that  $\beta_a \equiv \beta_{ai} \pmod{p_i}$  for  $i \in [n]$ . With high probability the ranks of  $P$  and  $Q$  are  $p$  and  $n$ , respectively. Defining  $W'_0 = W_1$  and  $W'_a = W_{a-1}$  for  $2 \leq a \leq t$  we obtain an instance similar to Problem  $\mathbb{C}$  of

**Definition 1.1**, but without a “special input matrix”  $PQ$  (see [Section 2B](#)). Using Algorithm  $\mathcal{A}_{\mathbb{C}}$ , we reveal eigenvalues (the diagonal entries) of the matrices  $\{U_a U_1^{-1}\}_a$  as it is likely that  $U_1$  will be invertible. We finally deduce the prime factorization of  $x_0$  by taking greatest common divisors, as in [\[CHL<sup>+</sup>15\]](#).

By the optimization in [Section 3C](#), we choose  $t = \lceil \sqrt{2n} \rceil$  and  $\#A = p = \lceil \sqrt{2n} \rceil$ .

*Minimizing the total number of encodings.* We now explain how to use Algorithm  $\mathcal{A}_{\mathbb{D}}$  to factor  $x_0$  using  $\#\mathcal{E} = \frac{4}{3}n + \mathcal{O}(\sqrt{n})$  instead of  $\#\mathcal{E} = 2n + 2$  as in [\[CHL<sup>+</sup>15\]](#).

Contrary to the previous case, we now use a set  $\mathcal{C}$  with  $\#\mathcal{C} = p$ ; so  $\#\mathcal{E} = 2p + t$ . It is now straightforward to see that upon correct zero-testing we derive equations as in (5-4) but with  $Q \in \mathbb{Z}^{n \times p}$  instead. Thus, if both  $P$  and  $Q$  have rank  $p$ , we obtain Problem  $\mathbb{D}$  of [Definition 1.1](#) without “special input matrix”  $W_0$ . Then Algorithm  $\mathcal{A}_{\mathbb{D}}$  reveals ratios of diagonal entries of  $\{U_a U_1^{-1}\}$  and we consequently factor  $x_0$ .

Following [Section 4C](#), we are led to minimize  $\#\mathcal{E}(n) = 2p + t$  as a function of  $n$ . We can let  $p = \lceil \frac{2}{3}n + \frac{1}{3\sqrt{2}}\sqrt{n} \rceil$  and  $t = \lceil \frac{1}{3}\sqrt{2n} + \frac{5}{3} \rceil$  and obtain

$$\#\mathcal{E}(n) = 2 \lceil \frac{2}{3}n + \frac{1}{3\sqrt{2}}\sqrt{n} \rceil + \lceil \frac{1}{3}\sqrt{2n} + \frac{5}{3} \rceil = \frac{4}{3}n + \mathcal{O}(\sqrt{n}).$$

*Cryptanalysis with independent slots.* In [\[CN19\]](#), Coron and Notarnicola cryptanalyze CLT13 when no encodings of zero are available beforehand, but instead only “partial-zero” encodings. Messages are nonzero modulo a product of several primes  $g_1 \cdots g_\theta$  for some integer  $\theta \in [n]$ . We can improve this cryptanalysis following the same techniques as above. Let  $\ell$  the number of partial-zero encodings. Since [\[CN19\]](#) is based on the algorithm of Cheon et al. to factor  $x_0$ , we can now replace it by Algorithm  $\mathcal{A}_{\mathbb{C}}$  once  $\ell$  encodings of zero are created. This means that we can set  $\ell = \mathcal{O}(\sqrt{n})$ , which brings a twofold improvement: first, lattice reduction (in the orthogonal lattice attack [\[CN19, Section 4\]](#)) is only run on a lattice of dimension  $\mathcal{O}(\sqrt{n})$ ; and second, the number of partial-zero encodings is reduced to  $\mathcal{O}(\sqrt{n})$ .

## 6. Computational aspects and practical results

We describe practical parameters for algorithms  $\mathcal{A}_{\mathbb{C}}$  and  $\mathcal{A}_{\mathbb{D}}$ . We have implemented our algorithms in SageMath: our source code is provided in <https://pastebin.com/Yg6QgZTh>. Our experiments are done on a standard Intel Core i7 3.3 GHz processor.

**6A. Instance generation of problems  $\mathbb{C}$  and  $\mathbb{D}$ .** As for applications in cryptanalysis, we consider matrices with integer entries. To generate instances of Problems  $\mathbb{C}$  and  $\mathbb{D}$ , given fixed integers  $n, t, p$ , we uniformly at random generate matrices  $P, Q$  and  $\{U_a\}_a$  with entries in  $[-k, k] \cap \mathbb{Z}$  for some  $k \in \mathbb{Z}_{\geq 1}$  as in [Definition 1.1](#). Setting  $W_0 = PQ$  and  $W_a = P U_a Q$  for  $a \in [t]$  gives instances of Problems  $\mathbb{C}$  or  $\mathbb{D}$ .

We perform the linear algebra over  $\mathbb{Z}/\ell\mathbb{Z}$  for a large prime  $\ell$ , instead of over  $\mathbb{Q}$ . It suffices to choose  $\ell$  slightly larger than the diagonal entries of  $\{U_a\}_a$  (e.g.,  $\ell = \mathcal{O}(\max_{a,i} |u_{ai}|)$ , where  $u_{ai}$  for  $i \in [n]$  denote the diagonal entries of  $U_a$ ). The running time depends on the entry size of the generated matrices. The overall computational cost of our algorithms  $\mathcal{A}_{\mathbb{C}}$  and  $\mathcal{A}_{\mathbb{D}}$  is dominated by the cost of solving systems of linear equations and performing simultaneous diagonalization, which can be done by standard algorithms for nonsparse linear algebra.

$n$	entry size	Algorithm $\mathcal{A}_{\mathbb{C}}$					Algorithm $\mathcal{A}_{\mathbb{D}}$				
		practice $p$ $t$		theory $p_0(n)$ $t_0(n)$		running time	practice $p$ $t$		theory $p_0(n)$ $t_0(n)$		running time
15	1000	6	4	6	5	4 min 4 s	11	4	11	4	4 min 2 s
25	750	8	7	8	7	3 min 45 s	18	4	18	5	1 min 54 s
50	600	10	9	10	9	4 min 34 s	35	5	35	5	1 min 39 s
100	200	15	14	15	14	1 h 17 min	70	7	70	7	5 min 14 s
150	100	18	16	18	17	6 h 29 min	103	8	103	8	23 min 14 s
500	20	32	31	32	31	29 min 3 s	339	13	339	13	6 min 57 s

**Table 1.** Experimental data for Algorithms  $\mathcal{A}_{\mathbb{C}}$  and  $\mathcal{A}_{\mathbb{D}}$ .

**6B. Practical experiments.** We gather in [Table 1](#) practical parameters for problems  $\mathbb{C}$  and  $\mathbb{D}$ , and our applications of [Section 5](#). We compare  $p, t$  with the theoretical values  $p_0(n), t_0(n)$  obtained in the two algorithms. For [Section 3](#),  $p_0(n) = \lceil \sqrt{2n} \rceil$  and  $t_0(n) = \lceil \sqrt{2n} - 1 \rceil$ . For [Section 4](#),  $p_0(n) = \lceil \frac{2}{3}n + \frac{\sqrt{n}}{3\sqrt{2}} \rceil$  and  $t_0(n) = \lceil \frac{1}{3}(\sqrt{2n} + 5) \rceil$ . Here “entry size” is an approximation of the bit-size of the max-norm of each input matrix.

Our work is compared with [\[CP19\]](#) for the CRT-ACD problem in [Table 2](#) and with [\[CHL<sup>+</sup>15\]](#) for the cryptanalysis of CLT13 in [Table 3](#). We give parameters for obtaining a complete factorization of  $M$  (in CRT-ACD) and  $x_0$  (in CLT13) of approximate bit-size  $n\eta$ . For CRT-ACD, the column “this work” equals  $\#S = p + t$  (Series 1). For CLT13, “this work” shows  $\#\mathcal{E} = 2p + t$  (Series 2) and  $\#\mathcal{E}_0 = p$  (Series 3). Thus, for  $n = 50$ , our algorithm factors  $M$  (in CRT-ACD) using only 19 public samples, whereas [\[CP19\]](#) requires 51 samples; and similarly breaks CLT13 with only 10 public encodings of zero, while [\[CHL<sup>+</sup>15\]](#) uses 50.

In conclusion, these practical experiments overall confirm our theory, as well as the quadratic improvement over [\[CP19\]](#) and [\[CHL<sup>+</sup>15\]](#).

Series 1					num. of samples	
$n$	$\eta$	$\rho$	$p$	$t$	this work	<a href="#">[CP19]</a>
20	1000	200	7	6	13	21
30	1000	100	8	7	15	31
50	800	100	10	9	19	51

**Table 2.** Experimental data for the CRT-ACD problem.

Series 2					num. of encodings		Series 3		num. of encodings of zero	
$n$	$\eta$	$\rho$	$p$	$t$	this work	<a href="#">[CHL<sup>+</sup>15]</a>	$p$	$t$	this work	<a href="#">[CHL<sup>+</sup>15]</a>
20	1000	200	15	4	34	42	7	6	7	20
30	1000	100	22	5	49	62	8	7	8	30
50	800	100	35	5	75	102	10	9	10	50

**Table 3.** Experimental data for the CLT13 Problem.

## Acknowledgments

We thank the anonymous reviewers of ANTS-XIV for their helpful comments. Notarnicola acknowledges support by the Luxembourg National Research Fund through grant PRIDE15/10621687/-SPsquared.

## References

- [CH13] Henry Cohn and Nadia Heninger, *Approximate common divisors via lattices*, ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium (Berkeley, CA) (Everett W. Howe and Kiran S. Kedlaya, eds.), Open Book Ser., no. 1, Math. Sci. Publ., 2013, pp. 271–293. [MR 3207418](#)
- [CHL<sup>+</sup>15] Jung Hee Cheon, Kyoohyung Han, Changmin Lee, Hansol Ryu, and Damien Stehlé, *Cryptanalysis of the multilinear map over the integers*, Advances in cryptology—EUROCRYPT 2015, I, Lecture Notes in Comput. Sci., no. 9056, Springer, 2015, pp. 3–12. [MR 3344918](#)
- [CLLT16] Jean-Sébastien Coron, Moon Sung Lee, Tancrède Lepoint, and Mehdi Tibouchi, *Cryptanalysis of GGH15 multilinear maps*, Advances in cryptology—CRYPTO 2016, II, Lecture Notes in Comput. Sci., no. 9815, Springer, 2016, pp. 607–628. [MR 3565321](#)
- [CLT13] Jean-Sébastien Coron, Tancrède Lepoint, and Mehdi Tibouchi, *Practical multilinear maps over the integers*, Advances in cryptology—CRYPTO 2013, I (Ran Canetti and Juan A. Garay, eds.), Lecture Notes in Comput. Sci., no. 8042, Springer, 2013, pp. 476–493. [MR 3126439](#)
- [CN19] Jean-Sébastien Coron and Luca Notarnicola, *Cryptanalysis of CLT13 multilinear maps with independent slots*, Advances in Cryptology—ASIACRYPT 2019, II, no. 11922, Springer, 2019, pp. 356–385.
- [CP19] Jean-Sébastien Coron and Hilder V. L. Pereira, *On Kilian’s randomization of multilinear map encodings*, Advances in Cryptology—ASIACRYPT 2019, II, vol. 11922, Springer, 2019, pp. 325–355.
- [GGH13] Sanjam Garg, Craig Gentry, and Shai Halevi, *Candidate multilinear maps from ideal lattices*, Advances in cryptology—EUROCRYPT, 2013 (Thomas Johansson and Phong Q. Nguyen, eds.), Lecture Notes in Comput. Sci., no. 7881, Springer, 2013, pp. 1–17. [MR 3095515](#)
- [GGH15] Craig Gentry, Sergey Gorbunov, and Shai Halevi, *Graph-induced multilinear maps from lattices*, Theory of cryptography, II (Yevgeniy Dodis and Jesper Buus Nielsen, eds.), Lecture Notes in Comput. Sci., no. 9015, Springer, 2015, pp. 498–527. [MR 3354209](#)
- [GGM16] Steven D. Galbraith, Shishay W. Gebregiyorgis, and Sean Murphy, *Algorithms for the approximate common divisor problem*, LMS J. Comput. Math. **19** (2016), 58–72, suppl. A. [MR 3540946](#)
- [HJ16] Yupu Hu and Huiwen Jia, *Cryptanalysis of GGH map*, Advances in cryptology—EUROCRYPT 2016, I, Lecture Notes in Comput. Sci., no. 9665, Springer, 2016, pp. 537–565. [MR 3516383](#)
- [NS99] Phong Nguyen and Jacques Stern, *The hardness of the hidden subset sum problem and its cryptographic implications*, Advances in cryptology—CRYPTO 1999, Lecture Notes in Comput. Sci., no. 1666, Springer, 1999, pp. 31–46. [MR 1729292](#)
- [vDGHV10] Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan, *Fully homomorphic encryption over the integers*, Advances in cryptology—EUROCRYPT 2010, Lecture Notes in Comput. Sci., no. 6110, Springer, 2010, pp. 24–43. [MR 2660481](#)

Received 27 Feb 2020.

JEAN-SÉBASTIEN CORON: [jean-sebastien.coron@uni.lu](mailto:jean-sebastien.coron@uni.lu)

Faculté des Sciences, de la Technologie et de la Communication, University of Luxembourg, Esch-sur-Alzette, Luxembourg

LUCA NOTARNICOLA: [luca.notarnicola@uni.lu](mailto:luca.notarnicola@uni.lu)

Faculté des Sciences, de la Technologie et de la Communication, Université du Luxembourg, Esch-sur-Alzette, Luxembourg

GABOR WIESE: [gabor.wiese@uni.lu](mailto:gabor.wiese@uni.lu)

Faculté des Sciences, de la Technologie et de la Communication, University of Luxembourg, Esch-sur-Alzette, Luxembourg

# Hypergeometric $L$ -functions in average polynomial time

Edgar Costa, Kiran S. Kedlaya, and David Roe

We describe an algorithm for computing, for all primes  $p \leq X$ , the mod- $p$  reduction of the trace of Frobenius at  $p$  of a fixed hypergeometric motive in time quasilinear in  $X$ . This combines the Beukers–Cohen–Mellit trace formula with average polynomial time techniques of Harvey et al.

## 1. Introduction

In the past, computation of arithmetic  $L$ -functions has largely been limited to familiar classes of low-dimensional geometric objects, such as hyperelliptic curves or K3 surfaces [CHK19]. Recently, it has emerged that families of motives whose associated (Picard–Fuchs) differential equation is a hypergeometric equation also have  $L$ -functions which can be computed at large scale. Such motives provide accessible examples of arithmetic  $L$ -functions with diverse configurations of Hodge numbers, some of which arise in heretofore unanticipated applications. For example, certain hypergeometric motives appear among families of Calabi–Yau threefolds, where they give rise to arithmetic manifestations of mirror symmetry (as in [DKS<sup>+</sup>18]).

Using finite hypergeometric sums in the manner of Greene [Gre87], Katz [Kat90], and especially McCarthy [McC13], an explicit formula for the  $L$ -function of a hypergeometric motive was given by Beukers, Cohen and Mellit [BCM15]. It was then modified by Cohen and Rodriguez Villegas, using the Gross–Koblitz formula [GK79] to replace classical Gauss sums with the Morita  $p$ -adic gamma function. That work is unpublished, but is documented in the manuscript [Wat15]; the resulting formula appears in [Coh15, §8] and [FKS16, §7.1]; it is implemented in PARI/GP [PAR19], Magma [Magma], and SageMath [SageMath]; and it is being used to tabulate hypergeometric  $L$ -functions in the  $L$ -functions and modular forms database [LMFDB]. (For an alternative approach using the  $p$ -adic Frobenius structure on a hypergeometric equation, see [Ked19].)

The purpose of this paper is to describe a preliminary adaptation of *average polynomial time* techniques for computation of  $L$ -functions to the setting of hypergeometric motives. Such techniques, based on

---

Costa and Roe were supported by the Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation via Simons Foundation grant 550033. Kedlaya was supported by NSF (DMS-1802161) and UCSD (Warschawski Professorship). MSC2010: primary 11Y16, 33C20; secondary 11G09, 11M38, 11T24.

*Keywords:* hypergeometric  $L$ -functions, average polynomial time.

*accumulating remainder trees*, were introduced by Costa, Gerbicz and Harvey [CGH14] for the problem of finding Wilson primes; adapted to computing  $L$ -functions by Harvey [Har14; Har15]; and further elaborated (and made practical in particular cases) by Harvey and Sutherland [HS14; HS16] and Harvey, Massierer and Sutherland [HMS16].

To simplify matters, we consider here only a limited form of the problem: given a hypergeometric motive over  $\mathbb{Q}$  and a bound  $X$ , for each prime  $p \leq X$ , we compute the reduction modulo  $p$  of the trace of Frobenius at  $p$  in time quasilinear in  $X$ . This eliminates some technical issues that would arise when computing the mod- $p^e$  reduction for  $e > 1$ , such as the computation of multiplicative lifts and evaluation of the Morita  $p$ -adic gamma function in average polynomial time. Modulo  $p$ , the trace formula at  $p$  for a parameter value  $t$  is a polynomial in  $t$  of degree  $O(p)$  whose coefficients are essentially ratios of Pochhammer symbols. Computing the Pochhammer symbols themselves in average polynomial time is a straightforward adaptation of the corresponding computation for factorials done in [CGH14]; this approach can then be modified to include the polynomial evaluation.

At the end of the paper, we discuss the prospects of lifting our present restrictions of working modulo  $p$  (rather than a higher power) and of computing only the trace of the  $p$ -power Frobenius (rather than a higher power). Eliminating both restrictions would yield an average polynomial time algorithm for computing arbitrary hypergeometric  $L$ -series. However, the restricted computation described here is already of significant value for hypergeometric motives of weight 1, for which the trace of the  $p$ -power Frobenius is determined uniquely by its reduction modulo  $p$  (except when  $p$  is very small). Since the formula for the trace of the  $q$ -power Frobenius involves a summation over  $q - 1$  terms, our method reduces the complexity of computing the first  $X$  terms of the  $L$ -series from  $X^2$  to  $X^{3/2}$  (see Theorem 2.29).

We end this introduction by asking (as in [Ked19]) whether a similar trace formula exists for  $A$ -hypergeometric systems in the sense of Gelfand, Kapranov and Zelevinsky [GKZ08]. Such a formula might unlock even more classes of previously inaccessible  $L$ -functions.

## 2. Background

**2A. The  $p$ -adic  $\Gamma$  function.** For a detailed development of the following material, we recommend [Rob00, §7.1] and [RV07, §6.2].

**Definition 2.1.** The (Morita)  $p$ -adic gamma function is the unique continuous function  $\Gamma_p : \mathbb{Z}_p \rightarrow \mathbb{Z}_p^\times$  which satisfies

$$\Gamma_p(n+1) = (-1)^{n+1} \prod_{\substack{i=1 \\ (i,p)=1}}^n i = (-1)^{n+1} \frac{\Gamma(n+1)}{p^{\lfloor n/p \rfloor} \Gamma(\lfloor n/p \rfloor + 1)} \quad (2.2)$$

for all  $n \in \mathbb{Z}_{\geq 0}$ . For  $p \geq 3$ , it is Lipschitz continuous with  $C = 1$ ; i.e.,

$$|\Gamma_p(x) - \Gamma_p(y)|_p \leq |x - y|_p. \quad (2.3)$$

There is also a functional equation analogous to the one for the complex  $\Gamma$  function:

$$\Gamma_p(x+1) = \omega(x)\Gamma_p(x), \quad \omega(x) := \begin{cases} -x & \text{if } x \in \mathbb{Z}_p^\times \\ -1 & \text{if } x \in p\mathbb{Z}_p. \end{cases} \quad (2.4)$$

**Remark 2.5.** It was originally observed by Dwork (writing pseudonymously in [Boy80], as corroborated in [KT99]; see [RV07, §6.2] for the formulation given here) that  $\Gamma_p$  admits an easily computable Mahler expansion on any mod- $p$  residue disc:

$$\Gamma_p(-a + px) = \sum_{k \geq 0} p^k c_{a+kp}(x)_k, \quad (2.6)$$

where  $(x)_k := x(x+1) \cdots (x+k-1)$  is the usual Pochhammer symbol, and  $c_n$  is defined by the recursion

$$nc_n = c_{n-1} + c_{n-p}, \quad c_0 = 1, c_n = 0 \text{ for } n < 0. \quad (2.7)$$

Thus, one may compute  $\Gamma_p(x)$  modulo  $p^f$  using  $O(pf)$  ring operations.

**2B. Hypergeometric motives and their  $L$ -functions.** While the following discussion is needed to put our work in context, the reader is encouraged to skip ahead to (2.22), as the essential content of the paper is the computation of that formula.

**Definition 2.8.** A *hypergeometric datum* is a pair of disjoint tuples  $\alpha = (\alpha_1, \dots, \alpha_r)$  and  $\beta = (\beta_1, \dots, \beta_r)$  valued in  $\mathbb{Q} \cap [0, 1)$  which are *Galois-stable* (or *balanced*): any two reduced fractions with the same denominator occur with the same multiplicity.

**Remark 2.9.** There are several equivalent ways to specify a hypergeometric datum. One is to specify two tuples  $A$  and  $B$  for which the identity

$$\prod_{j=1}^r \frac{x - e^{2\pi i \alpha_j}}{x - e^{2\pi i \beta_j}} = \frac{\prod_{a \in A} \Phi_a(x)}{\prod_{b \in B} \Phi_b(x)}$$

holds in  $\mathbb{C}(x)$ , where  $\Phi_n(x)$  denotes the  $n$ -th cyclotomic polynomial.

**Definition 2.10.** The *zigzag function*  $Z_{\alpha, \beta} : [0, 1] \rightarrow \mathbb{Z}$  associated to a hypergeometric datum  $(\alpha, \beta)$  is defined by

$$Z_{\alpha, \beta}(x) := \#\{j : \alpha_j \leq x\} - \#\{j : \beta_j \leq x\}.$$

**Notation 2.11.** We denote by  $M^{\alpha, \beta}$  the putative (see Remark 2.17) hypergeometric family over  $\mathbb{P}^1$  associated to the hypergeometric datum  $(\alpha, \beta)$ . Its expected properties are as follows:

- It is a pure motive of degree  $r$  with base field  $\mathbb{Q}(t)$  and coefficient field  $\mathbb{Q}$ .
- Its Hodge realization is the one constructed by Fedorov in [Fed18]. This means that as per [Fed18, Theorem 2], its minimal motivic weight is

$$\begin{aligned} w &= \max\{Z_{\alpha, \beta}(x) : x \in [0, 1]\} - \min\{Z_{\alpha, \beta}(x) : x \in [0, 1]\} - 1 \\ &= \max\{Z_{\alpha, \beta}(x) : x \in \alpha\} - \min\{Z_{\alpha, \beta}(x) : x \in \beta\} - 1 \end{aligned} \quad (2.12)$$



and a similar recipe (see [CG11, Conjecture 1.4] or [Fed18, Theorem 1]) computes the Hodge numbers. Note that  $rw$  is even [Wat15, §1.2].

- Its  $\ell$ -adic étale realization is Katz’s perverse sheaf [Kat90, Chapter 8].
- For  $z \in \mathbb{Q} \setminus \{0, 1, \infty\}$ , let  $M_z^{\alpha, \beta}$  denote the specialization of  $M^{\alpha, \beta}$  at  $t = z$ . Then the primes of bad reduction for  $M_z^{\alpha, \beta}$  are those primes  $p$  at which  $z$  and  $z - 1$  are not both  $p$ -adic units (called *tame* primes) and those primes  $p$  at which the  $\alpha_i$  and  $\beta_i$  are not all integral (called *wild* primes). By the compatibility with Katz, the  $L$ -function associated to  $M_z^{\alpha, \beta}$  is given by the Beukers–Cohen–Mellit trace formula [BCM15].

**Remark 2.13.** In order to avoid some case subdivisions in what follows, we assume hereafter that  $0 \notin \alpha$ . This is relatively harmless because of the isomorphism

$$M_z^{\alpha, \beta} \cong M_{1/z}^{\beta, \alpha}. \quad (2.14)$$

**Example 2.15.** As per [Ono98],  $M^{(1/2, 1/2), (0, 0)}$  is the motive  $H^1(E, \mathbb{Q})$ , where

$$E : y^2 = -x(x - 1)(x - t). \quad (2.16)$$

For other (putative) examples, see [BK12] and [Nas17].

**Remark 2.17.** We use the qualifier “putative” in Notation 2.11 for two reasons. One is to avoid any precision about motives; while [BCM15] describes a specific variety whose  $\ell$ -adic cohomology includes Katz’s perverse sheaf, lifting this containment to the motivic level would require a deeper dive into motivic categories (including a choice of which such category to consider).

The other, more serious issue is that there is no existing reference that provides this missing precision on hypergeometric motives. The reader seeking to remedy this should start with [And04] for a user’s guide to motives.

**2B1. Trace formulas.** We are particularly interested in computing

$$\det(1 - T \text{Frob} | M_z^{\alpha, \beta}), \quad (2.18)$$

where  $\text{Frob}$  is the Frobenius automorphism at a prime  $p$  of good reduction for  $M_z^{\alpha, \beta}$ . (For concreteness, we may replace  $M_z^{\alpha, \beta}$  with an étale realization.) We ignore primes of bad reduction both because they are small enough to be handled individually and because a somewhat different recipe is required (see [Wat15, § 11] for a partial description, noting that our  $z$  is Watkins’s  $1/t$ ).

**Definition 2.19.** Let  $\{x\} := x - \lfloor x \rfloor$  be the fractional part of  $x$ . For  $q = p^f$ , define

$$\Gamma_q^*(x) := \prod_{v=0}^{f-1} \Gamma_p(\{p^v x\}), \quad (2.20)$$



and then define a  $p$ -adic analogue of the Pochhammer symbol by setting

$$(x)_m^* := \frac{\Gamma_q^*\left(x + \frac{m}{1-q}\right)}{\Gamma_q^*(x)}. \quad (2.21)$$

Let  $[z]$  be the multiplicative representative in  $\mathbb{Z}_p$  of the residue class of  $z$  (the unique  $(p-1)$ -st root of 1 congruent to  $z$  modulo  $p$ ). As in [Wat15, § 2], write

$$H_q\left(\frac{\alpha}{\beta} \middle| z\right) := \frac{1}{1-q} \sum_{m=0}^{q-2} (-p)^{\eta_m(\alpha) - \eta_m(\beta)} q^{D + \xi_m(\beta)} \left( \prod_{j=1}^r \frac{(\alpha_j)_m^*}{(\beta_j)_m^*} \right) [z]^m, \quad (2.22)$$

using the notation

$$\eta_m(x_1, \dots, x_r) := \sum_{j=1}^r \sum_{v=0}^{f-1} \left\{ p^v \left( x_j + \frac{m}{1-q} \right) \right\} - \{p^v x_j\}, \quad (2.23)$$

$$\xi_m(\beta) := \#\{j : \beta_j = 0\} - \#\left\{j : \beta_j + \frac{m}{1-q} = 0\right\}, \quad (2.24)$$

$$D := \frac{w + 1 - \#\{j : \beta_j = 0\}}{2}. \quad (2.25)$$

By adapting [BCM15, Theorem 1.3] using the Gross–Koblitz formula as in [Wat15, §2] (and twisting by  $q^D$  to minimize the weight), we deduce the following.

**Theorem 2.26.** *We have*

$$H_{p^f}\left(\frac{\alpha}{\beta} \middle| z\right) = \text{Tr}(\text{Frob}^f | M_z^{\alpha, \beta}) \in \mathbb{Z}.$$

From [Wat15, §11], we also have a precise formula for the functional equation which is associated to  $\det(1 - T \text{Frob} | M_z^{\alpha, \beta})$ .

**Theorem 2.27.** *We have*

$$\det(1 - q^{-w} T^{-1} \text{Frob} | M_z^{\alpha, \beta}) = \pm q^{-rw/2} T^{-r} \det(1 - T \text{Frob} | M_z^{\alpha, \beta}), \quad (2.28)$$

where  $\pm$  denotes  $+1$  if  $w$  is even, and otherwise is given by

$$\begin{cases} (\Delta|p), & \Delta = z(z-1) \prod_{a \in A} \text{Disc}(\Phi_a(x)) \quad \text{for } r \equiv 0 \pmod{2}, \\ -(\Delta|p), & \Delta = (1-z) \prod_{b \in B} \text{Disc}(\Phi_b(x)) \quad \text{for } r \equiv 1 \pmod{2}. \end{cases}$$

Here  $A, B, \Phi_a, \Phi_b$  are as in Remark 2.9 and  $(\Delta|p)$  is the Kronecker symbol.

Using these two results, we recover  $\det(1 - T \text{Frob} | M_z^{\alpha, \beta})$  from the values  $H_{p^f}\left(\frac{\alpha}{\beta} \middle| z\right)$  for  $f = 1, \dots, \lfloor \frac{r}{2} \rfloor$ .

**2B2. Complexity considerations.** Computing  $H_{p^f}\left(\frac{\alpha}{\beta} \middle| z\right)$  via (2.22) requires  $O(fp^f)$  arithmetic operations,<sup>1</sup> due to the number of terms in the sum and product [Wat15, §2.1.4]. As these operations are in  $\mathbb{Z}_p$ ,

<sup>1</sup>The factor of  $f$  comes from computing  $\Gamma_p$ . We do not incur a factor of  $f$  from computing  $\Gamma_q^*$  because the latter is invariant under  $x \mapsto \{px\}$ , so we only need  $O(q/f)$  evaluations of  $\Gamma_q^*$ .

we must also pay attention to  $p$ -adic working precision; since  $H_{p^f}(\frac{\alpha}{\beta} | z)$  is the sum of  $r$  algebraic integers of complex norm  $p^{wf/2}$ , it is uniquely determined by its reduction modulo  $p^e$  for  $e > \frac{1}{2}wf + \log_p(2r)$ .

For the use case of computing  $L$ -series, a different analysis applies.

**Theorem 2.29.** *Fix a hypergeometric datum  $(\alpha, \beta)$ . Given  $H_p(\frac{\alpha}{\beta} | z)$  for all primes  $p \leq X$ , one can compute the first  $X$  coefficients of the Dirichlet  $L$ -series associated to  $M_z^{\alpha, \beta}$  in at most  $O(X^{3/2})$  arithmetic operations.*

*Proof.* The first  $X$  coefficients of the Dirichlet series are determined by the coefficients indexed by prime powers up to  $X$ , and hence by the values  $H_q(\frac{\alpha}{\beta} | z)$  for all prime powers  $q \leq X$ . The number of such  $q$  which are not prime is

$$O(X^{1/2} / \log X),$$

for  $q = p^f$ ; evaluating (2.22) takes  $O(fp^f) = O(X \log X)$  arithmetic operations.  $\square$

### 3. Accumulating remainder trees

The use of a *remainder tree* to expedite modular reduction has its origins in the fast Fourier transform (FFT). An early description was given by Borodin and Moenck [BM74]; for a modern treatment with more historical references, see [Ber08].

*Accumulating remainder trees* were introduced in [CGH14] in order to compute  $(p-1)! \pmod{p^2}$  for many primes  $p$ . We use the variant described in [HS14, §4].

**Definition 3.1.** Suppose  $\mathcal{P}$  is a sequence  $p_1, \dots, p_{b-1}$  of pairwise coprime integers with  $p_i \leq X$ , and  $A_0, \dots, A_{b-2}$  is a sequence of  $2 \times 2$  integer matrices. We may use an accumulating remainder tree to compute

$$C_n := A_0 \cdots A_{n-1} \pmod{p_n} \tag{3.2}$$

for  $1 \leq n < b$  as follows. For notational convenience we assume  $b = 2^\ell$ , set  $A_{b-1} = 0$  and  $p_0 = 1$ . Then as in [HS14, §4], write

$$\begin{aligned} m_{i,j} &:= p_{j2^{\ell-i}} p_{j2^{\ell-i}+1} \cdots p_{(j+1)2^{\ell-i}-1}, \\ A_{i,j} &:= A_{j2^{\ell-i}} A_{j2^{\ell-i}+1} \cdots A_{(j+1)2^{\ell-i}-1}, \\ C_{i,j} &:= A_{i,0} \cdots A_{i,j-1} \pmod{m_{i,j}}. \end{aligned} \tag{3.3}$$

This leads us to [Algorithm 1](#).

**Theorem 3.4** [HS14, Theorem 4.1]. *Let  $B$  be an upper bound on the bit size of  $\prod_{j=0}^{b-1} p_j$  and  $H$  an upper bound on the bit size of any  $p_i$  or  $A_i$ . The running time of [Algorithm 1](#) is*

$$O((B + bH) \log(B + bH) \log(b))$$

(using [HVDH19] for the runtime of integer multiplication) and its space complexity is

$$O((B + bH) \log(b)).$$

**Algorithm 1:** Accumulating Remainder Tree

---

**Input:**  $A_0, \dots, A_{b-1}, p_0, \dots, p_{b-1}$  as in [Definition 3.1](#)  
**Output:**  $\{C_i\}$

```

1 def RemTree( $\{A_i\}, \{p_i\}$ ):
2   for  $j := 0$  to  $b - 1$  do
3      $m_{\ell,j} := p_j$  and  $A_{\ell,j} := A_j$ 
4   for  $i := \ell - 1$  to  $0$  do
5     for  $j := 0$  to  $2^i - 1$  do
6        $m_{i,j} := m_{i+1,2j}m_{i+1,2j+1}$  and  $A_{i,j} := A_{i+1,2j}A_{i+1,2j+1}$ 
7    $C_{0,0} := \text{id}$ 
8   for  $i := 1$  to  $\ell$  do
9     for  $j := 0$  to  $2^i - 1$  do
10      if  $j$  even then
11         $C_{i,j} := C_{i-1,\lfloor j/2 \rfloor} \bmod m_{i,j}$ 
12      else
13         $C_{i,j} := C_{i-1,\lfloor j/2 \rfloor} A_{i,j-1} \bmod m_{i,j}$ 
14   return  $\{C_{\ell,j}\}_{j=1,\dots,b-1}$ 

```

---

**3A. Accumulating remainder tree with spacing.** In most applications (including this one), there is not a one-to-one correspondence between the moduli  $p_i$  and the multiplicands  $A_i$ . Rather, we will be given

- a list of matrices  $A_0, \dots, A_{b-1}$ ,
- a list of primes  $p_1, \dots, p_c$ , and
- a list of distinct cut points  $b_1, \dots, b_c$ ,

with the aim of computing  $C_n := A_0 \cdots A_{b_n-1} \bmod p_n$  for  $1 \leq n < c$ . This reduces to [Algorithm 1](#) by suitably grouping terms; see [Algorithm 2](#). (One may also handle repeated cut points, as long as the cut points up to  $X$  occur at most  $O(X)$  times.)

**Remark 3.5.** In practice, we split our products to work around discontinuities of (2.22) (see [Section 5B](#)). One gains some savings (particularly in space complexity) by splitting a bit further, replacing remainder trees with *remainder forests* [[HS14](#), Theorem 4.2]; we omit the details here.

## 4. Nuts and bolts

We record two technical lemmas used in the description of our algorithm. For the rest of the paper, we make the simplifying assumption  $q = p$  in [Theorem 2.26](#).

**Lemma 4.1.** *Set  $I_b := [0, 1] \cap \frac{1}{b}\mathbb{Z}$ . Suppose  $\gamma \in I_b$  and  $p$  is a prime not dividing  $b$ . Let  $m = \lfloor \gamma(p-1) \rfloor$ . Then there exist  $\delta \in I_b$  and  $\epsilon \in \{1, 2\}$  so that*

$$m + \epsilon \equiv \delta \pmod{p}.$$

*Moreover,  $\delta$  and  $\epsilon$  only depend on  $b$ ,  $\gamma$ , and  $p \pmod{b}$ .*

**Algorithm 2:** Accumulating Remainder Tree with Spacing

---

**Input:**  $A_0, \dots, A_{b-1}, p_1, \dots, p_c, b_1, \dots, b_c$  as in [Section 3A](#)  
**Output:**  $C_1, \dots, C_{c-1}$

```

1 def RemTreeWithSpacing( $\{A_i\}, \{p_i\}, \{b_i\}$ ):
2    $\ell := \lceil \log_2(b) \rceil$ 
3   for  $j := b$  to  $2^\ell - 1$  do
4      $A_j := 0$ 
5   for  $j := 0$  to  $2^\ell - 1$  do
6      $p'_j := 1$ 
7   for  $i := 1$  to  $c$  do
8      $p'_{b_i} := p_i$ 
9    $C'_i := \text{RemTree}(\{A_i\}, \{p'_i\})$ 
10  return  $\{C'_{b_i}\}_{i=0, \dots, c-1}$ 

```

---

*Proof.* Write  $\gamma = \frac{a}{b}$  and define an integer  $r \in \{0, \dots, b-1\}$  by the condition that

$$a(p-1) = mb + r.$$

We then set

$$\begin{cases} \epsilon := 1, \delta := \frac{1}{b}(b-a-r) & \text{if } a+r < b, \\ \epsilon := 2, \delta := \frac{1}{b}(2b-a-r) & \text{otherwise.} \end{cases}$$

Note that

$$b(\delta - \epsilon) = -(a+r) = mb - ap$$

so  $m + \epsilon \equiv \delta \pmod{p}$ . The fact that  $\delta \in I_b$  follows from the bounds  $0 \leq a, r \leq b$ .  $\square$

**Lemma 4.2.** Suppose  $0 \leq m < p-1$  and either  $\eta_m(\alpha) - \eta_m(\beta) \neq \eta_{m+1}(\alpha) - \eta_{m+1}(\beta)$  or  $\xi_m(\beta) \neq \xi_{m+1}(\beta)$ . Then  $\lfloor \gamma(p-1) \rfloor \in \{m, m+1\}$  for some  $\gamma \in \alpha \cup \beta$ .

*Proof.* Since  $q = p$ , we have

$$\eta_m(\alpha) - \eta_m(\beta) = \sum_{j=1}^r \left( \left\{ \alpha_j - \frac{m}{p-1} \right\} - \{\alpha_j\} \right) - \sum_{j=1}^r \left( \left\{ \beta_j - \frac{m}{p-1} \right\} - \{\beta_j\} \right). \quad (4.3)$$

For  $x, y \in [0, 1)$  we have

$$\{x - y\} = \begin{cases} x - y, & (x \geq y), \\ x - y + 1, & (x < y). \end{cases} \quad (4.4)$$

Consequently, the only way for  $\eta_m(\alpha) - \eta_m(\beta)$  to change values when  $m$  goes to  $m+1$  is for there to exist  $\gamma \in \alpha \cup \beta$  such that

$$\gamma - \frac{m}{p-1} \geq 0, \quad \gamma - \frac{m+1}{p-1} < 0.$$

This occurs precisely when  $m = \lfloor \gamma(p-1) \rfloor$ . Meanwhile, by (2.24),  $\xi_m(\beta) = \xi_{m+1}(\beta)$  unless  $\beta_j = m/(p-1)$  or  $\beta_j = (m+1)/(p-1) = 0$  for some  $j$ .  $\square$

### 5. Computing trace functions of hypergeometric motives

Throughout this section, fix  $\alpha, \beta$  and  $z$ . We now describe how to compute the trace  $H_p(\alpha | \beta | z)$  modulo  $p$  in average polynomial time using (2.22), which we duplicate here modulo  $p$  for ease of reference:

$$H_p\left(\alpha \middle| \beta \middle| z\right) \equiv \sum_{m=0}^{p-2} (-p)^{\eta_m(\alpha) - \eta_m(\beta)} p^{D + \xi_m(\beta)} \left( \prod_{j=1}^r \frac{(\alpha_j)_m^*}{(\beta_j)_m^*} \right) z^m \pmod{p}. \quad (5.1)$$

**5A. Overview of the algorithm.** In order to apply Algorithm 2, we would like to identify  $2 \times 2$  integer matrices  $B(m)$ , such that we may extract  $H_p(\alpha | \beta | z) \pmod{p}$  from  $B(0)B(1) \cdots B(p-2)$ . In practice, we will consider shorter subproducts and choose  $B(m)$  based on the residue of  $p$  modulo a fixed integer (independent of  $m$  and  $p$ ); we will then apply Algorithm 2 once for each subproduct and residue class.

As a first approximation, let us instead model the sum  $\sum_{m=0}^{p-2} P_m$  where

$$P_m := z^m \prod_{j=1}^r \frac{(\alpha_j)_m^*}{(\beta_j)_m^*} \in \mathbb{Z}_p^\times. \quad (5.2)$$

If we can find  $f(m), g(m) \in \mathbb{Z}[m]$  so that

$$P_{m+1} \equiv \frac{f(m)}{g(m)} P_m \pmod{p}, \quad (5.3)$$

we can then set

$$B(m) := \begin{pmatrix} g(m) & 0 \\ g(m) & f(m) \end{pmatrix} = g(m) \begin{pmatrix} 1 & 0 \\ 1 & f(m)/g(m) \end{pmatrix} \quad (5.4)$$

and  $\tilde{B} = B(0) \cdots B(p-2) \pmod{p}$ , so that

$$\tilde{B} \equiv g(0) \cdots g(p-2) \begin{pmatrix} 1 & 0 \\ \sum_{m=0}^{p-2} P_m & P_{p-1} \end{pmatrix} \pmod{p}$$

and so  $\sum_{m=0}^{p-2} P_m \equiv \tilde{B}_{21}/\tilde{B}_{11} \pmod{p}$ . That is,  $\tilde{B}_{11}$  tracks a common denominator,  $\tilde{B}_{22}$  tracks the product  $P_m$ , and  $\tilde{B}_{12}$  computes the sum of the  $P_m$ .

There are two problems with the approach described above. First, to correctly simulate (5.1) we must sum not  $P_m$  but

$$P'_m := (-p)^{\eta_m(\alpha) - \eta_m(\beta)} p^{D + \xi_m(\beta)} P_m, \quad (5.5)$$

which we cannot directly handle by modifying  $B(m)_{21}$  because the extra factor depends on both  $p$  and  $m$ . Second, while we can find polynomials  $f$  and  $g$  satisfying (5.3) for most values of  $m$  using (2.21) and the functional equation (2.4), there will be a few values of  $m$  where  $f(m)$  or  $g(m)$  is a multiple of  $p$ . We cannot filter these values out during the remainder tree because  $p$  is not fixed.

The solution to both of these issues is to break up the range  $[0, p-2]$  into intervals on which (5.3) holds and the values  $\eta_m(\alpha) - \eta_m(\beta)$  and  $\xi_m(\beta)$  are constant. The breaks between these intervals occur when  $m = \lfloor \gamma(p-1) \rfloor$ , where  $\gamma \in \alpha \cup \beta$ . We thus use a separate accumulating remainder tree for each

interval, yielding for each  $p$  a fixed number of subproducts with isolated missing terms in between; we then compute separately for each  $p$  to bridge the gaps.

A third issue is that while we can vary the endpoint in an accumulating remainder tree as a function of  $p$  (as described in [Section 3](#)), it is more difficult to change the start point. Our solution is to use [Lemma 4.1](#) to find a rational number  $\delta$  so that adding  $\delta$  to each  $\alpha_j$  and  $\beta_j$  has the effect of shifting the start point to 0.

**5B. Construction of the matrix product.** We now construct the matrix product described above. We begin with the division of the interval  $[0, p - 1]$  and the division of primes into residue classes. We assume that  $q = p$  is good and not 2.

**Definition 5.6.** Given a hypergeometric motive  $M_z^{\alpha, \beta}$ , let  $0 = \gamma_0 < \cdots < \gamma_s = 1$  be the distinct elements in  $\alpha \cup \beta \cup \{0, 1\}$ . Let  $b$  be the least common denominator of  $\alpha \cup \beta$  and fix  $c \in (\mathbb{Z}/b\mathbb{Z})^\times$ . Let  $p$  be a prime congruent to  $c$  modulo  $b$  and not dividing the denominator of  $z$ . Write  $m_i$  for  $\lfloor \gamma_i(p - 1) \rfloor$ .

We next exhibit polynomials that we use to compute Pochhammer symbols and their partial sums on the interval  $(\gamma_i, \gamma_{i+1})$ .

**Definition 5.7.** Fix an interval  $(\gamma_i, \gamma_{i+1})$ , choose  $\delta_i$  and  $\epsilon_i$  associated to  $\gamma_i$  as in [Lemma 4.1](#), and let

$$\iota(x, y) := \begin{cases} 1, & x \leq y, \\ 0, & x > y. \end{cases} \quad (5.8)$$

Define polynomials  $f_{i,c}(k), g_{i,c}(k) \in \mathbb{Z}[k]$  as follows: set

$$\begin{aligned} F_{i,c}(k) &:= z \prod_{j=1}^r (\alpha_j + \delta_i + \iota(\alpha_j, \gamma_i) + k - \epsilon_i), \\ G_{i,c}(k) &:= \prod_{j=1}^r (\beta_j + \delta_i + \iota(\beta_j, \gamma_i) + k - \epsilon_i), \end{aligned} \quad (5.9)$$

let  $d_{i,c}$  be the least common multiple of the denominators of  $F_{i,c}$  and  $G_{i,c}$ , and set  $f_{i,c}(k) := d_{i,c} F_{i,c}(k)$  and  $g_{i,c}(k) := d_{i,c} G_{i,c}(k)$ .

**Lemma 5.10.** Define  $P_m$  as in [\(5.2\)](#), and suppose  $m_i < m < m_{i+1}$ . Then

$$P_{m+1} \equiv \frac{f_{i,c}(k)}{g_{i,c}(k)} P_m \pmod{p},$$

where  $1 \leq k < m_{i+1} - m_i$  and  $m = m_i + k$ .

*Proof.* We first focus on a single Pochhammer symbol  $(\alpha_j)_m^*$ . First note that, for  $m_i < m \leq m_{i+1}$ , by [\(4.4\)](#) we have

$$\left\{ \alpha_j + \frac{m}{1-p} \right\} = \alpha_j + \frac{m}{1-p} + \begin{cases} 0 & m \leq \lfloor \alpha_j(p - 1) \rfloor \\ 1 & m > \lfloor \alpha_j(p - 1) \rfloor \end{cases} = \alpha_j + \frac{m}{1-p} + \iota(\alpha_j, \gamma_i). \quad (5.11)$$

Combining (5.11) with Lipschitz continuity (2.3) and the functional equation for  $\Gamma_p$  (2.4) and Lemma 4.1, for  $m_i < m < m_{i+1}$  we obtain

$$\begin{aligned} \Gamma_p\left(\left\{\alpha_j + \frac{m+1}{1-p}\right\}\right) &\equiv \Gamma_p(\alpha_j + m + 1 + \iota(\alpha_j, \gamma_i)) \\ &= -(\alpha_j + m + \iota(\alpha_j, \gamma_i))\Gamma_p(\alpha_j + m + \iota(\alpha_j, \gamma_i)) \\ &\equiv -(\alpha_j + \delta_i + \iota(\alpha_j, \gamma_i) + k - \epsilon_i)\Gamma_p\left(\left\{\alpha_j + \frac{m}{1-p}\right\}\right) \pmod{p}. \end{aligned} \quad (5.12)$$

Taking the product over all the Pochhammer symbols, the minus sign cancels out, and we obtain (5.9), as desired.  $\square$

We next account for the power of  $p$  in the product, and assemble a matrix product that computes the sum between two breaks.

**Definition 5.13.** Let  $\xi(\beta) = \#\{j : \beta_j = 0\}$  and

$$\sigma_i := \begin{cases} 1, & Z_{\alpha,\beta}(\gamma_i) + \xi(\beta) + D = 0 \text{ and } Z_{\alpha,\beta}(\gamma_i) \equiv 0 \pmod{2}, \\ -1, & Z_{\alpha,\beta}(\gamma_i) + \xi(\beta) + D = 0 \text{ and } Z_{\alpha,\beta}(\gamma_i) \equiv 1 \pmod{2}, \\ 0, & \text{otherwise.} \end{cases} \quad (5.14)$$

By Lemma 4.2,  $\sigma_i$  gives the value of  $(-p)^{\eta_m(\alpha) - \eta_m(\beta)} p^{\xi_m(\beta) + D} \pmod{p}$  for all  $m$  with  $m_i < m < m_{i+1}$ . Now set

$$A_{i,c}(k) := \begin{pmatrix} g_{i,c}(k) & 0 \\ \sigma_i g_{i,c}(k) & f_{i,c}(k) \end{pmatrix}. \quad (5.15)$$

Since  $A_{i,c}(k)$  depends only on  $c$  and not  $p$ , we can use an accumulating remainder tree for each  $c$  to compute

$$S_i(p) := A_{i,c}(1)A_{i,c}(2) \cdots A_{i,c}(m_{i+1} - m_i - 1) \pmod{p}. \quad (5.16)$$

**Lemma 5.17.** For  $P'_m$  as defined in (5.5),

$$S_i(p)^{-1}_{11} S_i(p) \equiv \begin{pmatrix} 1 & 0 \\ \sum_{m=m_i+1}^{m_{i+1}-1} P'_m / P_{m_i+1} & P_{m_{i+1}} / P_{m_i+1} \end{pmatrix} \pmod{p}. \quad (5.18)$$

*Proof.* By Lemma 5.10, for  $k = 1, \dots, m_{i+1} - m_i - 1$ ,

$$\frac{(A_{i,c}(1) \cdots A_{i,c}(k))_{22}}{(A_{i,c}(1) \cdots A_{i,c}(k))_{11}} \equiv \frac{P_{m_i+k+1}}{P_{m_i+1}} \pmod{p}$$

and hence

$$\frac{(A_{i,c}(1) \cdots A_{i,c}(k))_{21}}{(A_{i,c}(1) \cdots A_{i,c}(k))_{11}} \equiv \sigma_i \sum_{l=1}^k \frac{P_{m_i+l}}{P_{m_i+1}} \pmod{p}.$$

Taking  $k = m_{i+1} - m_i - 1$ , and then applying Lemma 4.2 to replace  $\sigma_i$  with  $P'_m / P_m$ , yields the desired result.  $\square$

It remains to deal with the breaks. Since the number of breaks is independent of  $p$ , we have the luxury of computing matrices  $T_i(p)$  separately for each  $p$  that move the Pochhammer symbols and partial sums past the break  $\gamma_i$ .

**Definition 5.19.** With  $\omega$  defined as in (2.4), let

$$h_i(\gamma, p) := \begin{cases} \omega(\gamma + m_i + 1) & \text{if } \gamma(p-1) < m_i, \\ \omega(\gamma + m_i) & \text{if } \gamma(p-1) \geq m_i + 1, \\ \omega(\gamma + m_i + 1)\omega(\gamma + m_i) & \text{otherwise,} \end{cases} \quad (5.20)$$

$$\tau_i := \begin{cases} 0 & \gamma_i = 0, \\ 1 & Z_{\alpha, \beta}(\gamma_{i-1}) + \xi_{m_i}(\beta) + D = 0 \text{ and } Z_{\alpha, \beta}(\gamma_{i-1}) \equiv 0 \pmod{2}, \\ -1 & Z_{\alpha, \beta}(\gamma_{i-1}) + \xi_{m_i}(\beta) + D = 0 \text{ and } Z_{\alpha, \beta}(\gamma_{i-1}) \equiv 1 \pmod{2}, \\ 0 & \text{otherwise,} \end{cases} \quad (5.21)$$

and then set

$$T_i(p) := \begin{pmatrix} 1 & 0 \\ \tau_i & z \prod_{j=1}^r \frac{h_i(\alpha_j, p)}{h_i(\beta_j, p)} \end{pmatrix}, \quad (5.22)$$

$$S(p) := \prod_{i=0}^{s-1} T_i(p) S_i(p). \quad (5.23)$$

Note that modulo  $p$ ,  $T_i(p)$  is congruent to a matrix that depends on  $p$  only via  $c$ .

**Lemma 5.24.** For suitable choices of scalars, we have

$$\begin{aligned} \prod_{j=0}^{i-1} T_j(p) S_j(p) &\equiv (\text{scalar}) \begin{pmatrix} 1 & 0 \\ \sum_{m=0}^{m_i-1} P'_m & P_{m_i} \end{pmatrix} \pmod{p}, \\ \left( \prod_{j=0}^{i-1} T_j(p) S_j(p) \right) T_i(p) &\equiv (\text{scalar}) \begin{pmatrix} 1 & 0 \\ \sum_{m=0}^{m_i} P'_m & P_{m_i+1} \end{pmatrix} \pmod{p}. \end{aligned}$$

*Proof.* This follows by induction on  $i$  using Lemma 5.17. □

Summing up, we obtain the following:

**Proposition 5.25.** For  $p \equiv c \pmod{b}$  not dividing the denominator of  $z$ ,

$$H_p \left( \alpha \middle| \beta \right| z \right) \equiv S(p)_{21} / S(p)_{11} \pmod{p}.$$

*Proof.* This follows from (5.1) and the case  $i = s$  of Lemma 5.24. □

**5C. Algorithm and runtime.** We summarize with Algorithm 3.

**Theorem 5.26.** For fixed  $\alpha, \beta$ , Algorithm 3 is correct and runs in time

$$O(X \log(X)^3).$$



**Algorithm 3:** Trace mod  $p$ 


---

**Input:**  $\alpha, \beta \in (\mathbb{Q} \cap [0, 1))^r$ ,  $z \in \mathbb{Q}$  and a bound  $X$

**Output:**  $H_p(\alpha | \beta | z) \pmod{p}$  for all good  $p \leq X$

```

1 def Traces( $\alpha, \beta, z, X$ ):
2   if  $0 \in \alpha$  then
3      $\alpha, \beta, z := \beta, \alpha, 1/z$ 
4    $\text{gamma} := \text{Sorted}(\text{Set}(\alpha \cup \beta \cup \{0, 1\}))$ 
5   for good primes  $p \leq X$  do
6      $\text{result}[p] := \text{IdentityMatrix}(2)$ 
7   for start, end consecutive elements of  $\text{gamma}$  do
8      $b := \text{Denominator}(\text{start})$ 
9     for  $c \in (\mathbb{Z}/b\mathbb{Z})^\times$  do
10       $\delta, \epsilon := \text{RationalShift}(\text{start}, c)$  // Using Lemma 4.1
11       $\text{mats} := \text{Matrices}(z, \text{start}, \delta, \epsilon)$  // As in (5.15)
12       $\text{cut} := (p \mapsto \lfloor \text{end} \cdot (p-1) \rfloor - \lfloor \text{start} \cdot (p-1) \rfloor)$ 
13       $\text{primes} := \{\text{good primes } p \equiv c \pmod{b}, p \leq X\}$ 
14       $\{C_i\} := \text{RemTreeWithSpacing}(\text{mats}, \text{primes}, \text{cut})$ 
15      for  $i := 0, \dots, \#\text{primes} - 1$  do
16         $p := \text{primes}[i]$ 
17         $\text{result}[p] := \text{result}[p] \cdot \text{FixBreak}(z, \text{start}, p)$  // As in (5.22)
18         $\text{result}[p] := \text{result}[p] \cdot C_i$ 
19      for good primes  $p \leq X$  do
20         $\text{result}[p] := \text{result}[p]_{21} / \text{result}[p]_{11} \pmod{p}$ 
21  return result

```

---

*Proof.* Correctness is immediate from Proposition 5.25. The runtime is dominated by the calls to Algorithm 2; these calls take place inside a loop over consecutive elements of  $\alpha \cup \beta \cup \{0, 1\}$  and a second loop over residue classes modulo a divisor of  $b$ . These two loops together have length  $O(rb)$ ; combining with the runtime estimate from Theorem 3.4 (taking  $B = b = O(X)$ ,  $H = O(\log X)$ ) yields the desired result.  $\square$

**5D. Implementation notes.** We have implemented Algorithm 3 in SageMath, using a variant of Algorithm 2 implemented in C by Drew Sutherland (see Remark 3.5). Our implementation is available at <https://github.com/edgarcosta/amortizedHGM>, and vastly outperforms SageMath and Magma while giving matching answers; see Table 1 for sample timings.

**5E. An example.** Let  $\alpha = (\frac{1}{4}, \frac{1}{2}, \frac{1}{2}, \frac{3}{4})$ ,  $\beta = (\frac{1}{3}, \frac{1}{3}, \frac{2}{3}, \frac{2}{3})$  and  $z = \frac{1}{5}$ . We plot the zigzag function in Figure 1. Using (2.12), we see that  $M^{\alpha, \beta}$  has weight 1 and the intervals contributing to the computation

$X$	Algorithm 3	Sage	Magma	$X$	Algorithm 3
$2^{10}$	0.07s	0.39s	0.11s	$2^{18}$	1.81s
$2^{11}$	0.05s	0.68s	0.35s	$2^{19}$	4.59s
$2^{12}$	0.06s	2.12s	1.29s	$2^{20}$	10.71s
$2^{13}$	0.08s	7.39s	4.83s	$2^{21}$	24.53s
$2^{14}$	0.12s	26.0s	18.24s	$2^{22}$	58.0s
$2^{15}$	0.18s	92.27s	68.35s	$2^{23}$	135s
$2^{16}$	0.34s	343s	280s	$2^{24}$	322s
$2^{17}$	0.80s	1328s	1190s	$2^{25}$	857s

**Table 1.** Comparison of Algorithm 3 against SageMath and Magma for  $\alpha = (\frac{1}{4}, \frac{1}{2}, \frac{1}{2}, \frac{3}{4})$ ,  $\beta = (\frac{1}{3}, \frac{1}{3}, \frac{2}{3}, \frac{2}{3})$  and  $z = \frac{1}{5}$ . Note the observable difference between linear and quadratic complexity.

of  $H_p(\alpha | z)$  are  $(\gamma_2, \gamma_3) = (\frac{1}{3}, \frac{1}{2})$  and  $(\gamma_4, \gamma_5) = (\frac{2}{3}, \frac{3}{4})$ . For the remainder of the example we will focus on the congruence class  $p \equiv 7 \pmod{12}$ . Applying Lemma 4.1 to  $\gamma_2 = \frac{1}{3}$  (resp.  $\gamma_4 = \frac{2}{3}$ ), we obtain  $\delta_2 = \frac{2}{3}$  and  $\epsilon_2 = 1$  (resp.  $\delta_4 = \frac{1}{3}$  and  $\epsilon_4 = 1$ ). By (5.9) and (5.14),

$$f_{2,7}(k) = 5184k^4 + 8640k^3 + 4428k^2 + 852k + 55,$$

$$g_{2,7}(k) = 25920k^4 + 69120k^3 + 63360k^2 + 23040k + 2880,$$

$$f_{4,7}(k) = 5184k^4 + 12096k^3 + 9612k^2 + 2820k + 175,$$

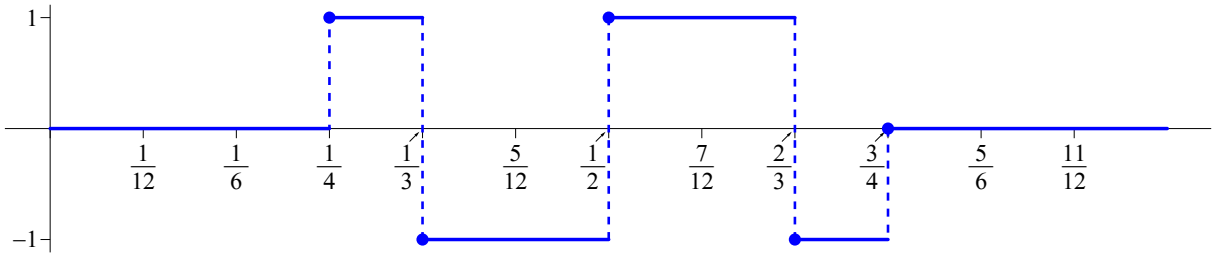
$$g_{4,7}(k) = 25920k^4 + 86400k^3 + 106560k^2 + 57600k + 11520,$$

and  $\sigma_2 = \sigma_4 = -1$ . Taking  $p = 67$ , we obtain  $(m_2, m_3) = (22, 33)$  and  $(m_4, m_5) = (44, 49)$ . Using an accumulating remainder tree (or simple multiplication), we get

$$S_2(67) = \begin{pmatrix} 65 & 0 \\ 34 & 5 \end{pmatrix}, \quad S_4(67) = \begin{pmatrix} 54 & 0 \\ 25 & 41 \end{pmatrix}.$$

However, we can't ignore the other intervals: they may not contribute to the sum, but they do track the Pochhammer symbols. Similar computations show

$$S_0(67) = \begin{pmatrix} 38 & 0 \\ 0 & 62 \end{pmatrix}, \quad S_1(67) = \begin{pmatrix} 50 & 0 \\ 0 & 47 \end{pmatrix}, \quad S_3(67) = \begin{pmatrix} 1 & 0 \\ 0 & 16 \end{pmatrix}, \quad S_5(67) = \begin{pmatrix} 1 & 0 \\ 0 & 38 \end{pmatrix}.$$



**Figure 1.**  $Z_{\alpha,\beta}(x)$  for  $\alpha = (\frac{1}{4}, \frac{1}{2}, \frac{1}{2}, \frac{3}{4})$ ,  $\beta = (\frac{1}{3}, \frac{1}{3}, \frac{2}{3}, \frac{2}{3})$ .

It remains to handle the break points. Using [Definition 5.19](#) we get

$$\begin{aligned} T_0(67) &= \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}, & T_1(67) &= \begin{pmatrix} 1 & 0 \\ 0 & 31 \end{pmatrix}, & T_2(67) &= \begin{pmatrix} 1 & 0 \\ -1 & 12 \end{pmatrix}, \\ T_3(67) &= \begin{pmatrix} 1 & 0 \\ -1 & 40 \end{pmatrix}, & T_4(67) &= \begin{pmatrix} 1 & 0 \\ -1 & 40 \end{pmatrix}, & T_5(67) &= \begin{pmatrix} 1 & 0 \\ -1 & 31 \end{pmatrix}. \end{aligned}$$

Putting them all together, we get

$$S(67) = T_0(67)S_0(67) \cdots T_5(67)S_5(67) = \begin{pmatrix} 21 & 0 \\ 33 & 21 \end{pmatrix}$$

yielding  $H_{67}(\alpha_\beta | \frac{1}{5}) \equiv \frac{33}{21} \equiv 59 \pmod{67}$ .

## 6. Future goals and challenges

We would like to be able to compute  $H_{p^f}(\alpha_\beta | z) \pmod{p^e}$  in average polynomial time for general  $e$  and  $f$ , but we currently only implement this for  $e = f = 1$ . We highlight the key points at which new ideas would be needed to achieve this goal.

**6A. The case  $e > 1$ .** Allowing  $e > 1$  creates two related issues where our computation exploits extra structure of the trace formula mod  $p$ : the replacement of  $[z]$  with  $z$ , and the use of the functional equation in [\(5.12\)](#) to compare two values of  $\Gamma_p$  at arguments that differ by  $\frac{1}{1-p}$ .

Such issues can usually be resolved using the “generic prime” technique of [\[Har15, §4.4\]](#): make the average polynomial time computation carrying suitable nilpotent variables, then make a separate specialization for each  $p$ .

**6B. The case  $f > 1$ .** Allowing  $f > 1$  creates more serious issues because of the change in the definition of  $\Gamma_q^*(x)$ , which interferes with our division of the summation into a fixed number of ranges. To see this in more detail, fix  $v \in \{0, \dots, f-1\}$ . For each  $\gamma \in \alpha \cup \beta$ , a break occurs when the value of  $\{p^v(\gamma - \frac{m}{q-1})\}$  changes when  $m$  goes to  $m+1$ ; there are  $p^v$  such breaks.

It is unclear whether one can rearrange the formula [\(2.22\)](#) to remedy this issue. It may help to implement the method of Frobenius structures suggested in [\[Ked19\]](#), which scales linearly in  $p$  rather than  $q$ . We may then argue as in [Theorem 2.29](#) to compute the first  $X$  coefficients of an  $L$ -series in average polynomial time.

## References

- [And04] Yves André, *Une introduction aux motifs (motifs purs, motifs mixtes, périodes)*, Panoramas et Synthèses, no. 17, Société Mathématique de France, Paris, 2004. [MR 2115000](#)
- [BCM15] Frits Beukers, Henri Cohen, and Anton Mellit, *Finite hypergeometric functions*, Pure Appl. Math. Q. **11** (2015), no. 4, 559–589. [MR 3613122](#)
- [Ber08] Daniel J. Bernstein, *Fast multiplication and its applications*, Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Pub., no. 44, Cambridge Univ. Press, 2008, pp. 325–384. [MR 2467550](#)

- [BK12] Rupam Barman and Gautam Kalita, *Hypergeometric functions and a family of algebraic curves*, Ramanujan J. **28** (2012), no. 2, 175–185. [MR 2925173](#)
- [BM74] A. Borodin and R. Moenck, *Fast modular transforms*, J. Comput. System Sci. **8** (1974), 366–386. [MR 371144](#)
- [Boy80] Maurizio Boyarsky,  *$p$ -adic gamma functions and Dwork cohomology*, Trans. Amer. Math. Soc. **257** (1980), no. 2, 359–369. [MR 552263](#)
- [CG11] Alessio Corti and Vasily Golyshev, *Hypergeometric equations and weighted projective spaces*, Sci. China Math. **54** (2011), no. 8, 1577–1590. [MR 2824960](#)
- [CGH14] Edgar Costa, Robert Gerbicz, and David Harvey, *A search for Wilson primes*, Math. Comp. **83** (2014), no. 290, 3071–3091. [MR 3246824](#)
- [CHK19] Edgar Costa, David Harvey, and Kiran S. Kedlaya, *Zeta functions of nondegenerate hypersurfaces in toric varieties via controlled reduction in  $p$ -adic cohomology*, Proceedings of the Thirteenth Algorithmic Number Theory Symposium (Berkeley, CA), Open Book Ser., no. 2, Math. Sci. Publ., 2019, pp. 221–238. [MR 3952014](#)
- [Coh15] Henri Cohen, *Computing  $L$ -functions: a survey*, J. Théor. Nombres Bordeaux **27**:3 (2015), 699–726. [MR 3429316](#)
- [DKS<sup>+</sup>18] Charles F. Doran, Tyler L. Kelly, Adriana Salerno, Steven Sperber, John Voight, and Ursula Whitcher, *Zeta functions of alternate mirror Calabi–Yau families*, Israel J. Math. **228** (2018), no. 2, 665–705. [MR 3874856](#)
- [Fed18] Roman Fedorov, *Variations of Hodge structures for hypergeometric differential operators and parabolic Higgs bundles*, Int. Math. Res. Not. **2018** (2018), no. 18, 5583–5608. [MR 3862114](#)
- [FKS16] Francesc Fité, Kiran S. Kedlaya, and Andrew V. Sutherland, *Sato–Tate groups of some weight 3 motives*, Frobenius distributions: Lang–Trotter and Sato–Tate conjectures, Contemp. Math., no. 663, Amer. Math. Soc., Providence, RI, 2016, pp. 57–101. [MR 3502939](#)
- [GK79] Benedict H. Gross and Neal Koblitz, *Gauss sums and the  $p$ -adic  $\Gamma$ -function*, Ann. of Math. (2) **109** (1979), no. 3, 569–581. [MR 534763](#)
- [GKZ08] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky, *Discriminants, resultants and multidimensional determinants*, Birkhäuser, Boston, 2008, Reprint of the 1994 edition. [MR 2394437](#)
- [Gre87] John Greene, *Hypergeometric functions over finite fields*, Trans. Amer. Math. Soc. **301** (1987), no. 1, 77–101. [MR 879564](#)
- [Har14] David Harvey, *Counting points on hyperelliptic curves in average polynomial time*, Ann. of Math. (2) **179** (2014), no. 2, 783–803. [MR 3152945](#)
- [Har15] David Harvey, *Computing zeta functions of arithmetic schemes*, Proc. Lond. Math. Soc. (3) **111** (2015), no. 6, 1379–1401. [MR 3447797](#)
- [HMS16] David Harvey, Maike Massierer, and Andrew V. Sutherland, *Computing  $L$ -series of geometrically hyperelliptic curves of genus three*, LMS J. Comput. Math. **19** (2016), no. suppl. A, 220–234. [MR 3540957](#)
- [HS14] David Harvey and Andrew V. Sutherland, *Computing Hasse–Witt matrices of hyperelliptic curves in average polynomial time*, LMS J. Comput. Math. **17** (2014), no. suppl. A, 257–273. [MR 3240808](#)
- [HS16] David Harvey and Andrew V. Sutherland, *Computing Hasse–Witt matrices of hyperelliptic curves in average polynomial time, II*, Frobenius distributions: Lang–Trotter and Sato–Tate conjectures, Contemp. Math., no. 663, Amer. Math. Soc., Providence, RI, 2016, pp. 127–147. [MR 3502941](#)
- [HVDH19] David Harvey and Joris Van Der Hoeven, *Integer multiplication in time  $O(n \log n)$* , preprint, 2019.
- [Kat90] Nicholas M. Katz, *Exponential sums and differential equations*, Annals of Mathematics Studies, no. 124, Princeton University Press, 1990. [MR 1081536](#)
- [Ked19] Kiran S. Kedlaya, *Frobenius structures on hypergeometric equations*, preprint, 2019. [arXiv 1912.13073v1](#)
- [KT99] Nicholas M. Katz and John Tate, *Bernard Dwork (1923–1998)*, Notices Amer. Math. Soc. **46** (1999), no. 3, 338–343. [MR 1669973](#)
- [LMFDB] The LMFDB collaboration, *The  $L$ -functions and modular forms database*.
- [Magma] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system, I: the user language*, J. Symbolic Comput., 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

- [McC13] Dermot McCarthy, *The trace of Frobenius of elliptic curves and the  $p$ -adic gamma function*, Pacific J. Math. **261** (2013), no. 1, 219–236. [MR 3037565](#)
- [Nas17] Bartosz Naskrecki, *On a certain hypergeometric motive of weight 2 and rank 3*, preprint, 2017. [arXiv 1702.07738v2](#)
- [Ono98] Ken Ono, *Values of Gaussian hypergeometric series*, Trans. Amer. Math. Soc. **350** (1998), no. 3, 1205–1223. [MR 1407498](#)
- [PAR19] PARI group, *PARI/GP*, 2019, version 2.11.2.
- [Rob00] Alain M. Robert, *A course in  $p$ -adic analysis*, Graduate Texts in Mathematics, no. 198, Springer, 2000. [MR 1760253](#)
- [RV07] Fernando Rodriguez Villegas, *Experimental number theory*, Oxford Graduate Texts in Mathematics, no. 13, Oxford University Press, 2007. [MR 2317419](#)
- [SageMath] The Sage Development Team, *SageMath, the Sage Mathematics Software System*.
- [Wat15] Mark Watkins, *Hypergeometric motives over  $\mathbb{Q}$  and their  $L$ -functions*, preprint, 2015.

Received 28 Feb 2020. Revised 4 Aug 2020.

EDGAR COSTA: [edgarc@mit.edu](mailto:edgarc@mit.edu)

*Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA, United States*

KIRAN S. KEDLAYA: [kedlaya@ucsd.edu](mailto:kedlaya@ucsd.edu)

*Department of Mathematics, University of California, San Diego, La Jolla, CA, United States*

DAVID ROE: [roed.math@gmail.com](mailto:roed.math@gmail.com)

*Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA, United States*



# Genus 3 hyperelliptic curves with CM via Shimura reciprocity

Bogdan Adrian Dina and Sorina Ionica

Up to isomorphism, every three-dimensional simple principally polarized abelian variety over  $\mathbb{C}$  is the Jacobian of a smooth projective curve of genus 3. Furthermore, this curve is either a hyperelliptic curve or a plane quartic. To define hyperelliptic class polynomials, we note that given a hyperelliptic Jacobian with CM, all principally polarized abelian varieties that are Galois conjugated to it are hyperelliptic. Using Shimura's reciprocity law, we then compute approximations of the invariants of the initial curve, as well as their Galois conjugates. We show examples of class polynomials computed using this method for the Shioda and Rosenhain invariants.

## 1. Introduction

Shimura and Taniyama's complex multiplication theory shows that it is possible to construct certain abelian extensions of CM fields by computing the values of Siegel modular functions evaluated at points with CM in the Siegel upper half-space. In addition, the effective computation of these modular forms makes it possible to compute models for CM curves, and also to effectively construct the related class fields.

For example, in genus one, the field of modular functions of level 1 is generated by the  $j$ -invariant. It is well known that the  $j$ -invariant of an elliptic curve with endomorphism ring isomorphic to the ring of integers of the CM field  $K$  generates the Hilbert class field of  $K$ . In the genus 2 case, the field of Siegel modular functions of level 1 is generated by the absolute Igusa invariants [11]. Similarly, when evaluated at CM points, their values give invariants of a hyperelliptic curve whose Jacobian has CM, and the class field equations, known as class polynomials, are recovered by computing these invariants for all curves with CM by the field [22; 8]. In genus 3, every simple principally polarized abelian variety (p.p.a.v.) over  $\mathbb{C}$  of dimension 3 is isomorphic to the Jacobian of a complete smooth projective curve, which is either a hyperelliptic curve or a plane quartic. Since two different sets of invariants for both genus 3 hyperelliptic curves and plane quartics are known in the literature, it is more difficult to tackle the problem of computing class polynomials for genus 3.

*MSC2010:* 11G10, 11G15, 11G30.

*Keywords:* hyperelliptic curve, complex multiplication, theta constants, class field.

In [27, Lemma 4.5], Weng shows that a simple principally polarized abelian threefold with CM by a sextic CM field containing  $\mathbb{Q}(i)$  is a hyperelliptic Jacobian. In the same paper, Weng gives an algorithm to compute hyperelliptic curves whose Jacobians have CM by a sextic field containing  $\mathbb{Q}(i)$ . In later work, Balakrishnan, Ionica, Lauter, and Vincent [1] give an algorithm which removes this restriction on the CM field, by performing a heuristic check. This heuristic relies on Mumford's Vanishing Criterion [16; 18], which states that a genus 3 curve is hyperelliptic if and only if one of the 36 even theta constants is 0. Given a period matrix with CM by a sextic CM field, the algorithm in [1] first computes the theta constants with enough precision to see if there is one which approximates zero, and then computes the Rosenhain invariants. These invariants generate a certain subfield of the ray class field of modulus 2 over the reflex field  $K^r$  of  $K$  and by approximating them with high precision, we can recognize them as algebraic numbers. This method has its limitations, since as soon as the degree of the class field over which the Rosenhains are defined is large ( $\geq 500$ ), the complexity of the algebraic dependence computation becomes a bottleneck. From a concrete point of view, only examples of CM fields with class number 1 were considered in [1].

In this paper, we extend the work in [1; 2] by considering the action on a hyperelliptic CM point of the Galois group  $\text{Gal}(CM_m(K^r)/K^r)$ , where  $CM_m(K^r)$  is a subfield of the ray class field of a given modulus  $m$ .

Once we identify a hyperelliptic curve  $X$  by verifying computationally and heuristically the vanishing criterion condition, we compute the Galois conjugates of its invariants via Shimura's reciprocity law. With these in hand, we compute the Shioda and Rosenhain class polynomials given by

$$H_{K^r,i}^R(t) = \prod_{\sigma} (t - \lambda_i^{\sigma}) \quad \text{and} \quad H_{K^r,j}^S(t) = \prod_{\sigma} (t - \text{Shi}_j^{\sigma}), \quad (1-1)$$

where  $\lambda_i$  ( $1 \leq i \leq 5$ ) and  $\text{Shi}_j$  ( $1 \leq j \leq 9$ ) denote the Rosenhain and Shioda invariants (introduced in Section 2) and  $\sigma \in \text{Gal}(CM_m(K^r)/K^r)$ , with  $m = (2)$  for the product in  $H_{K^r,i}^R$  and  $m = (1)$  for the product in  $H_{K^r,j}^S$ .

Aiming to implement our results in SageMath [25] and compute examples for the class polynomials of the Rosenhain and Shioda invariants, we also propose some methods to construct the reflex field associated to a given CM type, the typenorm, as well as the image of the typenorm as a subgroup in the Shimura class group.

## 2. Background

This section briefly recalls the necessary background and notation on complex abelian varieties, theta functions and the Vanishing Criterion which fully characterizes hyperelliptic principally polarized abelian varieties. We also define the invariants of hyperelliptic curves that we will be computing in the next sections.

**2A. Principally polarized abelian varieties over  $\mathbb{C}$  and period matrices.** A principally polarized abelian variety defined over  $\mathbb{C}$  is isomorphic to a complex torus admitting a Riemann form [3, Chapter 4]. Let



$g \geq 1$  and let  $A = \mathbb{C}^g / \Lambda$ , with  $\Lambda$  a full lattice in  $\mathbb{C}^g$  and  $E$  a Riemann form for  $(\mathbb{C}^g, \Lambda)$ . We will write  $(A, E)$  to denote the  $g$ -dimensional p.p.a.v. over  $\mathbb{C}$ . We consider a *symplectic* basis for the lattice  $\Lambda$ , by which we mean the action of  $E$  on  $\Lambda$  with respect to this basis is given by the matrix

$$J_g = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}, \quad (2-1)$$

where  $I_g$  is the  $g \times g$  identity matrix.

Let  $\Omega = [\Omega_1 \mid \Omega_2]$  be the  $g \times 2g$  matrix whose columns are the elements of this symplectic basis. By taking  $Z = \Omega_2^{-1} \Omega_1$  we obtain a  $g \times g$  matrix  $Z$  called a *period matrix*, i.e., an element of the Siegel upper half-space

$$\mathcal{H}_g = \{Z \in \mathcal{M}_g(\mathbb{C}) : Z^T = Z, \operatorname{Im}(Z) > 0\}.$$

We note that the lattice  $\Lambda$  can be written as  $Z\mathbb{Z}^g + \mathbb{Z}^g$ .

There is an action on  $\mathcal{H}_g$  by the symplectic group

$$\operatorname{Sp}_{2g}(\mathbb{Z}) = \{M \in \operatorname{GL}_{2g}(\mathbb{Z}) : M^T J_g M = J_g\},$$

where  $J_g$  is as in equation (2-1), given by

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : Z \mapsto M \cdot Z = (aZ + b)(cZ + d)^{-1}, \quad (2-2)$$

where on the right-hand side the multiplication of  $g \times g$  matrices is the usual matrix multiplication.

The association of  $Z$  to  $(\mathbb{C}^g / (Z\mathbb{Z}^g + \mathbb{Z}^g), E)$  gives a bijection between  $\operatorname{Sp}_{2g}(\mathbb{Z}) \backslash \mathcal{H}_g$  and the moduli space of p.p.a.v. of dimension  $g$  over  $\mathbb{C}$ . In the remainder of this paper, we will denote this moduli space by  $\mathcal{A}_g$ .

**2B. Theta functions.** For  $\omega = \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \in \mathbb{R}^{2g}$  and  $Z \in \mathcal{H}_g$ , we define the following important theta series:

$$\vartheta(\omega, Z) = \sum_{n \in \mathbb{Z}^g} \exp(\pi i(\omega_1 + n)^t Z(\omega_1 + n) + 2\pi i(\omega_1 + n)^t \omega_2). \quad (2-3)$$

Given a period matrix  $Z \in \mathcal{H}_g$ , we obtain a set of coordinates on the torus  $A = \mathbb{C}^g / (Z\mathbb{Z}^g + \mathbb{Z}^g)$  in the following way: a vector  $\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \in \mathbb{R}^{2g}$  corresponds to the point  $Z\omega_1 + \omega_2 \in \mathbb{C}^g / (Z\mathbb{Z}^g + \mathbb{Z}^g)$ . Under this identification, points of the form  $\xi = Z\xi_1 + \xi_2$  for  $\xi = \begin{pmatrix} \xi_1 \\ \xi_2 \end{pmatrix} \in \frac{1}{2}\mathbb{Z}^{2g}$  yield 2-torsion points on  $A$ . Using this notation we define

$$\vartheta[\xi](Z) = \exp(\pi i \xi_1^t Z \xi_1 + 2\pi i \xi_1^t \xi_2) \vartheta(\xi, Z). \quad (2-4)$$

In this context,  $\xi$  is called a *theta characteristic*, and the value  $\vartheta[\xi](Z)$  is called a *theta constant*. We call  $\xi$  a *even (odd)* theta characteristic if  $e_*(\xi) = 1$  ( $e_*(\xi) = -1$  respectively), where  $e_*(\xi) = \exp(4\pi i \xi_1^t \xi_2)$ . If  $\xi$  is an even (odd) theta characteristic we call  $\vartheta[\xi](Z)$  an *even (odd) theta constant*.

It can be easily shown that all odd theta constants are 0. We note that in the case where  $g = 3$  there are exactly 36 even classes of theta characteristics in  $\frac{1}{2}\mathbb{Z}^6 / \mathbb{Z}^6$ . We recall there is an action of the symplectic

group  $\mathrm{Sp}_{2g}(\mathbb{Z})$  on theta characteristics  $\xi \in \frac{1}{2}\mathbb{Z}^{2g}$  defined by

$$M.\xi = M^*\xi + \frac{1}{2}\delta_0, \quad (2-5)$$

with  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}_{2g}(\mathbb{Z})$ ,  $M^* = (M^{-1})^t$ , and  $\delta_0 = \begin{pmatrix} (c^t d)_0 \\ (a^t b)_0 \end{pmatrix}$  a column vector where  $(c^t d)_0$  and  $(a^t b)_0$  are the diagonal vectors of  $c^t d$  and  $a^t b$ , respectively. In this context, given a period matrix  $Z \in \mathcal{H}_g$ , we briefly recall the transformation formula on the theta constants [3, Formula 8.6.1]

$$\vartheta[M.\xi](M.Z) = \zeta(M) \exp(k(M, \xi)) \sqrt{\det(cZ + d)} \vartheta[\xi](Z), \quad (2-6)$$

where:

- (1)  $\zeta(M)$  is an eighth root of unity depending on  $M$ , having the same sign ambiguity as  $\sqrt{\det(cZ + d)}$ .
- (2)  $k(M, \xi) = \pi i (d\xi_1 - c\xi_2)^t (-b\xi_1 + a\xi_2 - (a^t b)_0) - \xi_1^t \xi_2$ .

For more details on  $\zeta(M)$ , we refer the reader to [3, Exercice 8.11(9)].

**2C. The Rosenhain invariants.** Let  $\mathcal{M}_g$  be the moduli space of smooth projective curves of genus  $g$ . By a theorem of Torelli [15, Theorem 12.1], there is an injective map  $\mathcal{M}_g \hookrightarrow \mathcal{A}_g$ . Inside  $\mathcal{M}_g$  we further restrict our attention to the subspace of hyperelliptic curves  $\mathcal{M}_g^{\mathrm{hyp}}$ . We will be interested in the effective reconstruction of a moduli point in  $\mathcal{M}_g^{\mathrm{hyp}}$  from a point in  $\mathcal{A}_g$ , whenever this point is in the image of  $\mathcal{M}_g^{\mathrm{hyp}} \hookrightarrow \mathcal{A}_g$ .

Let  $X$  be a hyperelliptic curve of genus  $g$  over  $\mathbb{C}$  defined by an equation  $y^2 = f(x)$ , where  $f$  is a polynomial with  $\deg(f) \in \{2g+1, 2g+2\}$ . Let  $(\lambda_i)_{1 \leq i \leq 2g+2}$  be the distinct complex roots of  $f$ , with the convention that  $\lambda_{2g}$  is  $\infty$  if  $\deg(f)$  is odd. We identify these roots with the branch points for the covering map  $\pi: X \rightarrow \mathbb{P}^1(\mathbb{C})$ , that we denote by  $P_1, \dots, P_{2g+1}, P_\infty$ . This motivates the following definition.

**Definition 2.1.** By a *marked* hyperelliptic curve  $X$  of genus  $g$  we understand a certain ordering of the branch points of the map  $\pi$ .

We will denote by  $\mathcal{M}_g^{\mathrm{hyp}}[2]$  the moduli space of marked hyperelliptic curves. Let us introduce more terminology. We note that the action on  $\mathcal{H}_g$  by the symplectic group of level 2

$$\Gamma_{2g}(2) = \{M \in \mathrm{Sp}_{2g}(\mathbb{Z}) : M \equiv I_{2g} \pmod{2}\},$$

fixes 2-torsion points on the p.p.a.v. This leads to the following definition.

**Definition 2.2.** We define by  $\mathcal{A}_g[2] = \Gamma_{2g}(2) \backslash \mathcal{H}_g$  the moduli space of principally polarized abelian varieties of dimension  $g$  over  $\mathbb{C}$  with a level 2-structure.

We will identify the Jacobian of a marked hyperelliptic curve to a point in  $\mathcal{A}_g[2]$  via the analytic construction. Let  $H_1(X, \mathbb{Z})$  be the first homology group of  $X$  and let  $H^0(\omega_X)$  be the group of 1-holomorphic forms on  $X$ . As explained in the literature, we view  $H_1(X, \mathbb{Z})$  as a lattice in  $H^0(\omega_X)^*$ , the dual of  $H^0(\omega_X)$  (see for example [3, Section 11.1]). As a consequence, we obtain the  $g$ -dimensional complex torus  $J(X) = H^0(\omega_X)^* / H_1(X, \mathbb{Z})$ . We choose a symplectic basis  $\gamma_1, \dots, \gamma_{2g}$  for  $H_1(X, \mathbb{Z})$  and

a basis  $\omega_1, \dots, \omega_g$  for  $H^0(\omega_X)$ . With the notation in [Section 2A](#), the corresponding  $g \times 2g$  matrix is  $\Omega = \left( \int_{\gamma_j} \omega_i \right)_{1 \leq i \leq g, 1 \leq j \leq 2g}$  and  $Z = \Omega_2^{-1} \Omega_1$ .

Let  $\text{Pic}^0(X) = \text{Div}^0(X) / \text{Princ}(X)$  be the group of degree zero divisors on  $X$  modulo principal divisors. The Abel–Jacobi map yields a canonical isomorphism [\[3, Theorem 11.1.3\]](#)

$$AJ: \text{Pic}^0(X) \rightarrow J(X). \quad (2-7)$$

Given a marked hyperelliptic curve  $X$ , we obtain a fixed set of 2-torsion points on  $J(X)$ . We take  $P_\infty$  as a base point and identify  $X$  with its image via the embedding  $X \hookrightarrow \text{Pic}^0(X)$ . Then the branch points  $P_i, i = 1, \dots, 2g + 2$ , correspond to points of the form  $e_i = [(P_i) - (P_\infty)]$  on  $\text{Pic}^0(X)$ . This allows us to choose an indexed set of characteristics  $\eta = (\eta_i)_{1 \leq i \leq 2g+2}$  in  $(1/2)\mathbb{Z}^{2g}$  such that

$$AJ(e_i) = Z(\eta_i)_1 + (\eta_i)_2 \pmod{Z\mathbb{Z}^g + \mathbb{Z}^g}. \quad (2-8)$$

This leads to the following definition.

**Definition 2.3.** Let  $V = \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$  the vector space over  $\mathbb{F}_2$ . By an *azygetic system* we understand an indexed set  $\eta = (\eta_1, \dots, \eta_{2g+2})$  of  $2g + 2$  vectors in  $\frac{1}{2}\mathbb{Z}^{2g}$  such that the images of  $\eta_i$  in  $V$ , denoted by  $\bar{\eta}_i$ , satisfy

$$V = \text{span}(\bar{\eta}_i), \quad \sum_{i=1}^{2g+1} \bar{\eta}_i = 0, \quad \bar{\eta}_{2g+2} = 0, \quad \text{and} \quad \bar{\eta}_i^t \bar{\eta}_j \equiv 1 \pmod{2}, \quad (2-9)$$

for  $i, j$  different from  $2g + 2$  and  $i \neq j$ .

Two azygetic sets  $\eta'$  and  $\eta''$  are said to be in the same *equivalence class* if  $\bar{\eta}'_i = \bar{\eta}''_i, i = 1, \dots, 2g + 2$ . Following [Poor \[18\]](#), the indexed set  $(\eta_1, \dots, \eta_{2g+2})$  obtained in equation (2-8) is an azygetic system and we call it an azygetic system *associated to the period matrix*  $Z$ .

If we change the homology basis by taking  $(\gamma'_1, \dots, \gamma'_{2g}) = (\gamma_1, \dots, \gamma_{2g})M^t$ , with  $M \in \text{Sp}_{2g}(\mathbb{Z})$ , the new period matrix obtained using the construction above is  $Z' = M.Z$ . The azygetic system associated to  $Z'$  is  $\eta' = (M^*\eta_1, \dots, M^*\eta_{2g+2})$ . Since the map  $\text{Sp}_{2g}(\mathbb{Z}) \rightarrow \text{Sp}_{2g}(\mathbb{F}_2) \cong \text{Sp}_{2g}(\mathbb{Z})/\Gamma_{2g}(2)$  is surjective, we further derive an action of  $\text{Sp}_{2g}(\mathbb{F}_2)$  on equivalence classes of azygetic systems, which was shown to be free and transitive [\[18, Lemma 1.4.13\]](#).

Let us introduce some further notations. Let  $T = \{1, \dots, 2g + 1, \infty\}$ . For a given azygetic system, [Poor](#) defines the set  $\mathcal{U}_\eta$  to be the set of indexes  $i \in T$  such that  $\eta_i$  is even. For any  $S_1, S_2 \subseteq T$  we denote the symmetric difference  $S_1 \circ S_2 = (S_1 \cup S_2) \setminus (S_1 \cap S_2)$ . For an azygetic system  $\eta$  and  $S \subseteq T$ , we define  $\eta_S = \sum_{s \in S} \eta_s$ . The following theorem, which we refer to as the *Vanishing Criterion*, gives a characterization of hyperelliptic period matrices in terms of their associated azygetic system and theta constants. For simplicity, we recall this theorem for genus 3 as stated in [\[1, Proposition 5\]](#) and refer the reader to [\[16, Chapter III.9\]](#) and [\[18, Theorem 2.6.1\]](#) for the general result in genus  $g \geq 1$ .

**Theorem 2.4** (The Vanishing Criterion). *Let  $Z \in \mathcal{H}_3$  and let  $\eta$  be an azygetic system. The following two statements are equivalent:*

- (1)  *$Z$  is the period matrix of a symplectically irreducible abelian variety and there is exactly one of even theta characteristic  $\delta$  such that  $\vartheta[\delta](Z) = 0$  and that  $\delta = \eta_{\mathcal{U}_\eta}$ .<sup>1</sup>*
- (2) *There is a marked hyperelliptic curve of genus 3 whose Jacobian has period matrix  $Z$  and  $\eta$  is the azygetic system associated to  $Z$ .*

In other words, [Theorem 2.4](#) shows that given a hyperelliptic period matrix  $Z \in \mathcal{H}_3$ , choosing one of its azygetic systems  $\eta$  such that  $\vartheta[\eta_{\mathcal{U}_\eta}] = 0$  fixes a labeling of the branch points. We recover the point in  $\mathcal{M}_g^{\text{hyp}}[2]$  using Takase's formulae [\[1; 24\]](#), which we recall in the following theorem.

**Theorem 2.5** [\[1, Theorem 3\]](#). *Let  $Z \in \Gamma_6(2) \setminus \mathcal{H}_3$  a period matrix and  $\eta$  be the azygetic system such that the Vanishing Criterion is satisfied. Then with notation as above, for any disjoint decomposition  $T - \{\infty\} = \mathcal{V} \sqcup \mathcal{W} \sqcup \{k, l, m\}$  with  $\#\mathcal{V} = \#\mathcal{W} = 2$ , we have*

$$\frac{\lambda_m - \lambda_l}{\lambda_m - \lambda_k} = \exp(4\pi i (\eta_k + \eta_l)_1 (\eta_m)_2) \left( \frac{\vartheta[\eta_{\mathcal{U}_\eta \circ (\mathcal{V} \cup \{m, l\})}] \cdot \vartheta[\eta_{\mathcal{U}_\eta \circ (\mathcal{W} \cup \{m, l\})}]}{\vartheta[\eta_{\mathcal{U}_\eta \circ (\mathcal{V} \cup \{k, m\})}] \cdot \vartheta[\eta_{\mathcal{U}_\eta \circ (\mathcal{W} \cup \{k, m\})}]}(Z) \right)^2. \quad (2-10)$$

Note that in [\[1\]](#) the sign before the quotient of theta constants in equation (2-10) is incorrect. We give here the correct formula, as stated in several sources [\[2; 13\]](#).

Finally, note that by considering an affine map of  $\mathbb{C}$ , we may assume without restricting the generality that  $\lambda_6 = 0$  and  $\lambda_7 = 1$ , i.e.,  $X$  is given by

$$X : y^2 = x(x-1) \prod_{i=1}^5 (x - \lambda_i). \quad (2-11)$$

In this case, we say that  $X$  is in *normalized Rosenhain form*. The moduli space  $\mathcal{M}_3^{\text{hyp}}[2]$  writes as

$$\mathcal{M}_3^{\text{hyp}}[2] \cong \{\lambda = (\lambda_1, \dots, \lambda_5), \lambda_i \in \mathbb{C} - \{0, 1\}, \lambda_i \neq \lambda_j\}.$$

The coefficients  $\lambda_i \in \mathbb{C} - \{0, 1\}$ , are called *the Rosenhain invariants* of the curve and will be the focus of our work.

**2D. Shioda invariants.** Shioda [\[20\]](#) gave a set of generators for the algebra of invariants of binary octavics over the complex numbers, which are now called *Shioda invariants*. Following Shioda's notation (see [\[20, page 1025\]](#)), these are 9 weighted projective invariants  $(J_2, J_3, J_4, J_5, J_6, J_7, J_8, J_9, J_{10})$ , where

<sup>1</sup>Poor defines symplectically irreducible on page 831 of [\[18\]](#). His condition is equivalent to requiring that the abelian variety is not isomorphic as a polarized abelian variety to a product of lower-dimensional polarized abelian varieties. In this work, our period matrices are constructed to be simple, i.e., not isogenous to a product of lower-dimensional polarized abelian varieties. Since isomorphism is stronger than isogeny, all of the period matrices we construct are symplectically irreducible, and we may apply the theorem.

$J_i$  has degree  $i$ . The invariants  $J_2, \dots, J_7$  are algebraically independent, while  $J_8, J_9, J_{10}$  depend algebraically on them. Note that over the complex numbers Shioda invariants completely determine points in  $\mathcal{M}_3^{\text{hyp}}$ .

Using Igusa's map between the graded ring of Siegel modular forms of degree 3, and the graded ring of invariants of binary octavics, Lorenzo García [9] proposes a set of invariants which can be written as quotients of modular forms. These invariants involve large powers of the modular form  $\chi_{28}$  in the denominators and we do not use them for experiments since they would need too much precision to compute.

Starting from the projective invariants  $J_i$ , we consider the following absolute Shioda invariants:<sup>2</sup>

$$\text{Shi} = \left( \frac{J_7^7}{\Delta}, \frac{J_2^4 J_3^2}{\Delta}, \frac{J_2^5 J_4}{\Delta}, \frac{J_5 J_9}{\Delta}, \frac{J_2^4 J_6}{\Delta}, \frac{J_7^2}{\Delta}, \frac{J_2^3 J_8}{\Delta}, \frac{J_2^5 J_9^2}{\Delta^2}, \frac{J_2^2 J_{10}}{\Delta} \right), \quad (2-12)$$

with  $\Delta$  the discriminant of the binary octavic, which is an invariant of degree 14. They are optimal for computations in the sense that they involve invariants of small weight and the values of their denominators for a given curve are products of powers of the primes of bad reduction of the curve; see [12]. Note that a subset of this set was already used by Weng [27] for computing models of hyperelliptic curves with CM by a field which contains  $i$ .

**Proposition 2.1.** *The invariants in equation (2-12) are modular, i.e., they can be written as quotients of Siegel modular forms of level 1.*

*Idea of the proof.* In [26], Tsuyumine proposed a set of invariants for the algebra of binary octavics and also computed them in terms of Siegel modular forms (see for instance [9, Theorem 3.4]). Using relations between Tsuyumine's invariants and the Shioda projective invariants (given in [9, Theorem 4.1]), we were able to write each invariant in equation (2-12) as a quotient of Siegel modular forms. The full computation is given in the arxiv version of this paper [7].

### 3. Computing abelian varieties with CM

In this section, we review results from the theory of complex multiplication, with the goal of describing our implementation of algorithms for computing several notions, such as the reflex field and the typenorm. Finally, we state the effective version of Shimura's second main theorem of CM.

**3A. Reflex field computation.** Let  $K/\mathbb{Q}$  be a CM field and let  $L$  be the Galois closure of  $K$  with Galois group  $\text{Gal}(L/\mathbb{Q})$ . A CM type of  $K$  is a set  $\Phi = \{\phi_1, \dots, \phi_g\}$  of  $g$  embeddings  $K \hookrightarrow \mathbb{C}$  such that no two embeddings appearing in  $\Phi$  are complex conjugates. We say that  $\Phi$  is *induced* from a CM subfield  $K'$  of  $K$  if the set  $\{\phi|_{K'} \mid \phi \in \Phi\}$  is a CM type of  $K'$ . A CM type of  $K$  is called *primitive* if it is not induced by a proper CM subfield  $K' \subset K$ . In this paper, we fix the tuple  $(K, \Phi)$  and call it a *CM-pair*. Since  $L$

<sup>2</sup>An absolute invariant is a ratio of homogeneous invariants of the same degree.

is a CM field [14, Corollary 1.5],  $\Phi$  extends to a CM type  $\Phi_L$  of  $L$ , namely by

$$\Phi_L = \{\phi : L \rightarrow \mathbb{C} \mid \phi|_K \in \Phi\}. \quad (3-1)$$

We fix once and for all an embedding  $\iota_K : K \rightarrow L$  and an embedding  $\pi : L \rightarrow \mathbb{C}$ . With these in hand, we associate to every element in  $\phi \in \Phi_L$  an element  $\sigma \in \text{Gal}(L/\mathbb{Q})$  such that the following diagram commutes:

$$\begin{array}{ccc} L & \xrightarrow{\sigma} & L \\ \iota_K \uparrow & & \downarrow \pi \\ K & \xrightarrow{\phi|_K} & \mathbb{C} \end{array} \quad (3-2)$$

Note that this identification is certainly dependent on the embeddings  $\iota_K$  and  $\pi$ . Let  $\Phi_L^{-1} = \{\pi \circ \sigma^{-1} \in \text{Hom}(L, \mathbb{C}) \mid \phi = \pi \circ \sigma \text{ for } \phi \in \Phi_L\}$ . One can easily check that  $\Phi_L^{-1}$  is a CM type on  $L$  if and only if  $\Phi_L$  is a CM type on  $L$ . We denote by  $H^r$  the subgroup of  $\text{Gal}(L/\mathbb{Q})$  of the form

$$H^r = \{\sigma \in \text{Gal}(L/\mathbb{Q}) \mid \sigma \Phi_L = \Phi_L\}. \quad (3-3)$$

**Definition 3.1.** The subfield of  $L$  fixed by the group  $H^r$  in equation (3-3) is called the *reflex field* of  $(K, \Phi)$ . We denote it by  $K^r$ .

Note that, from a computational point of view, choosing  $K^r$  as the field fixed by  $H^r$  also means fixing the embedding  $\iota_{K^r} : K^r \rightarrow L$ . As shown for instance in [14, Proposition 1.18],  $K^r$  is also a CM field and the associated CM type to  $K^r$  is given by the following construction:

$$\Phi^r = \Phi_L^{-1}|_{K^r} = \{\phi|_{K^r} \mid \phi \in \Phi_L^{-1}\}. \quad (3-4)$$

We call the tuple  $(K^r, \Phi^r)$  the *reflex CM-pair* of  $(K, \Phi)$ . We implemented a procedure for computing the CM-pair  $(K^r, \Phi^r)$  based on Definition 3.1 (see Algorithm 1 in [7] for full details). Our approach is similar to the implementation of the reflex field in the code of [23].

**3B. The reflex typenorm.** Let  $(K, \Phi)$  be a primitive CM-pair with Galois closure  $L$  of  $K$  and reflex CM-pair  $(K^r, \Phi^r)$ . The *reflex typenorm* is the map

$$N_{\Phi^r} : K^r \rightarrow K \subset L, \quad x \mapsto \prod_{\phi \in \Phi^r} \phi(x). \quad (3-5)$$

We denote by  $I(K)$  and  $I(K^r)$  the set of nonzero fractional ideals of  $\mathcal{O}_K$  and  $\mathcal{O}_{K^r}$ , respectively.

**Lemma 3.1** [19, Chapter 2, Proposition 29]. *The reflex typenorm in equation (3-5) induces a map between ideals*

$$N_{\Phi^r} : I(K^r) \rightarrow I(K), \quad \mathfrak{a} \mapsto \prod_{\phi \in \Phi^r} \phi(\mathfrak{a}),$$

which extends to a homomorphism between class groups  $N_{\Phi^r} : \text{Cl}(K^r) \rightarrow \text{Cl}(K)$ .

When computing the typenorm of an ideal  $\mathfrak{a} \in I(K^r)$ , the product  $\prod_{\phi \in \Phi^r} \phi(\mathfrak{a})$  gives a priori an ideal in  $L$ . To identify the ideal in  $K$  lying below this ideal, we first compute the factorization of this ideal and rely on an algorithm in [5, Algorithm 2.5.3] to get the prime ideal lying below each of the ideals appearing in this factorization. Algorithm 2 in [7] gives the pseudocode of our method. We remark that an alternative implementation for computing the typenorm, based on the proof of Lemma 3.1, is given in the code of [23].

**3C. Class field theory.** For a number field  $K$  and a finite modulus  $\mathfrak{m}$  (i.e., a product of prime ideals in  $K$ ), let  $I_{\mathfrak{m}}(K)$  be the group of all fractional  $\mathcal{O}_K$  ideals coprime to  $\mathfrak{m}$ , and consider the subgroup

$$P_{\mathfrak{m}}(K) = \{\mathfrak{a} \in I_{\mathfrak{m}}(K) : \mathfrak{a} = \alpha \mathcal{O}_F, \alpha \equiv 1 \pmod{*}\mathfrak{m}\},$$

where the congruence  $\alpha \equiv 1 \pmod{*}\mathfrak{m}$  means that for all primes  $\mathfrak{p}$  appearing in the factorization of  $\mathfrak{m}$  we have  $v_{\mathfrak{p}}(\alpha - 1) \geq v_{\mathfrak{p}}(\mathfrak{m})$ . The *ray class group* of  $K$  for the modulus  $\mathfrak{m}$  is defined as the quotient group  $Cl_{\mathfrak{m}}(K) = I_{\mathfrak{m}}(K)/P_{\mathfrak{m}}(K)$ .

For a modulus  $\mathfrak{m}$  in  $K$  we denote by  $\mathcal{H}_{\mathfrak{m}}$  the unique (up to isomorphism) abelian extension of  $K$  whose ramified primes divide  $\mathfrak{m}$  and such that the kernel of the *Artin map*

$$\Phi_{\mathfrak{m}} : I_{\mathfrak{m}}(K) \rightarrow \text{Gal}(\mathcal{H}_{\mathfrak{m}}/K)$$

is equal to  $P_{\mathfrak{m}}(K)$ . The field  $\mathcal{H}_{\mathfrak{m}}$  is called the *ray class field* of  $K$  of modulus  $\mathfrak{m}$ ; see for instance [6, Theorem 8.6].

Let  $(K, \Phi)$  be a primitive CM-pair with reflex pair  $(K^r, \Phi^r)$ . Let  $m \in \mathbb{Z}$  such that  $m\mathbb{Z} = \mathfrak{m} \cap \mathbb{Z}$  and denote by  $I_m(K^r)$  the group of fractional ideals in  $K^r$  coprime to  $m$ . Following Shimura [19, Chapter 16], we consider

$$H_{\mathfrak{m}}(K^r) = \{\mathfrak{a} \in I_m(K^r) : \exists \alpha \in K^* \text{ with } N_{\Phi^r}(\mathfrak{a}) = \alpha \mathcal{O}_K, N_{K^r/\mathbb{Q}}(\mathfrak{a}) = \alpha \bar{\alpha}, \alpha \equiv 1 \pmod{*}\mathfrak{m}\}. \quad (3-6)$$

Note that  $P_m(K^r) \subset H_{\mathfrak{m}}(K^r)$ . Then, after [6, Theorem 8.6], up to isomorphism there is a unique Abelian extension of  $K^r$ , denoted by  $CM_{\mathfrak{m}}(K^r)$ , such that

$$\text{Gal}(CM_{\mathfrak{m}}(K^r)/K^r) \cong I_m(K^r)/H_{\mathfrak{m}}(K^r). \quad (3-7)$$

The effective construction of  $CM_{\mathfrak{m}}(K)$  relies on Shimura's Main Theorem 2, that we state in Section 3D. In order to compute Galois conjugates of elements in this number field in Section 4, we will need to compute the group  $I_m(K^r)/H_{\mathfrak{m}}(K^r)$ . In order to do this, we will need the following group introduced by Shimura:

$$\mathcal{C}_{\mathfrak{m}}(K) = \{(\mathfrak{a}, \alpha) : \mathfrak{a} \in I_{\mathfrak{m}}(K) \text{ such that } \mathfrak{a}\bar{\mathfrak{a}} = (\alpha), \alpha \in K_0 \text{ totally positive, } \alpha \equiv 1 \pmod{*}\mathfrak{m}\} / \simeq, \quad (3-8)$$

where  $(\mathfrak{a}, \alpha) \simeq (\mathfrak{a}', \alpha')$  if and only if there exists  $\mu \in K^*$  such that  $\mathfrak{a} = \mu \mathfrak{a}'$  and  $\alpha = \alpha' \mu \bar{\mu}$  and  $\mu \equiv 1 \pmod{*}\mathfrak{m}$ . Given a pair  $(\mathfrak{a}, \alpha)$  satisfying the conditions in equation (3-8), we denote by  $(\mathfrak{a}, \alpha)_{\mathfrak{m}}$  the corresponding equivalence class.

**Lemma 3.2.** *We denote by  $T : \text{Cl}_m(K^r) \rightarrow \mathfrak{C}_m(K)$  the map given by  $\mathfrak{a} \rightarrow (N_{\Phi^r}(\mathfrak{a}), N_{K^r/\mathbb{Q}}(\mathfrak{a}))_m$ . Then:*

- (a) *The kernel of this map is  $\ker T = H_m(K^r)/P_m(K^r)$ .*
- (b) *The image of the map  $T$  is isomorphic to  $I_m(K^r)/H_m(K^r)$ .*

*Proof.* (a) Let  $\mathfrak{a} \in \ker T$ , i.e.,  $(N_{\Phi^r}(\mathfrak{a}), N_{K^r/\mathbb{Q}}(\mathfrak{a}))_m = (\mathcal{O}_K, 1)_m$ . Then there exists an element  $\mu \in K^*$  such that  $N_{\Phi^r}(\mathfrak{a}) = \mu \mathcal{O}_K$  and  $N_{K^r/\mathbb{Q}}(\mathfrak{a}) = \mu \bar{\mu}$  and  $\mu \equiv 1 \pmod{*m}$ . Conversely, by the definition of  $H_m(K^r)$ , any element in  $H_m(K^r)/P_m(K^r)$  is in  $\ker T$ .

(b) It follows immediately from point (a) that

$$T(\text{Cl}_m(K^r)) \cong \text{Cl}_m(K^r)/\ker T \cong (I_m(K^r)/P_m(K^r))/(H_m(K^r)/P_m(K^r)) \cong I_m(K^r)/H_m(K^r). \quad \square$$

In our implementation we computed a set of generators for  $\text{Cl}_m(K^r)$  using Magma, and then implemented an algorithm for enumerating the elements in the set  $T(\text{Cl}_m(K^r))$ . Due to Lemma 3.2, this allowed us to compute the group  $I_m(K^r)/H_m(K^r)$  and enumerate Galois conjugates of a CM point (see Definition 4.1).

**3D. CM abelian varieties.** Before stating Shimura's second main theorem, we briefly set the notation and recall the terminology. Let  $A$  an abelian variety of dimension  $g$  defined over a field  $k$ . We say that  $A$  has *complex multiplication* (CM) by a number field  $K$  if there exists an embedding  $\iota : K \rightarrow \text{End}(A) \otimes \mathbb{Q}$ . If  $\mathcal{O}_K$  is the maximal order of  $K$ , then we say that  $A$  has CM by  $\mathcal{O}_K$  if  $\iota^{-1}(\text{End}(A)) = \mathcal{O}_K$ . Let  $\mathfrak{D}_{K/\mathbb{Q}}$  be the different of  $K$ , and let  $\mathfrak{a}$  be a fractional ideal of  $\mathcal{O}_K$ . Suppose that the ideal  $(\mathfrak{D}_{K/\mathbb{Q}} \mathfrak{a} \bar{\mathfrak{a}})^{-1}$  is principal and generated by  $\xi \in K^\times$  such that  $\text{Im}(\phi(\xi)) > 0$  for all  $\phi \in \Phi$ . Then by tensoring the map

$$\Phi(\mathfrak{a}) \times \Phi(\mathfrak{a}) \rightarrow \mathbb{Q}, \quad (\Phi(x), \Phi(y)) \mapsto \text{Tr}_{K/\mathbb{Q}}(\xi \bar{x}y)$$

with  $\mathbb{R}$  we obtain a Riemann form  $E_{\Phi, \xi} : \mathbb{C}^g \times \mathbb{C}^g \rightarrow \mathbb{R}$ . Hence for any triple  $(\Phi, \mathfrak{a}, \xi)$  as above, the pair  $(\mathbb{C}^g/\Phi(\mathfrak{a}), E_{\Phi, \xi})$  is a p.p.a.v. of dimension  $g$  with CM by  $\mathcal{O}_K$  and of CM type  $\Phi$ . Conversely, every p.p.a.v. of dimension  $g$  with CM by  $\mathcal{O}_K$  is isomorphic to a complex torus for some triple  $(\Phi, \mathfrak{a}, \xi)$  as above. Note that to go from the triple  $(\Phi, \mathfrak{a}, \xi)$  to a period matrix as described in Section 2A, it suffices to write a basis for the ideal  $\mathfrak{a}$  that is symplectic with respect to the Riemann form  $E_{\Phi, \xi}$ . This basis gives the matrix  $\Omega$ , and then the period matrix is simply  $Z = \Omega_2^{-1} \Omega_1$ .

Let  $(A, E)$  be a p.p.a.v. with CM by  $\mathcal{O}_K$ ,  $G$  the automorphism group of  $A$  and let  $k_0$  be its field of moduli. To state Shimura's second main theorem of CM, we consider the *normalized Kummer variety* [19, Theorem 3, Section 4.4] of  $A$ . This is given by a tuple  $(W, h)$ , where  $W$  is the quotient of  $A$  by  $G$ , which is defined over  $k_0$ , and  $h : A \rightarrow W$  is the corresponding surjective map. Moreover, given a modulus  $\mathfrak{m}$ , we denote by  $A[\mathfrak{m}]$  the  $\mathfrak{m}$ -torsion points of  $A$ , i.e.,  $A[\mathfrak{m}] = \{x \in A \mid \iota(\alpha)x = 0, \forall \alpha \in \mathfrak{m}\}$ . A point  $t \in A[\mathfrak{m}]$  is called *proper* if for all  $a \in \mathcal{O}_K$ , we have that  $\iota(a)t = 0$  if and only if  $a \in \mathfrak{m}$ .

**Theorem 3.2** [19, Main Theorem 2]. *Let  $(A, E)$  be a principally polarized abelian variety with CM by  $\mathcal{O}_K$  and CM type  $\Phi$  and let  $(W, h)$  its normalized Kummer variety. Let  $\mathfrak{m}$  be an ideal of  $\mathcal{O}_K$  and  $t$  be*



a proper  $\mathfrak{m}$ -torsion point. Let  $k_0$  be the field of moduli of  $A$ ,  $K^r$  the reflex field of  $K$  and  $k_0^* = k_0 K^r$ . Then  $k_0^*(h(t))$  is the class field of  $K^r$  corresponding to the ideal group  $H_{\mathfrak{m}}(K^r)$ .

#### 4. Computing class polynomials

We turn our attention now to the computation of the Shioda and Rosenhain invariants of a hyperelliptic curve of genus 3 with CM by  $\mathcal{O}_K$ , and more precisely to obtaining their minimal polynomials over the reflex field.

Given a primitive CM-pair  $(K, \Phi)$ , we denote by  $\text{Princ}(K, \Phi, \mathfrak{m})$  the set of isomorphism classes of simple p.p.a.v. with CM by  $\mathcal{O}_K$  together with a proper  $\mathfrak{m}$ -torsion point. We denote by  $A(\Phi, \mathfrak{a}, \xi, t)$  the abelian variety given by the triple  $(\Phi, \mathfrak{a}, \xi)$  and the proper  $\mathfrak{m}$ -torsion point  $t$ . When  $\mathfrak{m} = (1)$ , we simply denote it by  $A(\Phi, \mathfrak{a}, \xi)$  and we take  $\text{Princ}(K, \Phi)$  to be the set of all such abelian varieties. In our computations of Galois conjugates, we will extensively use the following action of the class group  $I_{\mathfrak{m}}(K^r)/H_{\mathfrak{m}}(K^r)$  on  $\text{Princ}(K, \Phi, \mathfrak{m})$  given by Shimura [19, Section 16.3].

**Definition 4.1.** Let  $A = A(\Phi, \mathfrak{a}, \xi, t) \in \text{Princ}(K, \Phi, \mathfrak{m})$ . Then for any  $[\mathfrak{c}] \in I_{\mathfrak{m}}(K^r)/H_{\mathfrak{m}}(K^r)$  the action of  $[\mathfrak{c}]$  on  $A$  is given by the abelian variety

$$A(\Phi, N_{\Phi^r}(\mathfrak{c})^{-1}\mathfrak{a}, N_{K^r/\mathbb{Q}}(\mathfrak{c})\xi, t \pmod{N_{\Phi^r}(\mathfrak{c})^{-1}\mathfrak{a}}).$$

We will denote by  $A^{\mathfrak{c}}$  the p.p.a.v. obtained in this way.

Note that the action in Definition 4.1 yields in fact an isogeny between principally polarized abelian varieties  $I_{\mathfrak{c}} : A \rightarrow A^{\mathfrak{c}}$ . Since the ideal  $\mathfrak{c}$  is coprime to  $m$ , we have that  $\ker I_{\mathfrak{c}} \cap A[\mathfrak{m}] = 0$ . In particular, when  $\mathfrak{m} = (m)$  and we fix a level  $m$  structure on  $A$ , this isogeny fixes the level  $m$  structure on  $A^{\mathfrak{c}}$ .

**Notation 4.2.** In the remainder of this paper, we will restrict to  $\mathfrak{m} = (m)$ , where  $m = 1$  or  $m = 2$ . For a given  $\mathfrak{c} \in I_{\mathfrak{m}}(K^r)/H_{\mathfrak{m}}(K^r)$ , we will denote by  $\sigma_{\mathfrak{c}} \in \text{Gal}(CM_{\mathfrak{m}}(K^r)/K^r)$  the image of  $\mathfrak{c}$  via the isomorphism in equation (3-7). Let  $A = A(\Phi, \mathfrak{a}, \xi, t)$  be a p.p.a.v. in  $\text{Princ}(K, \Phi, \mathfrak{m})$ . Let  $B = (B_1|B_2)$  be a  $(3 \times 6)$  complex-valued matrix containing a symplectic basis for  $\Phi(\mathfrak{a})$  with respect to  $E_{\Phi, \xi}$ , and let  $Z = B_2^{-1}B_1 \in \mathcal{H}_3$  be the corresponding period matrix. The action of  $\mathfrak{c}$  on  $A$  yields a new p.p.a.v.  $A(\Phi, N_{\Phi^r}(\mathfrak{c})^{-1}\mathfrak{a}, N_{K^r/\mathbb{Q}}(\mathfrak{c})\xi, t \pmod{N_{\Phi^r}(\mathfrak{c})^{-1}\mathfrak{a}})$ . In a similar manner, let  $C = (C_1|C_2)$  be the matrix containing a symplectic basis for  $\Phi(N_{\Phi^r}(\mathfrak{c})^{-1}\mathfrak{a})$  with respect to  $E_{\Phi, N_{K^r/\mathbb{Q}}(\mathfrak{c})\xi}$  and let  $Z' = C_2^{-1}C_1 \in \mathcal{H}_3$ . We express  $C$  in terms of  $B$  by taking a matrix  $M$ , such that  $C = BM^T$ . The matrix  $M$  is in  $\text{GSp}_{2g}(\mathbb{Q})$  and is  $m$ -integral and invertible  $\pmod{m}$  with inverse  $U \in \text{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$ . We also denote by  $\tilde{U} \in \text{Sp}_{2g}(\mathbb{Z})$  a lift of  $U$ . Such a lift can be computed for instance thanks to [17, Theorem VII.21].

This notation will be used all throughout this section. We detail the computation of these matrices on an example.

**Example 4.3.** Let  $K$  be the CM field defined by the polynomial  $x^6 + 43x^4 + 451x^2 + 729$  and denote by  $a$  a generator for this field. We choose the first CM type given by the implementation [2] and we get that the tuple  $(\mathfrak{a}, \xi) = (\mathcal{O}_K, \frac{16}{114939}a^5 + \frac{1313}{229878}a^3 + \frac{5857}{114939}a)$  yields a CM point. We compute the action

on this CM point by the ideal  $\mathfrak{c} = (9, \frac{1}{48}a^5 + \frac{11}{24}a^3 + \frac{1}{2}a^2 - \frac{155}{48}a + \frac{15}{2})$  and get a second CM point given by

$$(\mathfrak{b}, \xi') = ((9, \frac{1}{48}a^5 + \frac{11}{24}a^3 + \frac{1}{2}a^2 - \frac{155}{48}a + \frac{15}{2}), \frac{16}{114939}a^5 + \frac{1313}{229878}a^3 + \frac{5857}{114939}a).$$

The code in [2] gives symplectic bases for  $(\mathfrak{a}, \xi)$  and  $(\mathfrak{b}, \xi')$  and we compute

$$M = \begin{pmatrix} -1 & 1 & -1 & 0 & 1 & 3 \\ 2 & -1 & 0 & -2 & 1 & 4 \\ 2 & 0 & 1 & 2 & 4 & -1 \\ 0 & -1 & -1 & -1 & 3 & -1 \\ 1 & 0 & -1 & 1 & -1 & 1 \\ -1 & -1 & 0 & 1 & 1 & 1 \end{pmatrix}, \quad U = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

The following result gives an explicit version of Shimura's reciprocity law.

**Theorem 4.4** [23, Theorem 2.4]. *Let  $\mathfrak{c} \in I_m(K^r)/H_m(K^r)$ ,  $\sigma_{\mathfrak{c}} \in \text{Gal}(CM_m(K^r)/K^r)$ ,  $Z, Z' \in \mathcal{H}_3$  and the matrix  $M$  as in Notation 4.2. For every Siegel modular function  $f$  of level  $m$  with Fourier expansion coefficients in  $\mathbb{Q}(\xi_m)$ , we have*

$$f(Z)^{\sigma_{\mathfrak{c}}} = f^U(Z'), \quad (4-1)$$

where we denote by  $f^U(Z') = f(\tilde{U} \cdot Z')$ , for any  $\tilde{U} \in \text{Sp}_{2g}(\mathbb{Z})$  a lift of  $U$ .

We will use Theorem 4.4 to compute the Galois conjugates of the Shioda invariants of a hyperelliptic curve whose period matrix is obtained via the complex multiplication construction.

**Proposition 4.1.** *Let  $A \in \text{Princ}(K, \Phi)$  and  $Z \in \mathcal{H}_3$  a period matrix for it. Let  $[\mathfrak{c}] \in \text{Cl}(K^r)$  corresponding to  $\sigma_{\mathfrak{c}} \in \text{Gal}(CM_1(K^r)/K^r)$  and  $Z'$  obtained as in Notation 4.2. Then  $A^{\mathfrak{c}}$  is isomorphic to a hyperelliptic Jacobian if and only if  $A$  is. Moreover, we have the following relation:*

$$S_j(Z)^{\sigma_{\mathfrak{c}}} = S_j(Z'), \quad (4-2)$$

where  $S_j$  denotes the Siegel modular function giving the  $j$ -th Shioda absolute invariant, for all  $j = 1, \dots, 9$ .

*Proof.* Suppose that  $A \cong \text{Jac}(X)$ , with  $X$  a hyperelliptic curve. Since  $\text{Jac}(X)^{\sigma_{\mathfrak{c}}} \cong \text{Jac}(X^{\sigma_{\mathfrak{c}}})$ , it follows that  $A^{\mathfrak{c}}$  is isomorphic to the Jacobian of the hyperelliptic curve  $X^{\sigma_{\mathfrak{c}}}$ . To prove equation (4-2), we apply Theorem 4.4 on the Siegel modular functions  $S_i$ .  $\square$

We now restrict to the case of the modulus  $\mathfrak{m} = (2)$ . The following result allows us to compute the Galois conjugates of the Rosenhain invariants.

**Theorem 4.5.** *Let  $A \in \text{Princ}(K, \Phi)$  which is isomorphic to the Jacobian of a marked genus 3 hyperelliptic curve and  $Z \in \Gamma_6(2) \backslash \mathcal{H}_3$  a period matrix for it. Let  $[\mathfrak{c}] \in I_2(K^r)/P_2(K^r)$  corresponding to  $\sigma_{\mathfrak{c}} \in \text{Gal}(CM_2(K^r)/K^r)$  and  $Z'$  obtained as in Notation 4.2. We consider  $\eta$  the azygetic system*

associated to  $Z$  and let  $(\lambda_l)_{1 \leq l \leq 5}$  be the Rosenhain invariants in equation (2-11). Then for any lift  $\tilde{U} = \begin{pmatrix} \tilde{A} & \tilde{B} \\ \tilde{C} & \tilde{D} \end{pmatrix} \in \mathrm{Sp}_6(\mathbb{Z})$  of the matrix  $U$  with  $\delta_0 = \begin{pmatrix} \tilde{C}^T & \tilde{D} \\ \tilde{A}^T & \tilde{B} \end{pmatrix}_0$ , we have that

$$\lambda_l^{\sigma_c} = \exp(4\pi i(\eta_l + \eta_7)_1(\eta_6)_2) \cdot \zeta_4(\tilde{U}, \eta) \cdot \lambda'_l, \quad (4-3)$$

where

$$\begin{aligned} \zeta_4(\tilde{U}, \eta) = \exp \Big( & 2 \left( k(\tilde{U}, \tilde{U}^T(\eta_{\mathcal{U}_\eta \circ (\mathcal{V} \cup \{6, l\})} - \tfrac{1}{2}\delta_0)) + k(\tilde{U}, \tilde{U}^T(\eta_{\mathcal{U}_\eta \circ (\mathcal{W} \cup \{6, l\})} - \tfrac{1}{2}\delta_0)) \right. \\ & \left. - k(\tilde{U}, \tilde{U}^T(\eta_{\mathcal{U}_\eta \circ (\mathcal{V} \cup \{6, 7\})} - \tfrac{1}{2}\delta_0)) - k(\tilde{U}, \tilde{U}^T(\eta_{\mathcal{U}_\eta \circ (\mathcal{W} \cup \{6, 7\})} - \tfrac{1}{2}\delta_0)) \right) \Big), \end{aligned}$$

and

$$\lambda'_l = \left( \frac{\vartheta[\tilde{U}^t(\eta_{\mathcal{U}_\eta \circ (\mathcal{V} \cup \{6, l\})} - \tfrac{1}{2}\delta_0)] \cdot \vartheta[\tilde{U}^t(\eta_{\mathcal{U}_\eta \circ (\mathcal{W} \cup \{6, l\})} - \tfrac{1}{2}\delta_0)]}{\vartheta[\tilde{U}^t(\eta_{\mathcal{U}_\eta \circ (\mathcal{V} \cup \{6, 7\})} - \tfrac{1}{2}\delta_0)] \cdot \vartheta[\tilde{U}^t(\eta_{\mathcal{U}_\eta \circ (\mathcal{W} \cup \{6, 7\})} - \tfrac{1}{2}\delta_0)]} \right)^2 (Z').$$

*Proof.* Using Theorem 2.5 when  $\lambda_6 = 0$  and  $\lambda_7 = 1$ , the coefficients  $\lambda_l$  with  $l = 1, \dots, 5$  can be computed as

$$\lambda_l = \exp(4\pi i(\eta_l + \eta_7)_1(\eta_6)_2) \left( \frac{\vartheta[\mathcal{U}_\eta \circ (\mathcal{V} \cup \{6, l\})] \cdot \vartheta[\mathcal{U}_\eta \circ (\mathcal{W} \cup \{6, l\})]}{\vartheta[\mathcal{U}_\eta \circ (\mathcal{V} \cup \{6, 7\})] \cdot \vartheta[\mathcal{U}_\eta \circ (\mathcal{W} \cup \{6, 7\})]} \right)^2 (Z).$$

For the sake of simplicity let

$$c_1 = \eta_{\mathcal{U}_\eta \circ (\mathcal{V} \cup \{6, l\})}, \quad c_2 = \eta_{\mathcal{U}_\eta \circ (\mathcal{W} \cup \{6, l\})}, \quad c_3 = \eta_{\mathcal{U}_\eta \circ (\mathcal{V} \cup \{6, 7\})} \quad \text{and} \quad c_4 = \eta_{\mathcal{U}_\eta \circ (\mathcal{W} \cup \{6, 7\})}.$$

By using Theorem 4.4, we have that

$$\begin{aligned} \lambda_l^{\sigma_c} &= \left( \exp(4\pi i(\eta_l + \eta_7)_1(\eta_6)_2) \left( \frac{\vartheta[c_1] \cdot \vartheta[c_2]}{\vartheta[c_3] \cdot \vartheta[c_4]} \right)^2 (Z) \right)^{\sigma_c} \\ &= \exp(4\pi i(\eta_l + \eta_7)_1(\eta_6)_2) \left( \left( \frac{\vartheta[c_1] \cdot \vartheta[c_2]}{\vartheta[c_3] \cdot \vartheta[c_4]} \right)^2 \right)^U (Z'). \end{aligned} \quad (4-4)$$

We denote by  $c'_j = \tilde{U}^T(c_j - \tfrac{1}{2}\delta_0)$ . By applying the theta transformation formula, we get that

$$\vartheta[c_j]^U(Z') = \vartheta[\tilde{U} \cdot c'_j](\tilde{U} \cdot Z') = \zeta(\tilde{U}) \exp(k(\tilde{U}, c'_j)) \sqrt{\det(\tilde{C}Z' + \tilde{D})} \vartheta[c'_j](Z').$$

Hence equation (4-4) becomes

$$\lambda_l^{\sigma_c} = \exp(4\pi i(\eta_l + \eta_7)_1(\eta_6)_2) \exp(2(k(\tilde{U}, c'_1) + k(\tilde{U}, c'_2) - k(\tilde{U}, c'_3) - k(\tilde{U}, c'_4))) \left( \frac{\vartheta[c'_1] \cdot \vartheta[c'_2]}{\vartheta[c'_3] \cdot \vartheta[c'_4]} \right)^2 (Z')$$

where one can easily see that  $\zeta_4(\tilde{U}, \eta) = \exp(2(k(\tilde{U}, c'_1) + k(\tilde{U}, c'_2) - k(\tilde{U}, c'_3) - k(\tilde{U}, c'_4)))^2$  is a fourth root of unity.  $\square$

We will now give a geometric interpretation to our results. Recall that the Rosenhain coefficients are invariants for the space  $\mathcal{M}_3^{\mathrm{hyp}}[2]$ . The Galois conjugates of the Rosenhain invariants are the Rosenhain invariants of another point in this moduli space and the following result gives a method to compute the corresponding  $Z' \in \Gamma_6(2) \backslash \mathcal{H}_3$  and the associated azygetic system.

**Corollary 4.1.** *Assume that  $A(\Phi, \mathfrak{a}, \xi)$  is isomorphic to the Jacobian of a marked hyperelliptic curve  $X$  and let  $Z \in \Gamma_6(2) \backslash \mathcal{H}_3$  be the corresponding period matrix for  $A$  and  $\eta$  be an azygetic system associated to  $Z$ . Given  $[\mathfrak{c}] \in I_2(K^r)/H_2(K^r)$ , there exist  $Z'$ ,  $M$  and  $\tilde{U}$  as in [Notation 4.2](#) such that  $\eta' = \tilde{U}^T \eta$  is an azygetic system associated to the period matrix  $Z'$  of the marked hyperelliptic curve with Rosenhain invariants  $(\lambda_l^{\sigma_c})_{l=1, \dots, 5}$ .*

*Proof.* We first note that we can choose  $C$  and the period matrix  $Z'$  in [Notation 4.2](#) such that  $\tilde{U} \in \Gamma_6(2)$ . Indeed, if this is not the case, we define  $C' = B M^T \tilde{U}^T = B M'^T$  with  $M' = \tilde{U} M \in \mathrm{GSp}_6(\mathbb{Q})$ . Then  $C'$  is still a symplectic basis for  $\Phi(N_{\Phi^r}(\mathfrak{c})^{-1} \mathfrak{a})$  with respect to  $E_{\Phi, N_{K^r}/\mathbb{Q}}(\mathfrak{c}) \xi$ . Let  $\bar{M} \in \mathrm{Sp}_6(\mathbb{Z}/2\mathbb{Z})$  the reduction of  $M \pmod{2}$ . We get that  $\bar{M}' = \tilde{U} \bar{M} = U \bar{M} = I_6$ . Then  $(\bar{M}')^{-1} = I_6$  in  $\mathrm{Sp}_6(\mathbb{Z}/2\mathbb{Z})$ . Therefore, by letting  $C = C'$  and  $Z'$  the period matrix obtained from this new symplectic basis, we ensure that  $\tilde{U} \in \Gamma_6(2)$ .

Recall that the action described in [Definition 4.1](#) yields an isogeny between  $A$  and  $A^c$  which is given by

$$I_c : \mathbb{C}^3 / \Phi(\mathfrak{a}) \rightarrow \mathbb{C}^3 / \Phi(N_{\Phi^r}(\mathfrak{c})^{-1} \mathfrak{a}), \quad x \mapsto x.$$

For simplicity, we will work with  $I_c$  as an isogeny between the nonnormalized tori, i.e.,  $I_c : \mathbb{C}^3 / (B_1 \mathbb{Z}^3 + B_2 \mathbb{Z}^3) \rightarrow \mathbb{C}^3 / (C_1 \mathbb{Z}^3 + C_2 \mathbb{Z}^3)$ . We consider the image of the fixed points  $B_1(\eta_i)_1 + B_2(\eta_i)_2 \pmod{(B_1 \mathbb{Z}^3 + B_2 \mathbb{Z}^3)}$  via  $I_c$ . We compute  $\eta'_i$  such that

$$B_1(\eta_i)_1 + B_2(\eta_i)_2 = C_1(\eta'_i)_1 + C_2(\eta'_i)_2 \pmod{(C_1 \mathbb{Z}^3 + C_2 \mathbb{Z}^3)}. \quad (4-5)$$

By writing  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  and using that  $C = B M^T$ , the 2-torsion point in equation (4-5) writes as

$$\begin{aligned} (B_1 a' + B_2 b')(\eta'_i)_1 + (B_1 c' + B_2 d')(\eta'_i)_2 \pmod{(C_1 \mathbb{Z}^3 + C_2 \mathbb{Z}^3)} = \\ B_1(a'(\eta'_i)_1 + c'(\eta'_i)_2) + B_2(b'(\eta'_i)_1 + d'(\eta'_i)_2) \pmod{(C_1 \mathbb{Z}^3 + C_2 \mathbb{Z}^3)}. \end{aligned}$$

Hence  $\bar{\eta}_i = \bar{M}^T \bar{\eta}'_i$ . Then it is easy to check that  $\eta'_i = \tilde{U}^T \eta_i$  is in fact an azygetic system associated to  $Z'$ . The first three facts in [Definition 2.3](#) are trivial to check, the fourth equality follows by applying [\[15, Proposition 13.2\(b\)\]](#) for the isogeny  $I_c$ , which has degree prime to 2.

To show that  $\eta'$  is associated to  $Z'$ , we will use the Vanishing Criterion. We choose an even theta characteristic  $u \in \frac{1}{2}\mathbb{Z}^6$  such that  $\vartheta[u](Z) \neq 0$  and  $\vartheta[u](Z') \neq 0$  and apply once more Shimura's reciprocity law [\[23\]](#) on the quotients of the type  $(\frac{\vartheta[v](Z)}{\vartheta[u](Z)})^2$ , with  $v \in \frac{1}{2}\mathbb{Z}^6$  even. We deduce that the unique even theta constant vanishing  $Z'$  is  $\vartheta[\eta_{\mathcal{U}_{\eta'}}]$  (since  $\eta_{\mathcal{U}_{\eta'}} = \eta_{\mathcal{U}_{\eta}}$ ).

Finally, by applying [Theorem 4.5](#) we get that

$$\lambda_l^{\sigma_c} = \exp(4\pi i (\eta_l + \eta_7)_1 (\eta_6)_2) \left( \frac{\vartheta[c_1] \cdot \vartheta[c_2]}{\vartheta[c_3] \cdot \vartheta[c_4]} \right)^2 (M'.Z), \quad (4-6)$$

for  $l = 1, \dots, 5$ . Hence the right-hand side expressions in equation (4-6) are the Rosenhain invariants of a marked genus 3 hyperelliptic curve.  $\square$

**Computing the Shioda and Rosenhain class polynomials.** From a computational point view, if we simply aim at computing the Galois conjugates of the Rosenhain invariants and deriving class field equations, one can choose between the approach in [Theorem 4.5](#) or the one in [Corollary 4.1](#). One can pick any period matrix for  $A^c$  and use the formula in [Theorem 4.5](#), or construct the period matrix  $Z'$  and its associated azygetic system as explained in the proof of the [Corollary 4.1](#) and compute the resulting Rosenhain invariants via Takase's formula.

Algorithm 1 in the [Appendix](#) gives all the steps of our computation of a list of approximations for the Galois conjugates of the Rosenhain invariants, that we use to get the polynomials  $H_{K^r,i}^R$  in equation (1-1). The algorithm for computing  $H_{K^r,j}^S$  is similar and relies on the computation of the Siegel modular functions  $S_j$  in [Equation \(4-2\)](#). Note that in applications, for  $i, j \geq 2$ , it is easier to use the Hecke representation as introduced by Gaudry et al [\[10\]](#):

$$\hat{H}_{K^r,i}^R(t) = \sum_{\sigma} \lambda_i^{\sigma} \prod_{\sigma' \neq \sigma} (t - \lambda_1^{\sigma'}), \quad \hat{H}_{K^r,j}^S(t) = \sum_{\sigma} \text{Shi}_j^{\sigma} \prod_{\sigma' \neq \sigma} (t - \text{Shi}_1^{\sigma'}),$$

where  $\sigma, \sigma' \in \text{Gal}(CM_m(K^r)/K^r)$  with  $m = (2)$  for the product in  $H_{K^r,i}^R$  and  $m = (1)$  for the product and sum in  $H_{K^r,j}^S$ .

## 5. Benchmarks and results

We implemented the algorithms described here using SageMath [\[25\]](#) and Magma [\[4\]](#) by building on an existing implementation [\[2\]](#). The computation of primitive CM types for genus 3 in [\[2\]](#) is dependent on the group structure of  $\text{Gal}(L/\mathbb{Q})$ . Our CM type computation is independent of this group isomorphism, and works for all genera. In this general setting, we also implemented the construction of the reflex field of  $K$  and of the typenorm, as explained in [Section 3](#). Since SageMath [\[25\]](#) does not implement ray class groups, we used an interface to Magma [\[4\]](#) to compute the group  $\text{Cl}_m(K^r)$  and enumerate elements in  $T(\text{Cl}_m(K^r))$ .

**5A. Practical experiments.** For space reasons, we reproduce here partially an example and give the full computation in [\[7\]](#). Let  $K$  be the CM field defined by the polynomial  $x^6 + 43x^4 + 451x^2 + 729$ . Since the field contains  $i$ , all p.p.a.v. with CM by  $K$  are hyperelliptic. For one of its primitive CM types, our implementation yields the reflex field as the field of equation  $x^6 + 1012x^4 + 262048x^2 + 3968064$ . The subgroup  $T(\text{Cl}_m(K^r))$ , for  $m = (1), (2)$ , has three elements, which means that the polynomials  $H_{K^r,i}^R$  and  $H_{K^r,j}^S$  have degree 3.

For most computations on the Rosenhains 500 bits of precision were enough, whereas for the Shiodas we used 5000 bits of precision. Indeed, the Siegel modular forms appearing in the expressions of the Shiodas have much larger weight, which results into much more precision needed when computing with the Shiodas. To compute the Shiodas, we first computed the Rosenhain coefficients and got an approximation of the equation of the curve, and afterwards computed the Shiodas from this equation. All computations were performed on a single core of a Intel Core i7-4790 CPU 3.60GHz and took

polynomial	$t^3$	$t^2$	$t$	1
$H_{K^r,1}$	1	$\frac{1}{16}\alpha^2 - \frac{19}{8}\alpha + \frac{181}{16}$	$\frac{1}{48}\alpha^2 - \frac{49}{24}\alpha + \frac{875}{16}$	$\frac{1}{6}\alpha^2 - \frac{16}{3}\alpha + \frac{19}{2}$
$\hat{H}_{K^r,2}$	1	$-\frac{7}{144}\alpha^2 + \frac{149}{72}\alpha - \frac{3331}{144}$	$\frac{3}{16}\alpha^2 - \frac{65}{8}\alpha + \frac{1295}{16}$	$-\frac{11}{4}8\alpha^2 + \frac{239}{24}\alpha - \frac{1521}{16}$
$\hat{H}_{K^r,3}$	1	$-\frac{1}{16}\alpha^2 + \frac{19}{8}\alpha - \frac{277}{16}$	$\frac{13}{48}\alpha^2 - \frac{277}{24}\alpha + \frac{1791}{16}$	$-\frac{11}{24}\alpha^2 + \frac{227}{12}\alpha - \frac{1377}{8}$
$\hat{H}_{K^r,4}$	1	$\frac{7}{144}\alpha^2 - \frac{149}{72}\alpha + \frac{2467}{144}$	$-\frac{1}{144}\alpha^2 + \frac{11}{72}\alpha + \frac{59}{144}$	$\frac{7}{144}\alpha^2 - \frac{143}{72}\alpha + \frac{2551}{144}$
$\hat{H}_{K^r,5}$	1	-6	12	-8

**Table 1.** Coefficients of polynomials  $H_{K^r,i}^R$  for the field of equation  $x^6 + 43x^4 + 451x^2 + 729$ .

approximately 5 minutes at 500 bits of precision and less than 2 hours for 5000 bits. Most time is spent on the theta constants computation, which is performed using the naive implementation in [2]. To compute the coefficients of the class polynomials  $H_{K^r,i}^R$  and  $H_{K^r,i}^S$  as algebraic integers, we use the algebraic dependence testing algorithm [5], implemented in PARI/GP by the function *algdep*. This algorithm gives us a conjectured minimal polynomial for each coefficient of the class polynomials.

Since  $\text{Princ}(K, \Phi)$  is stable under complex conjugation, it can be shown by using similar arguments as in [21, Section III.2] that the coefficients of the Shioda class polynomials are in fact in the field  $K_0^r$ , the real multiplication subfield of  $K^r$ . We conjecture that a similar result holds for the Rosenhain class polynomials. For the chosen example,  $K$  and  $K^r$  are equal, so we take  $K_0^r$  to be the field given by the equation

$$x^3 - 43x^2 + 451x^2 - 729$$

and we denote by  $\alpha$  a generator for this field. Tables 1 and 2 give the coefficients of Rosenhain and Shioda class polynomials, respectively. Table 2 gives the Shioda class polynomials for the first Shioda invariant, and the full example is given in [7]. As expected, the polynomials for the Shiodas have larger coefficients, which is due again to the shape of the modular forms in their expression.

In order to heuristically check the correctness of these computations, we use a well known approach in the literature which consists in choosing a prime number  $p$  such that the abelian varieties with CM by  $\mathcal{O}_K$  have good reduction, compute the roots of class polynomials (mod  $p$ ) and check that the Jacobians of the curves obtained in this way have the right number of points; see for instance [1] for details.

coefficients	
$t^3$	1
$t^2$	$-\frac{1504998103898184428692895719062876991414375}{1106030051237012236054152188167439553303783103}\alpha^2 + \frac{57602191791353412833575829180223091649340630}{1106030051237012236054152188167439553303783103}\alpha - \frac{182610135152410817952949427128063513960980968701}{247750731477090740876130090149506459940047415072}$
$t$	$\frac{271537582048409045934259507591982005281201875}{867127560169817593066435315323272609790165952752}\alpha^2 - \frac{17155947238202790094437950965078959001849495535}{1300691340254726389599682973284908914685248929128}\alpha + \frac{189221715181445169536136728129202262948355511744769}{1165419440868234845081315944063278387557983040498688}$
1	$-\frac{49701833439492428446745226194781840141344176875}{24473808258232931746707634825328846138717643850472448}\alpha^2 + \frac{11444255640191890315301399097052785606070607022115}{12236904129116465873353817412664423069358821925236224}\alpha - \frac{191953650625925394207069308222518633622840220848155861}{16446399149532530133787530602620984605218256667517485056}$

**Table 2.** Coefficients of the polynomial  $H_{K^r,1}^S$  for the field of equation  $x^6 + 43x^4 + 451x^2 + 729$ .

## Appendix

---

**Algorithm 1:** Computing the Galois action using Shimura's reciprocity law

---

**Input:** A CM-pair  $(K, \Phi)$ , where  $K$  is a sextic CM field and  $\Phi$  is a CM type, and precision  $\text{prec}$ .

**Output:** Lists containing the Galois conjugates of the Rosenhain invariants of hyperelliptic curves with CM by  $(K, \Phi)$ , if such curves exist.

- 1 Let  $\mathcal{R}_l$ ,  $1 \leq l \leq 5$  be an empty list.
  - 2 Compute the Galois closure  $L$  of  $K/\mathbb{Q}$ .
  - 3 Compute the reflex CM-pair  $(K^r, \Phi^r)$  and the fixed embedding  $\iota_{K^r} : K^r \rightarrow L$ .
  - 4 Determine the ray class group  $\text{Cl}_m(K^r)$  for the modulus  $\mathfrak{m} = (2)$ .
  - 5 Compute and store elements of  $T(\text{Cl}_m(K^r))$  in a list  $\mathfrak{H}(K^r, \Phi^r)$ .
  - 6 Choose a p.p.a.v.  $A$  with CM by  $\mathcal{O}_K$  given by the triple  $(\Phi, \mathfrak{a}, \xi)$  and construct period matrix  $Z$  with [1, Algorithm 2].
  - 7 **if** exactly one of the theta constants  $\vartheta[c](Z)$ , with  $c$  even, is zero **then**
  - 8     Compute the Rosenhain invariants  $\lambda_l$  with precision  $\text{prec}$  using Takase's formula (2-10).
  - 9     **for all**  $(N_{\Phi^r}(\mathfrak{c}), N_{K^r/\mathbb{Q}}(\mathfrak{c})) \in \mathfrak{H}(K^r, \Phi^r)$  **do**
  - 10         Compute the p.p.a.v.  $A(\Phi, N_{\Phi^r}(\mathfrak{c})^{-1}\mathfrak{a}, N_{K^r/\mathbb{Q}}(\mathfrak{c})\xi)$  and the corresponding  $Z'$ .
  - 11         Compute  $\lambda_l^{\sigma_{\mathfrak{c}}}$  using the formula in Theorem 4.5 and add it to the list  $\mathcal{R}_l$ .
  - 12 **return**  $\mathcal{R}_l$ ,  $1 \leq l \leq 5$ .
- 

## Acknowledgements

The first author is grateful to Jeroen Sijsling for many helpful discussions. The second author thanks Christelle Vincent for preliminary discussions which led to this research. We thank Andreas Enge for his remarks on an early version of this manuscript and the ANTS conference reviewers for their numerous comments. The authors acknowledge financial support from the FACE foundation.

## References

- [1] J.S. Balakrishnan, S. Ionica, K. Lauter, and C. Vincent, *Constructing genus-3 hyperelliptic Jacobians with CM*, LMS J. Comput. Math. **19** (2016), no. suppl. A, 283–300.
- [2] J. S. Balakrishnan, S. Ionica, K. Lauter, and C. Vincent, *Genus 3*, <https://github.com/christellevincent/genus3>, 2016.
- [3] C. Birkenhake and H. Lange, *Complex abelian varieties*, second ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 302, Springer-Verlag, Berlin, 2004.
- [4] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR 1484478
- [5] H. Cohen, *Advanced topics in computational number theory*, Springer-Verlag, New York, 1991.
- [6] D. A. Cox, *Primes of the form  $x^2 + ny^2$* , vol. 2, Wiley, 2012.
- [7] B. Dina and S. Ionica, *Genus 3 hyperelliptic curves with CM via Shimura reciprocity*, preprint, 2020. arXiv 2003.06386



- [8] A. Enge and E. Thomé, *Computing class polynomials for abelian surfaces*, *Experimental Mathematics* **23** (2014), no. 2, 129–145.
- [9] E. Lorenzo García, *On different expressions for invariants of hyperelliptic curves of genus 3*, preprint, 2019. [arXiv 1907.05776](https://arxiv.org/abs/1907.05776)
- [10] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng, *The 2-adic CM method for genus 2 curves with application to cryptography*, *ASIACRYPT*, 2006, pp. 114–129.
- [11] J. Igusa, *On Siegel modular forms of genus two*, *American Journal of Mathematics* **84** (1962), no. 1, 175–200.
- [12] S. Ionica, P. Kiliçer, K. E. Lauter, E. Lorenzo García, A. Mânzăţeanu, M. Massierer, and C. Vincent, *Modular invariants for genus 3 hyperelliptic curves*, *Research in Number Theory* **5** (2018), 1–22.
- [13] J.-C. Lario and A. Somoza (appendix by C. Vincent), *An inverse Jacobian algorithm for Picard curves*, preprint, 2020. [arXiv 1611.02582](https://arxiv.org/abs/1611.02582)
- [14] J. S. Milne, *Complex Multiplication*, <http://www.jmilne.org/math/CourseNotes/cm.html>, 2006.
- [15] J. S. Milne, *Abelian varieties*, [www.jmilne.org/math/](http://www.jmilne.org/math/), 2008, pp. 166+vi.
- [16] David Mumford, *Tata lectures on theta. II*, *Modern Birkhäuser Classics*, Birkhäuser Boston, Inc., Boston, MA, 2007.
- [17] M. Newman, *Integral matrices*, *Pure and Applied Mathematics*, vol. 45, Academic Press, 1972.
- [18] C. Poor, *The hyperelliptic locus*, *Duke Math. J.* **76** (1994), no. 3, 809–884.
- [19] G. Shimura, *Abelian varieties with complex multiplication and modular functions*, *Princeton Mathematical Series*, vol. 46, Princeton University Press, Princeton, NJ, 1998. [MR 1492449](https://www.jstor.org/stable/1492449)
- [20] T. Shioda, *On the graded ring of invariants of binary octavics*, *Amer. J. Math.* **89** (1967), 1022–1046. [MR 0220738](https://www.jstor.org/stable/2372738)
- [21] M. Streng, *Complex multiplication of abelian surfaces*, Ph.D. thesis, Leiden University, 2010.
- [22] M. Streng, *Computing Igusa class polynomials*, *Math. Comp.* **83** (2014), no. 285, 275–309. [MR 3120590](https://www.jstor.org/stable/3120590)
- [23] M. Streng, *An explicit version of Shimura’s reciprocity law for Siegel modular functions*, preprint, 2018. [arXiv 1201.0020](https://arxiv.org/abs/1201.0020)
- [24] K. Takase, *A generalization of Rosenhain’s normal form for hyperelliptic curves with an application*, *Proc. Japan Acad. Ser. A Math. Sci.* **72** (1996), no. 7, 162–165.
- [25] The Sage developers, *SageMath, the Sage mathematics software system*, 2016, <http://www.sagemath.org>.
- [26] S. Tsuyumine, *On the Siegel modular field of degree 3*, *Compos. Math.* **63** (1987), no. 1, 83–98.
- [27] A. Weng, *A class of hyperelliptic CM-curves of genus three*, *J. Ramanujan Math. Soc.* **16** (2001), no. 4, 339–372. [MR 1877806](https://www.jstor.org/stable/1877806)

Received 28 Feb 2020. Revised 1 Aug 2020.

BOGDAN ADRIAN DINA: [bogdan.dina@uni-ulm.de](mailto:bogdan.dina@uni-ulm.de)

*Institute of Theoretical Computer Science, Ulm University, Ulm, Germany*

SORINA IONICA: [sorina.ionica@u-picardie.fr](mailto:sorina.ionica@u-picardie.fr)

*Laboratoire Modélisation, Information & Systèmes, Université de Picardie Jules Verne, Amiens, France*



# A canonical form for positive definite matrices

Mathieu Dutour Sikirić, Anna Haensch, John Voight, and Wessel P.J. van Woerden

We exhibit an explicit, deterministic algorithm for finding a canonical form for a positive definite matrix under unimodular integral transformations. We use characteristic sets of short vectors and partition-backtracking graph software. The algorithm runs in a number of arithmetic operations that is exponential in the dimension  $n$ , but it is practical and more efficient than canonical forms based on Minkowski reduction.

## 1. Introduction

**1.1. Motivation.** For  $n$  a positive integer, let  $\mathcal{S}^n$  denote the  $\mathbb{R}$ -vector space of symmetric real  $n \times n$ -matrices and  $\mathcal{S}_{>0}^n \subset \mathcal{S}^n$  denote the cone of positive definite symmetric  $n \times n$ -matrices. For  $A \in \mathcal{S}_{>0}^n$ , the map  $x \mapsto x^\top A x$  (where  $^\top$  denotes transpose) defines a positive definite quadratic form, with  $A$  its Gram matrix in the standard basis; for brevity, we refer to  $A \in \mathcal{S}_{>0}^n$  as a *form*. The group  $\mathrm{GL}_n(\mathbb{Z})$  of unimodular matrices acts on  $\mathcal{S}_{>0}^n$  by the action  $(U, A) \mapsto U^\top A U$ ; the stabilizer of a form  $A$  under this action is the finite group

$$\mathrm{Stab}(A) := \{U \in \mathrm{GL}_n(\mathbb{Z}) : U^\top A U = A\}. \quad (1.1.1)$$

Two forms  $A, B \in \mathcal{S}_{>0}^n$  are said to be (*arithmetically*) *equivalent* if there exists a unimodular matrix  $U \in \mathrm{GL}_n(\mathbb{Z})$  such that

$$A = U^\top B U. \quad (1.1.2)$$

In the geometry of numbers [39], forms arise naturally as Gram matrices of Euclidean lattices under a choice of basis; in this context, two forms are arithmetically equivalent if and only if they correspond to isometric lattices.

Plesken and Souvignier [35] exhibited algorithms to compute stabilizers and test for arithmetic equivalence among forms, and these have been used widely in practice [2; 8; 10; 21; 37]. In a more theoretical direction, Haviv and Regev [13] proposed algorithms based on the shortest vector problem and an isolation lemma for these purposes as well, with a time complexity of  $n^{O(n)}$ .

---

MSC2010: 11H55, 11H56, 15A21.

Keywords: canonical form, quadratic form, positive definite matrix, lattice isomorphism, graph isomorphism.

While these algorithms have been sufficient for many tasks, they suffer from an unfortunate deficiency. Suppose we have many forms  $A_1, \dots, A_m \in \mathcal{S}_{>0}^n$  and we wish to identify them up to equivalence. A naive application of an equivalence algorithm requires  $O(m^2)$  equivalence tests (in the worst case). The number of tests can be somewhat mitigated if useful invariants are available, which may or may not be the case.

Our approach in this article is to compute a *canonical form*  $\text{Can}_{\text{GL}_n(\mathbb{Z})}(A)$  for  $A \in \mathcal{S}_{>0}^n$ . This canonical form should satisfy the following two basic requirements:

- (i) For every  $A \in \mathcal{S}_{>0}^n$ ,  $\text{Can}_{\text{GL}_n(\mathbb{Z})}(A)$  is equivalent to  $A$ .
- (ii) For every  $A \in \mathcal{S}_{>0}^n$  and  $U \in \text{GL}_n(\mathbb{Z})$ ,  $\text{Can}_{\text{GL}_n(\mathbb{Z})}(U^T A U) = \text{Can}_{\text{GL}_n(\mathbb{Z})}(A)$ .

(The equivalence in (i) is unique up to  $\text{Stab}(A)$ .) Combining a canonical form with a hash table, the identification of equivalence classes in a list of  $m$  forms takes only  $m$  canonical form computations (and  $m$  hash table lookups) and so has the potential to be much faster.

**1.2. Minkowski reduction and characteristic sets.** The theory of Minkowski reduction provides one possible approach to obtain a canonical form. The Minkowski reduction domain [31] is a polyhedral domain  $P_n \subset \mathcal{S}_{>0}^n$  with the property that there exists an algorithm for *Minkowski reduction*, taking as input a form  $A$  and returning as output an equivalent form in  $P_n$ . For example, for  $n = 2$  we recover the familiar Gaussian reduction of binary quadratic forms. An implementation of Minkowski reduction is available [34]; however, this reduction is quite slow in practice, and it is unsuitable for forms of large dimension  $n$  (say,  $n \geq 12$ ).

For those forms whose Minkowski reduction lies in the *interior* of the domain  $P_n$ , the Minkowski reduction is unique [7, page 203], thereby providing a canonical form. Otherwise, when the reduction lies on the boundary of  $P_n$ , there are finitely many possible Minkowski reduced forms; one can then order the facets of the polyhedral domain  $P_n$  to choose a canonical form among them. This approach was carried out explicitly by Seeber (in 1831) for  $n = 3$ ; and, citing an unpublished manuscript, Donaldson claimed “Recently, Hans J. Zassenhaus has suggested that Minkowski reduction can be applied to the problem of row reduction of matrices of integers” [7, page 201]. An extension to  $n = 5, 6, 7$  is possible at least in principle, since  $P_n$  is known in these cases [39]. However, the problem of determining the facets of the Minkowski reduction domain is hard in itself and so this strategy seems unrealistic in higher dimensions. Other reduction theories [11; 24] suffer from the same problem of combinatorial explosion on the boundary.

In contrast, the approach taken by Plesken and Souvignier [35] for computing the stabilizer and checking for equivalence of a form  $A$  uses the following notion.

**Definition 1.2.1.** A *characteristic vector set* function is a map that assigns to every  $n \geq 1$  and form  $A \in \mathcal{S}_{>0}^n$  a finite subset of vectors  $\mathcal{V}(A) \subseteq \mathbb{Z}^n$  such that

- (i)  $\mathcal{V}(A)$  generates  $\mathbb{Z}^n$  (as a  $\mathbb{Z}$ -module); and
- (ii) for all  $U \in \text{GL}_n(\mathbb{Z})$ , we have  $U^{-1}\mathcal{V}(A) = \mathcal{V}(U^T A U)$ .

The basic idea is then given a form  $A$  to define an edge-weighted graph from a characteristic vector set  $\mathcal{V}(A)$ ; using this graph, equivalence and automorphisms of forms becomes a problem about isomorphism and automorphisms of graphs (see [Lemma 3.1.1](#)). The graph isomorphism problem has recently been proved to be solvable in quasipolynomial time by Babai (see the exposition by Helfgott [\[15\]](#)); however, the current approaches to computing characteristic vector sets (including ours) use algorithms to solve the shortest vector problem which is known to be NP-hard [\[29\]](#), so it is difficult to take advantage of this complexity result in the general case. Nevertheless, we may hope to leverage some practical advantage from this approach.

**1.3. Our approach.** In this article, we adopt the approach of characteristic vector sets, using very efficient programs [\[17; 28\]](#) that compute a canonical form of a graph using partition backtrack. A subfield  $F$  of  $\mathbb{R}$  is *computable* if it comes equipped with a way of encoding elements in bits along with deterministic, polynomial-time algorithms to test equality, to perform field operations, and to compute (binary) expansions to arbitrary precision (for generalities, see e.g., Stoltenberg-Hansen and Tucker [\[40\]](#)). For example, a number field with a designated real embedding is computable using standard algorithms.

**Theorem 1.3.1.** *There exists an explicit, deterministic algorithm that, on input a (positive definite) form  $A \in \mathcal{S}_{>0}^n$  with entries in a computable subfield  $F \subset \mathbb{R}$ , computes a canonical form for  $A$ . For fixed  $n \geq 1$ , this algorithm runs in a bounded number of arithmetic operations in  $F$  and in a polynomial number of bit operations when  $F = \mathbb{Q}$ .*

This theorem is proven by combining [Proposition 3.4.2](#) for the first statement and [Corollary 4.1.2](#) for the running time analysis. The running time in [Theorem 1.3.1](#) is exponential in  $n$ , as we rely on short vector computations; we are not aware of general complexity results, such as NP-hardness, for this problem. In light of the comments about Minkowski reduction in the previous section, the real content of [Theorem 1.3.1](#) is in the word *explicit*. We also find this algorithm performs fairly well in practice (see [Section 4.2](#)) — an implementation is available online [\[1\]](#).

**1.4. Contents.** In [Section 2](#) we present the construction of some characteristic vector set functions. In [Section 3](#) we present how to construct a canonical form from a given characteristic set function. In [Section 4](#) we consider the time complexity of our algorithm; we conclude in [Section 5](#) with extensions and applications.

## 2. Construction of characteristic vector sets

In this section we build two characteristic vector set functions that can be used for the computation of the stabilizer, canonical form, and equivalence of forms.

**2.1. Vector sets.** The sets of vectors that we use throughout this work are based on short or shortest vectors. Given a set of vectors  $\mathcal{V} \subseteq \mathbb{Z}^n$ , let  $\text{span}(\mathcal{V})$  be the (not necessarily full) lattice spanned over  $\mathbb{Z}$

by  $\mathcal{V}$ . For  $A \in \mathcal{S}^n$  and  $x \in \mathbb{R}^n$ , we write

$$A[x] := x^T A x \in \mathbb{R}. \quad (2.1.1)$$

For a form  $A \in \mathcal{S}_{>0}^n$  we define the *minimum*

$$\min(A) := \min_{x \in \mathbb{Z}^n \setminus \{0\}} A[x], \quad (2.1.2)$$

the set of *shortest* (or *minimal*) *vectors* and its span

$$\begin{aligned} \text{Min}(A) &:= \{v \in \mathbb{Z}^n : A[v] = \min(A)\}, \\ \mathcal{L}_{\min}(A) &:= \text{span}(\text{Min}(A)). \end{aligned} \quad (2.1.3)$$

The set of shortest vectors satisfies the desirable transformation property

$$\text{Min}(U^T A U) = U^{-1} \text{Min}(A) \quad (2.1.4)$$

for all  $U \in \text{GL}_n(\mathbb{Z})$ . If  $\text{Min}(A)$  is full-dimensional, then  $A$  is called *well-rounded*.

Two obstacles remain for using  $\text{Min}(A)$  as a characteristic vector set:

**PB1.** If  $n \geq 2$ , then  $\text{span}(\text{Min}(A))$  may not have rank  $n$ .

**PB2.** If  $n \geq 5$ , then  $\text{span}(\text{Min}(A))$  may have rank  $n$  but may not equal  $\mathbb{Z}^n$ .

Thus we have to consider other vector sets. For  $\lambda > 0$ , let

$$\text{Min}_A(\lambda) := \{v \in \mathbb{Z}^n \setminus \{0\} : A[v] \leq \lambda\}. \quad (2.1.5)$$

The vector set used for computing the stabilizer and automorphisms in the AUTO/ISOM programs of Plesken and Souvignier [35] is:

$$\mathcal{V}_{\text{PS}}(A) := \text{Min}_A(\text{maxdiag}(A)), \quad (2.1.6)$$

where  $\text{maxdiag}(A) := \max\{A_{ii} : 1 \leq i \leq n\}$  is the maximum of the diagonal elements of  $A$ . The vector set  $\mathcal{V}_{\text{PS}}(A)$  contains the standard basis as a subset and as a result is adequate for computing the stabilizer. Typically LLL-reduction [25] is used, leading to a decrease in  $\text{maxdiag}(A)$ , to prevent large sets. However, when computing equivalence we have a potential problem since two forms  $A$  and  $B$  can be equivalent but satisfy  $\text{maxdiag}(A) \neq \text{maxdiag}(B)$ . This is a limitation of ISOM, which for equivalence can be resolved by taking the bound  $\max\{\text{maxdiag}(A), \text{maxdiag}(B)\}$  (something we cannot do for our canonical form).

To prevent this problem we can use a more reliable vector set that consists of those vectors whose length is at most the minimal spanning length:

$$\begin{aligned} \mathcal{V}_{\text{ms}}(A) &:= \text{Min}_A(\lambda_{\min}), \text{ where} \\ \lambda_{\min} &:= \min\{\lambda > 0 : \text{span}(\text{Min}_A(\lambda)) = \mathbb{Z}^n\}. \end{aligned} \quad (2.1.7)$$

This vector set  $\mathcal{V}_{\text{ms}}(A)$  is a characteristic vector set. However,  $\mathcal{V}_{\text{ms}}(A)$  can still be very large, making it impractical to use.

**Example 2.1.8.** For example, the matrix  $A_\lambda = \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}$  for  $\lambda \geq 1$  gives

$$\mathcal{V}_{\text{ms}}(A_\lambda) = \{\pm e_2\} \cup \{\pm e_1, \pm 2e_1, \dots, \pm \lfloor \sqrt{\lambda} \rfloor e_1\}.$$

while  $\{\pm e_1, \pm e_2\}$  would be adequate. This problem is related to **PB1**.

**2.2. An inductive characteristic vector set, using closest vectors.** Building on the observations made in the previous section, we now present a construction that deals with **PB1** and allows us to build a suitable characteristic vector set.

For a set of vectors  $\mathcal{V} \subseteq \mathbb{Z}^n$ , the saturated sublattice (of  $\mathbb{Z}^n$ ) spanned by  $\mathcal{V}$  is

$$\text{satspan}(\mathcal{V}) := \mathbb{Q}\mathcal{V} \cap \mathbb{Z}^n. \quad (2.2.1)$$

Beyond shortest vectors, we use the *closest vector distance*: for  $v \in \mathbb{Q}^n$ , we define

$$\text{cvd}(A, v) := \min_{x \in \mathbb{Z}^n} A[x - v] \quad (2.2.2)$$

as the minimum distance from  $\mathbb{Z}^n$  to the vector  $v$  and

$$\text{CV}(A, v) := \{x \in \mathbb{Z}^n : A[x - v] = \text{cvd}(A, v)\} \quad (2.2.3)$$

the set of closest vectors achieving this minimum.

Characteristic and closest vector sets behave well under restriction to a sublattice. The following lemma describes this explicitly, in terms of bases.

**Lemma 2.2.4.** *Let  $\mathcal{V}$  be a characteristic vector set function,  $A \in S_{>0}^n$  a form, and  $L \subset \mathbb{R}^n$  a lattice of rank  $r$ . Let  $B \in M_{n,r}(\mathbb{R})$  be such that the columns are a  $\mathbb{Z}$ -basis of  $L$ ; let  $c$  be in the real span of  $L$  and let  $c_B := B^{-1}c \in \mathbb{R}^r$  be the unique vector such that  $Bc_B = c$ . Then the sets*

$$B\mathcal{V}(B^T A B) \quad \text{and} \quad B\text{CV}(B^T A B, c_B)$$

*are independent of  $B$  (depending only on  $L, c$ ).*

*Proof.* The form  $A|_B := B^T A B \in S_{>0}^r$  is the restriction of  $A$  to  $L$  in the basis  $B$ , so  $B\mathcal{V}(A|_B)$  is the characteristic vector set of this restricted form, as elements of  $L \subset \mathbb{R}^n$ . Similarly,  $B\text{CV}(A|_B, c_B)$  is the set of vectors in  $L \subset \mathbb{R}^n$ , which are closest to  $c$ . Both sets only depend on  $L$  and are independent of the chosen basis.  $\square$

Suppose that  $A$  is well-rounded. Let  $v_1, \dots, v_n$  be a  $\mathbb{Z}$ -basis of the full rank lattice  $\mathcal{L}_{\min}(A)$  spanned by  $\text{Min}(A)$  and let  $B \in M_{n \times n}(\mathbb{Z})$  be the matrix with columns  $v_1, \dots, v_n$ . We then define

$$\mathcal{V}_{\text{wr-cv}}(A) := \text{Min}(A) \cup \bigcup_{c \in \mathbb{Z}^n / \mathcal{L}_{\min}(A)} (c - B\text{CV}(B^T A B, B^{-1}c)). \quad (2.2.5)$$

(It is possible to reduce the size of this set, e.g., by removing 0 or filtering by length.) The set  $\mathcal{V}_{\text{wr-cv}}(A)$  consists of the union of the shortest vectors together with the set of points in each coset closest to the origin. By [Lemma 2.2.4](#), the set  $\mathcal{V}_{\text{wr-cv}}(A)$  is well-defined, independent of the choice of basis.

Furthermore it satisfies the necessary transformation property and spans  $\mathbb{Z}^n$  (as a  $\mathbb{Z}$ -module) because it contains at least one point from each coset in  $\mathbb{Z}^n / \mathcal{L}_{\min}(A)$ .

For a general form  $A$ , in geometrical terms we follow the filtration defined from the minimum [4]. We define a set of vectors  $\mathcal{V}_{\text{cv}}(A)$  inductively (described in an algorithmic fashion), as follows:

- (1) Compute the set  $\text{Min}(A)$  of vectors of minimal length and compute the saturated sublattice  $L_1 := \text{satspan}(\text{Min}(A))$  spanned by these vectors.
- (2) Compute a  $\mathbb{Z}$ -basis  $v_1, \dots, v_r$  of  $L_1$ , where  $r$  is its rank. Let  $B_1 \in M_{n,r}(\mathbb{R})$  be the matrix with columns  $v_1, \dots, v_r$ , and let  $A_1 := B_1^T A B_1 \in S'_{>0}$ . Note that  $A_1$  is well-rounded by construction.
- (3) Let  $\text{proj}: \mathbb{Z}^n \rightarrow \mathbb{R}^n$  be the orthogonal projection on  $L_1^\perp$  with respect to the scalar product defined by  $A$ .
- (4) Compute a basis  $w_1, \dots, w_{n-r}$  of  $L_2 := \text{proj}(\mathbb{Z}^n)$  and let  $B_2 \in M_{n,(n-r)}(\mathbb{R})$  the matrix with columns  $w_1, \dots, w_{n-r}$ . Let  $A_2 := B_2^T A B_2$ .
- (5) If  $r = n$ , let  $\mathcal{V}_{\text{cv}}(A_2) := \emptyset$ ; otherwise, compute  $\mathcal{V}_{\text{cv}}(A_2)$  recursively and let

$$\mathcal{V}_{\text{cv}}(A) := B_1 \mathcal{V}_{\text{wr-cv}}(A_1) \cup \bigcup_{v \in B_2 \mathcal{V}_{\text{cv}}(A_2)} \text{CV}(A, v). \quad (2.2.6)$$

**Theorem 2.2.7.** *The following statements hold:*

- (a) *The set  $\mathcal{V}_{\text{cv}}(A)$  is well-defined (independent of the choices of bases).*
- (b) *The association  $A \mapsto \mathcal{V}_{\text{cv}}(A)$  is a characteristic vector set function.*
- (c) *We have  $\#\mathcal{V}_{\text{cv}}(A) = n^{O(n)}$ .*
- (d) *There is an explicit, deterministic algorithm that on input  $A$  computes the set  $\mathcal{V}_{\text{cv}}(A)$  in  $n^{O(n)}$  arithmetic operations over  $F$ . For  $F = \mathbb{Q}$  it has bit complexity  $n^{O(n)} s^{O(1)}$  with  $s$  the input size of  $A$ .*

*Proof.* We prove (a) by induction in the dimension  $n$  that  $\mathcal{V}_{\text{cv}}$  is a characteristic vector set. The base case  $n = 0$  is trivial. For  $n > 0$ , note that  $A_1$  is well rounded and  $A_2$  has dimension at most  $n - 1$  and thus  $B_1 \mathcal{V}_{\text{wr-cv}}(A_1)$  and  $B_2 \mathcal{V}_{\text{cv}}(A_2)$  are independent of the choice of basis by induction and Lemma 2.2.4. The lattice  $L_2$  is uniquely defined by the projection.

For (b), by part (a), we may choose convenient bases. Running the algorithm for  $A$  and  $A' = U^T A U$  we can assume that  $v'_i = U^{-1} v_i$  and  $w'_i = U^{-1} w_i$  by using the transformation property of  $\text{Min}(A)$ . Then  $A'_i = A_i$  and  $B'_i = U^{-1} B_i$  for  $i = 1, 2$ . We conclude by noting that  $\text{CV}$  also has the compatible transformation property

$$\text{CV}(U^T A U, U^{-1} v) = U^{-1} \text{CV}(A, v). \quad (2.2.8)$$

For (c), by Keller, Martinet and Schürmann [20, Proposition 2.1] for a well-rounded lattice the index of the sublattice determined by the shortest vectors is at most  $\lfloor \gamma_n^{n/2} \rfloor$  with  $\gamma_n$  the Hermite constant satisfying  $\gamma_n^{n/2} \leq (2/\pi)^{n/2} \cdot \Gamma(2 + n/2) = n^{O(n)}$ . The bound on  $\mathcal{V}_{\text{cv}}$  follows by combining this with exponential upper bounds on the kissing number [18] and the upper bound  $2^n$  on  $\#\text{CV}(A, v)$  [6, Proposition 13.2.8].

The running time estimate (d) for arithmetic operations follows by combining single exponential upper estimates for algorithms to solve the CVP and SVP (see e.g., Micciancio and Voulgaris [30]). We conclude with the bit complexity analysis for  $F = \mathbb{Q}$ . The bit complexity of SVP and CVP algorithms is indeed polynomial time in the input size [16; 36]. (We lack a reference for more general fields, and although we do not see major obstacles doing such an analysis, it would be out of the scope of this work). For the computed projection, the Gram–Schmidt orthogonalization process also has a polynomial bit complexity in the input size (in bounded dimension, by induction). The remaining steps in computing  $\mathcal{V}_{\text{cv}}(A)$ , including computing a basis out of a spanning set, computing a basis for the saturated sublattice, and computing representatives of the cosets  $\mathbb{Z}^n / \mathcal{L}_{\min}(A)$ , are standard applications of the computation of a Hermite normal form (HNF) — see also Section 3.4. A careful HNF computation can be achieved in polynomial time in the input size [19]. In particular, the obtained basis vectors and coset representatives also have a bit size that is polynomially bounded in the input size. Thus for  $F = \mathbb{Q}$  all arithmetic operations while computing  $\mathcal{V}_{\text{cv}}(A)$  have a bit complexity polynomial in  $s$ . We note for completeness that efficient versions of SVP, CVP, and HNF algorithms depend heavily on the famous LLL-algorithm.  $\square$

Although the cost of computing many closest vector problems may make it quite expensive to compute  $\mathcal{V}_{\text{cv}}(A)$  in the worst case, we find in many cases that it gives a substantial improvement in comparison to other characteristic vector sets.

**Example 2.2.9.** Returning to Example 2.1.8, we find that  $\mathcal{V}_{\text{cv}}(A_\lambda) = \{\pm e_1, \pm e_2\}$ .

The construction of  $\mathcal{V}_{\text{cv}}$  addresses **PB1**, but **PB2** remains — even for well-rounded lattices  $\#(\mathbb{Z}^n / \mathcal{L}_{\min}(A))$  can possibly be very large.

**Example 2.2.10.** The self-dual Niemeier lattice  $N_{23}$  [5, Chapter 18], whose root diagram is  $24A_1$  is well-rounded: it has minimum 2 with 48 shortest vectors, and  $\#\mathcal{V}_{\text{ms}}(N_{23}) = 194352$ . Since the index of the lattice spanned by the shortest vectors in  $N_{23}$  is  $2^{24}$ , the size of  $\mathcal{V}_{\text{cv}}(N_{23})$  is at least  $48 + 2^{24}$ .

**Remark 2.2.11.** It may be possible to deal with some cases (but still not Example 2.2.10) by working with characteristic vector sets on forms attached in a canonical way to  $A$ : for example, one could work with the *dual* form attached to  $A$ , for sometimes the dual has few minimal vectors (even if  $A$  has many).

**2.3. A characteristic vector set, using Voronoi-relevant vectors.** A well-known geometric shape associated to lattices is the *Voronoi cell*. The Voronoi cell is the set of all points closer to 0 with respect to  $A$  than to any other integer point. For a form  $A$ , the (open) Voronoi cell is the intersection of half-spaces

$$\text{Vor}(A) := \bigcap_{x \in \mathbb{Z}^n \setminus \{0\}} H_{A,x}, \quad (2.3.1)$$

with  $H_{A,x} := \{y \in \mathbb{R}^n : A[y] < A[y - x]\}$ . However, almost all vectors in this intersection are superfluous, and we only consider the set of *Voronoi-relevant vectors*  $\mathcal{V}_{\text{vor}}(A)$ , i.e., the (unique) minimal set of vectors

such that

$$\text{Vor}(A) = \bigcap_{x \in \mathcal{V}_{\text{vor}}(A)} H_{A,x}. \quad (2.3.2)$$

**Lemma 2.3.3.** *The following statements hold:*

- (a) *The association  $A \mapsto \mathcal{V}_{\text{vor}}(A)$  is a characteristic vector set function.*
- (b) *We have  $\#\mathcal{V}_{\text{vor}}(A) \leq 2 \cdot (2^n - 1)$ .*
- (c) *There is an explicit, deterministic algorithm that on input  $A$  computes the set  $\mathcal{V}_{\text{vor}}(A)$  in  $2^{2n+o(n)}$  arithmetic operations over  $F$ . For  $F = \mathbb{Q}$  it has bit complexity  $2^{2n+o(n)} s^{O(1)}$  with  $s$  the input size of  $A$ .*

*Proof.* Property (ii) of a characteristic vector set for  $\mathcal{V}_{\text{vor}}$  follows from the geometric definition, fully independent of the basis. For property (i), note that for any nonzero  $x \in \mathbb{Z}^n$ , we have  $x \notin \text{Vor}(A)$ , and thus there is a vector  $v \in \mathcal{V}_{\text{vor}}(A)$  such that  $x - v$  lies strictly closer to 0 with respect to  $A$ . Repeating this (a finite amount of time by a packing argument) we eventually end up at 0 and thus  $x$  is the sum of Voronoi-relevant vectors. The remaining statements follow from Micciancio and Voulgaris [30].  $\square$

Although this characteristic vector set has great theoretical bounds, we refrain from using it in practice: most lattices actually attain the  $2 \cdot (2^n - 1)$  Voronoi bound, whereas constructions based on short and close vectors often beat the theoretical worst-case bounds and give much smaller vector sets in practice.

### 3. Construction of a canonical form

Suppose now that we have chosen a characteristic vector set function  $\mathcal{V}$ , as in Section 2.2 or 2.3. From this, we will construct a canonical form, depending on  $\mathcal{V}$ .

**3.1. Graph construction.** Given a form  $A$ , let  $\mathcal{V}(A) = \{v_1, \dots, v_p\}$ . We define  $G_A$  to be the edge- and vertex-weighted complete (undirected) graph on  $p$  vertices  $1, \dots, p$  such that vertex  $i$  has weight  $w_{i,i} = A[v_i]$  and the edge between  $i$  and  $j$  has weight  $w_{i,j} = v_i^\top A v_j = w_{j,i}$ . In other words,  $G_A$  is the weighted complete graph whose adjacency matrix is  $B^\top A B$ , where  $B \in M_{n,p}(\mathbb{R})$  is the matrix whose columns are  $v_i$ . (The graph  $G_A$  depends on  $\mathcal{V}$ , but we do not include it in the notation as we consider  $\mathcal{V}$  fixed in this section.)

**Lemma 3.1.1.** *For a form  $A \in S_{>0}^n$  and the graph  $G_A$  constructed from a characteristic vector set  $\mathcal{V}(A)$  we have a group isomorphism*

$$\text{Stab}(A) \simeq \text{Stab}(G_A) := \{\sigma \in S_p : w_{i,j} = w_{\sigma(i),\sigma(j)} \text{ for all } 1 \leq i, j \leq p\}. \quad (3.1.2)$$

*Proof.* We first define the map  $\text{Stab}(A) \rightarrow \text{Stab}(G_A)$ . Let  $U \in \text{Stab}(A)$ . Then by property (ii) of a characteristic vector set, we have  $U\mathcal{V}(A) = \mathcal{V}(U^{-\top} A U^{-1}) = \mathcal{V}(A)$ ; therefore,  $U$  permutes the set  $\mathcal{V}(A)$ , giving a permutation  $\sigma_U \in S_p$  characterized by  $\sigma_U(i) = j$  if and only if  $U v_i = v_j$ . Accordingly, we have

$$w_{i,j} = v_i^\top A v_j = v_i^\top U^\top A U v_j = v_{\sigma_U(i)}^\top A v_{\sigma_U(j)} \quad (3.1.3)$$



so moreover  $\sigma_U \in \text{Stab}(G_A)$ . It is then straightforward to see that this map defines a group homomorphism. To show this map is an isomorphism, we use property (i) that  $\mathcal{V}(A)$  spans  $\mathbb{Z}^n$ . Indeed, the map is injective because if  $\sigma_U$  is the identity, then  $Uv_i = v_i$  for all  $i$  so  $U$  is the identity. Similarly, it is surjective: any  $\sigma \in \text{Stab}(G_A)$  fixes pairwise inner products with respect to  $A$ , so we obtain a unique  $\mathbb{Q}$ -stabilizer  $U \in \text{GL}_n(\mathbb{Q})$  such that  $U^T A U = A$ ; however, because  $\mathcal{V}(A)$  spans  $\mathbb{Z}^n$ , we obtain  $U\mathbb{Z}^n = \mathbb{Z}^n$  so  $U \in \text{Stab}(A)$ .  $\square$

**3.2. Graph transformations.** The software *nauty* [28] and *bliss* [17] allow to test equivalence and find the automorphism group and a canonical vertex ordering of vertex weighted graphs. Thus, we need graph transformations that allow to translate our vertex and edge weighted complete graphs into vertex weighted graphs (see also the *nauty* manual [28]).

Let  $G$  be a complete (undirected) graph on  $p$  vertices with vertex weights  $w_{i,i}$  and edge weights  $w_{i,j}$ . We construct a complete (undirected) graph  $T_1(G)$  on  $p+2$  vertices which is only edge weighted, as follows. Let  $a := 1 + \max_{i,j} w_{i,j}$  and  $b := a + 1$  be two distinct weights that do not occur as  $w_{i,j}$ . We define the new edge weight  $w'_{i,j}$  for  $i < j$  to be

$$w'_{i,j} := \begin{cases} w_{i,j} & \text{if } i < j \leq p, \\ w_{i,i} & \text{if } i \leq p \text{ and } j = p+1, \\ a & \text{if } i \leq p \text{ and } j = p+2, \\ b & \text{if } i = p+1 \text{ and } j = p+2. \end{cases} \quad (3.2.1)$$

We have a natural bijection  $\text{Isom}(G, G') \xrightarrow{\sim} \text{Isom}(T_1(G), T_1(G'))$  of morphisms in the categories of edge-and-vertex-weighted and edge-weighted graphs, hence taking  $G' = G$ , we have  $\text{Aut}(G) \simeq \text{Aut}(T_1(G))$ .

The next transformation takes a complete graph  $G$  with edge weights  $w_{i,j}$  and returns a vertex weighted graph  $T_2(G)$ . Let  $S$  be the list of possible edge weights, ordered from the smallest to the largest, and let  $w$  be the smallest integer such that  $\#S \leq 2^w$ . For an edge weight  $s \in S$ , denote  $l_k(s)$  the  $k$ -th value in the binary expansion of the position of  $s$  in  $S$ . If  $G$  has  $p$  vertices then  $T_2(G)$  will have  $pw$  vertices of the form  $(i, k)$  with  $1 \leq i \leq p$  and  $0 \leq k \leq w-1$ . The weight of the vertex  $(i, k)$  is  $k$ . Two vertices  $(i, k)$  and  $(i', k')$  are adjacent in the following cases:

- (1)  $i = i'$ .
- (2)  $k = k'$  and  $l_k(w_{i,i'}) = 1$ .

Condition (i) implies that vertices of  $G$  correspond to cliques in  $T_2(G)$ . Condition (ii) means that each digit  $k$  corresponds to a subgraph of  $T_2(G)$ . We have again have a natural bijection  $\text{Isom}(G, G') \xrightarrow{\sim} \text{Isom}(T_2(G), T_2(G'))$ .

Combining this we can lift an isomorphism between  $T_2(T_1(G_A))$  and  $T_2(T_1(G_B))$  to an isomorphism between  $G_A$  and  $G_B$  and thus to an isomorphism between  $A$  and  $B$  by solving an overdetermined linear system. Similarly, we can compute the group  $\text{Aut}(A)$  from  $\text{Aut}(T_2(T_1(G_A)))$ .

**3.3. Canonical orderings of characteristic vector sets.** The canonical vertex ordering functionality of `nauty` and `bliss` gives an ordering of the vertices of vertex weighted graphs. It is canonical in the sense that two isomorphic graphs will after this reordering be identical. We do not know a priori what this ordering is as it depends on the software, its version and the chosen running options. We still call it *canonical*, following standard terminology.

We need to lift the ordering of the vertex set of  $T_2(T_1(G_A))$  into an ordering of the vertex set of  $G_A$  and so the characteristic vector set. Every vertex  $i$  of  $G$  corresponds to a set  $S_i$  of  $w$  vertices in  $T_2(G)$  with  $S_i \cap S_j = \emptyset$  for  $i \neq j$ . For two vertices  $i, j$  of  $G$  we set  $i < j$  if and only if  $\min S_i < \min S_j$  in the canonical vertex ordering of  $T_2(G)$ . Similarly every vertex  $i$  of  $G$  maps to one vertex  $\phi(i)$  of  $T_1(G)$  with  $\phi(i) \neq \phi(j)$  if  $i \neq j$ . Thus we set  $i < j$  if and only if  $\phi(i) < \phi(j)$  in the canonical ordering.

Combining the above we obtain a canonical ordering of the vertex set of  $G_A$  and thus of the characteristic vector set of the matrix  $A$ .

**3.4. Canonical form.** We have a canonical ordering of the characteristic vector set  $\mathcal{V}(A)$ , which we write as  $v_1, \dots, v_p$ . This ordering is only canonical up to  $\text{Stab}(A)$ : for another canonical ordering, there is an element  $S \in \text{Stab}(A)$  such that  $w_i = Sv_i$  for  $i = 1, \dots, p$ , and conversely. We will now derive a canonical form from the vectors  $v_i$ .

The Hermite normal form (HNF) of a matrix  $Q \in M_{m,n}(\mathbb{Z})$  is the unique matrix  $H = (h_{ij})_{i,j} \in M_{m,n}(\mathbb{Z})$  for which there exists  $U \in \text{GL}_m(\mathbb{Z})$  such that  $Q = UH$  and moreover:

- (i) The first  $r$  rows of  $H$  are nonzero and the remaining rows are zero.
- (ii) For  $1 \leq i \leq r$ , if  $h_{i,j_i}$  is the first nonzero entry in row  $i$ , then  $j_1 < \dots < j_r$ .
- (iii)  $h_{i,j_i} > 0$  for  $1 \leq i \leq r$ .
- (iv) If  $1 \leq k < i \leq r$ , then  $0 \leq h_{k,j_i} < h_{i,j_i}$ .

In the cases that interest us, the matrix  $Q_A$  with columns  $v_1, \dots, v_p$  defined by the characteristic vector set  $\mathcal{V}(A)$  is of full rank and so the matrix  $U$ , obtained from the Hermite normal form  $Q_A = UH$ , is uniquely defined as well. Note that any other ordering  $sv_1, \dots, sv_p$  would lead to the matrix  $SU$  for some  $S \in \text{Stab}(A)$ . We denote the matrix  $U$  by  $U_{\mathcal{V}(A)}$  and note that its coset representative in  $\text{Stab}(A) \backslash \text{GL}_n(\mathbb{Z})$  is well-defined (determined by  $\mathcal{V}(A)$ ).

We now define

$$\text{Can}_{\text{GL}_n(\mathbb{Z})}(A) := U_{\mathcal{V}(A)}^T A U_{\mathcal{V}(A)} \in \mathcal{S}_{>0}^n. \quad (3.4.1)$$

Then  $\text{Can}_{\text{GL}_n(\mathbb{Z})}(A)$  depends only on  $\mathcal{V}(A)$  and  $A$ . [Proposition 3.4.2](#) proves the first statement of our main result, [Theorem 1.3.1](#) (for any characteristic vector set function  $\mathcal{V}$ ).

**Proposition 3.4.2.** *The matrix  $\text{Can}_{\text{GL}_n(\mathbb{Z})}(A)$  is a canonical form for  $A$ .*

*Proof.* Property (i) is clear by definition. For (ii), given  $P \in \text{GL}_n(\mathbb{Z})$ , we have

$$U_{\mathcal{V}(P^T A P)} \equiv U_{P^{-1} \mathcal{V}(A)} \equiv P^{-1} U_{\mathcal{V}(A)} \in \text{Stab}(P^T A P) \backslash \text{GL}_n(\mathbb{Z}). \quad (3.4.3)$$

Thus  $\text{Can}_{\text{GL}_n(\mathbb{Z})}(P^\top AP) = \text{Can}_{\text{GL}_n(\mathbb{Z})}(A)$ , as desired.  $\square$

**Remark 3.4.4.** An alternative to computing the canonical form would be to keep the canonicalized version of the graph  $G_A$ . However, this graph can be quite large, and the positive definite form allows a more compact representation even taking into account coefficient explosion that might occur with the Hermite normal form.

## 4. Analysis

**4.1. Theoretical time complexity.** We now analyze the algorithmic complexity of computing a canonical form using the characteristic vector set in [Section 2.3](#).

**Theorem 4.1.1.** *Given as input a positive definite symmetric matrix  $A \in S_{>0}^n$  with entries in a computable subfield  $F \subset \mathbb{R}$ , and a characteristic vector set  $\mathcal{V}(A)$ , we can compute a canonical form for  $A$  in time  $\exp(O(\log(N)^c) + s^{O(1)})$  where  $N := \#\mathcal{V}(A)$ ,  $s$  is the input size of  $(A, \mathcal{V}(A))$ , and  $c > 1$  is a constant.*

*Proof.* Given the characteristic vector set  $\mathcal{V}(A)$  the corresponding graph can be computed in time polynomial in the input size of  $A$  and  $\mathcal{V}(A)$  as this part is mostly dominated by the computation of  $v^\top A w$  for  $v, w \in \mathcal{V}(A)$ . Computing a Hermite normal form can be done in time polynomial in the matrix input size which is the same as  $\mathcal{V}(A)$  [\[19\]](#). Because the initial graph has at most  $O(N^2)$  distinct weights the final constructed vertex-weighted graph  $T_2(T_1(G_A))$  is of polynomial size in  $N$ . We can conclude if we have a quasipolynomial algorithm to find a canonical form of a graph. For this we refer to a recent report by Babai [\[14\]](#).  $\square$

**Corollary 4.1.2.** *For all  $n \geq 1$  and  $A \in S_{>0}^n$  with entries in a computable subfield  $F \subset \mathbb{R}$ , we can compute a canonical form in at most  $2^{O(n^c)}$  arithmetic operations in  $F$  for some constant  $c > 1$ . If  $F = \mathbb{Q}$ , the bit complexity is at most  $2^{O(n^c)} + s^{O(1)}2^{O(n)}$  with  $s$  the input size of  $A$ .*

*Proof.* By [Lemma 2.3.3](#) we have an characteristic vector set function  $\mathcal{V}_{\text{vor}}$  such that  $\mathcal{V}_{\text{vor}}(A)$  has cardinality at most  $2(2^n - 1)$  and can be computed in at most  $2^{O(n)}$  arithmetic operations. For the rational case, the bit complexity (and output size) is at most  $s^{O(1)}2^{O(n)}$ , with  $s$  the input size of  $A$ . We conclude by [Theorem 4.1.1](#).  $\square$

**4.2. Practical time complexity.** We give a short experimental review of the practical time complexity of our implementation [\[1\]](#). We selected a diverse set of test cases to benchmark our implementation: random forms, more than 500 000 perfect forms [\[8\]](#) and more than 100 special forms from the *catalog of lattices* [\[32\]](#). For the random  $n$ -dimensional forms a basis matrix  $B$  is constructed with entries uniform from  $\{-n, \dots, n\}$ , which, if full rank, is turned into a form  $A = B^\top B$ . The set of perfect forms contains all 10 963 perfect forms of dimension 2 up to 8 and in addition 524 288 perfect forms of dimension 9. The set of special forms consists of a diverse subset from the catalog up to dimension 16, including all laminated lattices. Up to dimension 20 we used 32-bit integers and above that (much slower) arbitrary precision integers to prevent overflow. The implementation currently supports the characteristic vector

Type	Samples	$n$	Time (s)			$\#\mathcal{V}_{\text{ms}}$		
			min	avg	max	min	avg	max
Perfect	10 963	2–8	0.00041	0.0032	0.086	6	73.74	240
	524 288	9	0.0039	0.00594	0.11	90	94.04	272
Random	100	10	0.0015	0.08	2.03	20	100.36	988
	100	20	0.016	0.17	4.18	40	114.34	812
	100	30	2.43	23.41	511.42	60	93.46	310
	100	40	5.18	24.91	251.51	82	107.7	240
Catalog	107	2–16	0.00018	2.12	36.71	4	630.47	4320

**Table 1.** Timings of our implementation [1].

set function  $\mathcal{V}_{\text{ms}}$  and has not been highly optimized. The main bottleneck seemed to be constructing the characteristic vector sets and the computation of all pairwise inner products (in arbitrary precision) for the graph. Perhaps surprisingly, determining the canonical graph itself took negligible time in most cases. In low dimensions where we can still use basic integer types, computing a canonical form takes a few milliseconds up to a few seconds. For random lattices we can expect relatively small characteristic sets even in large dimensions, therefore enumerating the minimal vectors quickly becomes the bottleneck in high dimensions. For special forms in higher dimensions such as the Leech lattice with 196 560 minimal vectors one can expect that the main bottleneck is related to the huge graph. Both storing the graph and computing a canonical representative might barely be in the feasible regime.

## 5. Extensions and applications

We conclude with an extension and a description of some applications.

**5.1. Extension to symplectic groups.** Let  $J_n := \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$  represent the standard alternating pairing and

$$\text{Sp}_{2n}(\mathbb{Z}) := \{Q \in \text{GL}_{2n}(\mathbb{Z}) : Q^T J_n Q = J_n\}. \quad (5.1.1)$$

The group  $\text{Sp}_{2n}(\mathbb{Z})$  acts on  $\mathcal{S}_{>0}^{2n}$  and we seek a canonical form for this action [27].

**Theorem 5.1.2.** *Given a ordered set of vectors  $\mathcal{V} = (v_1, \dots, v_m)$  that generates  $\mathbb{Z}^{2n}$  as a lattice, there exists an effectively computable symplectic basis  $\text{SympBas}(\mathcal{V})$  of  $\mathbb{Z}^{2n}$  such that for every  $P \in \text{Sp}_{2n}(\mathbb{Z})$  we have  $\text{SympBas}(\mathcal{V}P) = \text{SympBas}(\mathcal{V})P$ .*

*Proof.* Let  $w_1$  be the first nonzero vector in  $\mathcal{V}$  divided by the gcd of its coefficients. Since the family of vectors spans  $\mathbb{Z}^n$ , the gcd of the symplectic products  $\omega(w_1, v_j)$  is 1. Thus we can find in a deterministic manner integers  $\alpha_i$  such that  $w_{2n} = \sum_{i=1}^m \alpha_i v_i$  satisfies  $\omega(w_1, w_{2n}) = 1$ . We can then replace the vectors  $v_i$  of the vector family by  $v'_i = v_i - \omega(v_i, w_{2n})w_1 + \omega(v_i, w_1)w_{2n}$ . They satisfy  $\omega(v'_i, w_1) = \omega(v'_i, w_{2n}) = 0$ . Thus we apply the same construction inductively on them and get our basis. The invariance property follows from the fact that we never use specific coordinate systems.  $\square$

A canonical representative for a form  $A \in \mathcal{S}_{>0}^{2n}$  under the action of  $\mathrm{Sp}_{2n}(\mathbb{Z})$  can also be computed using our canonical form, as follows:

- (1) Compute a characteristic vector family using e.g.,  $\mathcal{V}_{\mathrm{cv}}$ .
- (2) Compute a graph on this characteristic set of vector by assigning to two vectors  $v, v'$  the weight  $(vAv', vJ_nv')$ .
- (3) Apply the canonicalization procedure and get a canonical ordering of  $\mathcal{V}_{\mathrm{cv}}$ .
- (4) Use [Theorem 5.1.2](#) in order to get a symplectic basis which then gives a reduction matrix.

**5.2. Lattice databases.** Several efforts have sought to enumerate lattice genera of either bounded discriminant or satisfying some arithmetic conditions such as small (spinor) class number. For example, the Brandt–Intrau tables [\[9\]](#) of reduced ternary forms with discriminant up to 1000, Nipp’s tables [\[33\]](#) of positive definite primitive quaternary quadratic forms with discriminant up to 1732, and more recently the complete table of lattices with class number one due to Kirschmer and Lorch [\[22\]](#), to name a few. A current project of interest in number theory is an extension of the L-functions and modular forms database (LMFDB) [\[26\]](#) to include lattices.

The general strategy for generating these tables can take several forms. For example, a list of isometry class candidates can be generated by extending lattices of lower rank in some systematic way [\[9; 33\]](#). Classes can also be generated by Kneser’s method of neighboring lattices [\[38\]](#) (see [Section 5.4](#) below). Although the completeness of the list of genus representatives can be verified using the Minkowski–Siegel mass formula, one critical bottleneck in most of these schemes is eliminating redundancy in the lists generated, especially for lattices with high rank and class number—it is here where we profit significantly from a canonical form.

Another current shortcoming of the database has been the lack of a deterministic naming scheme for lattices. Although lattices up to equivalence can be classified by dimension, determinant, level, and class number, beyond that point many genera of such lattices can exist, and each genus can potentially contain multiple classes. Finding a canonical form for lattices provides a way to establish a deterministic labeling. This has long been known to be a challenge: for example, it is exactly the problem of the boundary of a fundamental domain in Minkowski reduction (mentioned in the introduction) that is at issue. Ad hoc enumeration and labeling suffers from the deficiency that a computer failure or other issues in the database could result in new and different enumeration. A canonical form provides a mechanism for a canonical label for lattices. Such a scheme would still depend on the graph canonical form being called in the algorithm; but in the event of a switch a bijective dictionary could easily be stored between the new naming and the old, giving still a nearly permanent deterministic naming of lattices.

**5.3. Application to enumeration of perfect forms.** A canonical form really shows its strength compared to pairwise equivalence checks when the number of forms to be classified becomes very large. This is certainly the case during the enumeration of perfect forms using Voronoi’s algorithm in dimension 9 or higher. In dimension 9 already more than 20 million (inequivalent) perfect forms are found and the total

number could be on the order of half a billion [42]. Even though there are some useful invariants such as the number of minimal vectors, the determinant and the size of the automorphism group, the number of remaining candidates for equivalence for each found perfect form can become quite large. Removing equivalent forms is a large part of the computational cost during the enumeration.

Therefore, efficiently finding a canonical form seems to be a necessity in completing the full enumeration in dimensions 9 or higher. Luckily by the definition of a perfect form we always have that  $\text{Min}(A)$  is full dimensional. Furthermore for all perfect forms found so far  $\text{Min}(A)$  also spans  $\mathbb{Z}^n$  and therefore the function  $\mathcal{V}_{\text{ms}}$  seems to be an efficient way to obtain a small characteristic vector set. In Section 4.2 we saw that computing a canonical perfect form in dimension 9 takes just a few milliseconds.

**5.4. Application to algebraic modular forms.** Finally, we present an application to speed up computations of orthogonal modular forms, a special case of the theory of *algebraic modular forms* as defined by Gross [12]. We shift our perspective slightly, varying lattices in a (fixed) quadratic space.

Let  $L \subset V$  be a (full) lattice, the  $\mathbb{Z}$ -span of a  $\mathbb{Q}$ -basis for  $V$ . We say  $L$  is *integral* if  $x^\top A y \in \mathbb{Z}$  for all  $x, y \in L$ , and suppose that  $L$  is integral. We represent  $L$  in bits by a basis  $\{v_1, \dots, v_n\}$ ; letting  $U_L$  be the change of basis matrix, we obtain a form

$$A_L := (v_i^\top A v_j)_{1 \leq i, j \leq n} = U_L^\top A U_L. \quad (5.4.1)$$

(It is not necessarily the case that  $A_L$  is arithmetically equivalent to  $A$  — the change of basis need only belong to  $\text{GL}_n(\mathbb{Q})$ .)

In order to organize these lattices, we define the *orthogonal group*

$$\text{O}(V) := \{P \in \text{GL}_n(\mathbb{Q}) : P^\top A P = A\}. \quad (5.4.2)$$

Integral lattices  $L, L' \subset V$  are *isometric*, written  $L \simeq L'$ , if there exists  $P \in \text{O}(V)$  such that  $P(L) = L'$ . Choosing bases for  $L, L'$ , we see that  $L \simeq L'$  if and only if  $A_L$  and  $A_{L'}$  are arithmetically equivalent.

We repeat these definitions replacing  $\mathbb{Q}$  (and  $\mathbb{Z}$ ) by  $\mathbb{Q}_p$  (and  $\mathbb{Z}_p$ ) for a prime  $p$ , abbreviating  $L_p := L \otimes_{\mathbb{Z}} \mathbb{Z}_p$ . Then the *genus* of  $L$  is

$$\text{Gen}(L) := \{L' \subset V : L_p \simeq L'_p \text{ for all primes } p\}. \quad (5.4.3)$$

Finally, we define the *class set*  $\text{Cls}(L)$  as the set of isometry classes in  $\text{Gen}(L)$ . By the geometry of numbers, we have  $\#\text{Cls}(L) < \infty$ .

The theory of  $p$ -neighbors, due originally to Kneser [23], gives an effective method to compute representatives of the class set  $\text{Cls}(L)$ , as follows. Let  $p$  be prime (allowing  $p = 2$ ) not dividing  $\det(A_L)$ . We say that a lattice  $L' < V$  is a  $p$ -neighbor of  $L$ , and write  $L' \sim_p L$ , if  $L'$  is integral and

$$[L : L \cap L'] = [L' : L \cap L'] = p \quad (5.4.4)$$

(index as abelian groups). If  $L \sim_p L'$ , then  $\text{disc}(L) = \text{disc}(L')$  and  $L' \in \text{Gen}(L)$  [10, Lemma 5.7]. The set of  $p$ -neighbors can be computed in time  $O(p^{m+\epsilon} H_n(s))$ , where  $s$  is the input size and  $H_n$

is a polynomial depending on  $n$ . Moreover, by strong approximation [10, Theorem 5.8], there is an effectively computable finite set  $S$  of primes such that every  $[L'] \in \text{Cls}(L)$  is an *iterated  $S$ -neighbor*  $L \sim_{p_1} \cdots \sim_{p_r} L_r \simeq L'$  with  $p_i \in S$ . Typically, we may take  $S = \{p\}$  for any  $p \nmid \text{disc}(L)$ . In this way, we may compute a set of representatives for  $\text{Cls}(L)$  from iterated  $S$ -neighbors.

The space of *orthogonal modular forms* for  $L$  (with trivial weight) is

$$M(\text{O}(L)) := \text{Map}(\text{Cls}(L), \mathbb{C}). \quad (5.4.5)$$

In the basis of characteristic functions  $\delta_{[L']}$  for  $[L'] \in \text{Cls}(L)$  we have  $M(\text{O}(L)) \simeq \mathbb{C}^h$  where  $h := \# \text{Cls}(L)$ . For  $p \nmid \text{disc}(L)$ , define the *Hecke operator*

$$\begin{aligned} T_p: M(\text{O}(L)) &\rightarrow M(\text{O}(L)) \\ T_p(f)([L']) &= \sum_{M' \sim_p L'} f([M']). \end{aligned} \quad (5.4.6)$$

The operators  $T_p$  commute and are self-adjoint (with respect to a natural inner product); accordingly, there exists a basis of simultaneous eigenvectors for the Hecke operators, called *eigenforms*.

In this way, to compute the matrix representing the Hecke operator  $T_p$ , for each  $[L'] \in \text{Cls}(L)$ , we need to identify the isometry classes of the  $p$ -neighbors of  $L'$ . Here is where our canonical form algorithm applies, returning to our original motivation: after computing canonical forms for  $\text{Cls}(L)$ , for each  $p$ -neighbor, we compute their canonical forms and then a hash table look up on  $\text{Cls}(L)$ . This reduces our computation from  $O(h^2)$  *isometry tests* to  $O(h)$  *hash table lookups*. For medium-sized values of  $n$ , we hope that the use of canonical forms will allow us to peer more deeply into the world of automorphic forms on orthogonal groups.

## Acknowledgments

This work was advanced during the conference *Computational Challenges in the Theory of Lattices* at the Institute for Computational and Experimental Research in Mathematics (ICERM) and further advances were made during a visit to the Simons Institute for the Theory of Computing. The authors would like to thank ICERM and Simons for their hospitality and support. Voight was supported by a Simons Collaboration grant (550029) and Van Woerden was supported by the ERC Advanced Grant 740972 (ALGSTRONGCRYPTO). We also thank Achill Schürmann and Rainer Schulze-Pillot for help on Minkowski reduction theory and the anonymous referees for their detailed feedback.

## References

- [1] *Polytopes, lattices and quadratic forms programs*, [https://github.com/MathieuDutSik/polyhedral\\_common](https://github.com/MathieuDutSik/polyhedral_common), 2018.
- [2] E. Bayer-Fluckiger and I. Suarez, *Modular lattices over cyclotomic fields*, J. Number Theory **114** (2005), no. 2, 394–411.
- [3] D. Bremner, M. Dutour Sikirić, D. V. Pasechnik, T. Rehn, and A. Schürmann, *Computing symmetry groups of polyhedra*, LMS J. Comput. Math. **17** (2014), no. 1, 565–581.
- [4] B. Casselman, *Stability of lattices and the partition of arithmetic quotients*, Asian J. Math. **8** (2004), no. 4, 607–637.



- [5] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, third ed., Grundlehren Math. Wiss., vol. 290, Springer-Verlag, New York, 1999.
- [6] M. M. Deza and M. Laurent, *Geometry of cuts and metrics*, Algorithms and Combinatorics, vol. 15, Springer, Heidelberg, 2010.
- [7] J. L. Donaldson, *Minkowski reduction of integral matrices*, Math. Comp. **33** (1979), no. 145, 201–216.
- [8] M. Dutour Sikirić, A. Schürmann, and F. Vallentin, *Classification of eight-dimensional perfect forms*, Electron. Res. Announc. Amer. Math. Soc. **13** (2007), 21–32.
- [9] K. Germann, *Tabellen reduzierter, positiver quaternärer quadratischer Formen*, Comment. Math. Helv. **38** (1963), 56–83.
- [10] M. Greenberg and J. Voight, *Lattice methods for algebraic modular forms on classical groups*, Computations with modular forms, Contrib. Math. Comput. Sci., vol. 6, Springer, Cham, 2014, 147–179.
- [11] D. Grenier, *Fundamental domains for the general linear group*, Pacific J. Math. **132** (1988), no. 2, 293–317.
- [12] B. H. Gross, *Algebraic modular forms*, Israel J. Math. **113** (1999), no. 1, 61–93.
- [13] I. Haviv and O. Regev, *On the lattice isomorphism problem*, Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms, ACM, New York, 2014, 391–404.
- [14] L. Babai, *Canonical form for graphs in quasipolynomial time: preliminary report*, Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing, 2019, 1237–1246.
- [15] H. A. Helfgott, *Isomorphismes de graphes en temps quasi-polynomial*, Séminaire Bourbaki, vol. 2016/2017, Astérisque no. 407 (2019), exp. no. 1125, 135–182.
- [16] B. Helfrich, *Algorithms to construct Minkowski reduced and Hermite reduced lattice bases*, Theoretical Computer Science **41** (1985), 125–139.
- [17] T. Junttila and P. Kaski, *bliss*, <http://www.tcs.hut.fi/Software/bliss/>.
- [18] G. A. Kabatjanskiĭ and V. I. Levenšteĭn, *Bounds for packings on the sphere and in space*, Problemy Peredači Informacii **14** (1978), no. 1, 3–25.
- [19] R. Kannan and A. Bachem, *Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix*, SIAM J. Comput. **8** (1979), no. 4, 499–507.
- [20] W. Keller, J. Martinet, and A. Schürmann, *On classifying Minkowskian sublattices*, Math. Comp. **81** (2012), no. 278, 1063–1092, with an appendix by M. Dutour Sikirić.
- [21] M. Kirschmer, *One-class genera of maximal integral quadratic forms*, J. Number Theory **136** (2014), 375–393.
- [22] M. Kirschmer and D. Lorch, *Ternary quadratic forms over number fields with small class number*, J. Number Theory **161** (2016), 343–361.
- [23] M. Kneser, *Klassenzahlen definiter quadratischer Formen*, Archiv der Mathematik **8** (1957), no. 4, 241–250.
- [24] A. N. Korkin and E. I. Zolotarev, *Sur les formes quadratiques*, Math. Ann. **6** (1873), no. 1, 366–389.
- [25] A. K. Lenstra, H. W. Lenstra, and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534.
- [26] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, <http://www.lmfdb.org>, 2020.
- [27] R. MacPherson and M. McConnell, *Explicit reduction theory for Siegel modular threefolds*, Invent. Math. **111** (1993), no. 3, 575–625.
- [28] B. D. McKay and A. Piperno, *nauty and Traces*, <http://cs.anu.edu.au/people/bdm/nauty/>.
- [29] D. Micciancio, *The shortest vector problem is NP-hard to approximate to within some constant*, SIAM J. Comput. **30** (2001), 2008–2035.
- [30] D. Micciancio and P. Voulgaris, *A deterministic single exponential time algorithm for most lattice problems based on Voronoi cell computations*, SIAM J. Comput. **42** (2013), no. 3, 1364–1391.
- [31] H. Minkowski, *Diskontinuitätsbereich für arithmetische Äquivalenz*, J. Reine Angew. Math. **129** (1905), 220–274.
- [32] G. Nebe and N. Sloane, *A catalogue of lattices*, <http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/index.html>.
- [33] G. L. Nipp, *Quaternary quadratic forms*, Springer-Verlag, New York, 1991.



- [34] J. Opgenorth, W. Plesken, and T. Schulz, *CARAT, Crystallographic Algorithms And Tables*, v. 2.1b1 (2008), <https://github.com/lbfm-rwth/carat/>.
- [35] W. Plesken and B. Souvignier, *Computing isometries of lattices*, Computational algebra and number theory (London, 1993), J. Symbolic Comput. **24** (1997), no. 3-4, 327–334.
- [36] X. Pujol and D. Stehlé, *Rigorous and efficient short lattice vectors enumeration*, Advances in cryptology–ASIACRYPT 2008, Lecture Notes in Comput. Sci., vol. 5350, Springer, Berlin, 2008, 390–405.
- [37] S. Schönnenbeck, *Simultaneous computation of Hecke operators*, J. Algebra **501** (2018), 571–597.
- [38] R. Schulze-Pillot, *An algorithm for computing genera of ternary and quaternary quadratic forms*, Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation, ISSAC '91, ACM, 1991, 134–143.
- [39] A. Schürmann, *Computational geometry of positive definite quadratic forms*, University Lecture Series, vol. 48, Amer. Math. Soc., Providence, RI, 2009.
- [40] V. Stoltenberg-Hansen and J. V. Tucker, *Computable rings and fields*, Handbook of Computability Theory, Elsevier (1999), 363–447.
- [41] A. Storjohann and G. Labahn, *Asymptotically fast computation of Hermite normal forms of integer matrices*, Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation, ISSAC '96, ACM, New York, 1996, 259–266.
- [42] W. P. J. van Woerden, *Perfect quadratic forms: an upper bound and challenges in enumeration*, Master's thesis, Leiden University, 2018.

Received 28 Feb 2020.

MATHIEU DUTOIR SIKIRIĆ: [mathieu.dutour@gmail.com](mailto:mathieu.dutour@gmail.com)  
Institut Rudjer Bošković, Zagreb, Croatia

ANNA HAENSCH: [annahaensch@gmail.com](mailto:annahaensch@gmail.com)  
Department of Mathematics and Computer Science, Duquesne University, Pittsburgh, PA, United States

JOHN VOIGHT: [jvoight@gmail.com](mailto:jvoight@gmail.com)  
Department of Mathematics, Dartmouth College, Hanover, NH, United States

WESSEL P.J. VAN WOERDEN: [wessel.van.woerden@cwi.nl](mailto:wessel.van.woerden@cwi.nl)  
Centrum Wiskunde & Informatica (CWI), Amsterdam, Netherlands



# Computing Igusa's local zeta function of univariates in deterministic polynomial-time

Ashish Dwivedi and Nitin Saxena

Igusa's local zeta function  $Z_{f,p}(s)$  is the generating function that counts the number of integral roots,  $N_k(f)$ , of  $f(\mathbf{x}) \bmod p^k$ , for all  $k$ . It is a famous result, in analytic number theory, that  $Z_{f,p}$  is a rational function in  $\mathbb{Q}(p^s)$ . We give an elementary proof of this fact for a univariate polynomial  $f$ . Our proof is constructive as it gives a closed-form expression for the number of roots  $N_k(f)$ .

Our proof, when combined with the recent root-counting algorithm of Dwivedi, Mittal and Saxena (Computational Complexity Conference, 2019), yields the first deterministic  $\text{poly}(|f|, \log p)$ -time algorithm to compute  $Z_{f,p}(s)$ . Previously, an algorithm was known only in the case when  $f$  completely splits over  $\mathbb{Q}_p$ ; it required the rational roots to use the concept of generating function of a tree (Zúñiga-Galindo, J. Int. Seq., 2003).

## 1. Introduction

Over the years, the study of zeta functions has played a foundational role in the development of mathematics. They have applications in diverse science disciplines; in particular, machine learning [72], cryptography [2; 3], quantum cryptography [45], statistics [72; 47], theoretical physics [31; 53], string theory [51], quantum field theory [27; 31] and biology [57; 77]. Basically, a zeta function counts some mathematical objects. Often zeta functions show special analytic, or algebraic properties, the study of which can reveal striking information about the encoded object.

A classic example is the famous Riemann zeta function [54] (also known as the Euler–Riemann zeta function) which encodes the density and distribution of prime numbers [16; 64]. Later many *local* (i.e., associated to a specific prime  $p$ ) zeta functions were studied; e.g., the Hasse–Weil zeta function [73; 74], which encodes the count of zeros of a system of polynomial equations over finite fields (of a specific characteristic  $p$ ). The study of this function led to the development of modern algebraic geometry (see [19; 30]).

In this paper we are interested in a different local zeta function known as Igusa's local zeta function. It encodes the count of roots modulo prime powers of a given polynomial defined over a local field.

*MSC2010:* primary 11S40, 68Q01, 68W30; secondary 11Y16, 14G50.

*Keywords:* Igusa, local, zeta function, discriminant, valuation, deterministic, root, counting, modulo, prime power.

Formally, *Igusa's local zeta function*  $Z_{f,p}(s)$ , attached to a polynomial over  $p$ -adic integers

$$f(\mathbf{x}) \in \mathbb{Z}_p[x_1, \dots, x_n]$$

is defined as

$$Z_{f,p}(s) := \int_{\mathbb{Z}_p^n} |f(\mathbf{x})|_p^s \cdot |d\mathbf{x}|,$$

where  $s \in \mathbb{C}$  with  $\text{Re}(s) > 0$ ,  $|\cdot|_p$  denotes the absolute value over  $p$ -adic numbers  $\mathbb{Q}_p$ , and  $|d\mathbf{x}|$  denotes the Haar measure on  $\mathbb{Q}_p^n$  normalized so that  $\mathbb{Z}_p^n$  has measure 1.

Weil [75; 76] defined these zeta functions inspired by those of Riemann. Later they were studied extensively by Igusa [34; 35; 36]. Using the method of resolution of singularities, Igusa proved that  $Z_{f,p}(s)$  converges to a rational function. Later the convergence was proved by Denef [20] via a different method (namely,  $p$ -adic cell decomposition). The Igusa zeta function is closely related to *Poincaré series*  $P(t)$ , attached to  $f$  and  $p$ , defined as

$$P(t) := \sum_{i=0}^{\infty} N_i(f) \cdot (p^{-n}t)^i,$$

where  $t \in \mathbb{C}$  with  $|t| < 1$ , and  $N_i(f)$  is the count on roots of  $f \bmod p^i$  (also  $N_0(f) := 1$ ). In fact, it has been shown in [33] that

$$P(t) = \frac{1 - t \cdot Z_{f,p}(s)}{1 - t}$$

with  $t = p^{-s}$ . So rationality of  $Z_{f,p}(s)$  implies rationality of  $P(t)$  and vice versa; thus proving a conjecture of [52] that  $P(t)$  is a rational function. This relation makes the local zeta function interesting in arithmetic geometry (see [33; 21; 50; 44] for more on the Igusa zeta function).

Many researchers have tried to calculate the expression for the Igusa zeta function for various polynomial families [17; 56; 66; 1; 22; 48; 65; 32; 58; 79; 81] and this has led to the development of various methodologies; for example, the stationary phase formula (SPF), the Newton polygon method, resolution of singularities, etc. These methods have been fruitful in various other situations [23; 82; 83; 59; 39; 40; 84; 68; 61; 85]. However, not much has been said about their algorithmic aspect except in the case of resolution of singularities [6; 9; 8; 67]. These algorithms are impractical [7]. Indeed, the computation of the Igusa zeta function for a general multivariate polynomial seems to be an intractable problem since root-counting of a multivariate polynomial over a finite field is known to be #P-hard [28; 26].

In this paper, we focus on the computation of the Igusa zeta function when the associated polynomial is *univariate*. The Igusa zeta function for a univariate polynomial  $f$  is connected to root-counting of  $f$  modulo prime powers  $p^k$ , which is itself an interesting problem. It has applications in factoring [13; 14; 10], coding theory [4; 60], elliptic curve cryptography [43], arithmetic algebraic geometry [80; 22; 21], and the study of root sets [62; 15; 5; 18; 49]. After a long series of work [70; 71; 38; 60; 4; 63; 12; 42; 25], this problem was recently resolved in [24].

In the case of univariate polynomials one naturally expects an elementary proof of convergence, as well as an efficient algorithm to compute the Igusa zeta function. Our main result is:

We give the first deterministic polynomial time algorithm to compute the rational function form of the Igusa zeta function associated to a given univariate polynomial  $f \in \mathbb{Z}[x]$  and prime  $p$ .

To the best of our knowledge, this result was previously achieved only for the restricted class of univariate polynomials using methods that were sophisticated and nonexplicit. For example, Zúñiga-Galindo [80] achieved this for univariate polynomials which completely split over  $\mathbb{Q}$  (with the factorization given in the input), using the stationary phase formula (see Section 1.2). The methods to compute the Igusa zeta function for a multivariate, e.g., Denef [20], continue to be impractical in the case of univariate polynomials. On the other hand, our approach is elementary, uses explicit methods, and completely solves the problem.

**1.1. Our results.** We will compute the Igusa zeta function  $Z_{f,p}(s)$  by finding the related Poincaré series  $P(t) =: A(t)/B(t)$ .

**Theorem 1.** *We are given a univariate integral polynomial  $f(x) \in \mathbb{Z}[x]$  of degree  $d$ , with coefficients of magnitude bounded by  $C \in \mathbb{N}$ , and a prime  $p$ . Then, we compute the Poincaré series  $P(t) = A(t)/B(t)$ , associated with  $f$  and  $p$ , in deterministic  $\text{poly}(d, \log C + \log p)$ -time.*

*The degree of the integral polynomial  $A(t)$  is  $\tilde{O}(d^2 \log C)$  and that of  $B(t)$  is  $O(d)$ .*

- Remarks.* (1) Our method gives an elementary proof of rationality of  $Z_{f,p}(s)$  as a function of  $t = p^{-s}$ .  
 (2) Previously, Zúñiga-Galindo [80] gave a deterministic polynomial time algorithm to compute  $Z_{f,p}(s)$ , if  $f$  completely splits over  $\mathbb{Q}$  and the roots are provided. Our Theorem 1 works for *any* input  $f \in \mathbb{Z}[x]$  (see Section 1.2 for further discussion).  
 (3) Cheng et al. [12] could compute  $Z_{f,p}(s)$  in deterministic polynomial time, in the special case where the degree of  $A(t)$ ,  $B(t)$  is constant.  
 (4) Dwivedi et al. [24], using [80], remarked that  $Z_{f,p}(s)$  could be computed in deterministic polynomial time, in the special case when  $f$  completely splits over  $\mathbb{Q}_p$  *without* the roots being provided in the input. The detailed proof of this claim was not given and the convergence relied on the old method of [80].

We achieve the rational form of  $Z_{f,p}(s)$  by getting an explicit formula for the number of zeros  $N_k(f)$ , of  $f \bmod p^k$ , which sheds new light on the properties of the function  $N_k(\cdot)$ . Eventually, it gives an elementary proof of the rationality of the Poincaré series  $\sum_{i=0}^{\infty} N_i(f) \cdot (p^{-1}t)^i$ .

**Corollary 2.** *Let  $k$  be large enough, namely,  $k \geq k_0 := O(d^2(\log C + \log d))$ . Then, we give a closed form expression for  $N_k(f)$  (in Theorem 21).*

*Interestingly, if  $f$  has nonzero discriminant, then  $N_k(f)$  is constant (independent of  $k$ ) for all  $k \geq k_0$ .*

**1.2. Further remarks and comparison.** To the best of our knowledge, there have been very few results on the complexity of computing Igusa's zeta function for univariate polynomials [80; 12]. Other very

specialized algorithms are for bivariate polynomials (e.g., hyperelliptic curves) [11], and for the polynomial  $x^q - a$  [65]. In a recent related work [78, Appendix A], a different proof of rationality of Igusa's zeta function for univariate polynomials based on tree based algorithm of [42] is given.

An old proof technique called the *stationary phase formula* is the standard method used in the literature to compute Igusa's zeta function for various families of polynomials. Our work, on the other hand, uses elementary techniques and a tree-based root-counting algorithm [24] to compute some fixed parameters (independent of  $k$ ) involved in our formula of  $N_k(f)$ , for all  $k \geq k_0$ .

It is to be noted that just efficiently computing  $N_k(f)$ , for “several”  $k$ , is not enough to compute the rational form of  $Z_{f,p}(s)$ ; neither does it imply the rationality of  $Z_{f,p}(s)$  directly.

Our algorithm is *deterministic* and works for general  $f \in \mathbb{Z}_p[x]$  (provided  $f$  has computable representation). For earlier methods to work for  $f \in \mathbb{Z}_p[x]$  they may need factoring over  $p$ -adics  $\mathbb{Z}_p$  or  $\mathbb{Q}_p$  (for example [80]), but deterministic algorithms there are unknown. See [13; 14; 10] for randomized factoring algorithms.

**1.3. Proof idea.** We will compute the rational form of Igusa's zeta function via computing the rational form of corresponding Poincaré series

$$P(t) := \sum_{i=0}^{\infty} N_i(f) \cdot (p^{-1}t)^i.$$

In addition, our method proves that the Poincaré series is a rational function of  $t$ , in the case of univariate polynomial  $f(x)$ , via first principles; instead of using advanced tools like the stationary phase method or Newton polygon method or resolution of singularity.

To compute the rational form of Poincaré series, the idea is to compute the coefficient sequence

$$\{N_0(f), \dots, N_k(f), \dots\}$$

in a closed form. That is to say, we wish to get an explicit formula for  $N_k(f)$ , the number of roots of  $f \bmod p^k$ , only in terms of  $k$ ; with the hope that this will help in getting a rational function for the Poincaré series  $P(t)$ .

Indeed in [Theorem 21](#), we show that such a formula exists for each  $N_k(f)$  for sufficiently large  $k$ . We achieve this by establishing a connection among roots of  $f \bmod p^k$  and  $\mathbb{Z}_p$ -roots of  $f \in \mathbb{Z}_p[x]$ . Let  $f$  have  $n$  distinct  $\mathbb{Z}_p$ -roots  $\alpha_1, \dots, \alpha_n$ . An important concept we define is that of “neighborhood” of an  $\alpha_i \bmod p^k$  ([Definition 18](#)); these are basically roots of  $f \bmod p^k$  “associated” to  $\alpha_i$ . In [Lemma 15](#), we show that *each* root  $\bar{\alpha}$  of  $f \bmod p^k$  is associated to a *unique*  $\mathbb{Z}_p$ -root  $\alpha_i$  of  $f$ :  $\bar{\alpha}$  closely approximates  $\alpha_i$  but is quite far from other  $\alpha_j$ s, for all  $j \in [n], j \neq i$ . So, the root-set of  $f \bmod p^k$  can be partitioned into  $n$  subsets  $S_{k,i}$ ,  $i \in [n]$ , where neighborhood  $S_{k,i}$  is the set of those roots of  $f \bmod p^k$  which are associated to  $\mathbb{Z}_p$ -root  $\alpha_i$ .

Let the multiplicity of root  $\alpha_i$  be  $e_i$ ; then  $f(x) =: (x - \alpha_i)^{e_i} f_i(x)$  over  $\mathbb{Z}_p$ , where  $f_i(\alpha_i) \neq 0$ . We call  $f_i$  the  $\alpha_i$ -free part of  $f$ . Then, for  $\bar{\alpha}$  to be a root of  $f \bmod p^k$  we must have

$$f(\bar{\alpha}) = (\bar{\alpha} - \alpha_i)^{e_i} \cdot f_i(\bar{\alpha}) \equiv 0 \bmod p^k.$$

**Lemma 16** says that  $f_i$  possesses equal valuation  $v_i$ , for all roots of  $f \bmod p^k$  associated to  $\alpha_i$ , i.e., ones in  $S_{k,i}$ . That is, the maximum power of  $p$  dividing  $f_i(\bar{\alpha})$  is the same as that for  $f_i(\bar{\beta})$ , as long as  $\bar{\alpha}, \bar{\beta} \in S_{k,i}$ . Note that  $v_p((\bar{\alpha} - \alpha_i)^{e_i} \cdot f_i(\bar{\alpha})) \geq k$  if and only if  $v_p((\bar{\alpha} - \alpha_i)) \geq (k - v_i)/e_i$ .

Eventually, these two lemmas together give us the size of the neighborhood,  $|S_{k,i}| = p^{k - \lceil (k - v_i)/e_i \rceil}$ . Moreover, the neighborhoods disjointly cover all the roots of  $f \bmod p^k$ . Hence,  $N_k(f) = \sum_{i=1}^n |S_{k,i}|$ . This is a formula for  $N_k(f)$ , when  $k$  is large. But still the two parameters  $v_i$  and  $e_i$  are unknown as, unlike in [80], we are not provided the factorization of  $f$  over  $\mathbb{Z}_p$  (nor could we find it in deterministic polynomial time).

To compute  $v_i, e_i$ , we use the help of the root-counting algorithm of [24], which gives us the value of  $N_k(f)$ , and the underlying root-set structure that it developed. We show that each representative root  $\bar{\alpha}_i$  of  $f \bmod p^k$  is indeed the neighborhood  $S_{k,i}$  (**Theorem 19**), shedding new light on the root-set mod prime powers.

Now we can get two equations, for the two unknowns  $v_i, e_i$ , by calling the algorithm of [24] twice: first for  $k = k_i$  and second for  $k = k_i + e_i$ , where  $k_i$  is such that  $(k_i - v_i)/e_i$  is an integer (e.g., we can try all  $k_i$  in the range  $[k_0, \dots, k_0 + \deg(f)]$ ). So, we can efficiently compute  $v_i, e_i$  for a particular representative root  $\bar{\alpha}_i, i \in [n]$ . So, this calculation also reveals some new parameters of representative roots which were not mentioned in earlier related works [4; 24].

## 2. Preliminaries

**2.1. Root-set of a univariate polynomial mod prime powers.** We recall a structural property (and related objects) of the root-set of univariate polynomials in the ring  $\mathbb{Z}/\langle p^k \rangle$  [24; 25].

**Proposition 3.** *The root-set of an integral univariate polynomial  $f$ , over the ring of integers modulo prime powers, is the disjoint union of at most  $\deg(f)$  many efficiently representable subsets.*

We call these efficiently representable subsets *representative roots*, as defined and named in [25, Section 2]. This property of root-sets in  $\mathbb{Z}/\langle p^k \rangle$  is indeed a generalization of the property of root-sets over a field: there are at most  $\deg(f)$  many roots of  $f(x)$  in a field.

To present representative roots formally, we first reiterate some notation from [25, Section 2].

*Representatives.* An abbreviation  $*$  will be used to denote all of the underlying ring  $R$ . So for the ring  $R = \mathbb{Z}/\langle p^k \rangle$ ,  $*$  denotes all the  $p^k$  distinct elements. Perceiving any element of  $R$  in base- $p$  representation, like  $x_0 + px_1 + \dots + p^{k-1}x_{k-1}$  where  $x_i \in \{0, \dots, p-1\}$  for all  $i \in \{0, \dots, k-1\}$ , the set

$$\mathbf{a} := a_0 + pa_1 + \dots + p^{l-1}a_{l-1} + p^l*$$

“represents” the set of all the elements of  $R$  which are congruent to  $a_0 + pa_1 + \dots + p^{l-1}a_{l-1} \bmod p^l$ . Throughout the paper we call such sets *representatives* and we denote them using bold small letters, like  $\mathbf{a}, \mathbf{b}$  etc.

Let us denote the *length* of a representative  $\mathbf{a}$  by  $|\mathbf{a}|$ , so if  $\mathbf{a} := a_0 + pa_1 + \dots + p^{l-1}a_{l-1} + p^l*$  then its length is  $|\mathbf{a}| = l$ . Now we formally define representative roots of a univariate polynomial in  $\mathbb{Z}/\langle p^k \rangle$ .

**Definition 4** (representative roots). A set

$$\mathbf{a} = a_0 + pa_1 + \cdots + p^{l-1}a_{l-1} + p^l*$$

is called a *representative root* of  $f(x)$  modulo  $p^k$  if each  $\alpha \in \mathbf{a}$  is a root of  $f(x) \bmod p^k$ , but, not all  $\beta \in \mathbf{b} := a_0 + pa_1 + \cdots + p^{l-2}a_{l-2} + p^{l-1}* \bmod p^k$  are roots of  $f(x) \bmod p^k$ .

It was first observed in [4] that there are at most  $\deg(f)$ -many representative roots and they gave an efficient randomized algorithm to compute all these representative roots (for a simple exposition of the algorithm, see [25, Section B]).

We need a deterministic algorithm for our purpose (in Section 3.4) to count, if not find, the representative roots (as well as count the roots in each representative root). So we use the deterministic polynomial time algorithm of [24] which returns all these representative roots implicitly in the form of a data-structure they call *maximal split ideals* (MSI). The two explicit parameters, *length* and *degree* of an MSI immediately gives the count on the number of representative roots (as well as roots) encoded by them, which suffices for our purpose. A similar idea to use triangular ideals for encoding roots first appeared in [12], to count roots deterministically, but for “small”  $k$ .

We now define MSI from [24, Section 2].

**Definition 5** ([24, Section 2], maximal split ideals). A triangular ideal

$$I = \langle h_0(x_0), \dots, h_l(x_0, \dots, x_l) \rangle,$$

where  $0 \leq l \leq k-1$  and each  $h_i(x_0, \dots, x_i) \in \mathbb{F}_p[x_0, \dots, x_i]$ , is called a *maximal split ideal* of  $f(x) \bmod p^k$  if

- (1) the number of common zeros of  $h_0, \dots, h_l$  in  $\mathbb{F}_p^{l+1}$  is  $\prod_{i=0}^l \deg_{x_i}(h_i)$ , where  $\deg_{x_i}$  denotes the individual degree wrt  $x_i$ , and
- (2) for every common zero  $(a_0, \dots, a_l) \in \mathbb{F}_p^{l+1}$  of  $h_0, \dots, h_l$ ,  $f(x)$  vanishes identically modulo  $p^k$  with the substitution  $x \rightarrow a_0 + pa_1 + \cdots + p^l a_l + p^{l+1}x$  but not with  $x \rightarrow a_0 + \cdots + p^{l-1}a_{l-1} + p^l x$ .

For an MSI  $I$  given by its generators  $h_0(x_0), \dots, h_l(x_0, \dots, x_l)$  we define its *length* to be  $l+1$  and *degree*, denoted as  $\deg(I)$ , to be the number of common zeros of its generators, which is  $\prod_{i=0}^l \deg_{x_i}(h_i)$  by definition.

Essentially,  $I$  is encoding some representative roots of  $f \bmod p^k$  in the form of common roots of its generators. Indeed, condition (2) of the definition is similar to that of representative roots. If  $(a_0, \dots, a_l)$  is a common zero of the generators then by condition (2),  $a_0 + pa_1 + \cdots + p^l a_l + p^{l+1}*$  follows all the conditions to be a representative root. Then, it is apparent that:

**Lemma 6** ([24, Lemmas 6 and 8]). *The length of an MSI  $I$  is the length of each representative root encoded by it and the degree of  $I$  is the count on these representative roots. Thus, we get the count on the roots of  $f \bmod p^k$  encoded by  $I$  as  $\prod_{i=0}^l \deg_{x_i}(h_i) \times p^{k-l-1}$ .*

We state the result of [24] which returns all the representative roots, in MSI form, in deterministic polynomial time.



**Theorem 7** (compute  $N_k(f)$  [24]). *In deterministic  $\text{poly}(|f|, k \log p)$ -time one gets the maximal split ideals which collectively contain exactly the representative roots of a univariate polynomial  $f(x) \in \mathbb{Z}[x]$  modulo prime power  $p^k$ .*

Using Lemma 6 we can count them, and all roots of  $f \bmod p^k$ , in deterministic polynomial time.

**2.2. Some definitions and notation related to  $f$ .** We are given an integral univariate polynomial  $f(x)$  in  $\mathbb{Z}[x]$  of degree  $d$  with coefficients of magnitude at most  $C \in \mathbb{N}$ , and a prime  $p$ . Then,  $f$  can also be thought of as an element of  $\mathbb{Z}_p[x]$  (as  $\mathbb{Z} \subseteq \mathbb{Z}_p$ ), where  $\mathbb{Z}_p$  is the ring of integers of  $p$ -adic rational numbers  $\mathbb{Q}_p$ . In such a field  $\mathbb{Q}_p$  (called a nonarchimedean local field) there exists a valuation function  $v_p : \mathbb{Q}_p \rightarrow \mathbb{Z} \cup \{\infty\}$ . Formally, the valuation  $v_p(a)$  of  $a \in \mathbb{Z}_p$  ( $\mathbb{Z}_p$  is a UFD) is defined to be the highest power of  $p$  dividing  $a$ , when  $a \neq 0$ , and  $\infty$  when  $a = 0$ . This definition extends to the rationals  $\mathbb{Q}_p$  naturally as  $v_p(a/b) := v_p(a) - v_p(b)$ , where  $b \neq 0$  and  $a, b \in \mathbb{Z}_p$  (see [41]).

Now we define the factors of  $f$  in  $\mathbb{Z}_p[x]$  as follows (note: we do not require  $f$  to be monic).

**Definition 8.** Let the  $p$ -adic integral factorization of  $f$  into coprime irreducible factors be

$$f(x) =: \prod_{i \in [n]} (x - \alpha_i)^{e_i} \cdot \prod_{j=1}^m g_j(x)^{t_j},$$

where each  $\alpha_i$  is a  $\mathbb{Z}_p$ -root of  $f$  with multiplicity  $e_i$ . Each  $g_j(x) \in \mathbb{Z}_p[x]$  has multiplicity  $t_j$ ; it is irreducible over  $\mathbb{Z}_p$  and has no  $\mathbb{Z}_p$ -root.

For example, over  $\mathbb{Z}_2$ ,  $f = 2x^2 + 3x + 1 = (x + 1) \cdot (2x + 1)$  has  $n = m = 1$ .

**Definition 9.** For each  $i \in [n]$ , we define  $f_i(x) \in \mathbb{Z}_p[x]$ , called the  $\alpha_i$ -free part of  $f$ , as  $f_i(x) := f(x)/(x - \alpha_i)^{e_i}$ . We denote the valuation  $v_p(f_i(\alpha_i))$  as  $v_i$ , for all  $i \in [n]$ .

The radical of a univariate polynomial  $h(x)$  over a field  $\mathbb{F}$  is defined to be the univariate polynomial, denoted by  $\text{rad}(h)$ , which is the product of coprime irreducible factors of  $h$ . This gives rise to the following definition.

**Definition 10.** Define  $\text{rad}(f) := (\prod_{i=1}^n (x - \alpha_i)) \cdot (\prod_{j=1}^m g_j(x))$ . Analogously, the radical of  $f_i$ , for each  $i \in [n]$ , is defined as  $\text{rad}(f_i) := \text{rad}(f)/(x - \alpha_i)$ .

The discriminant of a polynomial  $h(x) \in \mathbb{F}[x]$  is defined as  $D(h) := h_m^{2m-1} \cdot \prod_{1 \leq i < j \leq m} (r_i - r_j)^2$ , where  $\mathbb{F}$  is a field, the  $r_i$ 's are the roots of  $h(x)$  over the algebraic closure  $\overline{\mathbb{F}}$ , the degree of  $h$  is  $m$ , and  $h_m$  is its leading coefficient.

The discriminant  $D(h)$  is an element of  $\mathbb{F}$ . It is clear by the definition that all the roots of  $h$  are distinct if and only if  $D(h) \neq 0$ ; i.e., the discriminant of the radical is nonzero.

**Definition 11.** We denote by  $\Delta$  the valuation with respect to  $p$  of the discriminant of the radical of  $f$ , i.e.,  $\Delta := v_p(D(\text{rad}(f)))$ .

We see that  $\Delta$  must be finite, since roots of  $\text{rad}(f)$  are distinct. The following fact is easily established by the definition of discriminant and the fact that  $\alpha_1, \dots, \alpha_n$  are also roots of  $\text{rad}(f)$ .

**Fact 12.** For  $i \neq j \in [n]$ , we have  $v_p(\alpha_i - \alpha_j) \leq \Delta/2 < \infty$ .

For our algorithm,  $\Delta$  will be crucial in informing us about the behavior of the roots of  $f \bmod p^k$ .

**Properties of discriminants.**

- (1) Over  $\mathbb{Z}_p$ , if  $u(x) \mid w(x)$  then  $D(u) \mid D(w)$  and  $v_p(D(u)) \leq v_p(D(w))$ .
- (2) The discriminant of a linear polynomial is defined to be 1.
- (3) If  $w(x) = (x - a) \cdot u(x)$  then by the definition of discriminant, it is clear that  $D(w) = D(u) \cdot u(a)^2$ .
- (4) The discriminant  $D(h)$  of a degree- $l$  univariate polynomial  $h(x) := h_l x^l + \dots + h_1 x + h_0$ , over  $\mathbb{Z}_p$ , is also a multivariate polynomial over  $\mathbb{Z}_p$  in the coefficients  $h_0, \dots, h_l$  (see [46, Chapter 1]). Moreover, it is computable in time polynomial in the size of a given  $h$  (e.g., using the determinant of a Sylvester matrix [69, Chapter 11, Section 2]).

### 3. Proof of main results

**3.1. Interplay of  $\mathbb{Z}_p$ -roots and  $(\mathbb{Z}/\langle p^k \rangle)$ -roots.** In this section we will establish a connection between  $(\mathbb{Z}/\langle p^k \rangle)$ -roots and  $\mathbb{Z}_p$ -roots of the given  $f$ , when  $k$  is sufficiently large, i.e.,  $k > d\Delta$  (see Section 2.2 for the related notation).

Recall that  $\alpha_1, \dots, \alpha_n$  are the distinct  $\mathbb{Z}_p$ -roots of  $f$  (Definition 8). The following claim establishes a notion of “closeness” of any  $\bar{\alpha} \in \mathbb{Z}_p$  to an  $\alpha_j$ . Later we will apply this to a representative root  $\bar{\alpha}$ .

**Claim 13** (close to a root). For some  $j \in [n]$ ,  $\bar{\alpha} \in \mathbb{Z}_p$ , if  $v_p(\bar{\alpha} - \alpha_j) > \Delta/2$ , then  $v_p(\bar{\alpha} - \alpha_i) = v_p(\alpha_j - \alpha_i) \leq \Delta/2$ , for all  $i \neq j, i \in [n]$ .

*Proof.* The valuation  $v_p(\bar{\alpha} - \alpha_i)$  is equal to  $v_p(\bar{\alpha} - \alpha_j + \alpha_j - \alpha_i)$ . Since  $v_p(\bar{\alpha} - \alpha_j) > \Delta/2$  and  $v_p(\alpha_j - \alpha_i) \leq \Delta/2$  (by Fact 12), we deduce  $v_p(\bar{\alpha} - \alpha_i) = \min\{v_p(\bar{\alpha} - \alpha_j), v_p(\alpha_j - \alpha_i)\} = v_p(\alpha_j - \alpha_i) \leq \Delta/2$ .  $\square$

The following lemma says that an irreducible cannot take values with ever-increasing valuation.

**Lemma 14** (valuation of an irreducible). Let  $h(x) \in \mathbb{Z}_p[x]$  be a polynomial with no  $\mathbb{Z}_p$ -root, and discriminant  $D(h) \neq 0$ . Then, for any  $\bar{\alpha} \in \mathbb{Z}_p$ ,  $v_p(h(\bar{\alpha})) \leq v_p(D(h))$ .

*Proof.* We give the proof by contradiction, i.e., we show that if  $v_p(h(\bar{\alpha})) > v_p(D(h))$ , then  $h(x)$  has a root in  $\mathbb{Z}_p$ .

Define  $v_p(D(h)) =: d(h)$ . Let  $\bar{\alpha} \in \mathbb{Z}_p$  such that  $h(\bar{\alpha}) \equiv 0 \bmod p^\delta$ , for  $\delta > d(h)$ . Then we write  $h(x) = (x - \bar{\alpha}) \cdot h_1(x) + p^\delta \cdot h_2(x)$ . The two things to note here are:

- (1).  $D(h) \equiv D(h \bmod p^\delta) \bmod p^\delta$  by discriminants’ property (4) in Section 2.2. Also,  $D(h) \neq 0$  is given.
- (2). Let  $h'(x)$  be the first derivative of  $h(x)$  and let  $i := v_p(h'(\bar{\alpha}))$ . Then, we claim that  $\delta > d(h) \geq 2i$ .

Consider  $h'(x) = h_1(x) + (x - \bar{\alpha})h'_1(x) + p^\delta h'_2(x)$ . So,  $h'(\bar{\alpha}) \equiv h_1(\bar{\alpha}) \bmod p^\delta$ . By property (3) (Section 2.2) of discriminants,  $D(h) \equiv D((x - \bar{\alpha}) \cdot h_1(x)) \equiv D(h_1) \cdot h_1(\bar{\alpha})^2 \equiv D(h_1) \cdot h'(\bar{\alpha})^2 \bmod p^\delta$ . Then, since  $D(h) \neq 0 \bmod p^\delta$ , we deduce  $2i \leq d(h) < \delta$ .

Now, we show that the root  $\bar{\alpha}$  of  $h \bmod p^\delta$  lifts to roots of  $h \bmod p^{\delta+j}$ , for all  $j \in \mathbb{Z}^+$ . This is due to Hensel's lemma (see [69, Chapter 15]); for completeness we give the proof.

By Taylor expansion, we have  $h(\bar{\alpha} + p^{\delta-i}x) = h(\bar{\alpha}) + h'(\bar{\alpha}) \cdot p^{\delta-i}x + h''(\bar{\alpha}) \cdot p^{2(\delta-i)}x^2/2! + \dots$ .

Note that there exists a unique solution  $x_0 \equiv (-h(\bar{\alpha})/h'(\bar{\alpha})p^{\delta-i}) \bmod p$ :  $h(\bar{\alpha} + p^{\delta-i}x_0) \equiv 0 \bmod p^{\delta+1}$ . This follows from the Taylor expansion and since  $2(\delta-i) > \delta$ .

So,  $\bar{\alpha} - p^{\delta-i}(h(\bar{\alpha})/h'(\bar{\alpha})p^{\delta-i}) \bmod p^{\delta+1}$  is a lift, of  $\bar{\alpha} \bmod p^\delta$ . By similar reasoning, it can be lifted further to arbitrarily high powers  $p^{\delta+j}$ . This proves  $h(x)$  has a  $\mathbb{Z}_p$ -root, which is a contradiction.  $\square$

The following lemma is perhaps the most important one. It associates every root  $\bar{\alpha}$  of  $f(x) \bmod p^k$  to a unique  $\mathbb{Z}_p$ -root of  $f$ . Recall the notation from Section 2.2.

**Lemma 15** (unique association). *Let  $k > d(\Delta + 1)$  and  $\bar{\alpha} \in \mathbb{Z}_p$  be a root of  $f(x) \bmod p^k$ . There exists a unique  $\alpha_i$  such that  $v_p(\bar{\alpha} - \alpha_i) > \Delta + 1$  and thus,  $v_p(\bar{\alpha} - \alpha_i) > v_p(\alpha_i - \alpha_j)$ , for all  $j \neq i$ ,  $j \in [n]$ .*

*Proof.* Let us first prove that there exists some  $i \in [n]$ , given  $\bar{\alpha}$ , such that  $v_p(\bar{\alpha} - \alpha_i) > \Delta + 1$ . For the sake of contradiction, assume that  $v_p(\bar{\alpha} - \alpha_i) \leq \Delta + 1$  for all  $i \in [n]$ . Then, by Definition 8,  $v_p(f(\bar{\alpha})) = \sum_{i=1}^n e_i \cdot v_p(\bar{\alpha} - \alpha_i) + \sum_{j=1}^m t_j \cdot v_p(g_j(\bar{\alpha})) \leq (\Delta + 1) \cdot \sum_{i=1}^n e_i + \sum_{j=1}^m t_j \cdot v_p(g_j(\bar{\alpha}))$ .

Since  $g_j$  has no  $\mathbb{Z}_p$ -root, for all  $j \in [m]$ , by Lemma 14,  $v_p(g_j(\bar{\alpha})) \leq v_p(D(g_j))$ . By the properties given in Section 2.2 we get  $v_p(D(g_j)) \leq v_p(D(\text{rad}(f))) = \Delta$ , proving that  $v_p(g_j(\bar{\alpha})) \leq \Delta$ .

Going back,  $v_p(f(\bar{\alpha})) \leq (\Delta + 1) \cdot (\sum_{i=1}^n e_i + \sum_{j=1}^m t_j) \leq d(\Delta + 1) < k$ . It implies that  $f(\bar{\alpha}) \not\equiv 0 \bmod p^k$ , which contradicts the hypothesis that  $\bar{\alpha}$  is a root of  $f \bmod p^k$ .

Thus, there exists  $i \in [n]$  such that  $v_p(\bar{\alpha} - \alpha_i) > \Delta + 1$ . The uniqueness of  $i$  follows from Claim 13.  $\square$

Having seen that every root  $\bar{\alpha}$  of  $f \bmod p^k$  is associated (or close) to a unique  $\mathbb{Z}_p$ -root  $\alpha_i$ , the following lemma tells us that the valuation of the  $\alpha_i$ -free part of  $f$  (resp. factors of  $f$  with no  $\mathbb{Z}_p$ -root) is the same on any  $\bar{\alpha}$  close to  $\alpha_i$ . This unique valuation is important in getting an expression for  $N_k(f)$ .

**Lemma 16** (unique valuation). *Fix  $i \in [n]$ . Fix  $\bar{\alpha} \in \mathbb{Z}_p$  such that  $v_p(\bar{\alpha} - \alpha_i) > \Delta$ . Recall  $g_j(x)$ ,  $f_i$  from Section 2.2. Then,*

- (1)  $v_p(g_j(\bar{\alpha})) = v_p(g_j(\alpha_i))$ , for all  $j \in [m]$ ,
- (2)  $v_p(f_i(\bar{\alpha})) = v_p(f_i(\alpha_i))$ .

In other words, the valuation with respect to  $p$  of  $f_i = f(x)/(x - \alpha_i)^{e_i}$ , on  $x \mapsto \bar{\alpha}$ , is fixed uniquely to  $v_i := v_p(f_i(\alpha_i))$ , for any “close” approximation  $\bar{\alpha} \in \mathbb{Z}_p$  of  $\alpha_i$ .

*Proof.* Since  $g_j \mid \text{rad}(f_i)$  and  $\text{rad}(f_i) \mid \text{rad}(f)$ , we have by the properties of discriminants (Section 2.2) that  $v_p(g_j(\alpha_i)) \leq v_p(\text{rad}(f_i)(\alpha_i)) \leq \Delta$ , for all  $j \in [m]$ .

Since  $v_p(\bar{\alpha} - \alpha_i) > \Delta$ , we deduce  $v_p(g_j(\bar{\alpha}) - g_j(\alpha_i)) > \Delta$ . Furthermore,  $v_p(g_j(\alpha_i)) \leq \Delta$  implies  $v_p(g_j(\bar{\alpha})) = v_p(g_j(\alpha_i))$ . This proves the first part.

By Claim 13,  $v_p(\bar{\alpha} - \alpha_u) = v_p(\alpha_i - \alpha_u)$ , for all  $u \neq i$ ,  $u \in [n]$ . Also, by the first part,  $v_p(g_w(\bar{\alpha})) = v_p(g_w(\alpha_i))$ , for all  $w \in [m]$ . Consequently,  $v_p(f_i(\bar{\alpha})) = \sum_{u=1, u \neq i}^n e_u \cdot v_p(\alpha_i - \alpha_u) + \sum_{w=1}^m t_w \cdot v_p(g_w(\alpha_i)) = v_p(f_i(\alpha_i))$ . This proves the second part.  $\square$

**3.2. Representative roots versus neighborhoods.** We now connect the  $\mathbb{Z}_p$ -roots of  $f$  to the representative roots (defined in [Section 2.1](#)) of  $f \bmod p^k$ . Later we characterize each representative root as a “neighborhood” in [Theorem 19](#).

**Lemma 17** (perturb a root). *Let  $k > d(\Delta + 1)$  and let  $\bar{\alpha}$  be a root of  $f(x) \bmod p^k$  with  $l := v_p(\alpha_i - \bar{\alpha}) > \Delta + 1$ , for some  $i \in [n]$  (as in [Lemma 15](#)). Then, every  $\bar{\beta} \in \bar{\alpha} + p^l \mathbb{Z}$  is also a root of  $f(x) \bmod p^k$ .*

*Proof.* Since  $f(\bar{\alpha}) \equiv 0 \bmod p^k$ , we have  $v_p(f(\bar{\alpha})) \geq k$ . Using [Lemma 16](#) we have  $v_p(f_i(\bar{\alpha})) = v_p(f_i(\alpha_i)) = v_i$ . Thus,  $v_p(f(\bar{\alpha})) = v_p(\alpha_i - \bar{\alpha}) \cdot e_i + v_p(f_i(\bar{\alpha})) = v_p(\alpha_i - \bar{\alpha}) \cdot e_i + v_i \geq k$ .

Similarly,  $v_p(f(\bar{\beta})) = v_p(\alpha_i - \bar{\beta}) \cdot e_i + v_p(f_i(\bar{\beta})) = v_p(\alpha_i - \bar{\beta}) \cdot e_i + v_i \geq v_p(\alpha_i - \bar{\alpha}) \cdot e_i + v_i$ . The last inequality follows from  $v_p(\alpha_i - \bar{\beta}) \geq l = v_p(\alpha_i - \bar{\alpha})$ .

From the above two paragraphs we get  $v_p(f(\bar{\beta})) \geq k$ . Hence,  $f(\bar{\beta}) \equiv 0 \bmod p^k$ .  $\square$

Now we define a notion of “neighborhood” of a  $\mathbb{Z}_p$ -root of  $f$ .

**Definition 18** (neighborhood). For  $i \in [n]$ ,  $k > d(\Delta + 1)$ , we define the *neighborhood*  $S_{k,i}$  of  $\alpha_i \bmod p^k$  to be the set of all those roots of  $f \bmod p^k$  which are close to the  $\mathbb{Z}_p$ -root  $\alpha_i$  of  $f$ . Formally,

$$S_{k,i} := \{\bar{\alpha} \in \mathbb{Z}/\langle p^k \rangle \mid v_p(\bar{\alpha} - \alpha_i) > \Delta + 1, f(\bar{\alpha}) \equiv 0 \bmod p^k\}.$$

The notion of representative root was first given in [\[25\]](#). Below we discover its new properties which will lead us to an understanding of *length* of a representative root, which in turn will give us the size of a neighborhood contributing to  $N_k(f)$ .

**Theorem 19** (representative root is a neighborhood). *Let  $k > d(\Delta + 1)$  and let*

$$\mathbf{a} := a_0 + pa_1 + p^2a_2 + \cdots + p^{l-1}a_{l-1} + p^l \mathbb{Z}$$

*be a representative root of  $f(x) \bmod p^k$ . Define the  $\mathbb{Z}_p$ -root reduction  $\bar{\alpha}_i := \alpha_i \bmod p^k$ , for all  $i \in [n]$ . Fix an  $i \in [n]$ , then:*

- (1) *The length of  $\mathbf{a}$  is large. Formally,  $l > \Delta + 1$ .*
- (2) *If  $\bar{\alpha}_i \in \mathbf{a}$ , then  $\bar{\alpha}_j \notin \mathbf{a}$  for all  $j \neq i, j \in [n]$ . (This means, using [Lemma 15](#),  $\mathbf{a}$  has a uniquely associated  $\mathbb{Z}_p$ -root.)*
- (3) *If  $\mathbf{a}$  contains  $\bar{\alpha}_i$  then it also contains the respective neighborhood. In fact, if  $\bar{\alpha}_i \in \mathbf{a}$ , then  $S_{k,i} = \mathbf{a}$ .*

*Proof.* (1) Consider  $\bar{\alpha} := a_0 + pa_1 + \cdots + p^{l-1}a_{l-1}$ . By [Lemma 15](#), there exists a unique  $s \in [n]$  such that  $v_p(\bar{\alpha} - \alpha_s) > \Delta + 1$ . Suppose  $l \leq \Delta + 1$ . Then,  $v_p(\bar{\alpha} + p^{\Delta+1} - \alpha_s) = \Delta + 1$ . As,  $\bar{\alpha}' := (\bar{\alpha} + p^{\Delta+1})$  is also in  $\mathbf{a}$ , it again has to be close to a unique  $\alpha_t$ , with  $s \neq t \in [n]$  such that  $v_p(\bar{\alpha}' - \alpha_t) > \Delta + 1$ . In other words,  $\alpha_s + p^{\Delta+1} \equiv \bar{\alpha} + p^{\Delta+1} \equiv \alpha_t \bmod p^{\Delta+2}$ . Thus,  $v_p(\alpha_s - \alpha_t) = \Delta + 1 > \Delta/2$ , contradicting [Fact 12](#). This proves  $l > \Delta + 1$ .

(2) Consider distinct  $\bar{\alpha}_i, \bar{\alpha}_j \in \mathbf{a}$ . Then, by the definition of  $\mathbf{a}$ , we have  $v_p(\bar{\alpha}_i - \bar{\alpha}_j) \geq l > \Delta + 1 > \Delta/2$ , contradicting [Fact 12](#). Thus, there is a unique  $i$ .

(3) Suppose there exists a neighborhood element  $\bar{\beta} \notin \mathbf{a}$ , satisfying the conditions  $v_p(\alpha_i - \bar{\beta}) > \Delta + 1$  and  $f(\bar{\beta}) \equiv 0 \pmod{p^k}$ . Let  $j$  be the index of the first coordinate where  $\bar{\beta}$  and  $\mathbf{a}$  differ; so,  $j < l$  since  $\bar{\beta} \notin \mathbf{a}$ . Clearly,  $j > \Delta + 1$ ; otherwise, since  $\bar{\alpha}_i \in \mathbf{a}$  and  $\bar{\beta} \notin \mathbf{a}$ , we deduce  $v_p(\alpha_i - \bar{\beta}) = j \leq \Delta + 1$ , which is a contradiction.

By  $v_p(\alpha_i - \bar{\beta}) = j > \Delta + 1$  and [Lemma 17](#), we get that every element in  $\bar{\beta} + p^j \ast$  is a root of  $f(x) \pmod{p^k}$ , and consequently each element in  $a_0 + pa_1 + p^2a_2 + \cdots + p^{j-1}a_{j-1} + p^j \ast$  is a root of  $f(x) \pmod{p^k}$ , which contradicts that  $\mathbf{a}$  is a representative root (because  $j < l$ ; see [Definition 4](#)). Thus,  $\bar{\beta} \in \mathbf{a}$ , implying  $S_{k,i} \subseteq \mathbf{a}$ .

Conversely, consider  $\bar{\alpha} \in \mathbf{a}$ . Then, as before,  $v_p(\bar{\alpha}_i - \bar{\alpha}) \geq l > \Delta + 1$ , implying  $\bar{\alpha} \in S_{k,i}$ . So,  $S_{k,i} \supseteq \mathbf{a}$ .  $\square$

Next, we get the expression for the length of a representative root.

**Theorem 20.** *For  $k > d(\Delta + 1)$ , the representative roots of  $f(x) \pmod{p^k}$  are in a one-to-one correspondence with  $\mathbb{Z}_p$ -roots of  $f$ . Moreover, the length of the representative root  $\mathbf{a}$ , corresponding to  $\alpha_i$ , is  $l_{i,k} := \lceil (k - v_i)/e_i \rceil$ .*

*Proof.* By [Proposition 3](#), every root of  $f \pmod{p^k}$  is in exactly one of the representative roots. So each reduced  $\mathbb{Z}_p$ -root  $\bar{\alpha}_i := \alpha_i \pmod{p^k}$  is in a unique representative root. Thus, by parts (2) and (3) of [Theorem 19](#), we get the one-to-one correspondence as claimed.

Consider a  $p$ -adic integer  $\bar{\alpha}$  with  $v_p(\bar{\alpha} - \alpha_i) =: l_{\bar{\alpha}} > \Delta$ . We have the following equivalences:

$$\begin{aligned} \bar{\alpha} \in \mathbf{a} &\iff v_p(f(\bar{\alpha})) \geq k \iff v_p((\bar{\alpha} - \alpha_i)^{e_i} \cdot f_i(\bar{\alpha})) \geq k \iff e_i l_{\bar{\alpha}} + v_i \geq k \quad (\text{by } \textcolor{blue}{\text{Lemma 16}}) \\ &\iff l_{\bar{\alpha}} \geq \lceil (k - v_i)/e_i \rceil = l_{i,k}. \end{aligned}$$

Write the representative root corresponding to  $\alpha_i$  as  $\mathbf{a} =: a_0 + pa_1 + p^2a_2 + \cdots + p^{l-1}a_{l-1} + p^l \ast$ . Clearly,  $l = \min\{l_{\bar{\alpha}} \mid \bar{\alpha} \in \mathbf{a}\} \geq l_{i,k}$ . Note that if  $l > l_{i,k}$  then by the equivalences we could reduce the length  $l$  of the representative root  $\mathbf{a}$ , which is a contradiction. Thus,  $l = l_{i,k}$ .  $\square$

**3.3. Formula for  $N_k(f)$  — Proof of [Corollary 2](#).** For large enough  $k$ , the previous section gives us an easy way to count the roots. In fact, we have the following simple formula for  $N_k(f)$ .

**Theorem 21** (roots mod  $p^k$ ). *For  $k > d(\Delta + 1)$ ,  $N_k(f) = \sum_{i \in [n]} p^{k - \lceil (k - v_i)/e_i \rceil}$ , where clearly  $v_i, e_i$  and  $n$  (as in [Section 2.2](#)) are independent of  $k$ .*

*Proof.* Fix  $i \in [n]$  and  $k > d(\Delta + 1)$ . By [Theorem 20](#) we get that in the unique representative root  $\mathbf{a}$ , corresponding to  $\alpha_i \pmod{p^k}$ , the  $(k - \lceil (k - v_i)/e_i \rceil)$ -many higher-precision coordinates could be set arbitrarily from  $[0, \dots, p - 1]$  (while the rest, the lower-precision ones, are fixed). That gives us the count via contribution for each  $i \in [n]$ . Moreover, the sum over neighborhoods, for each  $i \in [n]$ , gives us exactly  $N_k(f)$ .

Also, note that if  $n = 0$  then the count  $N_k(f)$  is equal to 0.  $\square$

*Proof of [Corollary 2](#).* [Theorem 21](#) gives a closed form expression for  $N_k(f)$ , when

$$k \geq k_0 := d(\Delta + 1) + 1 \leq d(2d - 1)(\log_p C + \log_p d) + 1.$$

For the other part, note the discriminant  $D(f)$  is not equal to 0 if and only if  $f$  is squarefree. In the squarefree case  $e_i = 1$ , for all  $i \in [n]$ . By [Theorem 21](#),  $N_k(f) = \sum_{i \in [n]} p^{v_i}$ , which is independent of  $k$ .  $\square$

**3.4. Computing Poincaré series — Proof of [Theorem 1](#).** Building upon the ideas of the previous sections, we will show how to deterministically compute Poincaré series  $P(t) = \sum_{k=0}^{\infty} N_k(f)(p^{-1}t)^k$  associated to the input  $f(x)$  efficiently, thereby proving [Theorem 1](#). Before that, we need some notation:

Set  $k_0 := d(\Delta + 1) + 1$  so we know by [Theorem 21](#) that for  $k \geq k_0$ ,  $N_k(f) = \sum_{i=1}^n N_{k,i}(f)$ , where  $N_{k,i}(f) := p^{k - \lceil (k - v_i)/e_i \rceil}$ . For each  $i \in [n]$ , define  $k_i$  to be the least integer such that  $k_i \geq k_0$  and  $(k_i - v_i)/e_i$  is an integer. Then, Poincaré series  $P(t)$  can be partitioned into finite and infinite sums as

$$P(t) = P_0(t) + \sum_{i=1}^n P_i(t),$$

where

$$P_i(t) := \sum_{k=k_i}^{\infty} N_{k,i}(f) \cdot (p^{-1}t)^k \quad \text{and} \quad P_0(t) := \left( \sum_{k=0}^{k_0-1} N_k(f) \cdot (p^{-1}t)^k \right) + \sum_{i=1}^n \sum_{k=k_0}^{k_i-1} N_{k,i}(f) \cdot (p^{-1}t)^k.$$

We now compute the multiplicity  $e_i$  by viewing it as the *step* that increments the length of the representative root associated to  $\alpha_i$  as  $k$  keeps growing above  $k_0$ .

**Lemma 22** (compute  $e_i$ ). *We can compute the number of  $\mathbb{Z}_p$ -roots  $n$  of  $f$  as well as  $k_i$ ,  $v_i$  and  $e_i$ , for each  $i \in [n]$ , in deterministic  $\text{poly}(d, \log C + \log p)$ -time.*

*Proof.* By [Theorem 7](#), we get all representative roots of  $f \bmod p^k$  implicitly in the form of maximal split ideals (for brevity, we call these split ideals). By [Lemma 6](#), the length of a split ideal is also the length of all representative roots represented by it and the degree is the number of representative roots represented by it. Since, by [Theorem 20](#),  $n$  is also the number of representative roots of  $f \bmod p^k$  for  $k \geq k_0$ , we run the algorithm of [Theorem 7](#) for  $k = k_0$  and sum up the degree of all split ideals obtained, to get  $n$ .

Suppose the split ideal  $I$  we find contains a representative root  $\mathbf{a}$  of  $f \bmod p^k$  corresponding to  $\alpha_i$ , with  $k_i$  as defined before. How do we compute  $k_i$ ? By [Theorem 20](#), the length of  $\mathbf{a}$ , when  $k = k_i$ , is  $l_{i,k_i} = (k_i - v_i)/e_i$ . Now, for all  $k = k_i + 1, k_i + 2, \dots, k_i + e_i$ , the length  $l_{i,k}$  remains equal to  $l_{i,k_i} + 1$ , while for the next  $k = k_i + e_i + 1$ ,  $l_{i,k}$  increments by one.

So we run the algorithm of [Theorem 7](#) for several  $k \geq k_0$ . When we find the length incrementing by one, namely, at the two values  $k = k_i + 1$  and  $k = k'_i := k_i + 1 + e_i$ , then we have found  $e_i$  (and  $k_i$ ). From the equation,  $k_i - v_i = e_i \cdot l_{i,k_i}$ , we also find  $v_i$ .

Suppose the split ideal  $I$  we find contains *two* representative roots  $\mathbf{a}$  and  $\mathbf{b} \bmod p^k$ , corresponding to  $\mathbb{Z}_p$ -roots  $\alpha_i$  and  $\alpha_j$  respectively, such that  $e_i \neq e_j$  (without loss of generality, say,  $e_i < e_j$ ). In this case, even if  $\mathbf{a}$  and  $\mathbf{b}$  have the same length, when  $k = k_i$ , they will evolve to different length representative roots when we go to a “higher-precision” arithmetic mod  $p^{k_i+1+e_i}$  (by the formula in [Theorem 20](#)). So  $\mathbf{a}, \mathbf{b}$  must lie in different length split ideals, say,  $I_a$  and  $I_b$  respectively.

Now, for another representative root  $\mathbf{c}$  in  $I_a$ , say corresponding to  $\alpha_s$ , we have  $e_i = e_s$  and hence  $v_i = v_s$ . By computing  $e_i$  and  $v_i$  as before, now using the length of  $I$  and  $I_a$ , we compute  $e_s$  and  $v_s$ .

(and  $k_s$ ) for every  $\mathbf{c}$  in  $I_a$ . Since, by [Lemma 6](#), the degree of  $I_a$  is the number of such representative roots in  $I_a$ , we can compute  $n$ ; moreover, we get  $k_i, v_i, e_i$  for all  $i \in [n]$ .

Clearly, we need to run the algorithm of [Theorem 7](#) at most  $2 \max_{i \in [n]} \{e_i\} = O(d)$  times, to study the evolution of split ideals (implicitly, that of the underlying representative roots). Also  $\Delta$  is the logarithm (to base  $p$ ) of the determinant of a Sylvester matrix which gives  $\Delta = O(d \cdot (\log_p C + \log_p d))$ . So, the algorithm runs in polynomial time as claimed.  $\square$

Now we prove that the infinite sums  $P_i(t)$  are formally equal to rational functions of  $t = p^{-s}$ .

**Lemma 23** (infinite sums are rational). *For each  $i \in [n]$ , the series  $P_i(t)$  is a rational function of  $t$  as*

$$P_i(t) = \frac{t^{k_i} \cdot (p - t(p - 1) - t^{e_i})}{p^{(k_i - v_i)/e_i} \cdot (1 - t) \cdot (p - t^{e_i})}.$$

*Proof.* Recall that  $P_i(t) = \sum_{k=k_i}^{\infty} N_{k,i}(f) \cdot (p^{-1}t)^k$ . For simplicity write  $T := p^{-1}t$  and define an integer  $\delta_i := k_i - (k_i - v_i)/e_i$ . Now  $P_i$  can be rewritten using residues mod  $e_i$  as

$$P_i(t) = \sum_{l=k_i}^{k_i+e_i-1} \sum_{k=0}^{\infty} N_{l+ke_i,i}(f) \cdot T^{l+ke_i}.$$

For simplicity take  $l = k_i$  and consider the sum,  $\sum_{k=0}^{\infty} N_{k_i+ke_i,i}(f) \cdot T^{k_i+ke_i}$ . We find that  $N_{k_i,i}(f) = p^{\delta_i}$ ,  $N_{k_i+e_i,i}(f) = p^{\delta_i+e_i-1}$ ,  $N_{k_i+2e_i,i}(f) = p^{\delta_i+2(e_i-1)}$ , and so on. Hence,  $\sum_{k=0}^{\infty} N_{k_i+ke_i,i}(f) \cdot T^{k_i+ke_i} = p^{\delta_i} T^{k_i} \cdot [1 + p^{e_i-1} T^{e_i} + (p^{e_i-1} T^{e_i})^2 + \dots] = p^{\delta_i} \cdot T^{k_i} / (1 - p^{e_i-1} T^{e_i})$ . So

$$\begin{aligned} P_i(t) &= \frac{p^{\delta_i} T^{k_i}}{1 - p^{e_i-1} T^{e_i}} + \frac{p^{\delta_i} T^{k_i+1}}{1 - p^{e_i-1} T^{e_i}} + \frac{p^{\delta_i+1} T^{k_i+2}}{1 - p^{e_i-1} T^{e_i}} + \dots + \frac{p^{\delta_i+e_i-2} T^{k_i+e_i-1}}{1 - p^{e_i-1} T^{e_i}} \\ &= \frac{p^{\delta_i} T^{k_i}}{1 - p^{e_i-1} T^{e_i}} + \frac{p^{\delta_i} T^{k_i+1}}{1 - p^{e_i-1} T^{e_i}} \cdot (1 + pT + (pT)^2 + \dots + (pT)^{e_i-2}) \\ &= \frac{p^{\delta_i} T^{k_i}}{1 - p^{e_i-1} T^{e_i}} \cdot \left( 1 + T \cdot \frac{1 - (pT)^{e_i-1}}{1 - pT} \right). \end{aligned}$$

Putting  $T = t/p$  and  $\delta_i = k_i - (k_i - v_i)/e_i$  we get

$$P_i(t) = \frac{t^{k_i} (p - t(p - 1) - t^{e_i})}{p^{(k_i - v_i)/e_i} (1 - t) (p - t^{e_i})}.$$

$\square$

Now we are in a position to prove our main theorem.

*Proof of Theorem 1.* Recall  $P(t) = P_0(t) + \sum_{i=1}^n P_i(t)$ . We first compute  $P_0(t)$ , which is the sum of two polynomials in  $t$ , namely,

$$Q_1(t) := \sum_{j=0}^{k_0-1} N_j(f) (p^{-1}t)^j \quad \text{and} \quad Q_2(t) = \sum_{i=1}^n \sum_{l=k_0}^{k_i-1} N_{l,i}(f) (p^{-1}t)^l,$$

both of degree  $O(d\Delta)$ . By a standard determinant or Sylvester matrix calculation one shows  $d\Delta \leq O(d^2 \cdot (\log_p C + \log_p d))$ .



We can compute the polynomial  $Q_1(t)$  in deterministic  $\text{poly}(d, \log C + \log p)$ -time by calling the root-counting algorithm of [24] (Theorem 7)  $k_0 - 1$  times, getting each  $N_j(f)$ , for  $j = 1, \dots, k_0 - 1$  (note:  $N_0(f) := 1$ ).

Polynomial  $Q_2(t)$  is a sum of  $n \leq d$  polynomials, each with  $k_i - k_0 \leq d$  many simple terms. Using Lemma 22, we can compute each  $v_i, e_i$ , hence,  $N_{l,i}(f)$ . So, computation of  $Q_2$  again takes time  $\text{poly}(d, \log C + \log p)$ .

Lemma 23 gives us the rational form expression for  $P_i(t)$ , for each  $i \in [n]$ . So, using Lemma 22 we can compute the Poincaré series

$$P(t) = P_0(t) + \sum_{i=1}^n \frac{t^{k_i} (p - t(p-1) - t^{e_i})}{p^{(k_i - v_i)/e_i} (1-t)(p - t^{e_i})}$$

in deterministic  $\text{poly}(d, \log C + \log p)$ -time.

By inspecting the above expression, the degree of the denominator  $B(t)$  is  $1 + \sum_{i=1}^n e_i = O(d)$ . The degree of the numerator  $A(t)$  is  $\leq k_0 + 2d \leq O(d^2 \cdot (\log_p C + \log_p d))$ .  $\square$

#### 4. Conclusion and open questions

We presented the first complete solution to the problem of computing Igusa's local zeta function for any given integral univariate polynomial and a prime  $p$ . Indeed, our methods work for given  $f \in \mathbb{Z}_p[x]$  (with  $f$  having computable representation) as our proof for integral  $f$  goes via considering its factorization over  $\mathbb{Z}_p$  (Section 2.2).

We also found an explicit closed-form expression for  $N_k(f)$  and efficiently computed the explicit parameters involved therein, which could be used to compute Greenberg's constants associated with a univariate  $f$  and a prime  $p$ . Greenberg's constants appear in a classical theorem of Greenberg [29, Theorem 1] which is a generalization of Hensel's lemma to several  $n$ -variate polynomials. We hope that our methods for the one variable case could be generalized to compute Greenberg's constants for the  $n$  variable case to give an effective version of Greenberg's theorem.

We also hope that our methods extend computing Igusa's local zeta function from characteristic zero ( $\mathbb{Z}_p$ ) to positive characteristic ( $\mathbb{F}_p[[T]]$ ) at least if some standard restrictions are imposed on the characteristic, for example,  $p$  is "large enough". This is supported by the fact that the root counting algorithm of [24] also extends to  $\mathbb{F}[[T]]$  for a field  $\mathbb{F}$ .

The following important open questions need to be addressed:

- (1) A natural question to study is whether we could generalize our method to compute Igusa's local zeta function for  $n$ -variate integral polynomials (say,  $n = 2$ ?). Note that for growing  $n$  this problem is at least #P-hard [26].
- (2) A related problem is of counting roots of  $n$ -variate polynomials mod prime power  $p^k$ . We know an efficient quantum algorithm mod  $p$  for  $n = 2$  due to Kedlaya [37]. Kedlaya further asks, if we can reduce the problem of counting points mod  $p^k$  to counting points mod  $p$  for fixed  $k$  and  $n = 2$ . This question has affirmative answer known only for variable-separated curves due to Robelle et al. [55].



- (3) Following up the problem of point counting on curves for constant  $k$ , we ask another important related open question — how to find a single point on curves mod  $p^k$  efficiently. It has an application in factoring a univariate  $f(x) \bmod p^k$  [25]. Can we efficiently reduce finding a single point mod  $p^k$  to finding a single point mod  $p$ , even for fixed  $k$  and  $n = 2$ ?

### Acknowledgements

We thank anonymous reviewers for their helpful comments and pointing out relevant references to improve the draft of the paper. In particular we thank them for their suggestion which greatly improved the conclusion section and for pointing out a connection to Greenberg's work. We thank Kiran Kedlaya for pointing out some minor corrections and asking a relevant open question (Section 4, open question (2)) during the conference ANTS '20. Nitin Saxena thanks the funding support from DST (DST/SJF/MSA-01/2013-14) and N. Rama Rao Chair.

### References

- [1] V Albis and WA Zúñiga-Galindo, *An elementary introduction to the theory of Igusa local zeta functions*, Lect. Mat **20** (1999), no. 1, 5–33.
- [2] Michael Anshel and Dorian Goldfeld, *Zeta functions, one-way functions, and pseudorandom number generators*, Duke Math. J. **88** (1997), no. 2, 371–390.
- [3] Michael Anshel and Dorian Goldfeld, *Multi-purpose high speed cryptographically secure sequence generator based on zeta-one-way functions*, May 12 1998, US Patent 5,751,808.
- [4] Jérémy Berthomieu, Grégoire Lecerf, and Guillaume Quintin, *Polynomial root finding over local rings and application to error correcting codes*, Applicable Algebra in Engineering, Communication and Computing **24** (2013), no. 6, 413–443, <https://link.springer.com/article/10.1007/s00200-013-0200-5>.
- [5] Manjul Bhargava, *P-orderings and polynomial functions on arbitrary subsets of Dedekind rings*, Journal für die Reine und Angewandte Mathematik **490** (1997), 101–128.
- [6] Edward Bierstone, *Canonical desingularization in characteristic zero by blowing up the maximum strata of a local invariant*, Inventiones mathematicae **128** (1997), no. 2, 207–302.
- [7] Edward Bierstone, Dima Grigoriev, Pierre Milman, and Jarosław Włodarczyk, *Effective Hironaka resolution and its complexity*, Asian Journal of Mathematics **15** (2011), no. 2, 193–228.
- [8] Gábor Bodnár and Josef Schicho, *Automated resolution of singularities for hypersurfaces*, Journal of Symbolic Computation **30** (2000), no. 4, 401–428.
- [9] Gábor Bodnár and Josef Schicho, *A computer program for the resolution of singularities*, Resolution of singularities, Springer, 2000, pp. 231–238.
- [10] David G Cantor and Daniel M Gordon, *Factoring polynomials over  $p$ -adic fields*, International Algorithmic Number Theory Symposium, Springer, 2000, pp. 185–208.
- [11] Edwin León Cardenal, *An algorithm for computing the local zeta function of an hyperelliptic curve*.
- [12] Qi Cheng, Shuhong Gao, J Maurice Rojas, and Daqing Wan, *Counting roots of polynomials over prime power rings*, Thirteenth Algorithmic Number Theory Symposium, ANTS-XIII, Mathematical Sciences Publishers, 2018, arXiv:1711.01355.
- [13] AL Chistov, *Efficient factorization of polynomials over local fields*, Dokl. Akad. Nauk SSSR **293** (1987), no. 5, 1073–1077.
- [14] AL Chistov, *Algorithm of polynomial complexity for factoring polynomials over local fields*, Journal of mathematical sciences **70** (1994), no. 4, 1912–1933.

- [15] M Chojnacka-Pniewska, *Sur les congruences aux racines données*, Annales Polonici Mathematici, vol. 3, Instytut Matematyczny Polskiej Akademii Nauk, 1956, pp. 9–12.
- [16] J Brian Conrey, *The riemann hypothesis*, Notices of the AMS **50** (2003), no. 3, 341–353.
- [17] Raemeon A Cowan, Daniel J Katz, and Lauren M White, *A new generating function for calculating the Igusa local zeta function*, Advances in Mathematics **304** (2017), 355–420.
- [18] Bruce Dearden and Jerry Metzger, *Roots of polynomials modulo prime powers*, European Journal of Combinatorics **18** (1997), no. 6, 601–606.
- [19] Pierre Deligne, *La conjecture de Weil. I*, Publications Mathématiques de l’Institut des Hautes Études Scientifiques **43** (1974), no. 1, 273–307.
- [20] Jan Denef, *The rationality of the Poincaré series associated to the  $p$ -adic points on a variety*, Inventiones mathematicae **77** (1984), no. 1, 1–23.
- [21] Jan Denef et al., *Local zeta functions and Euler characteristics*, Duke Mathematical Journal **63** (1991), no. 3, 713–721.
- [22] Jan Denef and Kathleen Hoornaert, *Newton polyhedra and Igusa’s local zeta function*, Journal of number Theory **89** (2001), no. 1, 31–64.
- [23] Marcus PF du Sautoy and Fritz Grunewald, *Analytic properties of zeta functions and subgroup growth*, Ann. of Math.(2) **152** (2000), no. 3, 793–833.
- [24] Ashish Dwivedi, Rajat Mittal, and Nitin Saxena, *Counting basic-irreducible factors mod  $p^k$  in deterministic poly-time and  $p$ -adic applications*, Computational Complexity Conference (2019), <https://www.cse.iitk.ac.in/users/nitin/papers/basic-irred-mod-pk.pdf>.
- [25] Ashish Dwivedi, Rajat Mittal, and Nitin Saxena, *Efficiently factoring polynomials modulo  $p^4$* , The 44th International Symposium on Symbolic and Algebraic Computation (ISSAC) (2019), <https://www.cse.iitk.ac.in/users/nitin/papers/factor-mod-p4.pdf>.
- [26] Andrzej Ehrenfeucht and Marek Karpinski, *The Computational Complexity of (XOR, AND)-Counting Problems*, International Computer Science Inst., 1990.
- [27] Emilio Elizalde, *Applications of zeta function regularization in QFT*, Quantum Field Theory Under the Influence of External Conditions, Springer, 1996, pp. 122–130.
- [28] Michael R Garey and David S Johnson, *Computers and intractability*, vol. 174, freeman San Francisco, 1979.
- [29] Marvin J Greenberg, *Rational points in henselian discrete valuation rings*, Publications Mathématiques de l’IHÉS **31** (1966), 59–64.
- [30] Alexander Grothendieck, *Formule de Lefschetz et rationalité des fonctions L*, Séminaire Bourbaki **9** (1964), 41–55.
- [31] Stephen W Hawking, *Zeta function regularization of path integrals in curved spacetime*, Communications in Mathematical Physics **55** (1977), no. 2, 133–148.
- [32] Denis Ibadula, *On the plane cubics over  $\mathbb{Q}_p$  and the associated igusa zeta function*, Bull. Math. Soc. Sci. Math. Roumanie (NS) **49** (2005), no. 97, 3.
- [33] Jun-ichi Igusa, *An introduction to the theory of local zeta functions*, AMS/IP Studies in Advanced Mathematics, vol. 14, American Mathematical Society, Providence, RI; International Press, Cambridge, MA.
- [34] Jun-ichi Igusa, *Complex powers and asymptotic expansions. I. Functions of certain types.*, Journal für die reine und angewandte Mathematik **268** (1974), 110–130.
- [35] Jun-ichi Igusa, *Complex powers and asymptotic expansions. II.*, Journal für die reine und angewandte Mathematik **278** (1975), 307–321.
- [36] Jun-ichi Igusa and S Raghavan, *Lectures on forms of higher degree*, vol. 59, Springer Berlin-Heidelberg-New York, 1978.
- [37] Kiran S Kedlaya, *Quantum computation of zeta functions of curves*, computational complexity **15** (2006), no. 1, 1–19.
- [38] Adam Klivans, *Factoring polynomials modulo composites*, tech. report, Carnegie-Mellon Univ, Pittsburgh PA, Dept of CS, 1997.
- [39] Benjamin Klopsch and Christopher Voll, *Igusa-type functions associated to finite formed spaces and their functional equations*, Transactions of the American Mathematical Society **361** (2009), no. 8, 4405–4436.

- [40] Benjamin Klopsch and Christopher Voll, *Zeta functions of three-dimensional  $p$ -adic Lie algebras*, *Mathematische Zeitschrift* **263** (2009), no. 1, 195–210.
- [41] Neal Koblitz,  *$p$ -adic numbers,  $p$ -adic Numbers,  $p$ -adic Analysis, and Zeta-Functions*, Springer, 1977, pp. 1–20.
- [42] Leann Kopp, Natalie Randall, Joseph Rojas, and Yuyu Zhu, *Randomized polynomial-time root counting in prime power rings*, *Mathematics of Computation* (2019).
- [43] Alan GB Lauder, *Counting solutions to equations in many variables over finite fields*, *Foundations of Computational Mathematics* **4** (2004), no. 3, 221–267.
- [44] Edwin León-Cardenal and WA Zúñiga-Galindo, *An introduction to the theory of local zeta functions from scratch*, *Revista Integración* **37** (2019), no. 1, 45–76.
- [45] Xiangdong Li and M Anshel, *Application of zeta function to quantum cryptography*, *Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop*, IEEE, 2005, pp. 430–431.
- [46] Rudolf Lidl and Harald Niederreiter, *Introduction to finite fields and their applications*, Cambridge university press, 1994.
- [47] Shaowei Lin, *Ideal-theoretic strategies for asymptotic approximation of marginal likelihood integrals.*, *Journal of Algebraic Statistics* **8** (2017), no. 1.
- [48] Benjamin D Marko, Jeffrey M Riedl, et al., *Igusa local zeta function of the polynomial  $f(x) = x_1^m + x_2^m + \cdots + x_m^m$* , (2005).
- [49] Daveshe Maulik, *Root sets of polynomials modulo prime powers*, *Journal of Combinatorial Theory, Series A* **93** (2001), no. 1, 125–140.
- [50] Diane Meuser, *A survey of Igusa's local zeta function*, *American Journal of Mathematics* **138** (2016), no. 1, 149–179.
- [51] Joseph Polchinski, *String theory: Volume 1, an introduction to the bosonic string*, Cambridge university press, 1998.
- [52] H Reichardt, *SI Borewicz und IR Safarevic, Zahlentheorie. (Mathematische Reihe, Band 32). 468 S. Basel/Stuttgart 1966. Birkhäuser Verlag. Preis geb. sFr. 56,-, Zeitschrift Angewandte Mathematik und Mechanik* **49** (1969), 187–187.
- [53] Nicolai Reshetikhin and Boris Vertman, *Combinatorial quantum field theory and gluing formula for determinants*, *Letters in Mathematical Physics* **105** (2015), no. 3, 309–340.
- [54] Bernhard Riemann, *Über die Anzahl der Primzahlen unter einer gegebenen Grosse*, *Ges. Math. Werke und Wissenschaft. Nachlaß* **2** (1859), 145–155.
- [55] Caleb Robelle, J Maurice Rojas, and Yuyu Zhu, *Sub-linear point counting for variable separated curves over prime power rings*, manuscript, <https://www.math.tamu.edu/rojas/curve.pdf>.
- [56] Margaret M Robinson, *The Igusa local zeta function associated with the singular cases of the determinant and the Pfaffian*, *Journal of number theory* **57** (1996), no. 2, 385–408.
- [57] Barry Robson, *Clinical and pharmacogenomic data mining: 3. Zeta theory as a general tactic for clinical bioinformatics*, *Journal of proteome research* **4** (2005), no. 2, 445–455.
- [58] M Saia and WA Zúñiga-Galindo, *Local zeta function for curves, non-degeneracy conditions and Newton polygons*, *Transactions of the American Mathematical Society* **357** (2005), no. 1, 59–88.
- [59] Yiannis Sakellaridis, *On the unramified spectrum of spherical varieties over  $p$ -adic fields*, *Compositio Mathematica* **144** (2008), no. 4, 978–1016.
- [60] Ana Sălăgean, *Factoring polynomials over  $\mathbb{Z}_4$  and over certain Galois rings*, *Finite fields and their applications* **11** (2005), no. 1, 56–70.
- [61] Dirk Segers and WA Zúñiga-Galindo, *Exponential sums and polynomial congruences along  $p$ -adic submanifolds*, *Finite Fields and Their Applications* **17** (2011), no. 4, 303–316.
- [62] Wacław Sierpiński, *Remarques sur les racines d'une congruence*, *Annales Polonici Mathematici* **1** (1955), no. 1, 89–90.
- [63] Carlo Sircana, *Factorization of polynomials over  $\mathbb{Z}/(p^n)$* , *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*, ACM, 2017, pp. 405–412.
- [64] Edward Charles Titchmarsh and DR Heath-Brown, *The theory of the Riemann zeta-function*, Oxford University Press, 1986.

- [65] John Jaime Rodriguez Vega, *The Igusa local zeta function for  $x^q - a$* , *Lecturas Matemáticas* **26** (2005), no. 2, 173–176.
- [66] Willem Veys, *Zeta functions for curves and log canonical models*, *Proceedings of the London Mathematical Society* **74** (1997), no. 2, 360–378.
- [67] Orlando Villamayor, *Constructiveness of Hironaka’s resolution*, *Annales scientifiques de l’École Normale Supérieure*, vol. 22, 1989, pp. 1–32.
- [68] Christopher Voll, *Functional equations for zeta functions of groups and rings*, *Annals of mathematics* (2010), 1181–1218.
- [69] Joachim Von Zur Gathen and Jürgen Gerhard, *Modern computer algebra*, Cambridge university press, 2013.
- [70] Joachim von zur Gathen and Silke Hartlieb, *Factorization of polynomials modulo small prime powers*, tech. report, Paderborn Univ, 1996.
- [71] Joachim von zur Gathen and Silke Hartlieb, *Factoring modular polynomials*, *Journal of Symbolic Computation* **26** (1998), no. 5, 583–606, (Conference version in ISSAC’96).
- [72] Sumio Watanabe, *Algebraic geometry and statistical learning theory*, vol. 25, Cambridge University Press, 2009.
- [73] André Weil, *Variétés abéliennes et courbes algébriques*, Paris: Hermann, 1948.
- [74] André Weil, *Numbers of solutions of equations in finite fields*, *Bull. Amer. Math. Soc* **55** (1949), no. 5, 497–508.
- [75] André Weil, *Sur certains groupes d’opérateurs unitaires*, *Acta mathematica* **111** (1964), no. 143–211, 14.
- [76] André Weil, *Sur la formule de Siegel dans la théorie des groupes classiques*, *Acta mathematica* **113** (1965), 1–87.
- [77] Keith R Willison, *An intracellular calcium frequency code model extended to the Riemann zeta function*, [arXiv:1903.07394](https://arxiv.org/abs/1903.07394) (2019).
- [78] Yuyu Zhu, *Trees, point counting beyond fields, and root separation*, Ph.D. thesis, Texas A&M University, 2020.
- [79] WA Zúñiga-Galindo, *Igusa’s local zeta functions of semiquasihomogeneous polynomials*, *Transactions of the American Mathematical Society* **353** (2001), no. 8, 3193–3207.
- [80] WA Zúñiga-Galindo, *Computing Igusa’s local zeta functions of univariate polynomials, and linear feedback shift registers*, *Journal of Integer Sequences* **6** (2003), no. 2, 3.
- [81] WA Zúñiga-Galindo, *Local zeta functions and Newton polyhedra*, *Nagoya Mathematical Journal* **172** (2003), 31–58.
- [82] WA Zúñiga-Galindo, *Pseudo-differential equations connected with  $p$ -adic forms and local zeta functions*, *Bulletin of the Australian Mathematical Society* **70** (2004), no. 1, 73–86.
- [83] WA Zúñiga-Galindo, *Decay of solutions of wave-type pseudo-differential equations over  $p$ -adic fields*, *Publications of the Research Institute for Mathematical Sciences* **42** (2006), no. 2, 461–479.
- [84] WA Zúñiga-Galindo, *Local zeta functions supported on analytic submanifolds and Newton polyhedra*, *International Mathematics Research Notices* **2009** (2009), no. 15, 2855–2898.
- [85] WA Zúñiga-Galindo, *Local zeta functions and fundamental solutions for pseudo-differential operators over  $p$ -adic fields*,  *$p$ -adic Numbers, Ultrametric Analysis, and Applications* **3** (2011), no. 4, 344–358.

Received 22 Feb 2020. Revised 24 Feb 2020.

ASHISH DWIVEDI: [ashish@cse.iitk.ac.in](mailto:ashish@cse.iitk.ac.in)

Department of Computer Science and Engineering, Indian Institute of Technology Kanpur, Kanpur, India

NITIN SAXENA: [nitin@cse.iitk.ac.in](mailto:nitin@cse.iitk.ac.in)

Department of Computer Science and Engineering, Indian Institute of Technology Kanpur, Kanpur, India

# Computing endomorphism rings of supersingular elliptic curves and connections to path-finding in isogeny graphs

Kirsten Eisenträger, Sean Hallgren, Chris Leonardi, Travis Morrison, and Jennifer Park

Computing endomorphism rings of supersingular elliptic curves is an important problem in computational number theory, and it is also closely connected to the security of some of the recently proposed isogeny-based cryptosystems. We give a new algorithm for computing the endomorphism ring of a supersingular elliptic curve  $E$  defined over  $\mathbb{F}_{p^2}$  that runs, under certain heuristics, in time  $O((\log p)^2 p^{1/2})$ . The algorithm works by first finding two cycles of a certain form in the supersingular  $\ell$ -isogeny graph  $G(p, \ell)$ , generating an order  $\Lambda \subseteq \text{End}(E)$ . Then all maximal orders containing  $\Lambda$  are computed, extending work of Voight (2013). The final step is to determine which of these maximal orders is the endomorphism ring. As part of the cycle-finding algorithm, we give a lower bound on the set of all  $j$ -invariants  $j$  that are adjacent to  $j^p$  in  $G(p, \ell)$ , answering a question of Arpin et al. (2019).

We also give a polynomial-time reduction from computing  $\text{End}(E)$  to path-finding in the  $\ell$ -isogeny graph which is simpler in several ways than previous ones. We show that this reduction leads to another algorithm for computing endomorphism rings which runs in time  $\tilde{O}(p^{1/2})$ . This allows us to break the second preimage resistance of a hash function in the family constructed by Charles, Goren and Lauter.

## 1. Introduction

Computing the endomorphism ring of an elliptic curve defined over a finite field is a fundamental problem in computational arithmetic geometry. For ordinary elliptic curves the fastest algorithm is due to Bisson and Sutherland [5] who gave a subexponential time algorithm to solve this problem. No subexponential time algorithm is known for general supersingular elliptic curves.

Computing endomorphism rings of supersingular elliptic curves has emerged as a central problem for isogeny-based cryptography. The first cryptographic application of isogenies between supersingular

---

Eisenträger was partially supported by National Science Foundation award CNS-1617802 and a Vannevar Bush Faculty Fellowship from the US Department of Defense. Hallgren was partially supported by National Science Foundation awards CCF-1618287, CNS-1617802, and a Vannevar Bush Faculty Fellowship from the US Department of Defense. Morrison was supported by the Natural Sciences and Engineering Research Council of Canada, the Canada First Research Excellence Fund, CryptoWorks21, Public Works and Government Services Canada, and the Royal Bank of Canada. Park was partially supported by National Science Foundation award DMS-1902199. This work was done in part while Eisenträger and Hallgren were visiting the Simons Institute for the Theory of Computing.

*MSC2010:* 11T71, 14G50, 14H52, 14Q05.

*Keywords:* supersingular elliptic curves, endomorphism ring, isogeny-based cryptography, quaternion algebras, isogeny graph.

elliptic curves was the hash function in [9]. An efficient algorithm for computing the endomorphism ring of a supersingular elliptic curve would, under certain assumptions, completely break this hash function and also SIKE [18; 2]. It would also have a major impact on the security of CSIDH [7].

Computing the endomorphism ring of a supersingular elliptic curve  $E$  was first studied by Kohel [20, Theorem 75], who gave an approach for generating a subring of finite index of the endomorphism ring  $\text{End}(E)$ . The algorithm was based on finding cycles in the  $\ell$ -isogeny graph of supersingular elliptic curves in characteristic  $p$ , and the running time of the probabilistic algorithm was  $O(p^{1+\varepsilon})$ . In this paper we complete Kohel's approach by showing how to compute  $\text{End}(E)$  from a suborder when the order is Bass. In a different direction, in [14] it is argued that heuristically one expects  $O(\log p)$  calls to a cycle-finding algorithm until the cycles generate  $\text{End}(E)$ . An algorithm for computing powersmooth endomorphisms with complexity  $\tilde{O}(p^{1/2})$  and polynomial storage is given by Delfs and Galbraith [11].

One can also compute  $\text{End}(E)$  using an isogeny  $\phi : \tilde{E} \rightarrow E$ , where  $\tilde{E}$  is an elliptic curve with known endomorphism ring. McMurdy was the first to compute  $\text{End}(E)$  via such an approach [24], but did not determine its complexity. In [14] a polynomial-time reduction from computing  $\text{End}(E)$  to finding an isogeny  $\phi$  of powersmooth degree was given assuming some heuristics, while [10] used an isogeny  $\phi$  of  $\ell$ -power degree.

In this paper we give a new algorithm for computing the endomorphism ring of a supersingular elliptic curve  $E$ : first we compute two cycles through  $E$  in the supersingular  $\ell$ -isogeny graph that generate an order  $\Lambda$  in  $\text{End}(E)$ . We show that this order will be a Bass order with constant probability, assuming that the discriminants of the two cycles are random in a certain way. Then we compute all maximal orders that contain the Bass order  $\Lambda$  by first solving the problem locally, showing how to efficiently compute all maximal superorders of  $\Lambda$  when  $\Lambda$  is local and Bass. This extends work of Voight [29, Theorem 7.14]. The main property of local Bass orders used here is that there are at most  $e + 1$  maximal orders containing a local Bass order  $\Lambda \otimes \mathbb{Z}_q$ , where  $e = v_q(\text{discrd}(\Lambda))$  is the valuation of the reduced discriminant of  $\Lambda$  (see [6]). To solve the global case, we use the local data and a local-global principle for quaternionic orders. To bound the running time in this step, we prove that the number of maximal global orders containing  $\Lambda$  is  $O(p^\varepsilon)$  for any  $\varepsilon > 0$  when the size of  $\Lambda$  is polynomial in  $\log p$  and  $\text{discrd}(\Lambda)$  is square-free. We conjecture that this bound also holds when  $\text{discrd}(\Lambda)$  is not square-free. Finally, as we compute each global maximal order, we check if it is isomorphic to  $\text{End}(E)$ . As part of the analysis of the cycle-finding algorithm, we give a lower bound on the size of the set of all  $j$ -invariants  $j$  that are adjacent to  $j^p$  in  $G(p, \ell)$ , answering the lower-bound part of Question 3 in [1].

Our overall algorithm is still exponential: the two cycles are found in time  $O((\log p)^2 p^{1/2})$ , and the overall algorithm has the same running time, assuming several heuristics. This saves at least a factor of  $\log p$  versus the previous approach in [14] that finds cycles in  $G(p, \ell)$  until they generate all of  $\text{End}(E)$ . This is because with that approach one expects to compute  $O(\log p)$  cycles, while our algorithm for the endomorphism ring computes just one pair of cycles and succeeds with constant probability, assuming that the above heuristic about the discriminants of cycles holds. Also, our cycle-finding algorithm requires



only polynomial storage, while a generic collision-finding algorithm that relies on the birthday paradox has the same running time as our algorithm but requires exponential storage.

In the last section of the paper we give a new polynomial-time reduction from computing  $\text{End}(E)$  to path-finding in the  $\ell$ -isogeny graph which is simpler in several ways than previous ones. For this we need to assume GRH and the heuristics of [14]. We use this to break the second preimage resistance of a hash function in the family constructed in [9].

The paper is organized as follows. Section 2 gives some necessary background. In Section 3 we give an algorithm for computing cycles in the  $\ell$ -isogeny graph  $G(p, \ell)$  so that the corresponding endomorphisms generate an order in the endomorphism ring of the associated elliptic curve. In Section 4 we show how to compute all maximal local orders containing a given  $\mathbb{Z}_q$ -order  $\Lambda$ . In Section 5 we construct global orders from these local orders and compute  $\text{End}(E)$ . In Section 6 we give a reduction from the endomorphism ring problem to the problem of computing  $\ell$ -power isogenies in  $G(p, \ell)$  that is then used to attack the second preimage resistance of the hash function in [9].

## 2. Background on elliptic curves and quaternion algebras

For the definition of an elliptic curve, its  $j$ -invariant, isogenies of elliptic curves, their degrees, and the dual isogeny see [26].

**2A. Endomorphism rings, supersingular curves,  $\ell$ -power isogenies.** Let  $E$  be an elliptic curve defined over a finite field  $\mathbb{F}_q$ . An isogeny of  $E$  to itself is called an *endomorphism* of  $E$ . The set of endomorphisms of  $E$  defined over  $\overline{\mathbb{F}}_q$  together with the zero map is called the endomorphism ring of  $E$ , and is denoted by  $\text{End}(E)$ .

If the endomorphism ring of  $E$  is noncommutative,  $E$  is called a *supersingular elliptic curve*. Otherwise we call  $E$  *ordinary*. Every supersingular elliptic curve over a field of characteristic  $p$  has a model that is defined over  $\mathbb{F}_{p^2}$ .

Let  $E, E'$  be two supersingular elliptic curves defined over  $\mathbb{F}_{p^2}$ . For each prime  $\ell \neq p$ ,  $E$  and  $E'$  are connected by a chain of isogenies of degree  $\ell$ . By [20, Theorem 79],  $E$  and  $E'$  can be connected by  $m$  isogenies of degree  $\ell$ , where  $m = O(\log p)$ . For  $\ell$  a prime different from  $p$ , the *supersingular  $\ell$ -isogeny graph in characteristic  $p$*  is the multigraph  $G(p, \ell)$  whose vertex set is

$$V = V(G(p, \ell)) = \{j \in \mathbb{F}_{p^2} : j = j(E) \text{ for } E \text{ supersingular}\},$$

and the number of directed edges from  $j$  to  $j'$  is equal to the multiplicity of  $j'$  as a root of  $\Phi_\ell(j, Y)$ . Here, given a prime  $\ell$ ,  $\Phi_\ell(X, Y) \in \mathbb{Z}[X, Y]$  is the *modular polynomial*. This polynomial has the property that  $\Phi_\ell(j, j') = 0$  for  $j, j' \in \mathbb{F}_q$  and  $q = p^r$  if and only if there exist elliptic curves  $E(j), E(j')$  defined over  $\mathbb{F}_q$  with  $j$ -invariants  $j, j'$  such that there is a separable  $\ell$ -isogeny from  $E(j)$  to  $E(j')$ .

**2B. Quaternion algebras, orders and sizes of orders.** For  $a, b \in \mathbb{Q}^\times$ , let  $H(a, b)$  denote the quaternion algebra over  $\mathbb{Q}$  with basis  $1, i, j, ij$  such that  $i^2 = a$ ,  $j^2 = b$  and  $ij = -ji$ . That is,  $H(a, b) = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij$ . Any quaternion algebra over  $\mathbb{Q}$  can be written in this form. There is a *canonical*

involution on  $H(a, b)$  which sends an element  $\alpha = a_1 + a_2i + a_3j + a_4ij$  to  $\bar{\alpha} := a_1 - a_2i - a_3j - a_4ij$ . Define the *reduced trace* of an element  $\alpha$  as above to be  $\text{Trd}(\alpha) = \alpha + \bar{\alpha} = 2a_1$ , and the *reduced norm* to be  $\text{Nrd}(\alpha) = \alpha\bar{\alpha} = a_1^2 - aa_2^2 - ba_3^2 + aba_4^2$ .

A subset  $I \subseteq H(a, b)$  is a *lattice* if  $I$  is finitely generated as a  $\mathbb{Z}$ -module and  $I \otimes \mathbb{Q} \simeq H(a, b)$ . If  $I \subseteq H(a, b)$  is a lattice, the *reduced norm of  $I$* , denoted  $\text{Nrd}(I)$ , is the positive generator of the fractional  $\mathbb{Z}$ -ideal generated by  $\{\text{Nrd}(\alpha) : \alpha \in I\}$ . An *order*  $\mathcal{O}$  of  $H(a, b)$  is a subring of  $H(a, b)$  which is also a lattice, and if  $\mathcal{O}$  is not properly contained in any other order, we call it a *maximal order*. We call an order  $\mathcal{O} \subseteq H(a, b)$   *$q$ -maximal* if  $\mathcal{O} \otimes \mathbb{Z}_q$  is a maximal order in  $H(a, b) \otimes \mathbb{Z}_q$ .

We define  $\mathcal{O}_R(I) := \{x \in H(a, b) : Ix \subseteq I\}$  to be the *right order of the lattice  $I$* , and we similarly define its *left order*  $\mathcal{O}_L(I)$ . If  $\mathcal{O}$  is a maximal order in  $H(a, b)$  and  $I \subseteq \mathcal{O}$  is a left ideal of  $\mathcal{O}$ , then  $\mathcal{O}_R(I)$  is also a maximal order. Here a *left ideal of  $\mathcal{O}$*  is an additive subgroup of  $\mathcal{O}$  that is closed under scalar multiplication on the left. In our setting, a lattice or an order is always specified by a basis. The *size* of a lattice or an order  $\Lambda$  specified by a basis  $\mathcal{B}$  in a quaternion algebra  $B$  is the number of bits needed to write down the coefficients of the basis  $\mathcal{B}$  plus the size of  $B$ , which is specified by a basis and a multiplication table. In the following we write  $\text{size}(\Lambda)$  for simplicity even though the size depends on the basis chosen to represent  $\Lambda$ . If  $\{a_1, a_2, a_3, a_4\}$  is a basis of  $\Lambda$ , the *Gram matrix* of this basis is the  $4 \times 4$  matrix whose  $ij$ -th entry is  $\text{Trd}(a_i a_j)$ . We denote by  $B_{p,\infty}$  the unique quaternion algebra over  $\mathbb{Q}$  that is ramified exactly at  $p$  and  $\infty$ , and this algebra has a standard basis [25, Proposition 5.1]. The endomorphism ring of a supersingular elliptic curve is isomorphic to a maximal order in  $B_{p,\infty}$ .

**2C. Bass, Eichler, and Gorenstein orders in quaternion algebras; discriminants and reduced discriminants.** Let  $B$  be a quaternion algebra over  $\mathbb{Q}$ . We define the *discriminant of  $B$* , denoted  $\text{disc } B$ , to be the product of primes that ramify in  $B$ ; then  $\text{disc } B$  is a squarefree positive integer. If  $\mathcal{O} \subset B$  is an order, we define the *discriminant of  $\mathcal{O}$*  to be  $\text{disc}(\mathcal{O}) := |\det(\text{Trd}(\alpha_i \alpha_j))_{i,j}| \in \mathbb{Z} > 0$ , where  $\alpha_1, \dots, \alpha_4$  is a  $\mathbb{Z}$ -basis for  $\mathcal{O}$  [28, §15.2].

The discriminant of an order is always a square, and the *reduced discriminant*  $\text{discrd}(\mathcal{O})$  is the positive integer square root so that  $\text{discrd}(\mathcal{O})^2 = \text{disc}(\mathcal{O})$  [28, §15.4]. The discriminant of an order measures how far the order is from being a maximal order. The order  $\mathcal{O}$  is maximal if and only if  $\text{discrd}(\mathcal{O}) = \text{disc } B$  [28, Theorem 23.2.9]. Associated to a quaternion algebra  $B$  over  $\mathbb{Q}$  there is a *discriminant form*  $\Delta : B \rightarrow \mathbb{Q}$ , defined by  $\Delta(\alpha) = \text{Trd}(\alpha)^2 - 4 \text{Nrd}(\alpha)$ , and we refer to  $\Delta(\alpha)$  as the *discriminant of  $\alpha$* . Now let  $\mathcal{O} \subset B$  be a  $\mathbb{Z}$ -order. We say that  $\mathcal{O}$  is an *Eichler order* if  $\mathcal{O} \subseteq B$  is the intersection of two (not necessarily distinct) maximal orders. The *codifferent* of an order is defined as  $\text{codiff}(\mathcal{O}) = \{\alpha \in B : \text{Trd}(\alpha\mathcal{O}) \subseteq \mathbb{Z}\}$ . Following [28, Definition 24.2.1], we say that  $\mathcal{O}$  is *Gorenstein* if the lattice  $\text{codiff}(\mathcal{O})$  is invertible as a lattice as in [28, Definition 16.5.1]. An order  $\mathcal{O}$  is *Bass* if every superorder  $\mathcal{O}' \supseteq \mathcal{O}$  is Gorenstein. An order is *basic* if it contains a commutative, quadratic subalgebra  $R$  such that  $R$  is integrally closed in  $\mathbb{Q}R$  [28, §24.5]. Given an order  $\Lambda$ , its *radical idealizer*  $\Lambda^\natural$  is defined as  $\Lambda^\natural = \mathcal{O}_R(\text{rad } \Lambda)$ , where  $\text{rad } \Lambda$  is the Jacobson radical of the ring  $\Lambda$ . When  $B$  is a quaternion algebra over  $\mathbb{Q}_p$  and  $\mathcal{O}$  is a  $\mathbb{Z}_p$ -order in  $B$ , we similarly define lattices, ideals, and orders in  $B$ .



### 3. Computing an order in the endomorphism ring of a supersingular elliptic curve

**3A. Computing cycles in  $G(p, \ell)$ .** Fix a supersingular elliptic curve  $E_0$  defined over  $\mathbb{F}_{p^2}$  with  $j$ -invariant  $j_0$ . In this section we describe and analyze an algorithm for computing two cycles through  $j_0$  in  $G(p, \ell)$  that generate an order in  $\text{End}(E_0)$ .

We will first show how to construct two distinct paths from  $j_0$  to  $j_0^p$ . Given two such paths  $P$  and  $P'$ , then first traversing through  $P$  and then traversing through  $P'$  in reverse gives a cycle through  $j_0$ . This uses the fact that if  $j$  is adjacent to  $j'$ , then  $j^p$  is adjacent to  $(j')^p$ .

Let  $P_1$  be a path of length  $k$  from  $j_0$  to  $j_k$  in  $G(p, \ell)$ . Denote the not necessarily distinct vertices on the path by  $j_0, j_1, \dots, j_k$  and assume that  $j_k$  is adjacent to  $j_k^p$  in  $G(p, \ell)$ . Let

$$P_1^p = [j_k, j_k^p, j_{k-1}^p, \dots, j_1^p, j_0^p].$$

The concatenation  $P := P_1 P_1^p$  is a path from  $j_0$  to  $j_0^p$ . Such paths were also considered in [9, Section 7].

If  $j_0 = j_0^p$ , then  $P$  is already a cycle. Otherwise, we repeat this process to find another path  $P' := P_2 P_2^p$  that passes through at least one vertex not in  $P$ . Concatenating  $P$  and  $P'$  (in reverse order) gives a cycle starting and ending at  $j_0$ ; this corresponds to an endomorphism of  $E$ . We will need the notion of a path/cycle with no *backtracking* and *trimming a path/cycle* to remove backtracking.

**Definition 3.1.** Suppose  $e_j, e_{j'}$  are edges in  $G(p, \ell)$  that correspond to  $\ell$ -isogenies

$$\phi_j : E(j) \rightarrow E(j') \quad \text{and} \quad \phi_{j'} : E(j') \rightarrow E(j)$$

between curves  $E(j)$  and  $E(j')$  with  $j$ -invariants  $j, j'$ . We say that  $e_j$  is *dual* to  $e_{j'}$  if up to isomorphism  $\phi_{j'}$  equals the dual isogeny  $\hat{\phi}_j$  of  $\phi_j$ . That is  $\phi_{j'} = \alpha \hat{\phi}_j$ , where  $\alpha \in \text{Aut}(E(j))$ . We say that a path or cycle with a specified start vertex  $j_0$ , following edges  $(e_1, \dots, e_k)$  and ending at vertex  $j_k$  has *no backtracking* if  $e_{i+1}$  is not dual to  $e_i$  for  $i = 1, \dots, k-1$ .

In our definition, a cycle has a specified start vertex  $j_0$ . According to our definition, if the first edge  $e_1$  and the last edge  $e_k$  in such a cycle are dual to each other, it is not considered backtracking.

**Definition 3.2.** Given a path  $(e_1, \dots, e_k)$  from  $j_0$  to  $j_k$  (with  $j_0 \neq j_k$ ) or a cycle with specified start vertex  $j_0 = j_k$ , define *trimming* as the process of iteratively removing pairs of adjacent dual edges until none are left.

One can show that given a path  $P$  from  $j_0$  to  $j_k$  with  $j_0 \neq j_k$ , or a cycle  $C$  with start vertex  $j_0 = j_k$ , the trimmed versions  $\tilde{P}$  or  $\tilde{C}$  may result in a smaller set of vertices. The vertices  $j_0$  and  $j_k$  will still be there in  $\tilde{P}$ , and the only way that  $j_0$  and  $j_k$  may disappear from  $\tilde{C}$  is if the whole cycle gets removed.

**Definition 3.3.** Given a path  $P$  in  $G_{p,\ell}$  from  $j_0$  to  $j_k$ , we define  $P^R$  to be the path  $P$  traversed in reverse order, from  $j_k$  to  $j_0$ , using the dual isogenies.

Let

$$S^p := \{j \in \mathbb{F}_{p^2} : j \text{ is supersingular and } j \text{ is adjacent to } j^p \text{ in } G(p, \ell)\}.$$

We can now give the algorithm to find cycle pairs:

**Algorithm 3.4.** Find cycle pairs for prime  $\ell$ .

*Input:* A prime  $p \neq \ell$  and a supersingular  $j$ -invariant  $j_0 \in \mathbb{F}_{p^2}$ .

*Output:* Two cycles in  $G(p, \ell)$  through  $j_0$ .

- (1) Perform  $N = \Theta(\sqrt{p} \log p \log \log p)$  random walks of length  $k = \Theta(\log(p^{3/4}(\log \log p)^{1/2}))$  starting at  $j_0$  and select a walk that hits a vertex  $j_k \in S^p$ , i.e., such that  $j_k$  is  $\ell$ -isogenous to  $j_k^p$ ; let  $P_1$  denote the path from  $j_0$  to  $j_k$ .
- (2) Let  $P_1^p$  be the path given by  $j_k, j_k^p, j_{k-1}^p, \dots, j_0^p$ .
- (3) Let  $P$  denote the path from  $j_0$  to  $j_0^p$  given as the concatenation of  $P_1$  and  $P_1^p$ . Remove any self-dual self-loops and trim  $P_1 P_1^p$ .
- (4) If  $j_0 \in \mathbb{F}_p$  then  $P_1 P_1^p$  is a cycle through  $j_0$ .
- (5) If  $j_0 \in \mathbb{F}_{p^2} - \mathbb{F}_p$  repeat Steps (1)–(3) again to find another path  $P' = P_2 P_2^p$  from  $j_0$  to  $j_0^p$ ; then  $P(P')^R$  is a cycle. Remove any self-dual self-loops and trim the cycle.
- (6) Repeat Steps (1)–(5) a second time to get a second cycle.

**Remark 3.5.** Instead of searching for a vertex  $j$  in Step (1) such that  $j$  is adjacent to  $j^p$ , one could also search for a vertex  $j \in \mathbb{F}_p$ , i.e.,  $j$  with  $j = j^p$ , or a vertex  $j$  whose distance from  $j^p$  in the graph is bounded by some fixed integer  $B$ . Our algorithm that searches for a vertex  $j$  such that  $j$  is adjacent to  $j^p$  was easier to analyze because there were fewer cases to consider.

To analyze the running time of [Algorithm 3.4](#), we will use the mixing properties in the Ramanujan graph  $G(p, \ell)$ . This is captured in the following proposition, which is an extension of [\[19, Lemma 2.1\]](#) in the case that  $G(p, \ell)$  is not regular or undirected (that is, when  $p \not\equiv 1 \pmod{12}$ ).

**Proposition 3.6.** *Let  $p > 3$  be prime, and let  $\ell \neq p$  also be a prime. Let  $S$  be any subset of the vertices of  $G(p, \ell)$  not containing 0 or 1728. Then a random walk of length at least*

$$t = \frac{\log\left(\frac{p}{6|S|^{1/2}}\right)}{\log\left(\frac{\ell+1}{2\sqrt{\ell}}\right)}$$

*will land in  $S$  with probability at least  $6|S|/p$ .*

One can prove this since the eigenvalues for the adjacency matrix of  $G(p, \ell)$  satisfy the Ramanujan bound. This allows us to prove the following theorem.

**Theorem 3.7.** *Let  $\ell, p$  be primes such that  $\ell < p/4$ . Under GRH, [Algorithm 3.4](#) computes two cycles in  $G(p, \ell)$  through  $j_0$  that generate an order in the endomorphism ring of  $E_0$  in time  $O(\sqrt{p} (\log p)^2)$ , as long as the two cycles do not pass through the vertices 0 or 1728, with probability  $1 - O(\log p/p)$ . The algorithm requires  $\text{poly}(\log p)$  space.*

**Remark 3.8.** In [Section 5](#) we use this proposition to compute endomorphism rings, and from this point there is no problem with excluding paths through 0 or 1728. This is because the endomorphism rings of the curves with  $j$ -invariants 0 and 1728 are known, and a path of length  $\log P$ , starting at  $j_0$  going through 0 or 1728 lets us compute  $\text{End}(E_0)$  via the reduction in [Section 6](#).

*Proof.* We implement Step (1) by letting  $j_{i+1}$  be a random root of  $\Phi_\ell(j_i, Y)$ . To test if  $j \in S^P$  we check if  $\Phi_\ell(j, j^P) = 0$ . Assuming GRH, [Theorem 3.9](#) implies that  $|S^P| = \Omega(\sqrt{p}/\log \log p)$  (treating  $\ell$  as a constant). [Proposition 3.6](#) implies that the endpoint  $j_k$  of a random path found in Step (1) is in  $S^P$  with probability  $\Omega(1/(\sqrt{p} \log \log p))$ . The probability that none of the  $N + 1$  paths land in  $S^P$  is at most  $(1 - C/(\sqrt{p} \log \log p))^{N+1} \leq (1 + C/(\sqrt{p} \log \log p))^{-(N+1)} \leq e^{-c \log p/C} = O(1/p)$  if  $c = C$ , where  $C$  is from [Theorem 3.9](#) and  $c$  is the constant used in the choice of  $N$ .

Now we show that with high probability the two cycles  $C_0, C_1$  returned by the algorithm are linearly independent. We will use Corollary 4.12 of [\[3\]](#). This corollary states that two cycles  $C_0$  and  $C_1$  with no self-loops generate an order inside  $\text{End}(E_0)$  if they

- (1) do not go through 0 or 1728,
- (2) have no backtracking, and
- (3) have the property that one cycle contains a vertex that the other does not contain.

By construction, the cycles  $C_0$  and  $C_1$  returned by our algorithm do not have any self-loops or backtracking. To prove that condition (3) holds, we first claim that with high probability, the end vertex  $j_k \in S^P$  in the path  $P_1$  from  $j_0$  to  $j_k$  will not get removed when the path  $P_1 P_1^P$  is trimmed in Step (3). Then we show it's also still there in the trimmed cycle after Step (5). Observe that if the path  $P_1$  were to be trimmed to obtain a path  $\tilde{P}_1$  with no backtracking, then  $\tilde{P}_1$  is still a nontrivial path that starts at  $j_0$  and ends at  $j_k$  as long as  $j_0$  and  $j_k$  are different which occurs with probability  $1 - O(1/p)$ . After concatenating  $\tilde{P}_1$  with its corresponding path  $\tilde{P}_1^P$ , the path  $\tilde{P}_1 \tilde{P}_1^P$  has backtracking only if the last edge of  $\tilde{P}_1$  is dual to the first edge in  $\tilde{P}_1^P$ , i.e., if  $j_{k-1} = j_k^P$ . If that is the case, remove the last edge from  $\tilde{P}_1$  and the first edge from  $\tilde{P}_1^P$ , and call the remaining path  $\hat{P}_1$ . The new path  $\hat{P}_1$  still has the property that it ends in a vertex  $j = j_k^P$  that is  $\ell$ -isogenous to its conjugate  $(j_k^P)^P = j_k$ . After concatenating  $\hat{P}_1$  with its corresponding  $\hat{P}_1^P$ , this still gives a path from  $j_0$  to  $j_0^P$ . Again, the concatenation of these two paths has no backtracking unless the last edge in  $\hat{P}_1$  is the first edge in  $\hat{P}_1^P$ , i.e., if the last edge in  $\hat{P}_1$  is an edge from  $j_k$  to  $j_k^P$ . But this cannot happen, because otherwise the trimmed path  $\tilde{P}_1$  would have backtracking because it would go from  $j_k$  to  $j_k^P$  and back to  $j_k$ , contradicting the definition of a trimmed cycle. (With negligible probability, the vertex  $j_k$  has multiple edges, so we exclude this case here.) Hence the trimmed version of  $P_1 P_1^P$  is  $\hat{P}_1 \hat{P}_1^P$ , and this path still contains the vertex  $j_k$ , since  $\hat{P}_1^P$  contains the vertex  $j_k$ . Now we can finish the argument by considering two cases:

**Case 1:**  $j_0 \in \mathbb{F}_p$ . The above argument about trimming shows that if the vertex  $j_k$  appearing in the second cycle  $C_1$  is different from all the vertices appearing in  $C_0$  and their conjugates, which happens with probability  $1 - O(\log p/p)$ , then that vertex  $j_k$  will appear in the trimmed cycle  $\tilde{C}_1$ , but not in  $\tilde{C}_0$ . (This

is because in this case the trimmed path  $P_1 P_1^p$  is already a cycle.) Hence by [3, Corollary 4.12],  $\tilde{C}_0$  and  $\tilde{C}_1$  are linearly independent.

**Case 2:**  $j_0 \in \mathbb{F}_{p^2} - \mathbb{F}_p$ . Here, with probability  $1 - O(\log(p)/p)$ , the endpoint  $j_k$  of  $P_2$  is a vertex such that neither it nor its conjugate appear as a vertex in  $P_1$ . The concatenation of the two paths  $P = P_1 P_1^p$  and  $P' = P_2 P_2^p$  in reverse is a cycle  $C_0$  through  $j_0$ . When we trim it, it is still a cycle through  $j_0$  in which the endpoint  $j_k$  from  $P_2$  appears because neither that  $j_k$  nor its conjugate appeared in  $P_1$ . Similarly, Algorithm 3.4 finds a second cycle  $C_1$  with probability  $1 - \log(p)/p$  that contains a random vertex that was not on the first cycle  $C_0$ . This means that by Corollary 4.12 of [3],  $\tilde{C}_0$  and  $\tilde{C}_1$  and hence  $C_0$  and  $C_1$  are linearly independent.

The running time is  $O(\sqrt{p} (\log p)^2)$  because we are considering  $O(\sqrt{p})$  paths of length  $O(\log p)$ , going from one vertex to the next takes time polynomial in  $\ell \log p$ , and we are assuming that  $\ell$  is fixed. The storage is polynomial in  $\log p$  because we only have to store the paths  $P_1, P_2$  that land in  $S^p$ .  $\square$

**3B. Determining the size of  $S^p$ .** We will now determine a lower bound for the size of the set

$$S^p := \{j \in \mathbb{F}_{p^2} : j \text{ is supersingular and } j \text{ is adjacent to } j^p \text{ in } G(p, \ell)\}.$$

In [9, Section 7], an upper bound is given for  $S^p$ , but in order to estimate the chance that a path lands in  $S^p$  we need a lower bound for this set.

Let  $\ell, p$  be primes such that  $\ell < p/4$ . Let  $\mathcal{O}_K$  be the ring of integers of  $K := \mathbb{Q}(\sqrt{-\ell p})$ . We use the terminology and notation in [13; 4]. Let  $\text{Emb}_{\mathcal{O}_K}(\mathbb{F}_{p^2})$  be the collection of pairs  $(E, f)$  such that  $E$  is an elliptic curve over  $\mathbb{F}_{p^2}$  and  $f : \mathcal{O}_K \hookrightarrow \text{End}(E)$  is a normalized embedding, taken up to isomorphism. We say  $f : \mathcal{O}_K \hookrightarrow \text{End}(E)$  is *normalized* if each  $\alpha \in \mathcal{O}_K$  induces multiplication by its image in  $\mathbb{F}_{p^2}$  on the tangent space of  $E$ , and  $(E, f)$  is isomorphic to  $(E', f')$  if there exists an isomorphism  $g : E \rightarrow E'$  such that  $f(\alpha)' = g f(\alpha) g^{-1}$  for all  $\alpha \in \mathcal{O}_K$ .

**Theorem 3.9.** *Let  $\ell$  be a prime and assume that  $\ell < p/4$ . Let*

$$S^p = \{j \in \mathbb{F}_{p^2} : j \text{ is supersingular and } \Phi_\ell(j, j^p) = 0\}.$$

*Under GRH there is a constant  $C > 0$  (depending on  $\ell$ ) such that  $|S^p| > C \sqrt{p} / \log \log(p)$ .*

*Proof.* First, if  $E$  is a supersingular elliptic curve defined over  $\mathbb{F}_{p^2}$  with  $j$ -invariant  $j$  and  $E^{(p)}$  is a curve with  $j$ -invariant  $j^p$  and  $\ell < p/4$  is also a prime, then  $E$  is  $\ell$ -isogenous to  $E^{(p)}$  if and only if  $\mathbb{Z}[\sqrt{-\ell p}]$  embeds into  $\text{End}(E)$  [9, Lemma 6].

For any element  $(E, f) \in \text{Emb}_{\mathcal{O}_K}(\mathbb{F}_{p^2})$ ,  $E$  is supersingular, since  $p$  ramifies in  $\mathbb{Q}(\sqrt{-\ell p})$ . Moreover  $j(E) \in S^p$  by the above fact. Thus the map  $\rho : \text{Emb}_{\mathcal{O}_K}(\mathbb{F}_{p^2}) \rightarrow S^p$  that sends  $(E, f)$  to  $\rho(E, f) = j(E)$  is well-defined.

To get a lower bound for  $S^p$  we will show that for  $j \in S^p$ , the size of  $\rho^{-1}(j)$  is bounded by  $(\ell + 1) \cdot 6$  and that  $|\text{Emb}_{\mathcal{O}_K}(\mathbb{F}_{p^2})| \gg \sqrt{\ell p} / \log \log(\ell p)$ . These two facts imply

$$|S^p| \geq |\text{Emb}_{\mathcal{O}_K}(\mathbb{F}_{p^2})| / ((\ell + 1) \cdot 6) > \frac{1}{(\ell + 1) \cdot 6} \cdot \frac{\sqrt{\ell p}}{\log \log(\ell p)}.$$

To get a lower bound for  $|\text{Emb}_{\mathcal{O}_K}(\mathbb{F}_{p^2})|$  we can use [15, Proposition 2.7] to show that  $\text{Emb}_{\mathcal{O}_K}(\mathbb{F}_{p^2})$  is in bijection with  $\text{Ell}_{\mathcal{O}_K}(\hat{L}_{\mathfrak{P}})$ , where  $\hat{L}_{\mathfrak{P}}$  is the algebraic closure of the completion of the ring class field  $H_{\mathcal{O}_K}$  at a prime  $\mathfrak{P}$  above  $p$ , and  $\text{Ell}_{\mathcal{O}_K}(\hat{L}_{\mathfrak{P}})$  is the set of isomorphism classes of elliptic curves over  $\hat{L}_{\mathfrak{P}}$  with endomorphism ring  $\mathcal{O}_K$ . Hence  $|\text{Emb}_{\mathcal{O}_K}(\mathbb{F}_{p^2})| = |\text{Ell}_{\mathcal{O}_K}(\hat{L}_{\mathfrak{P}})|$ , whose order equals  $|\text{Cl}(\mathcal{O}_K)|$ . Class group estimates from [23] give

$$|\text{Cl}(\mathcal{O}_K)| = h(-\ell p) \gg \sqrt{\ell p} / \log \log(\ell p).$$

It remains to bound the size of  $\rho^{-1}(j)$ . We claim that an equivalence class of pairs  $(E, f)$  determines an edge in  $G(p, \ell)$ . Let  $[(E, f)] \in \text{Emb}_{\mathcal{O}_K}(\mathbb{F}_{p^2})$  be given by some representative curve  $E$ . First assume that  $j(E) \neq 0, 1728$ . Then  $(E, f) \simeq (E, g)$  implies that  $f = g$ , since  $\text{Aut}(E) = \pm 1$ . Thus we may identify  $[(E, f)]$  with the edge in  $G(p, \ell)$  corresponding to the kernel of  $f(\sqrt{-\ell p})$ . When  $j(E) = 0$  or  $1728$ , we may assume that  $E$  is defined over  $\mathbb{F}_p$ . Then let  $[(E, f)] \in \text{Emb}_{\mathcal{O}_K}(\mathbb{F}_{p^2})$  and suppose  $(E, f)$  is equivalent to  $(E, g)$ . We can factor  $f(\sqrt{-\ell p}) = \pi \circ \phi$  and  $g(\sqrt{-\ell p}) = \pi \circ \phi'$ , where  $\phi, \phi'$  are degree  $\ell$  endomorphisms of  $E$  and  $\pi$  is the Frobenius endomorphism of  $E$ . Additionally,  $\pi \phi = u \pi \phi' u^{-1}$ . We claim that  $u$  and  $\phi$  commute. If not, then they generate an order  $\Lambda$  such that the following formula holds (see [22]):

$$\text{discrd}(\Lambda) = \frac{1}{4}(\Delta(u)\Delta(\phi) - (\text{Trd}(u)\text{Trd}(\phi) - 2\text{Trd}(u\hat{\phi}))^2) \leq \frac{1}{4}\Delta(u)\Delta(\phi). \quad (3-1)$$

One can show that this contradicts our assumption that  $p/4 > \ell$ . Thus  $u$  and  $\phi$  commute, and we see that  $f(\sqrt{-\ell p})$  and  $g(\sqrt{-\ell p})$  have the same kernel and thus determine the same edge in  $G(p, \ell)$ .

We now count how many elements of  $\text{Emb}_{\mathcal{O}_K}(\mathbb{F}_{p^2})$  determine the same edge in  $G(p, \ell)$ . Suppose that  $[(E, f)], [(E, g)] \in \text{Emb}_{\mathcal{O}_K}(\mathbb{F}_{p^2})$  and that  $\ker(f(\sqrt{-\ell p})) = \ker(g(\sqrt{-\ell p}))$ . Writing  $f(\sqrt{-\ell p}) = \phi \circ \pi$  and  $g(\sqrt{-\ell p}) = \phi' \circ \pi$  we see that  $\phi$  and  $\phi'$  must have the same kernel. Thus  $\phi' = u\phi$  for some  $u \in \text{Aut}(E)$ . Because  $p > 4\ell > 3$ ,  $\text{Aut}(E) \leq 6$  and we conclude that there are at most 6 classes  $[(E, f)]$  determining the same edge emanating from  $j(E)$  in  $G(p, \ell)$ . Thus

$$|\rho^{-1}(j)| \leq (\ell + 1) \cdot 6. \quad \square$$

Assuming GRH, this result settles the lower-bound portion of Question 3 in [1]. See Lemma 6 of [9] for the upper-bound.

#### 4. Enumerating maximal superorders: the local case

Let  $q$  be a prime. In this section, we give an algorithm for the following problem:

**Problem.** Given a  $\mathbb{Z}_q$ -order  $\Lambda \subseteq M_2(\mathbb{Q}_q)$ , find all maximal orders containing  $\Lambda$ .

For general  $\Lambda$  there might be an exponential number of maximal orders containing it, so the algorithm for enumerating them would also be exponential time. However, we will show that the above problem can be solved efficiently when  $\Lambda$  is Bass. The main property of local Bass orders  $\Lambda$  we use is that there are at most  $e + 1$  maximal orders containing  $\Lambda$ , where  $e = v_q(\text{discrd}(\Lambda))$  [6, Corollaries 2.5, 3.2, 4.3 and Proposition 3.1].

We use the Bruhat–Tits tree  $\mathcal{T}$  [28, §23.5] to compute the maximal superorders of  $\Lambda$ . The vertices of  $\mathcal{T}$  are in bijection with maximal orders in  $M_2(\mathbb{Q}_q)$ .

A homothety class of lattices  $[L] \subseteq \mathbb{Q}_q^2$  corresponds to a maximal order via

$$L \mapsto \text{End}_{\mathbb{Z}_q}(L) = \{x \in M_2(\mathbb{Q}_q) : xL \subseteq L\} \subseteq M_2(\mathbb{Q}_q) \quad (4-1)$$

for every choice of  $L \in [L]$ . Two maximal orders  $\mathcal{O}$  and  $\mathcal{O}'$  are adjacent in  $\mathcal{T}$  if there exist lattices  $L$  and  $L'$  for  $\mathcal{O}$  and  $\mathcal{O}'$  such that  $qL \subsetneq L' \subsetneq L$ . Hence the neighbors of  $\mathcal{O}$  in  $\mathcal{T}$  correspond to the one-dimensional subspaces of  $L/qL \cong \mathbb{F}_q \times \mathbb{F}_q$ .

A division quaternion algebra  $B$  over  $\mathbb{Q}_q$  has only one maximal order, which can be found using the algorithm in [29]. The split case is solved by [Algorithm 4.1](#), and also relies on the algorithm in [29].

**Algorithm 4.1.** Enumerate all maximal orders containing a local order.

*Input:* A  $\mathbb{Z}_q$ -order  $\Lambda \subseteq M_2(\mathbb{Q}_q)$ , represented by a  $\mathbb{Z}_q$ -basis.

*Output:* The maximal orders in  $M_2(\mathbb{Q}_q)$  containing  $\Lambda$ , each specified by a  $\mathbb{Z}_q$ -basis.

- (1) Compute a maximal order  $\tilde{\mathcal{O}} \supseteq \Lambda$  with [29, Algorithm 7.10] and a lattice  $\tilde{L}$  in  $\mathbb{Q}_q \times \mathbb{Q}_q$  such that  $\tilde{\mathcal{O}} = \text{End}_{\mathbb{Z}_q}(\tilde{L})$ .
- (2) Let  $A = \{\tilde{\mathcal{O}}\}$  and  $B = \{\tilde{L}\}$ .
- (3) While  $B \neq \emptyset$ :
  - (a) Remove  $L$  from  $B$ , and label it as discovered. Set  $\mathcal{O} = \text{End}_{\mathbb{Z}_q}(L)$ .
  - (b) Compute the set of neighbors  $\mathcal{N}_{\mathcal{O}}$  of  $\mathcal{O}$  that contain  $\Lambda$ .
  - (c) For each  $\mathcal{O}' \in \mathcal{N}_{\mathcal{O}}$  not labeled as discovered, add  $\mathcal{O}'$  to  $A$  and its corresponding lattice to  $B$ .
- (4) Return  $A$ .

Now we show that [Algorithm 4.1](#) is efficient when the input lattice  $\Lambda$  is Bass.

**Proposition 4.2.** *Let  $\Lambda \subseteq M_2(\mathbb{Q}_q)$  be a Bass  $\mathbb{Z}_q$ -order, and  $e := v_q(\text{discrd}(\Lambda))$ . [Algorithm 4.1](#) computes  $A := \{\mathcal{O} \supseteq \Lambda : \mathcal{O} \text{ is maximal}\}$ , and  $|A| \leq e + 1$ . The runtime is polynomial in  $\log q \cdot \text{size}(\Lambda)$ .*

*Proof.* To prove correctness we first show that the maximal orders containing an arbitrary order  $\Lambda'$  in  $M_2(\mathbb{Q}_q)$  form a subtree of  $\mathcal{T}$ . If  $\mathcal{O}, \mathcal{O}'$  are two maximal orders containing  $\Lambda'$ , then the maximal orders containing  $\mathcal{O} \cap \mathcal{O}'$  are precisely the vertices in the path between  $\mathcal{O}$  and  $\mathcal{O}'$  in  $\mathcal{T}$  [28, §23.5.15]. Each order on this path also contains  $\Lambda'$ , so the maximal orders containing  $\Lambda'$  form a connected subset of  $\mathcal{T}$ . The above algorithm explores this subtree.

If  $\Lambda$  is Bass and Eichler, i.e.,  $\Lambda = \mathcal{O} \cap \mathcal{O}'$  for maximal orders  $\mathcal{O}, \mathcal{O}'$ , then there are  $e + 1$  maximal orders containing  $\Lambda$  [6, Corollary 2.5], and they are exactly the vertices on the path from  $\mathcal{O}$  to  $\mathcal{O}'$ . If  $\Lambda$  is Bass but not Eichler, then there are either 1 or 2 maximal orders containing  $\Lambda$  by [6, Proposition 3.1 and Corollaries 3.2 and 4.3]. Since they form a tree, they must also form a path. In either case,  $|A| \leq e + 1$ , and the vertices in  $A$  form a path.

As for the running time, in Step (1) we run [29, Algorithm 7.10], which is polynomial in  $\log q \cdot \text{size}(\Lambda)$ . Let  $L$  be a lattice such that  $\mathcal{O} = \text{End}_{\mathbb{Z}_q}(L)$  contains  $\Lambda$ . The neighbors of  $\mathcal{O}$  containing  $\Lambda$  are in bijection with the lines in  $L/qL$  fixed by the action of the image of  $\Lambda$  in  $\mathcal{O}/q\mathcal{O} \simeq M_2(\mathbb{F}_q)$ . For each such line, let  $\bar{v} \in L/qL$  be a nonzero vector, and let  $v$  be a lift to  $L$ . Let  $w \in L$  be such that  $\{v, w\}$  is a  $\mathbb{Z}_q$ -basis of  $L$ . Then  $L' := \text{span}\{v, qw\}$  is a  $\mathbb{Z}_q$ -lattice such that  $\mathcal{O}' := \text{End}_{\mathbb{Z}_q}(L')$  contains  $\Lambda$ . So we can efficiently compute the lattices  $L'$  corresponding to the neighbors of  $\mathcal{O}$  which contain  $\Lambda$ . Given such an  $L'$ , let  $x \in M_2(\mathbb{Q}_q)$  be the base change matrix from  $L$  to  $L'$ . If  $\mathcal{B}$  is a basis for  $\mathcal{O}$ , then  $\mathcal{B}' := x\mathcal{B}x^{-1}$  is a basis for  $\mathcal{O}'$ . The size of  $\mathcal{B}'$  is  $c(\log q) + \text{size}(\mathcal{O})$  for some constant  $c$ , so each neighbor of  $\mathcal{O}$  containing  $\Lambda$  can be computed in time polynomial in  $\log q \cdot \text{size}(\mathcal{O})$ .

Since the length of the path explored in the algorithm is at most  $e$ , where  $e = v_q(\text{discrd}(\Lambda))$  is polynomial in  $\text{size}(\Lambda)$ , and the size of the starting order  $\tilde{\mathcal{O}}$  is polynomial in  $\log q \cdot \text{size}(\Lambda)$  we obtain that the size of any maximal order containing  $\Lambda$  is polynomial in  $\text{size}(\Lambda) \cdot \log q$ . Each step takes time polynomial in  $\log q \cdot \text{size}(\Lambda)$ , so the whole algorithm is polynomial in  $\log q \cdot \text{size}(\Lambda)$ .  $\square$

Later we will need to enumerate the  $q$ -maximal  $\mathbb{Z}$ -orders containing a Bass  $\mathbb{Z}$ -order  $\Lambda$ . The algorithm below uses Algorithm 4.1 to accomplish this.

**Algorithm 4.3.** Enumerate the  $q$ -maximal  $\mathbb{Z}$ -orders  $\mathcal{O}$  containing  $\Lambda$ .

*Input:* A  $\mathbb{Z}$ -order  $\Lambda$ , specified by a  $\mathbb{Z}$ -basis, and prime  $q$  such that  $\Lambda \otimes \mathbb{Z}_q$  is Bass.

*Output:* All  $\mathbb{Z}$ -orders  $\mathcal{O} \supseteq \Lambda$  such that  $\mathcal{O}$  is  $q$ -maximal and  $\mathcal{O} \otimes \mathbb{Z}_{q'} = \Lambda \otimes \mathbb{Z}_{q'}$  for all primes  $q \neq q'$ .

- (1) Compute an embedding  $f : \Lambda \otimes \mathbb{Q} \hookrightarrow M_2(\mathbb{Q}_q)$  such that  $f(\Lambda) \subseteq M_2(\mathbb{Z}_q)$ .
- (2) Let  $A$  be the output of Algorithm 4.1 on input  $f(\Lambda)$ .
- (3) Return  $\{f^{-1}(\mathcal{O}) + \Lambda : \mathcal{O} \in A\}$ .

**Lemma 4.4.** Algorithm 4.3 is correct. The run time is polynomial in  $\log q \cdot \text{size}(\Lambda)$ .

*Proof.* Step (1) can be accomplished with Algorithms 3.12, 7.9, and 7.10 in [29], which run in time polynomial in  $\log q \cdot \text{size} \Lambda$ . For each maximal  $\mathbb{Z}_q$ -order  $\mathcal{O} \supseteq f(\Lambda)$ , we then compute a corresponding  $\mathbb{Z}$ -lattice  $\mathcal{O}' \supseteq \Lambda$ , whose generators are  $\mathbb{Z}[q^{-1}]$ -linear combinations of generators of  $\Lambda$ . The denominator of these coefficients is at most  $q^e$  where  $e := v_q(\text{discrd}(\Lambda))$ . By Proposition 4.2, there are at most  $e + 1$  maximal orders containing  $f(\Lambda)$  if  $\Lambda \otimes \mathbb{Z}_q$  is Bass. It is straightforward to check that the lattice  $\Lambda + \mathcal{O}'$  is actually a  $\mathbb{Z}$ -order and has the desired completions. Moreover, these are all such orders by the local-global principle for orders, [28, Theorem 9.5.1].  $\square$

**Remark 4.5** (global case). Algorithm 4.3 can be used to enumerate all maximal orders  $\mathcal{O}$  of a quaternion algebra  $B$  over  $\mathbb{Q}$  that contain a  $\mathbb{Z}$ -order  $\Lambda$  which is Bass, given  $\Lambda$  and the factorization of  $\text{discrd}(\Lambda)$  as  $\text{discrd}(\Lambda) = \prod_{i=1}^m q_i^{e_i}$ :

We run Algorithm 4.3  $m$  times, namely on  $(\Lambda, q_1), \dots, (\Lambda, q_m)$ . Let  $\{X_1, \dots, X_m\}$  be the output, where  $X_i = \{\mathcal{O}_{i1}, \dots, \mathcal{O}_{in_i}\}$ . The global orders containing  $\Lambda$  are in bijection with  $\prod_i X_i$ , by associating to  $(\mathcal{O}_{1j_1}, \dots, \mathcal{O}_{mj_m}) \in \prod_i X_i$  the order  $\sum_i \mathcal{O}_{ij_i}$ . In particular, the number of such orders is at most  $\prod_i (e_i + 1)$ .



The correctness of this follows from the local-global principle for maximal orders [28, Lemma 10.4.2]. The above results show that each order in the enumeration can be computed in time polynomial in the size of  $\Lambda$ . However, for an arbitrary order  $\Lambda$ , there might be an exponential number of orders containing it.

## 5. Computing $\text{End}(E)$

Now we describe our algorithm to compute the endomorphism ring of  $E$ . By computing  $\text{End}(E)$  we mean computing a basis for an order  $\mathcal{O}$  in  $B_{p,\infty}$  that is isomorphic to  $\text{End}(E)$ , and that we can evaluate the basis at all points of  $E$  via an isomorphism  $B_{p,\infty} \rightarrow \text{End}(E) \otimes \mathbb{Q}$ . First we give an algorithm that uses [Algorithm 3.4](#) to generate a Bass suborder of  $\text{End}(E)$ . A heuristic about the distribution of discriminants of cycles is used to show that just one call to [Algorithm 3.4](#) generates a Bass order with constant probability. Then we give an algorithm which recovers  $\text{End}(E)$  from a Bass suborder. The key property used here is that Bass orders  $\Lambda$  (whose basis is of size polynomial in  $\log p$  and whose discriminant is  $O(p^k)$ ) only have  $O(p^\varepsilon)$  maximal orders containing them for any  $\varepsilon > 0$ . This is proved in [Proposition 5.5](#) when the reduced discriminant is square-free. Based on our numerical evidence, we conjecture that this holds for general Bass orders as well.

### 5A. Computing a Bass order.

**Algorithm 5.1.** Compute a Bass suborder  $\Lambda \subseteq \text{End}(E)$ .

*Input:* A supersingular elliptic curve  $E$ .

*Output:* A Bass order  $\Lambda \subseteq \text{End}(E)$  and the factorization of  $\text{discrd}(\Lambda)$ , or “false”.

- (1) Compute two cycles in  $G(p, \ell)$  through  $j(E)$  using [Algorithm 3.4](#).
- (2) Let  $\alpha, \beta$  be the endomorphisms corresponding to the cycles from Step (1). Compute the Gram matrix for  $\{1, \alpha, \beta, \alpha\beta\}$  and from it an abstract representation for  $\Lambda = \langle 1, \alpha, \beta, \alpha\beta \rangle$ .
- (3) Factor  $\text{discrd}(\Lambda) = \prod_{i=1}^n q_i^{e_i}$ .
- (4) If  $\Lambda$  is Bass return  $\Lambda$  and the factorization of  $\text{discrd}(\Lambda)$ , else return “false”.

To analyze the algorithm we introduce a new heuristic:

**Heuristic 5.2.** The probability that the discriminants of the two endomorphisms corresponding to the cycles produced by [Algorithm 3.4](#) are coprime is at least  $\mu$  for some constant  $\mu > 0$  not depending on  $p$ .

This heuristic is based on our numerical experiments. Intuitively, we are assuming that the endomorphisms we compute with [Algorithm 3.4](#) have discriminants which are distributed like random integers that satisfy the congruency conditions to be the discriminant of an order in a quadratic imaginary field in which  $p$  is inert and  $\ell$  splits. Two random integers are coprime with probability  $6/\pi^2$ . We are assuming that the discriminants of our cycles are coprime with constant probability.

**Theorem 5.3.** Assume GRH and [Heuristic 5.2](#). Then with probability at least  $\mu$ , [Algorithm 5.1](#) computes a Bass order  $\Lambda \subseteq \text{End}(E)$ , and the runtime is  $O(\sqrt{p}(\log p)^2)$ .



*Proof.* In Step (2), the Gram matrix for  $\Lambda$ , whose entries are the reduced traces of pairwise products of the basis elements, is computed. This uses a generalization of Schoof's algorithm (see Theorem A.6 of [3]), which runs in time polynomial in  $\log p$  and  $\log$  of the norm of  $\alpha, \beta$ . Since  $\alpha$  and  $\beta$  arise from cycles of length at most  $c \lceil \log p \rceil$ , for some constant  $c$  which is independent of  $p$ , the norms of  $\alpha$  and  $\beta$  are at most  $p^c$ . From the Gram matrix we can efficiently compute  $\text{discrd}(\Lambda)$ .

To check that  $\Lambda$  is Bass, it is enough to check that  $\Lambda$  is Bass at each  $q$  dividing  $\text{discrd}(\Lambda)$  [8, Theorem 1.2]. To check that  $\Lambda$  is Bass at  $q$  it is enough to check that  $\Lambda \otimes \mathbb{Z}_q$  and  $(\Lambda \otimes \mathbb{Z}_q)^\natural$  are Gorenstein [8, Corollary 1.3]. An order is Gorenstein if and only if its ternary quadratic form is primitive [28, Corollary 24.2.10], and this can be checked efficiently. Thus, given a factorization of  $\text{discrd}(\Lambda)$ , we can efficiently decide if  $\Lambda$  is Bass.

Finally, we compute the probability that the order returned by Algorithm 3.4 is Bass. By [8, Theorem 1.2], an order is Bass if and only if it is basic, and being basic is a local property. It follows that the order  $\Lambda$  is Bass whenever the conductors of  $\mathbb{Z}[\alpha]$  and  $\mathbb{Z}[\beta]$  are coprime. A sufficient condition for this is that the discriminants of  $\alpha$  and  $\beta$  are coprime which will happen with probability at least  $\mu$  by the above heuristic. This sufficient condition also covers the case when the cycle for  $\alpha$  or  $\beta$  goes through 0 or 1728 even though Theorem 3.7 does not apply here.  $\square$

**5B. Computing  $\text{End}(E)$  from a Bass order.** In this section we compute  $\text{End}(E)$  from a given Bass suborder  $\Lambda$ . For this we enumerate the maximal orders containing  $\Lambda$  by taking sums of the  $q$ -maximal orders returned by Algorithm 4.3. As we enumerate the orders, we check each one to see if it is isomorphic to  $\text{End}(E)$ .

**Algorithm 5.4.** Compute  $\text{End}(E)$  from a Bass order.

*Input:* A Bass order  $\Lambda \subseteq \text{End}(E)$  with factored reduced discriminant  $\prod_{i=1}^n q_i^{e_i}$ .

*Output:* A compact representation of  $\text{End}(E)$ , as defined in [12, Section 8.2].

- (1) For each  $i = 1$  to  $n$ :
  - (a) Compute all orders  $\{\mathcal{O}_{i,1}, \dots, \mathcal{O}_{i,m_i}\}$  which are maximal at  $q_i$  and equal to  $\Lambda$  at primes  $q' \neq q_i$  by running Algorithm 4.3 with input  $\Lambda$  and prime  $q_i$ .
- (2) Compute  $f : \Lambda \otimes \mathbb{Q} \rightarrow B_{p,\infty}$ .
- (3) For each choice of indices  $(i_1, \dots, i_n) \in [m_1] \times \dots \times [m_n]$ :
  - (a) Set  $\mathcal{O} := \mathcal{O}_{1,i_1} + \dots + \mathcal{O}_{n,i_n}$ .
  - (b) Compute  $E'/\mathbb{F}_{p^2}$  such that  $\text{End}(E') \simeq f(\mathcal{O})$  along with a compact representation of  $\text{End}(E')$ .
  - (c) If  $j(E') = j(E)$  or  $j(E') = j(E)^p$ , return  $f(\mathcal{O})$  and the compact representation of  $\text{End}(E')$ .

**Proposition 5.5.** Fix a positive integer  $k$ , and let  $\Lambda$  be a Bass order whose size is polynomial in  $\log p$  and whose reduced discriminant is square-free and of size  $O(p^k)$ . Assume that the factorization of the reduced discriminant is given. There are  $O(p^\varepsilon)$  maximal orders containing  $\Lambda$  and Algorithm 5.4 terminates in time  $\tilde{O}(p^\varepsilon)$  for any  $\varepsilon > 0$ , assuming that the heuristics in [14; 12] hold.

$p$	orders	Bass orders	average $N(\Lambda)$
70,001	92	76	122.21
90,001	80	67	322.04
100,003	81	75	337.59

**Table 1.** Results from computing 100 pairs of cycles in  $G(p, 2)$  at random  $j \in \mathbb{F}_{p^2} - \mathbb{F}_p$ .

*Proof.* Computing the isomorphism  $f : \Lambda \otimes \mathbb{Q} \simeq B_{p,\infty}$  requires one call to an algorithm for factoring integers (and  $\text{poly}(\log p)$  calls to algorithms for factoring polynomials over  $\mathbb{F}_p$ , see [17]). Let

$$\text{discrd}(\Lambda) = p \cdot \prod_{i=1}^m q_i$$

with  $q_1, \dots, q_m$  distinct and different from  $p$ . By the local-global principle for maximal orders there is one maximal order corresponding to each collection of  $q_i$ -maximal orders  $\{\mathcal{O}_i\}$  with  $\mathcal{O}_i \supseteq \Lambda \otimes \mathbb{Z}_{q_i}$ . We loop through these orders in Step (3). The size of the index set in that loop and hence the number of distinct maximal orders containing  $\Lambda$  is at most  $2^{\omega(\text{discrd}(\Lambda))-1}$ , where  $\omega(n)$  denotes the number of distinct prime factors of an integer  $n$ . Fix  $\varepsilon > 0$ . Since  $\omega(n) = O(\log n / \log \log n)$  [16, Chapter 22, §10], for  $p$  large enough, the number of maximal orders  $\mathcal{O} \supseteq \Lambda$  is at most

$$2^{c' \frac{\log c \cdot p^k}{\log \log c \cdot p^k}} = (c \cdot p^k)^{\frac{c'}{\log \log c \cdot p^k}}$$

for some  $c, c' > 0$ , which is  $O(p^\varepsilon)$ .

As we loop through the maximal orders  $\mathcal{O}$  containing  $\Lambda$ , we check each one to see if it is isomorphic to  $\text{End}(E)$ : after constructing such an order in Step (3)(a), we compute in Step (3)(b) a curve  $E'$  whose endomorphism ring is isomorphic to  $\mathcal{O}$ . This can be solved efficiently with the algorithms in [14]: one computes a connecting ideal  $I$  between  $\mathcal{O}$  and a special order  $\mathcal{O}'$  and then applies Algorithm 2 of [14] (see also Algorithm 12 of [12]). Then, in Step (3)(c), we compare  $j$ -invariants. Checking each order takes time polynomial in  $\log p$  (assuming the heuristics in [14; 12]), so the total running time of the algorithm is  $\tilde{O}(p^\varepsilon)$  for any  $\varepsilon > 0$ .  $\square$

Our computational data from Section 5C suggests that we will get the same running time when the reduced discriminant of  $\Lambda$  is not square-free. This motivates the following conjecture:

**Conjecture 5.6.** *Fix an integer  $k \geq 0$  and assume that  $\Lambda \subseteq \text{End}(E)$  is a Bass order of size polynomial in  $\log p$  and with  $\text{discrd}(\Lambda) = O(p^k)$ . Then for any  $\varepsilon > 0$ , the number of maximal orders containing  $\Lambda$  is  $O(p^\varepsilon)$ .*

**Theorem 5.7.** *Assume GRH, Conjecture 5.6, Heuristic 5.2, and the heuristics in [14]. Let  $E$  be a super-singular elliptic curve. Then the algorithm which combines Algorithm 5.1 and Algorithm 5.4 computes  $\text{End}(E)$  with probability at least  $\mu$ , in time  $O((\log p)^2 \sqrt{p})$ .*

*Proof.* By the proof of Theorem 5.3, the norms of the endomorphisms  $\alpha_1, \alpha_2$  computed by Algorithm 3.4 are bounded by  $p^c$  for some constant  $c$  independent of  $p$ , so their discriminants satisfy  $|\Delta(\alpha_i)| < 4p^c$ .

Hence by (3-1), they generate an order  $\Lambda$  whose reduced discriminant satisfies  $\text{discrd}(\Lambda) = O(p^{2c})$ . This means we can apply [Conjecture 5.6](#), so the theorem follows from [Theorem 5.3](#).  $\square$

**5C. Computational data.** We implemented a cycle-finding algorithm in Sage along with an algorithm for computing traces of cycles in  $G(p, \ell)$ , which is based on the implementation of Schoof's algorithm available in [27]. For each  $p$  in [Table 1](#), and for 100 iterations, we computed a pair of cycles in  $G(p, 2)$ . We then tested whether they generated a Bass order by testing whether the two quadratic orders had coprime conductors and computed the discriminant of the order that they generated. We also computed an upper bound on the number of maximal orders containing  $\Lambda$  when  $\Lambda$  was Bass: suppose  $\text{discrd}(\Lambda) = p \prod_i q_i^{e_i}$ , then there are at most  $N(\Lambda) := \prod_i (e_i + 1)$  maximal orders containing  $\Lambda$ . We report how often the two cycles generated an order, how many of those orders were Bass, and the average value of  $N(\Lambda)$ . The cycle-finding algorithm we implemented is the variant discussed in [Remark 3.5](#): it searches for  $j \in \mathbb{F}_p$  to construct the cycles using walks of length  $\lceil \log p \rceil$ . We also did not avoid a second cycle which may commute with the first since even without that more than 80% of cases were orders. We also only computed cycles at  $j \in \mathbb{F}_{p^2} - \mathbb{F}_p$  because this is the case of interest as there are no obvious noninteger endomorphisms.

## 6. Computing $\text{End}(E)$ via path-finding in the $\ell$ -isogeny graph

In this section, we give a reduction from the endomorphism ring problem to the problem of computing  $\ell$ -power isogenies in  $G(p, \ell)$ , using ideas from [21], [14], and [12]. This reduction is simpler than the one in [12], and uses only one call to a path-finding oracle (rather than  $\text{poly}(\log p)$  calls to an oracle for finding cycles in  $G(p, \ell)$ , as in [12]). We apply this reduction in two ways, noting that it gives an algorithm for computing the endomorphism ring, and that it breaks second preimage resistance of the variable-length version of the hash function in [9].

**6A. Reduction from computing  $\text{End}(E)$  to path-finding in the  $\ell$ -isogeny graph.** We first define the path-finding problem in  $G(p, \ell)$ :

**Problem ( $\ell$ -PowerIsogeny).** Given a prime  $p$  and supersingular elliptic curves  $E$  and  $E'$  over  $\mathbb{F}_{p^2}$ , output a chain of  $\ell$ -isogenies of length  $O(\log p)$  from  $E$  to  $E'$ .

Computing the endomorphism ring of a supersingular elliptic curve via an oracle for  $\ell$ -PowerIsogeny proceeds as follows. On input  $p$ , Algorithm 3 of [12] returns a supersingular elliptic curve  $\tilde{E}$  defined over  $\mathbb{F}_{p^2}$  and a maximal order  $\tilde{\mathcal{O}} \subseteq B_{p,\infty}$  with an explicit  $\mathbb{Z}$ -basis  $\{x_1, \dots, x_4\}$ . Proposition 3 of [12] gives an isomorphism  $g : \tilde{\mathcal{O}} \rightarrow \text{End}(\tilde{E})$  such that we can efficiently evaluate  $g(x_i)$  at points of  $E_0$ . From this, the endomorphism ring of any supersingular elliptic curve  $E$  defined over  $\mathbb{F}_{p^2}$  can be computed, given a path in  $G(p, \ell)$  from  $\tilde{E}$  to  $E$ , with  $\ell \neq p$  a small fixed prime, for example  $\ell = 2$  or  $3$ .

The following algorithm gives a polynomial time reduction from computing endomorphism rings to the path-finding problem, which uses only one call to the path-finding oracle. It assumes the heuristics of [14] and GRH (to compute  $\tilde{E}$ ). A similar algorithm appeared in [10].

**Algorithm 6.1.** Reduction from computing  $\text{End}(E)$  to  $\ell$ -PowerIsogeny.

*Input:* A prime  $p$ , and  $E/\mathbb{F}_{p^2}$  supersingular.

*Output:* A maximal order  $\mathcal{O} \simeq \text{End}(E)$ , whose elements can be evaluated at any point of  $E$ , and a powersmooth isogeny  $\psi_e : \tilde{E} \rightarrow E$ , with  $\tilde{E}$  as above.

- (1) Compute  $\tilde{E}, \tilde{\mathcal{O}}$  with Algorithm 3 in [12].
- (2) Run the oracle for path-finding on  $\tilde{E}, E$  to obtain an  $\ell$ -power isogeny  $\phi = \phi_e \circ \dots \circ \phi_1 : \tilde{E} \rightarrow E$  of degree  $\ell^e$ .
- (3) Let  $J_0 := \tilde{\mathcal{O}}, P_0 := \tilde{\mathcal{O}}, \mathcal{O}_0 := \tilde{\mathcal{O}}$ .
- (4) For  $k := 1, \dots, e$ :
  - (a) Compute  $I_k \subseteq \mathcal{O}_{k-1}$ , the kernel ideal of  $\phi_k$ .
  - (b) Compute  $J_k := J_{k-1} I_k$ .
  - (c) Compute  $P_k$ , an ideal equivalent to  $J_k$  of powersmooth norm.
  - (d) Compute an isogeny  $\psi_k : \tilde{E} \rightarrow E_k$  corresponding to  $P_k$ .
  - (e) Set  $\mathcal{O}_k := \mathcal{O}_R(P_k)$ .
- (5) Return  $\mathcal{O}_R(P_e), \psi_e$ .

Orders and ideals appearing in the above algorithm are represented by a  $\mathbb{Z}$ -basis, and we can compute right orders of ideals using linear algebra over  $\mathbb{Z}$ , as in [12]. The ideal  $I_k$ , which is the ideal of  $\mathcal{O}_{k-1}$  of norm  $\ell$  corresponding to  $\phi_k$ , can be computed efficiently because we can evaluate endomorphisms efficiently using Proposition 3 of [12]. The algorithm is correct because  $\mathcal{O}_R(P_e) = \mathcal{O}_R(J_e) = \text{End}(E_e) = \text{End}(E)$ .

**6B. Using Algorithm 6.1 to compute endomorphism rings and break the second preimage of the CGL hash.** Algorithm 6.1 can be used to give an algorithm for computing the endomorphism ring of a supersingular elliptic curve  $E$  by combining it with algorithms from [11; 14; 12]. This yields a  $O((\log p)^2 p^{1/2})$  time algorithm with polynomial storage, assuming the relevant heuristics in [14; 12].

We now consider the hash function in [9] constructed from Pizer’s graphs  $G(p, 2)$ . For each supersingular elliptic curve  $\tilde{E}$ , there is an associated hash function. An input  $s \in \{0, 1\}^*$  to the hash function determines a walk in  $G(p, 2)$  from  $\tilde{E}$  to another curve  $E$ , and the output of the hash function is  $j(E)$ . The following is an improvement over [12], which gave a collision attack for this specific hash function.

**Proposition 6.2.** *Let  $\tilde{E}$  be the elliptic curve computed in Step (1) of Algorithm 6.1. For the hash function associated to  $\tilde{E}$ , Algorithm 6.1 gives a second preimage attack (and hence, also a collision attack) that runs in time polynomial in  $\log p$ .*

*Proof.* The attack works as follows: Given a path from  $\tilde{E}$  to  $E$ , use Algorithm 6.1 to compute  $\text{End}(E)$ . Then use Algorithm 7 of [12] to compute new paths from  $\tilde{E}$  to  $E$ .  $\square$

## Acknowledgements

We would like to thank Ben Diamond, Daniel Smertnig and John Voight for several helpful discussions and suggestions. We would like to thank an anonymous reviewer of an earlier version of this paper whose suggestions greatly simplified [Section 4](#).

## References

- [1] Sarah Arpin, Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Travis Scholl, and Jana Sotáková. Adventures in supersingularland. Preprint, 2019. [arXiv:1909.07779](#).
- [2] Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Amir Jalali, David Jao, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Joost Renes, Vladimir Soukharev, and David Urbanik. Supersingular isogeny key encapsulation. Submission to the NIST Post-Quantum Standardization project, 2017. [csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions](#).
- [3] Efrat Bank, Catalina Camacho-Navarro, Kirsten Eisenträger, Travis Morrison, and Jennifer Park. Cycles in the supersingular  $\ell$ -isogeny graph and corresponding endomorphisms. *Proceedings of the Women in Numbers 4 Conference*, To appear in WIN 4 proceedings, 2019. [arXiv:1804.04063](#).
- [4] Juliana Belding, Reinier Bröker, Andreas Enge, and Kristin Lauter. Computing Hilbert class polynomials. In *Algorithmic number theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 282–295. Springer, Berlin, 2008.
- [5] Gaetan Bisson and Andrew V. Sutherland. Computing the endomorphism ring of an ordinary elliptic curve over a finite field. *J. Number Theory*, 131(5):815–831, 2011.
- [6] Juliusz. Brzeziński. On orders in quaternion algebras. *Comm. Algebra*, 11(5):501–522, 1983.
- [7] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: an efficient post-quantum commutative group action. In *Advances in cryptology—ASIACRYPT 2018. Part III*, volume 11274 of *Lecture Notes in Comput. Sci.*, pages 395–427. Springer, Cham, 2018.
- [8] Sara Chari, Daniel Smertnig, and John Voight. On basic and Bass quaternion orders. Preprint, 2019. [arXiv:1903.00560](#).
- [9] Denis X. Charles, Eyal Z. Goren, and Kristin Lauter. Cryptographic hash functions from expander graphs. *J. Cryptology*, 22(1):93–113, 2009.
- [10] Luca De Feo, Simon Masson, Christophe Petit, and Antonio Sanso. Verifiable delay functions from supersingular isogenies and pairings. In *Advances in Cryptology – ASIACRYPT 2019*, volume 11921 of *Lecture Notes in Comput. Sci.*, pages 248–277. Springer, 2019.
- [11] Christina Delfs and Steven D. Galbraith. Computing isogenies between supersingular elliptic curves over  $\mathbb{F}_p$ . *Des. Codes Cryptography*, 78(2):425–440, February 2016.
- [12] Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit. Supersingular isogeny graphs and endomorphism rings: reductions and solutions. *Eurocrypt 2018, LNCS 10822*, pages 329–368, 2018.
- [13] Noam D. Elkies. Supersingular primes for elliptic curves over real number fields. *Compositio Math.*, 72(2):165–172, 1989.
- [14] Steven D. Galbraith, Christophe Petit, and Javier Silva. Identification protocols and signature schemes based on supersingular isogeny problems. In *Advances in cryptology—ASIACRYPT 2017. Part I*, volume 10624 of *Lecture Notes in Comput. Sci.*, pages 3–33. Springer, 2017.
- [15] Benedict Gross and Don Zagier. On singular moduli. *J. Reine Angew. Math.*, 355:191–220, 1985.
- [16] Godfrey H. Hardy and Edward M. Wright. *An introduction to the theory of numbers*. Oxford University Press, Oxford, sixth edition, 2008.
- [17] Gábor Ivanyos, Lajos Rónyai, and Josef Schicho. Splitting full matrix algebras over algebraic number fields. *J. Algebra*, 354:211–223, 2012.
- [18] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *Post-quantum cryptography*, volume 7071 of *Lecture Notes in Comput. Sci.*, pages 19–34. Springer, Heidelberg, 2011.

- [19] David Jao, Stephen D. Miller, and Ramarathnam Venkatesan. Expander graphs based on GRH with an application to elliptic curve cryptography. *J. Number Theory*, 129(6):1491–1504, 2009.
- [20] David Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California, Berkeley, 1996.
- [21] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion  $\ell$ -isogeny path problem. *LMS Journal of Computation and Mathematics*, 17:418–432, 2014.
- [22] Kristin Lauter and Bianca Viray. An arithmetic intersection formula for denominators of Igusa class polynomials. *Amer. J. Math.*, 137(2):497–533, 2015.
- [23] John E. Littlewood. On the class-number of the corpus  $P(\sqrt{-k})$ . *Proc. London Math. Soc. (2)*, 27(5):358–372, 1928.
- [24] Ken McMurdy. Explicit representations of the endomorphism rings of supersingular elliptic curves. 2014.
- [25] Arnold Pizer. An algorithm for computing modular forms on  $\Gamma_0(N)$ . *J. Algebra*, 64(2):340–390, 1980.
- [26] Joseph H. Silverman. *The arithmetic of elliptic curves*. Springer, New York, 2009.
- [27] Andrew Sutherland. 18.783 Elliptic Curves. Massachusetts Institute of Technology: MIT OpenCourseWare, [ocw.mit.edu](https://ocw.mit.edu) License: Creative Commons BY-NC-SA.
- [28] John Voight. *Quaternion algebras*. Version v.0.9.14, July 7, 2018.
- [29] John Voight. Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms. *Developments in Mathematics*, 31:255–298, 2013.

Received 27 Feb 2020. Revised 31 Jul 2020.

KIRSTEN EISENTRÄGER: [eisentra@math.psu.edu](mailto:eisentra@math.psu.edu)

Department of Mathematics, The Pennsylvania State University, University Park, PA, United States

SEAN HALLGREN: [hallgren@cse.psu.edu](mailto:hallgren@cse.psu.edu)

Department of Computer Science and Engineering, Penn State University, University Park, PA, United States

CHRIS LEONARDI: [cfoleona@uwaterloo.ca](mailto:cfoleona@uwaterloo.ca)

Department of Combinatorics and Optimization, The University of Waterloo, Waterloo, ON, Canada

TRAVIS MORRISON: [travis.morrison@uwaterloo.ca](mailto:travis.morrison@uwaterloo.ca)

Institute for Quantum Computing, The University of Waterloo, Waterloo, ON, Canada

JENNIFER PARK: [park.2720@osu.edu](mailto:park.2720@osu.edu)

Department of Mathematics, The Ohio State University, Columbus, OH, United States

# New rank records for elliptic curves having rational torsion

Noam D. Elkies and Zev Klagsbrun

We present rank-record breaking elliptic curves having torsion subgroups  $\mathbb{Z}/n\mathbb{Z}$  for  $n = 2, 3, 4, 5, 6$ , and  $7$ .

## 1. Introduction

Given an elliptic curve  $E/\mathbb{Q}$ , the Mordell–Weil theorem states that the group of rational points  $E(\mathbb{Q})$  is isomorphic to  $\mathbb{Z}^r \times T$ , where  $r$  is the *rank* of  $E$  and  $T$  is a finite group called the *torsion subgroup* of  $E$  [21]. While the groups that can appear as  $T$  were fully characterized by Mazur [16], which ranks occur is a question that goes back to Poincaré [26] and has been the subject of competing folklore conjectures.

One side, claiming ranks are bounded, was recently bolstered by several different models [30; 31; 25] that predict that all but finitely many elliptic curves have rank at most 21, with stronger conjectured bounds on which ranks occur infinitely often for each possible torsion group  $T$ . (For example, if  $T = \mathbb{Z}/n\mathbb{Z}$  for  $n = 2, 3, \dots, 8$  then the bound 21 is replaced by 13, 9, 7, 5, 5, 3, 3.) The other side, arguing that ranks are unbounded, has relied on periodically exhibiting curves of larger and larger rank.

Our work continues that tradition, exhibiting rank-record breaking curves for the torsion subgroups  $\mathbb{Z}/n\mathbb{Z}$  for each  $n = 2, 3, 4, 5, 6, 7$ , which constitute two-fifths of the 15 groups that Mazur showed can appear as the torsion subgroup of an elliptic curve over  $\mathbb{Q}$ .

At the same time, our work provides, at best, limited evidence that ranks are unbounded. We broke six different records, and found numerous new curves whose ranks tie the old records (and many more whose ranks exceed the heuristically conjectured asymptotic upper bounds). But the scale of this search was vastly larger than any previously attempted, and yet we could not break any of the previous records by more than 1, and in each case found only a handful of curves (in most cases, a single curve) with the new record rank. This suggests that the growth of ranks of elliptic curves might indeed peter out at some point.

---

Elkies was supported by NSF grants DMS-0501029, DMS-1100511, and DMS-1502161, a Radcliffe Fellowship, and the Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation.

MSC2020: 11G05.

Keywords: elliptic curves, ranks of elliptic curves.



**1.1. Organization.** This paper largely splits into three parts. The first consists of Sections 2–6, which describe the methods that we used to search for curves of high rank, as well as Section 7, which presents some open questions about our methods. The second, Sections 8–14, describes our results, including details of our searches in each of the torsion families considered. Section 9 also includes a previously unpublished family of elliptic K3 surfaces  $\mathcal{E}_u/\mathbb{Q}(t)$  that have Mordell–Weil group  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^9$  for each  $u \neq \pm 1, \pm 2$  for which  $5 - u^2$  is a square. We exhibit generators for  $\mathcal{E}_u(\mathbb{Q}(t))$  in Appendix A. The third and final part of this paper is Appendix B, which presents models for the record-breaking curves we discovered and points that generate their Mordell–Weil groups.

## 2. The method of Mestre and Nagao

The core ingredient in our search was a well-known method, originally from Mestre, to find elliptic curves having large Mordell–Weil rank. We start with an elliptic fibration  $\mathcal{E}/\mathbb{Q}(t)$  having Mordell–Weil rank  $r$ , and then attempt to find good values of  $t$  for which the specialization  $E_t$  has particularly large rank [20].

A theorem of Silverman [27] states that all but finitely many specializations  $E_t$  of  $\mathcal{E}$  have rank at least  $r$ , so this approach effectively gives us  $r$  independent rational points on each specialization for free.

The method for finding values of  $t$  for which the rank of  $E_t$  is significantly larger than  $r$  has its roots in the observation of Birch and Swinnerton-Dyer that curves that have unusually many points modulo  $p$  for most  $p$  should have many rational points as well [3], and in Mestre’s work on Weil’s explicit formula for elliptic curves [18]. The idea is to construct a score  $S(t, B)$  that incorporates the number of points  $N_p(E_t)$  on  $\overline{E}_t(\mathbb{F}_p)$  for all primes  $p \leq B$  where  $E_t$  has good reduction, and then to search for rational points on  $E_t$  for those values of  $t$  in a search region for which  $S(t, B)$  is above some threshold. While this basic method was first used by Mestre to find the first curves over  $\mathbb{Q}$  having rank 12 [17], its first use in a family  $\mathcal{E}/\mathbb{Q}(t)$  appears to be due to Nagao [23].

Nagao considered the scores

$$S_1(t, B) = \sum_{\substack{p < B, \\ E_t \text{ has good reduction at } p}} \frac{-a_p(E_t) + 2}{N_p(E_t)} \log p \quad \text{and} \quad S_2(t, B) = \frac{1}{B} \sum_{\substack{p < B, \\ E_t \text{ has good reduction at } p}} -a_p(E_t) \log p,$$

which, when large, suggest via Weil’s explicit formula for elliptic curves [18] that the order of the vanishing of the  $L$ -function  $L_{E_t}(s)$  at  $s = 1$  should be large as well.

We choose to evaluate a different sum,

$$S(t, B) = \sum_{\substack{p < B, \\ E_t \text{ has good reduction at } p}} \log \left( \frac{N_p(E_t)}{p} \right), \tag{1}$$

as in [8], so that  $\exp(-S(t, B))$  is the partial product

$$\prod_{\substack{p < B, \\ E_t \text{ has good reduction at } p}} (1 - a_p(E_t)p^{-s} + p^{1-2s})^{-1} \tag{2}$$

of the Euler product for  $L_{E_t}(s)$  evaluated at  $s = 1$  (ignoring the finitely many factors at primes of bad



reduction). The conjecture of Birch and Swinnerton-Dyer suggests that when  $E_t$  has large rank such partial products should rapidly approach zero, and thus that  $S(t, B)$  should be large.

### 3. Computational techniques

Computing any of the sums in [Section 2](#) would be computationally infeasible for a large range of  $t$  if one needed to individually compute  $a_p(E_t)$  for each  $p < B$  and each value of  $t$ . To scale Mestre's method to extremely large search regions, we took advantage of three computational tricks.

First, as observed by Nagao [\[24\]](#),  $a_p(t)$  depends only on  $t \pmod{p}$ . As a result, one can first compute  $a_p(t)$  for all  $p \leq B$  and for all  $t \in \mathbb{F}_p$  for which  $\Delta_{E_t} \neq 0$ , and then use the precomputed values to calculate  $S(t, B)$  for each  $t$  in the search region.

The second trick, also due to Nagao [\[24\]](#), lets us concentrate our computation on the most promising values of  $t$ . Rather than compute  $S(t, B)$  for all  $t$  in the search region, we choose an increasing series of bounds  $B_0 \leq B_1 \leq \dots \leq B_m = B$  and cutoffs  $C_0 \leq C_1 \leq \dots \leq C_m = C$ , and only compute  $S(t, B_i)$  for  $i \geq 1$  for those values of  $t$  for which  $S(t, B_j) \geq C_j$  for all  $0 \leq j < i$ .

These first two tricks appear to be well known (see [\[12\]](#), for example). The third trick, which is apparently due to Elkies [\[8\]](#), seems to be less widely known, and we describe it in detail below.

**3.1. Sieving.** Rather than computing  $S(t, B)$  for each value of  $t$  by looking up the values of  $N_p(t)$  (or more likely,  $\log(N_p(t)/p)$ ) for each prime  $p < B$ , sieving computes  $S(t, B)$  for a large number of values of  $t = a/b$  at once. The algorithm works as follows:

Fix a value of  $b$  and an interval  $[a_0, a_0 + N)$ . We allocate a counter array  $\mathcal{C}$  of length  $N$  initialized to zero. For each prime  $p \nmid b$ , we initialize an update array  $\mathcal{P}$  of length  $p$  such that the  $i$ -th entry of  $\mathcal{P}$  is equal to  $\log(N_p(b^{-1}(a_0 + i))/p)$ . We then repeatedly add the update array  $\mathcal{P}$  into  $\mathcal{C}$ , starting with position zero in  $\mathcal{C}$  and shifting the starting position by  $p$  with each iteration. Doing this for each prime  $p \leq B$  tallies the sum  $S(t, B)$  into the counter array  $\mathcal{C}$  for all  $t = a/b$  with  $a_0 \leq a < a_0 + N$ .

By loading  $\mathcal{P}$  nonsequentially, we can read the values of  $\log(N_p(b^{-1}(a_0 + i))/p)$  sequentially from memory, while requiring only a single inversion modulo  $p$  and no additional multiplications, divisions, or modular reductions.

To avoid the cost of floating point operations, we do not store  $\log(N_p(t)/p)$  as a floating-point number, but round it to a rational number with fixed denominator  $D$  and store the numerator  $\lfloor D \log(N_p(t)/p) + \frac{1}{2} \rfloor$ . The sieve then tallies these numerators for each  $t$  using integer addition, which is faster than floating-point arithmetic. The common denominator  $D$  should be large enough that rounding errors do not appreciably degrade the score, but small enough that we can keep a large counter array in the high-speed cache. We found that by taking  $D = 1024$ , we were able to fit all of our scores into 16-bit integers.

We further took advantage of a feature of modern processors known as vector instructions. These are processor level instructions that can be used to perform the same operation on multiple consecutive elements of an array simultaneously. This allowed us to add 16 elements from the update array  $\mathcal{P}$  into the counter array  $\mathcal{C}$  at once, rather than one at a time.

Compared with computing each  $S(t, B)$  individually, sieving is extremely fast. For example, for a fixed value of  $b$ , we are able to compute  $S(a/b, 2^{16})$  for  $2^{20}$  values of  $a$  in 3.2 seconds on a single thread of a hyperthreaded 2.3 GHz Intel Skylake Xeon processor. Smaller values of  $B$  take even less time; for example, computing  $S(a/b, 2^{13})$  for  $2^{20}$  values of  $a$  takes only 0.19 seconds on the same processor.

The large speed-up offered by this sieve-like technique is available only in the first step of Nagao's second trick described above: we can use it to quickly compute  $S(t, B_0)$  for all  $t$  in the search region, but not to compute  $S(t, B_i)$  for  $i \geq 1$  on a restricted set of  $t$ . For  $i \geq 1$  we must look up individual values of  $\log(N_p(t)/p)$ . However, because the sieve-like technique is so efficient, we can set  $B_0$  large enough that computing  $S(t, B_0)$  is the dominant portion of the work — see [Section 6](#).

#### 4. Choosing fibrations

Perhaps the most important ingredient in searching for high-rank elliptic curves is choosing a good fibration to search on. We'll describe the factors that guided our choices, while leaving the specific choices of fibrations to [Sections 9 — 14](#).

In the past, the largest rank elliptic curves having torsion subgroups  $\mathbb{Z}/2\mathbb{Z}$ ,  $\mathbb{Z}/3\mathbb{Z}$ , and  $\mathbb{Z}/4\mathbb{Z}$  have come from specializations of K3 surfaces having relatively large rank (9 for  $\mathbb{Z}/2\mathbb{Z}$ , 5 for  $\mathbb{Z}/3\mathbb{Z}$ , and 4 for  $\mathbb{Z}/4\mathbb{Z}$ ). Our search was no different, focusing on the same families in which the previous records were found.

By contrast, high-rank K3 surfaces are not known to exist for the other torsion groups we considered. The largest known rank of a K3 surface having torsion subgroup  $\mathbb{Z}/5\mathbb{Z}$  or  $\mathbb{Z}/6\mathbb{Z}$  is 1, and the universal elliptic curve having a point of order 7 is already a K3 surface, of generic rank zero. As a result, previous searches have focused on high-degree elliptic surfaces of larger rank [\[15; 6\]](#).

We initially attempted to do the same for the group  $\mathbb{Z}/6\mathbb{Z}$  using a degree 4 elliptic surface of Kihara having rank 3 [\[14\]](#) considered in [\[6\]](#). We found that while this surface has a relatively large number of low-height rank 8 specializations, we could not find any such specializations of parameter height larger than  $\approx 2^{13.5}$ . This suggested that as the height of  $t$  grew, either the number of high-rank specializations in this family decayed rapidly or our scores quickly became less meaningful.

While [\[6\]](#) considered other degree 4 elliptic surfaces having Mordell–Weil group  $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}^3$ , we concluded that the low-hanging fruit on these had already been discovered, and that our best hope of finding a rank 9 curve having torsion subgroup  $\mathbb{Z}/6\mathbb{Z}$  was to search on the universal elliptic curve with a point of order 6, which is a rational surface. We made a similar decision regarding the groups  $\mathbb{Z}/n\mathbb{Z}$  for  $n = 5$  and  $n = 7$ , for which the universal elliptic curve over  $X_1(N)$  is respectively rational and K3.

**Remark.** Subsequent to ANTS-XIV but prior to publication, Maksym Voznyy discovered a rank 9 curve with torsion subgroup  $\mathbb{Z}/6\mathbb{Z}$  as a low-height specialization of an elliptic surface of degree 4 having Mordell–Weil group  $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}^2$  [\[29\]](#). This curve is somewhat larger than the one we present in [Section 13](#), and appears in [\[5\]](#).

## 5. Computing ranks

After finding a set of values of  $t$  such that  $S(t, B)$  is sufficiently large, we are left with the problem of identifying those that actually have large rank. We approach this problem in two stages. First, we use descent methods to obtain an upper bound on the rank. For those specializations where the upper bound is sufficiently large, we then search for points on whichever coverings we can efficiently compute.

**5.1. Descent computations.** For half of the families we considered, the torsion subgroup contains a point of order 2, so we could use Fisher’s machinery for computing rank bounds using 2-power isogeny Selmer groups, available in Magma via the command `TwoPowerIsogenyDescentRankBound` [13]. For all of the specializations we considered where this upper bound was at least as large as the previous record in the family, the upper bound was in fact equal to the rank (though of course we did not know this until after we searched for points).

For the specializations with torsion subgroup  $\mathbb{Z}/3\mathbb{Z}$ , there is no 2-isogeny over  $\mathbb{Q}$ , and a full 2-descent was out of reach. This forced us to consider a different approach.

As a first attempt, we ran all of the high scorers through a slightly modified version of Magma’s `ThreeIsogenySelmerGroups` command to obtain a coarse rank bound. While the rank bound coming from 3-descent via isogeny tends to be reasonably tight for small curves, many of the specializations we considered had a large number of places of split multiplicative reduction, which boosted this bound for structural reasons unconnected to rank. To deal with this, we then used our own implementation of the algorithm for computing the Cassels–Tate pairing developed by Fisher and van Beek [1; 2] to compute the 3-Selmer rank of each specialization for which the rank bound coming from 3-isogeny descent was at least 14.

For the curves with  $\mathbb{Z}/5\mathbb{Z}$  torsion, we were able to use a modified version of the `pIsogenyDescent` command in Magma to compute a rank bound coming from 5-descent via isogeny, which allowed us to eliminate close to 99% of the candidate specializations. Since the fibration with  $\mathbb{Z}/5\mathbb{Z}$  torsion that we searched is a rational surface over  $\mathbb{Q}(t)$ , the remaining specializations were sufficiently small that we could use Magma’s built-in implementations for computing both the 2-Selmer group and the Cassels–Tate pairings for each one.

The curves with  $\mathbb{Z}/7\mathbb{Z}$  torsion posed a unique challenge. While we were able to use our modified version of Magma’s `pIsogenyDescent` command to compute a rank bound coming from 7-descent via isogeny, this bound tended to be insufficiently sharp for our candidate specializations.

In addition, because the  $\mathbb{Z}/7\mathbb{Z}$  fibration we considered is a K3 surface over  $\mathbb{Q}(t)$ , we expected that the size of our specializations would overwhelm Magma’s 2-descent machinery. However, we discovered that while the discriminant of this surface has degree 24, the discriminant of the cubic subfield of its 2-division field has degree only 6. As a result, although the curves in question were quite large, it was still possible to perform 2-descent and the Cassels–Tate pairings on them.

**5.2. Searching for points.** Once we had candidate curves that our Selmer computations suggested had large rank, we needed to find enough independent points on them to verify that they had the expected rank.

Our main method for finding these points was by searching for points on 2-coverings of each curve using Magma’s built-in functionality. For most of the groups —  $\mathbb{Z}/4\mathbb{Z}$ ,  $\mathbb{Z}/5\mathbb{Z}$ ,  $\mathbb{Z}/6\mathbb{Z}$ , and  $\mathbb{Z}/7\mathbb{Z}$  — we were able to compute the complete 2-Selmer group for each of the curves in question.

For the group  $\mathbb{Z}/2\mathbb{Z}$ , we did the next best thing, computing the coverings corresponding to the elements of the Selmer group of a 2-isogeny and its dual, and searching on those.

In principle, we could have done something similar with the 3-isogeny coverings for the curves having torsion subgroup  $\mathbb{Z}/3\mathbb{Z}$  using Elkies’s lattice-based method of searching for points on cubic curves in  $\mathbb{P}^2$  [7]. However, due to a memory leak we discovered<sup>1</sup> in Magma’s implementation of Elkies’s method, doing so would have required additional effort. Instead, we searched the 2-coverings corresponding to the known points on each curve coming from the rational points on the surface  $\mathcal{E}$ , adding new 2-coverings to the mix whenever we discovered an additional point.

Somewhat surprisingly, this method worked extremely well. We suspect that because each of the curves in question has a large number of points of low height, we likely would have found them using nearly any method we attempted.

## 6. Choosing parameters

There is an art to choosing proper values for  $B_i$  and  $C_i$ . The goal, of course, is to minimize the total time spent searching, while not missing any of the top candidates. How to do this is unclear. We chose our values experimentally, and we suspect that our choices were far from optimal; see [Section 7](#). Some tradeoffs however are straightforward.

If  $C_0$  is too small, then too many values of  $t$  pass the initial cutoff, so the cost of computing  $S(t, B_i)$  for  $i \geq 1$  dominates, because looking up the values of  $\log(N_p(t)/p)$  individually is far more expensive than sieving. Conversely, if  $C_0$  is too large then we risk eliminating promising values of  $t$ .

We compromised by choosing  $C_0$  rather aggressively, targeting a cutdown on the order of  $10^3$ , but using a large enough value of  $B_0$  (between  $2^{13}$  and  $2^{16}$ ) to limit the risk of losing any good candidate  $t$ . (Previous searches have tended to take  $B < 10^3$ , so this seemed sufficiently conservative.)

The values of  $B_i$  for  $i \geq 1$  are less important. We chose the  $B_i$  to be successive powers of 2 up to  $B = 2^{18}$ . We also chose our  $C_i$  less aggressively for  $i \geq 1$ , since these have a smaller effect on the runtime.

**6.1. Skewed search regions.** For some of the fibrations we considered, the polynomials defining the nontrivial coefficients of  $\mathcal{E}$  were skew in the sense of [22]. Very roughly, this means that the higher degree coefficients tend to have larger magnitude than the smaller ones or vice versa.

As a result, the average magnitude of the coefficients of an integral model for  $E_t$  on a skewed search region (that is,  $t = a/b$  with  $\text{Max}(|a|) = s\text{Max}(|b|)$  for some  $s \in \mathbb{Q}$ ) will be smaller than the average magnitude of the coefficients of an integral model for  $E_t$  on a square search region having the same size. While we don’t have a firm grasp on how the existence of high-rank specializations is related to the

<sup>1</sup>While we discovered the presence of this memory leak, we did not attempt to identify its source.

coefficient size of  $E_t$ , it seems sensible to search for smaller curves, so we skewed our search regions accordingly.

## 7. Open questions

Although our search was largely successful, we are left with some open questions regarding the method of Mestre and Nagao.

- (1) How large a prime bound should we be using relative to the search region/degree of the family?

Our experience indicates that the score  $S(t, B)$  tends to be a poorer indicator of rank as the size of the search region grows, and that the rate at which it becomes less useful depends on the degree of the surface and on its torsion subgroup.

This is unsurprising, since we expect the convergence rate of the Euler product for  $L_{E_t}(s)$  to depend on the conductor, which in turn grows roughly as a power of the height  $H(t)$  depending on the degree and fiber types of the surface. (More precisely, the conductor is bounded above by a multiple of that power of  $H(t)$ , and for typical  $t$  this is the correct growth order.) We should therefore expect that we need to allow our prime bound  $B$  to grow as a function of  $\mathcal{E}$  and  $H(t)$  in order for  $S(t, B)$  to remain useful. Is it possible to make this relationship precise?

- (2) How can we incorporate the Tamagawa factors at the places where  $E_t$  has bad reduction?

It has been observed that the known curves of high rank tend to have split multiplicative reduction and large Tamagawa numbers at many small primes. While the  $L$ -function includes terms for the bad primes and these can be incorporated into  $S(t, B)$ , these terms don't incorporate the Tamagawa numbers.

One idea would be to include these primes into the score via the term  $\log(c_p(E_t)(p-1)/p)$ . However, this seems odd, because for surfaces with an isogeny, the Tamagawa numbers of  $E_t$  and its isogenous curves will generally not be the same, and any score that hopes to predict the rank should be isogeny-invariant.

In our searches, we found that including the term  $\log(c(p-1)/p)$  with various  $c$  between 1 and 2 in  $S(t, B)$  at each prime of split multiplicative reduction (effectively giving the specialization a fixed bonus for each such prime) tended to work reasonably well. At the same time, this is clearly a hack, and it would be nice to understand what the correct thing to do is.

- (3) How closely should the rank be expected to correlate with  $S(t, B)$ ?

One problem that we struggled with was understanding exactly how the score  $S(t, B)$  should relate to the rank of  $E_t$ . For now, we are forced to choose our bounds conservatively to avoid missing any high-rank curves, which results in an increased amount of work, particularly at the descent steps.

Ideally, we would have a Bayesian score  $\text{Prob}(E_t \text{ has rank at least } r \mid S(t, B) > C)$  that would let us set the bounds  $B_i$  and  $C_i$  optimally, and inform our decision about how many curves to apply descent methods to. (The use of a Bayesian score was suggested to us by Joel Rosenberg.) Such a score would also let us estimate the likelihood that we missed a curve of high rank.

torsion subgroup	previous record	current record
$\mathbb{Z}/2\mathbb{Z}$	19	20
$\mathbb{Z}/3\mathbb{Z}$	14	15
$\mathbb{Z}/4\mathbb{Z}$	12	13
$\mathbb{Z}/5\mathbb{Z}$	8	9
$\mathbb{Z}/6\mathbb{Z}$	8	9
$\mathbb{Z}/7\mathbb{Z}$	5	6

Table 1. Rank records for various torsion subgroups.

8. Main results

We obtained new rank records for elliptic curves with torsion subgroups  $\mathbb{Z}/n\mathbb{Z}$  for  $n = 2, 3, 4, 5, 6$ , and  $7$ . The current and previous records (as given by [5]) for each of these torsion subgroups are given in Table 1. We note that for the torsion subgroups  $\mathbb{Z}/n\mathbb{Z}$  with  $n = 2, 3, 4, 5, 6$ , the ranks of both our curves and the previous record-holding curves are known unconditionally. While the ranks of some of the previous record-holding curves for the torsion subgroup  $\mathbb{Z}/7\mathbb{Z}$  are known unconditionally, the ranks of our record holding curve as well as some of the previous record-holding curves are known only subject to the generalized Riemann hypothesis (GRH) for  $L$ -functions of number fields. The next sections describe in greater detail the searches we carried out in pursuit of these records.

9. Curves with torsion subgroup  $\mathbb{Z}/2\mathbb{Z}$

For torsion groups  $T = \mathbb{Z}/2\mathbb{Z}$ ,  $\mathbb{Z}/3\mathbb{Z}$ ,  $\mathbb{Z}/4\mathbb{Z}$  we proceeded as in [8], computing an elliptic fibration  $\mathcal{E}(\mathbb{Q}_t)$  of a K3 surface  $X$  whose Néron–Severi group  $\text{NS}(X)$  is defined over  $\mathbb{Q}$  and has high rank and large discriminant. For  $T = \mathbb{Z}/3\mathbb{Z}$  and  $T = \mathbb{Z}/4\mathbb{Z}$  we used the surface with  $\text{NS}(X)$  of rank 20 and discriminant  $-163$ . But for  $T = \mathbb{Z}/2\mathbb{Z}$  this discriminant is not large enough; it turns out [10] that the highest rank attained by an elliptic fibration of  $X$  with a 2-torsion point is 8. Instead we use  $X$  with  $\text{NS}(X)$  of rank 19 but larger discriminant, which can attain Mordell–Weil rank 9.

Such  $X$  are parametrized by elliptic or Shimura modular curves, call them  $C$ , of level  $\frac{1}{2}|\text{disc NS}(X)|$ . When  $|\text{disc NS}(X)|$  is large enough to allow Mordell–Weil rank 9, the curve  $C$  usually has genus at least 2, with few if any rational points (other than cusps and CM points, at which  $X$  or the elliptic fibration degenerates). In [8, pp. 8–9] Elkies reports using the sporadic rational point on the genus-2 curve  $X_0(191)/w$  to find such an  $X$ . A few years later he found a genus-zero Shimura curve of level 230 that could be used instead, giving a family of elliptic surfaces with Mordell–Weil group  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^9$ . Here  $C = \mathcal{X}/w_{230}$ , with  $\mathcal{X}$  associated to the congruence subgroup  $\Gamma_0(23)$  of the quaternion algebra ramified at  $\{2, 5\}$ . The family of surfaces with their elliptic fibrations was computed as in [9; 11]. The elliptic fibration is of the form  $\mathcal{E}_u/\mathbb{Q}(t) : y^2 = x^3 + 2Ax^2 + Bx$ , where

$$\begin{aligned} A = & (u^8 - 18u^6 + 163u^4 - 1152u^2 + 4096)t^4 + (3u^7 - 35u^5 - 120u^3 + 1536u)t^3 \\ & + (u^8 - 13u^6 + 32u^4 - 152u^2 + 1536)t^2 + (u^7 + 3u^5 - 156u^3 + 672u)t \\ & + (3u^6 - 33u^4 + 112u^2 - 80), \end{aligned} \tag{3}$$

and  $B = \prod_{i=1}^8 B_i(t, u)$  where

$$\begin{aligned} B_1(t, u) &= (u^2 + u - 8)t + (-u + 2), & B_3(t, u) &= (u^2 - u - 8)t + (u^2 + u - 10), \\ B_5(t, u) &= (u^2 - 7u + 8)t + (-u^2 + u + 2), & B_7(t, u) &= (u^2 + 5u + 8)t + (u^2 + 3u + 2), \end{aligned} \quad (4)$$

and  $B_i(t, u) = -B_{i-1}(-t, -u)$  for  $i = 2, 4, 6, 8$ . Thus  $\mathcal{E}_u \cong \mathcal{E}_{-u}$ . If  $5 - u^2$  is a square, and  $u \neq \pm 1, \pm 2$  (to exclude CM points), then  $\mathcal{E}_u$  has Mordell–Weil group  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^9$  over  $\mathbb{Q}(t)$ . Generators are exhibited in [Appendix A](#).

We searched for high-rank specializations of  $\mathcal{E}_u$  for several values of  $u$ .

For  $u = 2/5$ , we searched the region  $t = a/b$  with  $0 < a < 2^{21}$  and  $-2^{23} < b < 2^{23}$ , finding 17 curves of rank 19, including the previous record-holding curve of Elkies that appears in [\[5\]](#), which occurs at  $t = 11860/97527$ .

For  $u = 11/5$ , we first applied the linear fractional transformation  $t \mapsto (2 - t)/(t - 6)$  to  $\mathcal{E}_u$  and then searched the region  $t = a/b$  with  $0 < a < 3 \cdot 2^{21}$  and  $-2^{21} < b < 2^{21}$ . We found one specialization of rank 20 at  $t = -68559/32629$  ( $t = -721141/2026305$  on the original model of  $\mathcal{E}_u$ ), as well as another 20 specializations of rank 19, including one at  $t = 100782/104143$  ( $t = -26876/131019$  on the original model of  $\mathcal{E}_u$ ) with smaller discriminant than the rank 19 curve of Elkies appearing in [\[5\]](#).

Minimal models and  $x$ -coordinates of a set of generators for the rank 20 specialization and the smallest discriminant rank 19 specialization appear in [Appendix B.2](#). We note that this curve of rank 20 is the elliptic curve of largest rank for which the rank is known unconditionally.

We also searched regions of size roughly  $2^{44}$  on each of the fibrations coming from  $u = 2/13$  and  $u = 22/13$ , but did not find any specializations of rank greater than 18.

## 10. Curves with torsion subgroup $\mathbb{Z}/3\mathbb{Z}$

The singular K3 surface of discriminant  $-163$  has (up to isomorphism) 159 elliptic fibrations with torsion group  $\mathbb{Z}/3\mathbb{Z}$ ; their Mordell–Weil ranks range from 1 to 5. Rank 5 is attained by 13 of those fibrations, each giving rise to a family of elliptic curves whose Mordell–Weil group contains  $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}^5$ ; the explicit formula will appear in [\[10\]](#).

We searched an appropriately skewed region of size  $2^{43}$  on each of the 13 fibrations, finding 34 specializations of rank 14 (at least one on 11 of the 13 fibrations) as well as a single specialization of rank 15, given by

$$E : y^2 + 490738465519xy - 432802729180188878035670522423557875y = x^3.$$

Among the specializations having rank 14, the one with smallest conductor and discriminant is given by

$$E : y^2 + 6244332976xy + 2204421250641922174556630375y = x^3,$$

which has smaller conductor and discriminant than the previously known curve of rank 14 appearing in [\[5\]](#). The  $x$ -coordinates of a set of generators for each of these curves is given in [Appendix B.3](#).



### 11. Curves with torsion subgroup $\mathbb{Z}/4\mathbb{Z}$

We searched a pair of families each having Mordell–Weil group  $\mathbb{Z}^4 \times \mathbb{Z}/4\mathbb{Z}$ , both of which are elliptic fibrations of the singular K3 surface of discriminant  $-163$ . The first fibration is given by the equation

$$\begin{aligned} \mathcal{E}_1 : y^2 + (8t - 1)(32t + 7)xy + 8(8t - 1)(32t + 7)(t + 1)(15t - 8)(31t - 7)y \\ = x^3 + 8(t + 1)(15t - 8)(31t - 7)x^2 \end{aligned} \quad (5)$$

and appears (with a typo) in [8]. A choice of  $x$ -coordinates defining four independent sections is given by

$$\begin{aligned} &(-15/4)(t + 1)(31t - 7)(32t + 7), \quad (8t - 1)(15t - 8)(31t - 7)(32t + 7), \\ &-(t + 1)(8t - 1)(15t - 8)(32t + 7), \quad -4(t + 1)(2t + 5)(15t - 8)(32t + 7). \end{aligned}$$

The second fibration is given by the equation

$$\begin{aligned} \mathcal{E}_2 : y^2 - 8(80t + 9)xy - 16(80t + 9)(t - 2)(2t - 1)(18t - 1)(2t - 81)y \\ = x^3 + 2(t - 2)(2t - 1)(18t - 1)(2t - 81)x^2 \end{aligned} \quad (6)$$

and will appear in [10]. A choice of  $x$ -coordinates defining four independent sections is given by

$$\begin{aligned} &154(t - 2)(2t - 1)(18t - 1), \quad -1456(t - 2)(2t - 1)(2t - 81), \\ &16(t - 2)(2t - 81)(22t + 21), \quad 6(2t - 5)(t - 2)(2t - 81)(18t - 1). \end{aligned}$$

The previous rank record for torsion group  $\mathbb{Z}/4\mathbb{Z}$  was 12, attained by two curves in the family  $\mathcal{E}_1$ , found by Elkies in 2006 ( $t = 18745/6321$ ) and Dujella and Peral in 2014 ( $t = -13083/72895$ ). We searched up to height  $2^{22}$  on  $\mathcal{E}_1$  and found three rank 13 specializations at  $t = -1086829/638219$ ,  $t = -2856967/190447$ , and  $t = 973215/3135431$ , as well as 76 rank 12 specializations. Of the rank 12 specializations, the one with smallest conductor occurs at  $t = -447577/2601952$  ( $N_{E_t} \approx 2^{153.41}$ ) and the one with smallest discriminant occurs at  $t = 83497/251378$  ( $|\Delta_{E_t}| \approx 2^{392.96}$ ). Respectively, these have smaller conductor and discriminant than the previously known rank 12 curves.

We searched up to height  $2^{22}$  on  $\mathcal{E}_2$  and were unable to find any specializations of rank 13, though we did find 32 having rank 12. Among these, the specialization with smallest conductor and discriminant appears at  $t = -16307/121584$  ( $N_{E_t} \approx 2^{161.21}$  and  $|\Delta_{E_t}| \approx 2^{433.71}$ ).

Minimal models and  $x$ -coordinates of a set of generators for each of the rank 13 specializations are given in [Appendix B.4](#).

### 12. Curves with torsion subgroup $\mathbb{Z}/5\mathbb{Z}$

As noted in [Section 4](#), for the group  $\mathbb{Z}/5\mathbb{Z}$ , we chose to search for good specializations on the universal elliptic curve having a point of order 5, which is a rational elliptic surface. One particularly nice model for this surface is given by

$$y^2 + (t + 1)xy + ty = x^3 + tx^2,$$

which has the feature that the nontrivial automorphism of  $X_1(5)$  as a cover of  $X_0(5)$  is given by  $t \mapsto -1/t$ .



Changing  $t$  to  $-1/t$  yields the same curve with a different choice of generator of its torsion group. This allowed us to limit our search to  $t > 0$ . We searched for  $t$  up to height  $2^{29}$  on this surface, finding a single rank 9 curve at  $t = 266165145/442317512$ .

We also found 392 rank 8 specializations, three of which were previously known. Of these, the curve we found with smallest conductor appears at  $t = 1809535/5292661$  ( $N_{E_t} \approx 2^{85.86}$ ) and the curve we found with smallest discriminant appears at  $t = 5167107/723695$  ( $|\Delta_{E_t}| \approx 2^{254.77}$ ). Each of these has both smaller conductor and discriminant than all of the previously known rank 8 curves.

Minimal models and  $x$ -coordinates of a set of generators for the rank 9 specialization and the smallest conductor and discriminant rank 8 specializations appear in [Appendix B.5](#).

### 13. Curves with torsion subgroup $\mathbb{Z}/6\mathbb{Z}$

As was the case for  $\mathbb{Z}/5\mathbb{Z}$ , we chose to search for good specializations on the universal elliptic curve having a point of order 6, which is a rational elliptic surface. A model for this surface is given by

$$y^2 + txy + (t+2)y = x^3,$$

with torsion points of order 2, 3, 6 at  $(x, y) = (-1, -1), (0, 0), (t+2, t+2)$ , respectively.

We searched for good specializations of this model in the region  $t = a/b$  with  $0 < a < 2^{25}$  and  $-2^{26} < b < 2^{26}$ . In this case, the skewed search region was a fortuitous accident, rather than a deliberate choice. We found a single rank 9 curve at  $t = -22029701/37178488$  as well as 71 rank 8 specializations, all but one of which appear to be previously unknown. The rank 8 curve with the smallest conductor and smallest discriminant appears at  $t = 6308333/1000939$  ( $N_{E_t} \approx 2^{81.96}$  and  $|\Delta_{E_t}| \approx 2^{253.07}$ ). Its 2-isogenous curve that appears at  $t = -24627934/8310211$  shares the same conductor, but has larger discriminant.

Minimal models and  $x$ -coordinates of a set of generators for the rank 9 specialization and the smallest conductor/discriminant rank 8 specialization appear in [Appendix B.6](#).

**Remark.** In retrospect, we could have taken advantage of the involution  $w_2 : t \mapsto -(2t+12)/(t+2)$ , for which  $E_{w_2(t)}$  is the curve  $E'_t$  which is 2-isogenous with  $E_t$ , and thus also has torsion subgroup  $\mathbb{Z}/6\mathbb{Z}$ . This would let us restrict our search area to  $-4 < t < 2$ . In partial compensation, we could compare the scores of  $t$  and  $w_2(t)$  to corroborate that we are computing these scores correctly.

### 14. Curves with torsion subgroup $\mathbb{Z}/7\mathbb{Z}$

As noted in [Section 4](#), for the group  $\mathbb{Z}/7\mathbb{Z}$ , we chose to search for good specializations of the universal elliptic curve having a point of order 7. Unlike the groups  $\mathbb{Z}/5\mathbb{Z}$  and  $\mathbb{Z}/6\mathbb{Z}$ , the universal elliptic curve having a point of order 7 is a K3 surface rather than a rational one.

A model for this curve is given by

$$y^2 + (-t^2 + t + 1)xy + (-t^3 + t^2)y = x^3 + (-t^3 + t^2)x^2$$

(see, e.g., [\[28, p. 195\]](#)).

The modular curve  $X_1(7)$  has two nontrivial automorphisms as a cover of  $X_0(7)$ . These correspond to the transformations  $t \mapsto 1 - 1/t$  and  $t \mapsto -1/(t - 1)$  on this surface which allowed us to restrict ourselves to considering  $0 < t < 1$ .

We searched up to height  $2^{20}$  on this model and found a single specialization of rank 6 at  $t = -748328/820369$ . A minimal model and the set of  $x$ -coordinates of a set of generators of this specialization are given in [Appendix B.7](#).

**Remark.** In addition to the group  $\mathbb{Z}/7\mathbb{Z}$ , there are two other groups  $G$ , namely,  $G = \mathbb{Z}/8\mathbb{Z}$  and  $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ , for which the universal elliptic curve  $E$  with a copy of  $G$  in  $E(\mathbb{Q})$  is a K3 surface. The rank record for each of these two  $G$  is 6, and [\[5\]](#) lists several curves attaining this record in each case. We looked for curves of larger rank for each of these torsion subgroups by searching on a model of the corresponding universal elliptic curve, but failed to find any specialization having rank greater than 6. We suspect that the reason we found a record-breaking curve for  $\mathbb{Z}/7\mathbb{Z}$  but not for  $\mathbb{Z}/8\mathbb{Z}$  or  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$  is simply that the previous record was lower for  $\mathbb{Z}/7\mathbb{Z}$ .

### Appendix A: Points on $\mathcal{E}_u/\mathbb{Q}(t)$

Recall that in [\(3\)](#) and [\(4\)](#) we exhibit  $A$  and  $B_1, \dots, B_8$  in  $\mathbb{Q}[t, u]$  such that  $\mathcal{E}_u/\mathbb{Q}(t)$  has Weierstrass equation  $y^2 = x^3 + 2Ax^2 + Bx$  where  $B = \prod_{i=1}^8 B_i$ . The minimal height of a nontorsion section is 2, attained by 70 pairs  $(x, \pm y)$  with  $x, y \in \mathbb{Q}(u, \sqrt{5-u^2})[t]$ . We find that 58 of the 70 pairs have  $x, y \in \mathbb{Q}(u)[t]$ ; these generate a Mordell–Weil subgroup of rank 8. One simple choice of generators of this subgroup consists of points with  $x$ -coordinates

$$\begin{aligned} & -B_1 B_2 B_3 B_6, \quad -B_1 B_2 B_4 B_5, \quad 4B_1 B_2 B_5 B_6, \quad B_1 B_3 B_4 B_6, \\ & -B_1 B_3 B_4 B_7, \quad B_1 B_3 B_4 B_8, \quad B_1 B_3 B_5 B_6, \quad -B_1 B_5 B_6 B_7. \end{aligned} \tag{7}$$

Extending  $\mathbb{Q}(u)$  by  $\sqrt{5-u^2}$  yields  $\mathbb{Q}(m)$  where  $m$  is a rational coordinate on the parametrizing Shimura curve, with

$$u = 2 \frac{m^2 - m - 1}{m^2 + 1}, \quad (5 - u^2)^{1/2} = \pm \frac{m^2 + 4m - 1}{m^2 + 1}; \tag{8}$$

then adding  $-(m-1)^2 B_1 B_2 B_3 B_8$  to the list [\(7\)](#) gives  $x$ -coordinates of 9 Mordell–Weil generators modulo torsion. The Gram matrix of canonical height pairings is

$$\frac{1}{2} \begin{bmatrix} 4 & 0 & 1 & -1 & 0 & 2 & -1 & 0 & 1 \\ 0 & 4 & -1 & -2 & 0 & 2 & -2 & 0 & 0 \\ 1 & -1 & 4 & 0 & -1 & 1 & -1 & 1 & 2 \\ -1 & -2 & 0 & 4 & -1 & -1 & 1 & 0 & 0 \\ 0 & 0 & -1 & -1 & 4 & 1 & 0 & -2 & 0 \\ 2 & 2 & 1 & -1 & 1 & 4 & -2 & -1 & 1 \\ -1 & -2 & -1 & 1 & 0 & -2 & 4 & 1 & 0 \\ 0 & 0 & 1 & 0 & -2 & -1 & 1 & 4 & 1 \\ 1 & 0 & 2 & 0 & 0 & 1 & 0 & 1 & 4 \end{bmatrix}, \tag{9}$$

with determinant 115/16.

## Appendix B: Models for record breaking curves

**B.1. Overview.** This section gives minimal integral models for each of the record breaking curves we discovered, along with the  $x$ -coordinates of a set of points that, at a minimum, generates the torsion-free part of each of them. We expect that this set of points generates the full torsion-free part of each curve given, but have not tried to prove this rigorously.

By common convention we use a vector  $(a_1, a_2, a_3, a_4, a_6)$  to mean the extended Weierstrass model

$$y^2 + a_1xy + a_3x = x^3 + a_2x + a_4x + a_6$$

whose coefficients are the vector's entries. We usually depart from another common convention that chooses the model with  $a_1, a_3 \in \{0, 1\}$  and  $a_2 \in \{-1, 0, 1\}$ . Such models have the advantage of being unique, but for curves with nontrivial torsion there may be one or more other choices that put a torsion point at  $(x, y) = (0, 0)$  and have a coefficient vector with noticeably fewer digits (for starters  $a_6 = 0$  if  $(0, 0)$  is on the curve).

When possible we give a generating set of  $E(\mathbb{Q}) \bmod E(\mathbb{Q})_{\text{tors}}$  consisting of integral points of small height. For most of our curves there are plenty of such points to choose from, even though there can be other curves with the same torsion group and somewhat lower rank that have even more integral points.

**B.2.  $\mathbb{Z}/2\mathbb{Z}$ .** A minimal model for the rank 20 curve having  $\mathbb{Z}/2\mathbb{Z}$  torsion has coefficients

$$(1, -1, 1, -244537673336319601463803487168961769270757573821859853707, \\ 961710182053183034546222979258806817743270682028964434238957830989898438151121499931).$$

Here we reluctantly give a model with small  $a_1, a_2, a_3$  and huge  $a_4, a_6$ , because the torsion point has  $x = -69288588686111702678625616725/4$  and thus cannot be put at the origin on a minimal model.<sup>2</sup>

One choice of 20 points that generate its Mordell–Weil group modulo torsion has  $x$ -coordinates

$$\begin{array}{ll} -5976635286513806621064126789, & 595416388787490259443766591, \\ 2434562872293108275107029075, & 3513074027344435171140978981, \\ 399682145249051758133327419, & -10714754038296881855524018251, \\ -16034220456847626275437501599, & 1185828672355214392425799131, \\ -11190697582885409770718510409, & 2634316446310680332042122261, \\ 64222149978369055569434725591, & 23945425437351916471937562579, \\ 13094114400583295432756346651, & 2689776334541089917424552236511, \\ -2627014038979941829331861469, & 113605800622499112413124359631, \\ -7364938748841807757773625709, & -14298222927159284914180072349, \\ 785686589410787916270883192839, & -2250170491079839258934900709. \end{array}$$

Here and later we list generators in increasing order by canonical height.

<sup>2</sup>The coefficients  $(2, -207865766058335108035876850179, 0, 10490122792958386322093670444427223877319227761081795217921, 0)$  give a model with smaller coefficients that puts the torsion point at  $(0, 0)$  but is not minimal at 2.

A minimal model for the rank 19 curve with  $\mathbb{Z}/2\mathbb{Z}$  torsion having smallest known discriminant has coefficients

$$(1, 4040549489437705068551042, 0, 39096673111815206065773237234587256582331296000, 0).$$

One choice of 19 points that generate its Mordell–Weil group modulo torsion has  $x$ -coordinates

$$\begin{aligned} &-3613294426098135199878600, & 284077053735716552925900, \\ &-69786343891815820666800, & 6409078899434870587500, \\ &4711243262341394854929360, & -200862034480295787990300, \\ &49746704013683926431600, & 1283007628272047952000, \\ &601243680664306184613420, & 1681679070386109358006014, \\ &-178674347439204200162150, & -140058466067600728971180, \\ &4490592251930741573760, & -1245418009246864352006250, \\ &239435938047242410050720, & -2615926042511102882808000, \\ &-3662820474106418641536000, & 308679854892675472378120, \\ &-12130119373140047385600. \end{aligned}$$

**B.3.**  $\mathbb{Z}/3\mathbb{Z}$ . The rank 15 elliptic curve with coefficient vector

$$(490738465519, 0, -432802729180188878035670522423557875, 0, 0)$$

has a 3-torsion point at  $(x, y) = (0, 0)$ . One choice of 15 points that generate its Mordell–Weil group modulo torsion has  $x$ -coordinates

$$\begin{aligned} &414082294873186000299147, & -461076037958619691375950, & 136016697778663191410466, \\ &579811074194569447550775, & 4156065765459153070875350, & -379256436856490083222605, \\ &-480257266200757201099125, & 626879349686994759271350, & 319402198167922579675875, \\ &9987762741068630814895872, & 1025559076978453798187316, & 17710047123788181654048375, \\ &236426830570889446065942, & -162860681446721622110565, & 1093411474853808475876875. \end{aligned}$$

The rank 14 elliptic curve with coefficient vector

$$(6244332976, 0, -2204421250641922174556630375, 0, 0)$$

has a 3-torsion point at  $(x, y) = (0, 0)$ . One choice of 14 points that generate its Mordell–Weil group modulo torsion has  $x$ -coordinates

$$\begin{aligned} &2907919170263662, & -65199074165293250, & 71604990115331040, & 77567806466944000, \\ &108999498650081840, & 169617569990697350, & -171009947870163008, & -204167066230390100, \\ &-240427032442334750, & 243676691791782250, & -256142889038646510, & -276580713950955750, \\ &368313341140417750, & -449841531945448000. \end{aligned}$$

**B.4.**  $\mathbb{Z}/4\mathbb{Z}$ . The first rank 13 curve with  $\mathbb{Z}/4\mathbb{Z}$  torsion has a minimal model with coefficient vector

$$(282887999996745, -1871148179781457712818452480, -529325366275926422138597740307015937177600, 0, 0)$$

and a 4-torsion point at  $(x, y) = (0, 0)$ . One choice of 13 points that generate its Mordell–Weil group

modulo torsion has  $x$ -coordinates

37563104221873287230436120000, 1241851783771179145432296000,  
 1992140999686088390294877150, 30921042737991542683359263880,  
 -21195532433936174709304166400, -1464098167733086800531916800,  
 1670745991840921221771294750, 1252355926117744178967180450,  
 -1960920553671074388872220170, 1375293185347275499663130572800,  
 2549902537861429590505036800, 3272919221738028252106303872714,  
 102225511700163143939329914880.

The second rank 13 curve with  $\mathbb{Z}/4\mathbb{Z}$  torsion has a minimal model with coefficient vector

(230691818102905, -200100346570723590045845120,  
 -46161512753421616727023025112895852073600, 0, 0)

and a 4-torsion point at  $(x, y) = (0, 0)$ . One choice of 13 points that generate its Mordell–Weil group modulo torsion has  $x$ -coordinates

190412869629748629206788500, -11655521125151390350616252280,  
 -10482658909728296079200226100, -205253870232797421109008000,  
 193230556828647163522857600, 2390337099874364874239977850,  
 -10561431236301791011714683300, -1195165694989063921020955200,  
 876665740401972718169616600, -99112055810721390011710344,  
 -65566000913948267196883584, 166949951644450209072942720,  
 -26328612670314620364001050.

The third rank 13 curve with  $\mathbb{Z}/4\mathbb{Z}$  torsion has a minimal model with coefficient vector

(246888014319233, -8884285566590219865500325632,  
 -2193423622180481268696018169961040300480256, 0, 0)

and a 4-torsion point at  $(x, y) = (0, 0)$ . One choice of 13 points that generate its Mordell–Weil group modulo torsion has  $x$ -coordinates

-968516084234641058709370232, -1333726837303108113451614080,  
 1792794868671671366043266816, 2362595876319902581142656768,  
 -2746004168634841009972934984, 3469325866293712913010729024,  
 3644805279133239447459855232, 4449372053406414078540323280,  
 -4537829698895530474950049368, 5156996081584183666047796032,  
 5789474008645490085082165824, 5912795841516183863849831680,  
 10555676267250916670215460568.

**B.5.  $\mathbb{Z}/5\mathbb{Z}$ .** The rank 9 curve with  $\mathbb{Z}/5\mathbb{Z}$  torsion has a minimal model with coefficient vector

(708482657, 117729504717519240, 52073821615645373048930880, 0, 0).

The torsion group is generated by  $(x, y) = (0, 0)$ . One choice of 9 points that generate the Mordell–Weil

group modulo torsion has  $x$ -coordinates

$$\begin{aligned} &-95393153480017302, \quad 172086875265878580, \quad -12976225316716116, \\ &53638875373006560, \quad -147039491421732240, \quad 46489325594722920, \\ &-148084847397297720, \quad 21510303761449208160, \quad 79310646743033160. \end{aligned}$$

The rank 8 curve with  $\mathbb{Z}/5\mathbb{Z}$  torsion having smallest known conductor has a minimal model with coefficient vector

$$(7102196, 9577255322635, 50689165733152681735, 0, 0).$$

The torsion group is generated by  $(x, y) = (0, 0)$ . One choice of 8 points that generate the Mordell–Weil group modulo torsion has  $x$ -coordinates

$$\begin{aligned} &-11217531799903, \quad -10836503720185, \quad -4357099419673, \quad 1401549559410, \\ &256939125827615, \quad -10247328030940, \quad -6060818514894, \quad -6697297034428. \end{aligned}$$

The rank 8 curve with  $\mathbb{Z}/5\mathbb{Z}$  torsion having smallest known discriminant has a minimal model with coefficient vector

$$(5890802, 3739409500365, 2706191958366648675, 0, 0).$$

The torsion group is generated by  $(x, y) = (0, 0)$ . One choice of 8 points that generate the Mordell–Weil group modulo torsion has  $x$ -coordinates

$$\begin{aligned} &-21207376737, \quad 37660080920, \quad -89104376475, \quad 100531079550, \\ &117291419735, \quad -120660570135, \quad 148808336985, \quad -214614453600. \end{aligned}$$

**B.6.  $\mathbb{Z}/6\mathbb{Z}$ .** The rank 9 curve with  $\mathbb{Z}/6\mathbb{Z}$  torsion has a minimal model with coefficient vector

$$(-22029701, 0, 72328851024410157777600, 0, 0).$$

The torsion group is generated by  $(x, y) = (1945448965660200, 72328851024410157777600)$ ; multiplying this point by 2 yields the 3-torsion point  $(0, 0)$ . One choice of 9 points that generate the Mordell–Weil group modulo torsion has  $x$ -coordinates

$$\begin{aligned} &749629491053742, \quad 6092756193428190, \quad -1380249411088240, \\ &-1067429532233440, \quad 174532909579773030, \quad 949536320242950, \\ &1079473135677300, \quad 24157188371048640, \quad 3112751229126000. \end{aligned}$$

The rank 8 curve with  $\mathbb{Z}/6\mathbb{Z}$  torsion and smallest known conductor and discriminant has a minimal model with coefficient vector

$$(6308333, 0, 8325824903545553131, 0, 0).$$

The torsion group is generated by  $(x, y) = (8318014288129, 8325824903545553131)$ ; multiplying this point by 2 yields the 3-torsion point  $(0, 0)$ . One choice of 8 points that generate the Mordell–Weil group modulo torsion has  $x$ -coordinates

$$\begin{aligned} &-204062889121, \quad 211687889245, \quad -403788801990, \quad -410295468023, \\ &-733395115518, \quad -823562706096, \quad -859172099915, \quad -2828410292799. \end{aligned}$$

**B.7.  $\mathbb{Z}/7\mathbb{Z}$ .** The rank 6 curve with  $\mathbb{Z}/7\mathbb{Z}$  torsion has a minimal model with coefficient vector

$(-500894592455, 720663120331059917723712, 485010096730715360294683087532269632, 0, 0)$ .

The torsion group is generated by  $(x, y) = (0, 0)$ . One choice of 6 points that generate the Mordell–Weil group modulo torsion has  $x$ -coordinates

$-863240219455759708343872, 147841500613888155442368,$   
 $-655405721270483784258504, 227328163133810400709740,$   
 $17758591139156733971281176, 4457894404162347392127765558505920/79519^2.$

The large final generator is inevitable: the first five generators have canonical heights between 15.434 and 19.431, but the last generator must have height at least 42.058 (we have made the minimal choice, and with the smallest possible denominator among its seven torsion translates).

### Acknowledgements

We thank Tom Fisher for pointing out that we could easily compute  $p$ -descents via isogeny on the curves having torsion subgroups  $\mathbb{Z}/5\mathbb{Z}$  and  $\mathbb{Z}/7\mathbb{Z}$ . We thank the referees for making numerous helpful comments and suggestions. We also thank Andrej Dujella for alerting us to an inaccuracy in our original manuscript.

### References

- [1] Monique van Beek. *Computing the Cassels–Tate pairing*. Doctoral dissertation. University of Cambridge, 2015.
- [2] Monique van Beek and Tom Fisher. *Computing the Cassels–Tate pairing on 3-isogeny Selmer groups via cubic norm equations*. Acta Arithmetica Vol. 185 (2018): 367–396.
- [3] Bryan Birch and H. Peter F. Swinnerton-Dyer. *Notes on elliptic curves. I*. J. Reine Angew. Math Vol. 212.7 (1963): 7–25.
- [4] Wieb Bosma, John Cannon, and Catherine Playoust. *The Magma algebra system. I. The user language*. J. Symbolic Comput. Vol 24 (1997): 235–265.
- [5] Andrej Dujella. *High rank elliptic curves with prescribed torsion*. 2020, <https://web.math.pmf.unizg.hr/~duje/tors/tors.html>.
- [6] Andrej Dujella, Juan Carlos Peral, and Petra Tadić. *Elliptic curves with torsion group  $\mathbb{Z}/6\mathbb{Z}$* . Glasnik matematički Vol. 51.2 (2016): 321–333.
- [7] Noam D. Elkies. *Rational points near curves and small nonzero  $|x^3 - y^2|$  via lattice reduction*. International Algorithmic Number Theory Symposium. Springer LNCS Vol. 1838. Springer, Berlin, Heidelberg (2000): 33–63.
- [8] Noam D. Elkies. *Three lectures on elliptic surfaces and curves of high rank*. [arXiv:0709.2908](https://arxiv.org/abs/0709.2908)
- [9] Noam D. Elkies. *Shimura curve computations via  $K3$  surfaces of Néron–Severi rank at least 19*, Algorithmic Number Theory - ANTS VIII. Springer LNCS Vol. 5001. Springer, Berlin, Heidelberg (2008): 137–147.
- [10] Noam D. Elkies. *The 167889 even lattices of rank 18 and discriminant 163, and the 167889 elliptic fibrations of the singular  $K3$  surface of discriminant  $-163$* . Preprint, 2020.
- [11] Noam D. Elkies and Abhinav Kumar.  *$K3$  surfaces and equations for Hilbert modular surfaces*, Algebra and Number Theory Vol. 8.10 (2014): 2297–2411.
- [12] Stéfane Fermigier. *Une courbe elliptique définie sur  $\mathbb{Q}$  de rang  $\geq 22$* . Acta Arithmetica Vol. 82.4 (1997): 359–363.
- [13] Tom Fisher. *Higher descents on an elliptic curve with a rational 2-torsion point*. Mathematics of Computation Vol. 86.307 (2017): 2493–2518.

- [14] Shoichi Kihara. *On the rank of the elliptic curves with a rational point of order 6*. Proceedings of the Japan Academy, Series A, Mathematical Sciences Vol. 82.7 (2006): 81–82.
- [15] Odile Lecacheux. *Rang de courbes elliptiques sur  $\mathbb{Q}$  avec un groupe de torsion isomorphe à  $\mathbb{Z}/5\mathbb{Z}$* . Comptes Rendus de l'Académie des Sciences. Série 1, Mathématique Vol. 332.1 (2001): 1–6.
- [16] Barry Mazur. *Modular curves and the Eisenstein ideal*. Publications Mathématiques de l'Institut des Hautes Études Scientifiques Vol 47.1 (1977): 33–186.
- [17] Jean-François Mestre. *Construction d'une courbe elliptique de rang  $\geq 12$* . Comptes rendus de l'Académie des sciences. Série 1, Mathématique Vol. 295.12 (1982): 643–644.
- [18] Jean-François Mestre. *Courbes elliptiques et formules explicites*. Séminaire de théorie des nombres de Grenoble Vol. 10 (1982): 1–10.
- [19] Jean-François Mestre. *Courbes elliptiques de rang  $\geq 12$  sur  $\mathbb{Q}(T)$* . Comptes rendus de l'Académie des sciences. Série 1, Mathématique Vol. 313.4 (1991): 171–174.
- [20] Jean-François Mestre. *Un exemple de courbe elliptique sur  $\mathbb{Q}$  de rang  $\geq 15$* . Comptes rendus de l'Académie des sciences. Série 1, Mathématique Vol. 314.6 (1992): 453–455.
- [21] Louis Mordell. *On the rational solutions of the indeterminate equation of the third and fourth degree*. Proceedings of the Cambridge Philosophical Society. Vol. 21 (1922): 179–192.
- [22] Brian Murphy. *Modelling the yield of number field sieve polynomials*. Algorithmic Number Theory - ANTS III, Springer LNCS Vol. 1443. Springer, Berlin, Heidelberg, (1998): 137–150.
- [23] Koh-Ichi Nagao. *Examples of elliptic curves over  $\mathbb{Q}$  with rank  $\geq 17$* . Proceedings of the Japan Academy, Series A, Mathematical Sciences Vol. 68.9 (1992): 287–289.
- [24] Koh-ichi Nagao. *An example of elliptic curve over  $\mathbb{Q}$  with rank  $\geq 20$* . Proceedings of the Japan Academy, Series A, Mathematical Sciences Vol. 69.8 (1993): 291–293.
- [25] Jennifer Park, Bjorn Poonen, Melanie Matchett Wood, and John Voight. *A heuristic for boundedness of ranks of elliptic curves*. To appear in Journal of the European Mathematical Society.
- [26] Henri Poincaré. *Sur les propriétés arithmétiques des courbes algébriques*. J. Pures Appl. Math. Vol. 7.5 (1901): 161–234.
- [27] Joseph H. Silverman. *Heights and the specialization map for families of abelian varieties*. Journal für Mathematik. Band 342 (1983): 197–211.
- [28] John Tate. *The arithmetic of elliptic curves*. Inventiones Mathematicæ Vol. 23 (1974): 179–206.
- [29] Maksym Voznyy. Personal communication. August 2020.
- [30] Mark Watkins et al. *Ranks of quadratic twists of elliptic curves*. Publications Mathématiques de Besançon Vol. 2 (2014): 63–98.
- [31] Mark Watkins. *A discursus on 21 as a bound for ranks of elliptic curves over  $\mathbb{Q}$ , and sundry related topics*. August 20, 2015. Available at <http://magma.maths.usyd.edu.au/~watkins/papers/DISCURSUS.pdf>.

Received 24 Feb 2020.

NOAM D. ELKIES: [elkies@math.harvard.edu](mailto:elkies@math.harvard.edu)

Department of Mathematics, Harvard University, Cambridge, MA, United States

ZEV KLAGSBRUN: [zdklags@ccrwest.org](mailto:zdklags@ccrwest.org)

Center for Communications Research, San Diego, CA, United States



# The nearest-colattice algorithm: Time-approximation tradeoff for approx-CVP

Thomas Espitau and Paul Kirchner

We exhibit a hierarchy of polynomial time algorithms solving approximate variants of the closest vector problem (CVP). Our first contribution is a heuristic algorithm achieving the same distance tradeoff as HSVP algorithms, namely  $\approx \beta^{n/(2\beta)} \text{covol}(\Lambda)^{1/n}$  for a random lattice  $\Lambda$  of rank  $n$ . Compared to the so-called Kannan's embedding technique, our algorithm allows the use of precomputations and can be used for efficient batch CVP instances. This implies that some attacks on lattice-based signatures lead to very cheap forgeries, after a precomputation. Our second contribution is a proven reduction from approximating the closest vector with a factor  $\approx n^{3/2} \beta^{3n/(2\beta)}$  to the shortest vector problem (SVP) in dimension  $\beta$ .

## 1. Introduction

**Lattices, CVP, SVP.** In a general setting, a real *lattice*  $\Lambda$  is a finitely generated free  $\mathbb{Z}$ -module, endowed with a positive-definite quadratic form on its ambient space  $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$ , or equivalently is a discrete subgroup of a Euclidean space.

A fundamental lattice problem is the *closest vector problem*, or CVP for short. The goal of this problem is to find a lattice point that is closest to a given point in its ambient space. This problem is provably difficult to solve, being actually an **NP**-hard problem. It is known to be harder than the *shortest vector problem* (SVP) [19], which asks for the shortest nonzero lattice point. SVP is the cornerstone of lattice reduction algorithms (see, for instance, [33; 20; 29]). These algorithms are at the heart of lattice-based cryptography [31], and are invaluable in plenty of computational problems, including Diophantine approximation, algebraic number theory or optimization (see [30] for a survey on the applications of the LLL algorithm).

**On CVP-solving algorithms.** There are three families of algorithms solving CVP:

**Enumeration algorithms.** These consist in recursively exploring all vectors in a set containing a closest vector. Kannan's algorithm takes time  $n^{O(n)}$  and polynomial space [24]. This estimate was later refined to  $n^{n/2+o(n)}$  by Hanrot and Stehlé [21].

MSC2010: 11HXX, 68W40.

Keywords: lattice, closest vector problem.

*Voronoi cell computation.* Micciancio and Voulgaris' Voronoi cell algorithm solves CVP in  $(4 + o(1))^n$  time but uses a space of  $(2 + o(1))^n$  [28].

*Sieving algorithms.* Here, vectors are combined in order to get closer and closer to the target vector. Heuristic variants take as little as  $(\frac{4}{3} + o(1))^{n/2}$  time [7], but proven variants of classical sieves [3; 8; 15] could only solve CVP with approximation factor  $1 + \epsilon$  at a cost in the exponent. In 2015, a  $(2 + o(1))^n$  sieve for *exact* CVP was finally proven by Aggarwal, Dadush and Stephen-Davidowitz [1] thanks to the properties of discrete Gaussians.

Many algorithms for solving the relaxed variant, APPROX-CVP, have been proposed. However, they come with caveats. For example, Dadush, Regev and Stephens-Davidowitz [10] give algorithms for this problem, but only with exponential time precomputations. Babai [5, Theorem 3.1] showed that one can reach a  $2^{n/2}$ -approximation factor for CVP in polynomial time. To the authors' knowledge, this has never been improved (while keeping the polynomial-time requirement), though the approximation factor for SVP has been significantly reduced [33; 20; 29].

We aim to solve the relaxed version of CVP for relatively large approximation factors, and study the tradeoff between the quality of the approximation of the solution found and the time required to actually find it. In particular, we exhibit a hierarchy of polynomial-time algorithms solving APPROX-CVP, ranging from Babai's nearest plane algorithm to an actual CVP oracle.

**Contributions and summary of the techniques.** We introduce our so-called Nearest-Colattice algorithm in Section 3. Inspired by Babai's algorithm, it shows that in practice, we can achieve the performance of Kannan's embedding but with a basis which is *independent* of the target vector. Denote by  $T(\beta)$  (resp.  $T_{\text{CVP}}(\beta)$ ) the time required to solve  $\sqrt{\beta}$ -Hermite-SVP (resp. exactly solve CVP) in rank  $\beta$ ). Quantitatively, we show:

**Theorem 1.1** (informal). *Let  $\beta > 0$  be a positive integer and  $B$  be a basis of a lattice  $\Lambda$  of rank  $n > 2\beta$ . After precomputations using a time bounded by  $T(\beta)(n + \log \|B\|)^{O(1)}$ , given a target  $t \in \Lambda_{\mathbb{R}}$  and under a heuristic on the covering radius of a random lattice, the algorithm Nearest-Colattice finds a vector  $x \in \Lambda$  such that*

$$\|x - t\| \leq \Theta(\beta)^{\frac{n}{2\beta}} \text{covol}(\Lambda)^{\frac{1}{n}}$$

*in time  $T_{\text{CVP}}(\beta)(n + \log \|t\| + \log \|B\|)^{O(1)}$ .*

Furthermore, the structure of the algorithms allows time-memory tradeoff and batch CVP oracle to be used.

We believe that this algorithm has been in the folklore for some time, and it is somehow hinted at in ModFalcon's security analysis [9, Subsection 4.2], but without analysis of the heuristics introduced.

Our second contribution is an APPROX-CVP algorithm, which gives a time-quality tradeoff similar to the one given by the BKZ algorithm [33; 21], or variants of it [17; 2]. Note however that the approximation factor is significantly higher than the corresponding theorems for APPROX-SVP. Written as a reduction, we prove that, for a  $\gamma$ -HSVP oracle  $\mathcal{O}$ :

**Theorem 1.2** (APPROX-CVPP oracle from APPROX-SVP oracle). *Let  $\Lambda$  be a lattice of rank  $n$ . Then one can solve the  $(n^{3/2}\gamma^3)$ -closest vector problem in  $\Lambda$ , using  $2n^2$  calls to the oracle  $\mathcal{O}$  during precomputation, and polynomial-time computations.*

Babai's algorithm requires that the Gram-Schmidt norms do not decrease by too much in the reduced basis. While this is true for an LLL reduced basis [26], we do not know a way to guarantee this in the general case. To overcome this difficulty, the proof technique goes as follows: first we show that it is possible to find a vector within distance  $\frac{1}{2}(\sqrt{n}\gamma)\lambda_n(\Lambda)$  of the target vector, with the help of a highly-reduced basis. This is not enough, as the target can be very close compared to  $\lambda_n(\Lambda)$ . We treat this peculiar case by finding a short vector in the dual lattice and then directly computing the inner product of the close vectors with our short dual vector. In the other case, Banaszczyk's transference theorem [6] guarantees that  $\lambda_n(\Lambda)$  is comparable to the distance to the lattice, so that we can use our first algorithm directly.

**Remark 1.3.** Based on a result due to Kannan (see for instance [12]) that  $\sqrt{n}\gamma^2$  CVP reduces to  $\gamma$ -SVP. Combined with the reduction from  $\gamma^2$ -SVP to  $\gamma$ -HSVP of [27], we get a polynomial time reduction from  $\sqrt{n}\gamma^4$ -CVP to  $\gamma$ -HSVP. Hence, our result is better when  $n^{3/2}\gamma^3$  is at most  $\sqrt{n}\gamma^4$ , i.e., when  $n < \gamma$ .

## 2. Algebraic and computational background

In this preliminary section, we recall the notions of geometry of numbers used throughout this paper, the computational problems related to SVP and CVP, and a brief presentation of some lattice reduction algorithms solving these problems.

### *Notation and conventions.*

*General notations.*  $\mathbb{Z}$ ,  $\mathbb{Q}$  and  $\mathbb{R}$  refer as usual to the ring of integers and the fields of rational and real numbers. Given a real number  $x$ , the integral roundings *floor*, *ceil* and *round to the nearest integer* are denoted respectively by  $\lfloor x \rfloor$ ,  $\lceil x \rceil$ ,  $\lfloor x \rceil$ . All logarithms are taken in base 2, unless explicitly stated otherwise.

*Computational setting.* The generic complexity model used in this work is the random-access machine (RAM) model and the computational cost is measured in operations.

### 2.1. Euclidean lattices and their geometric invariants.

#### 2.1.1. Lattices.

**Definition 2.1** (lattice). A (real) *lattice*  $\Lambda$  is a finitely generated free  $\mathbb{Z}$ -module, endowed with a Euclidean norm  $\|\cdot\|$  on the real vector space  $\Lambda_{\mathbb{R}} = \Lambda \otimes_{\mathbb{Z}} \mathbb{R}$ .

We may omit to write down the norm to refer to a lattice  $\Lambda$  when any ambiguity is removed by the context. By definition of a finitely-generated free module, there exists a finite family  $(v_1, \dots, v_n) \in \Lambda^n$  such that  $\Lambda = \bigoplus_{i=1}^n v_i \mathbb{Z}$ , called a *basis* of  $\Lambda$ . Every basis has the same number of elements  $\text{rk}(\Lambda)$ , called the rank of the lattice.

**2.1.2. Sublattices and quotient lattice.** Let  $(\Lambda, \|\cdot\|)$  be a lattice, and let  $\Lambda'$  be a submodule of  $\Lambda$ . Then the restriction of  $\|\cdot\|$  to  $\Lambda'$  endows  $\Lambda$  with a lattice structure. The pair  $(\Lambda', \|\cdot\|)$  is called a *sublattice* of  $\Lambda$ . In the remainder of this paper, we restrict ourselves to so-called *pure sublattices*, that is, those such that the quotient  $\Lambda/\Lambda'$  is torsion-free. In this case, the quotient can be endowed with a canonical lattice structure by defining

$$\|v + \Lambda'\|_{\Lambda/\Lambda'} = \inf_{v' \in \Lambda'} \|v - v'\|_{\Lambda}.$$

This lattice is isometric to the projection of  $\Lambda$  orthogonally to the subspace of  $\Lambda_{\mathbb{R}}$  spanned by  $\Lambda'$ .

**2.1.3. On effective lifting.** Given a coset  $v + \Lambda'$  of the quotient  $\Lambda/\Lambda'$ , we might need to find a representative of this class in  $\Lambda$ . While any element could be theoretically taken, from an algorithmic point of view, we shall take an element of norm somewhat small, so that its coefficients remain polynomial in the input representation of the lattice. An effective solution to do so consists in using, for instance, the *Babai's rounding* or *Babai's nearest plane* algorithms. For completeness purposes we recast here the pseudo-code of such a `Lift` function using the nearest-plane procedure.

---

**Algorithm 1:** `Lift` (by Babai's nearest plane)

---

Input: A lattice basis  $B = (v_1, \dots, v_k)$  of  $\Lambda'$  in  $\Lambda$ , a vector  $t \in \Lambda_{\mathbb{R}}$ .

Result: A vector of the class  $\tilde{t} + \Lambda' \in \Lambda$ .

```

1 Compute the Gram-Schmidt orthogonalization  $(v_1^*, \dots, v_k^*)$  of  $B$ 
2  $s \leftarrow -t$ 
3 for  $i = k$  downto 1 do
4    $s \leftarrow s - \left\lfloor \frac{\langle s, v_i^* \rangle}{\|v_i^*\|^2} \right\rfloor v_i$ 
5 return  $t + s$ 
```

---

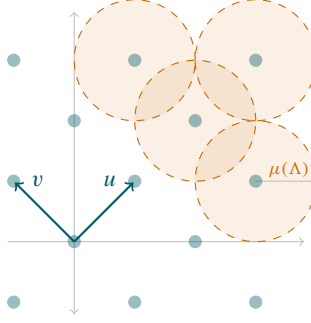
**2.1.4. Orthogonality and algebraic duality.** The *dual* lattice  $\Lambda^{\vee}$  of a lattice  $\Lambda$  is defined as the module  $\text{Hom}(\Lambda, \mathbb{Z})$  of integral linear forms, endowed with the derived norm defined by

$$\|\varphi\| = \inf_{v \in \Lambda_{\mathbb{R}} \setminus \{0\}} \frac{|\varphi(v)|}{\|v\|_{\Lambda}}$$

for  $\varphi \in \Lambda^{\vee}$ . By Riesz's representation theorem, it is isometric to  $\{x \in \Lambda_{\mathbb{R}} \mid \langle x, v \rangle \in \mathbb{Z} \text{ for all } v \in \Lambda\}$  endowed with the dual of  $\|\cdot\|_{\Lambda}$ .

Let  $\Lambda' \subset \Lambda$  be a sublattice. Define its *orthogonal* in  $\Lambda$  to be the sublattice  $\Lambda'_{\perp} = \{x \in \Lambda^{\vee} : \langle x, \Lambda' \rangle = 0\}$  of  $\Lambda^{\vee}$ . It is isometric to  $(\Lambda/\Lambda')^{\vee}$ , and by biduality  $\Lambda'_{\perp}^{\vee}$  shall be identified with  $\Lambda/\Lambda'$ .

**2.1.5. Filtrations.** A filtration (or flag) of a lattice  $\Lambda$  is an increasing sequence of submodules of  $\Lambda$ , i.e., each submodule is a proper submodule of the next:  $\{0\} = \Lambda_0 \subset \Lambda_1 \subset \Lambda_2 \subset \dots \subset \Lambda_k = \Lambda$ . If we write  $\text{rk}(\Lambda_i) = d_i$ , then we have  $0 = d_0 < d_1 < d_2 < \dots < d_k = \text{rk}(\Lambda)$ . A filtration is called *complete* if  $d_i = i$  for all  $i$ .



**Figure 1.** Covering radius  $\mu(\Lambda)$  of a two-dimensional lattice  $\Lambda$ .

**2.1.6. Successive minima, covering radius and transference.** Let  $\Lambda$  be a lattice of rank  $n$ . By discreteness in  $\Lambda_{\mathbb{R}}$ , there exists a vector of minimal norm in  $\Lambda$ . This parameter is called the *first minimum* of the lattice and is denoted by  $\lambda_1(\Lambda)$ . An equivalent way to define this invariant is to see it as the smallest positive real  $r$  such that the lattice points inside a ball of radius  $r$  span a space of dimension 1. This definition leads to the following generalization, known as successive minima.

**Definition 2.2** (successive minima). Let  $\Lambda$  be a lattice of rank  $n$ . For  $1 \leq i \leq n$ , define the  $i$ -th minimum of  $\Lambda$  as  $\lambda_i(\Lambda) = \inf\{r \in \mathbb{R} \mid \dim(\text{span}(\Lambda \cap B(0, r))) \geq i\}$ .

**Definition 2.3.** The covering radius of a lattice  $\Lambda$  or rank  $n$  is defined as

$$\mu(\Lambda) = \max_{x \in \Lambda_{\mathbb{R}}} \text{dist}(x, \Lambda).$$

It means that for any vector of the ambient space  $x \in \Lambda_{\mathbb{R}}$  there exists a lattice point  $v \in \Lambda$  at distance at most  $\mu(\Lambda)$ .

We now recall Banaszczyk's transference theorem, relating the extremal minima of a lattice and its dual:

**Theorem 2.4** (Banaszczyk's transference theorem [6]). *For any lattice  $\Lambda$  of dimension  $n$ , we have*

$$1 \leq 2\lambda_1(\Lambda^{\vee})\mu(\Lambda) \leq n,$$

implying

$$1 \leq \lambda_1(\Lambda^{\vee})\lambda_n(\Lambda) \leq n.$$

## 2.2. Computational problems in geometry of numbers.

**2.2.1. The shortest vector problem.** In this section, we introduce formally the SVP problem and its variants and discuss their computational hardness.

**Definition 2.5** ( $\gamma$ -SVP). Let  $\gamma = \gamma(n) \geq 1$ . The  $\gamma$ -shortest vector problem ( $\gamma$ -SVP) is defined as follows.

**Input:** A basis  $(v_1, \dots, v_n)$  of a lattice  $\Lambda$  and a target vector  $t \in \Lambda_{\mathbb{R}}$ .

**Output:** A lattice vector  $v \in \Lambda \setminus \{0\}$  satisfying  $\|v\| \leq \gamma\lambda_1(\Lambda)$ .

In the case where  $\gamma = 1$ , the corresponding problem is simply called SVP.

**Theorem 2.6** (Haviv and Regev [22]). *APPROX-SVP is  $\mathbf{NP}$ -hard under randomized reductions for every constant approximation factor.*

A variant of the problem consists of finding vectors in Hermite-like inequalities.

**Definition 2.7** ( $\gamma$ -HSVP). Let  $\gamma = \gamma(n) \geq 1$ . The  $\gamma$ -Hermite shortest vector problem ( $\gamma$ -HSVP) is defined as follows.

**Input:** A basis  $(v_1, \dots, v_n)$  of a lattice  $\Lambda$ .

**Output:** A lattice vector  $v \in \Lambda \setminus \{0\}$  satisfying  $\|v\| \leq \gamma \operatorname{covol}(\Lambda)^{1/n}$ .

There exists a simple polynomial-time dimension-preserving reduction between these two problems, as stated by Lovász in [27, 1.2.20]:

**Theorem 2.8.** *One can solve  $\gamma^2$ -SVP using  $2n$  calls to a  $\gamma$ -HSVP oracle and polynomial time.*

This can be slightly improved where the HSVP oracle is built from an HSVP oracle in lower dimension [2].

**2.2.2. An oracle for  $\gamma$ -HSVP.** We note a function  $T(\beta)$  such that we can solve  $O(\sqrt{\beta})$ -HSVP in time at most  $T(\beta)$  times the input size. We have the following bounds on  $T$ , depending on if we are looking at an algorithm which is:

*deterministic:*  $T(\beta) = (4 + o(1))^{\beta/2}$ , proven by Micciancio and Voulgaris in [28];

*randomized:*  $T(\beta) = (4/3 + o(1))^{\beta/2}$ , introduced by Wei, Liu and Wang in [36];

*heuristic:*  $T(\beta) = (3/2 + o(1))^{\beta/2}$ , given in [7] by Becker, Ducas, Gama, Laarhoven.

There also exist variants for quantum computers [25], and time-memory tradeoffs, such as [23]. By providing a back-and-forth strategy coupled with enumeration in the dual lattice, the *self dual block Korkine-Zolotarev* (DBKZ) algorithm provides an algorithm better than the famous BKZ algorithm.

**Theorem 2.9** (Micciancio and Walter [29]). *There exists an algorithm outputting a vector  $v$  of a lattice  $\Lambda$  satisfying*

$$\|v\| \leq \beta^{\frac{n-1}{2(\beta-1)}} \cdot \operatorname{covol}(\Lambda)^{\frac{1}{n}}.$$

*Such a bound can be achieved in time  $(n + \log \|B\|)^{O(1)} T(\beta)$ , where  $B$  is the integer input basis representing  $\Lambda$ .*

*Proof.* The bound we get is a direct consequence of [29, Theorem 1]. We only replaced the *Hermite constant*  $\gamma_\beta$  by an upper bound in  $O(\beta)$ . □

A stronger variant of this estimate is heuristically true, at least for “random” lattices, as it is suggested by the Gaussian heuristic in [29, Corollary 2]. Under this assumption, one can bound not only the length of the first vector but also the gap between the covolumes of the filtration induced by the outputted basis.

**Theorem 2.10.** *There exists an algorithm outputting a complete filtration of a lattice  $\Lambda$  satisfying:*

$$\text{covol}(\Lambda_i / \Lambda_{i-1}) \approx \Theta(\beta)^{\frac{n+1-2i}{2(\beta-1)}} \text{covol}(\Lambda)^{\frac{1}{n}}.$$

*Such a bound can be achieved in time  $(n + \log \|B\|)^{O(1)} T(\beta)$ , where  $B$  is the integer-valued input basis. Further, we have*

$$\Theta(\sqrt{\beta}) \text{covol}^{\frac{1}{\beta}}(\Lambda_n / \Lambda_{n-\beta}) \approx \text{covol}(\Lambda_{n-\beta+1} / \Lambda_{n-\beta}).$$

**2.3. The closest vector problem.** In this section we introduce formally the CVP problem and its variants and discuss their computational hardness.

**Definition 2.11** ( $\gamma$ -CVP). Let  $\gamma = \gamma(n) \geq 1$ . The  $\gamma$ -closest vector problem ( $\gamma$ -CVP) is defined as follows.

**Input:** A basis  $(v_1, \dots, v_n)$  of a lattice  $\Lambda$  and a target vector  $t \in \Lambda \otimes \mathbb{R}$ .

**Output:** A lattice vector  $v \in \Lambda$  satisfying  $\|x - t\| \leq \gamma \min_{v \in \Lambda} \|v - t\|$ .

In the case where  $\gamma = 1$ , the corresponding problem is called CVP.

**Theorem 2.12** (Dinur, Kindler and Shafra [11]).  $n^{c/(\log \log n)}$ -APPROX-CVP is **NP-hard** for any  $c > 0$ .

We let  $T_{\text{CVP}}(\beta)$  be such that we can solve CVP in dimension  $\beta$  in running time bounded by  $T_{\text{CVP}}(\beta)$  times the size of the input. Hanrot and Stehlé proved  $\beta^{\beta/2+o(\beta)}$  with polynomial memory [21]. Sieves can provably reach  $(2 + o(1))^\beta$  with exponential memory [1]. More importantly for this paper, heuristic sieves can reach  $(4/3 + o(1))^{\beta/2}$  for solving an entire batch of  $2^{0.058\beta}$  instances [13].

### 3. The nearest colattice algorithm

We aim to solve the  $\gamma$ -APPROX-CVP by recursively exploiting the datum of a filtration

$$\Lambda_0 \subset \Lambda_1 \subset \dots \subset \Lambda_k = \Lambda$$

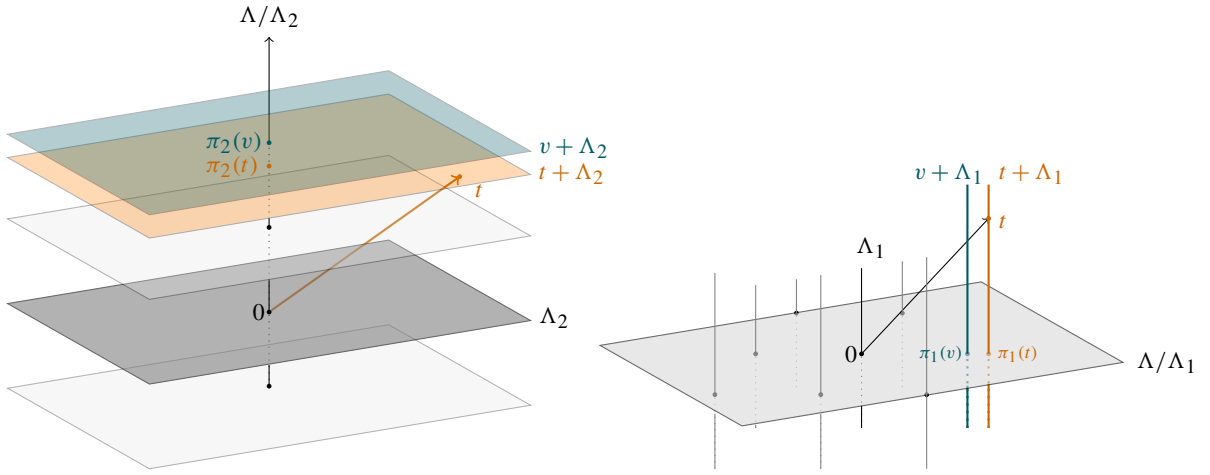
via recursive approximations. The central object used during this reduction is the *nearest colattice* relative to a target vector.

In this section, and the next one, we assume that the size of the bases is always small, essentially as small as the input basis. This is classic, and can be easily proven.

#### 3.1. Nearest colattice to a vector.

**Definition 3.1.** Let  $0 \rightarrow \Lambda' \rightarrow \Lambda \rightarrow \Lambda/\Lambda' \rightarrow 0$  be a short exact sequence of lattices, and set  $t \in \Lambda_{\mathbb{R}}$  to be a target vector. A nearest  $\Lambda'$ -colattice to  $t$  is a coset  $\bar{v} = v + \Lambda' \in \Lambda/\Lambda'$  which is the closest to the projection of  $t$  in  $\Lambda_{\mathbb{R}}/\Lambda'_{\mathbb{R}}$ , i.e., such that  $\bar{v} = \text{argmin}_{v \in \Lambda} \|(t - v) + \Lambda'\|_{\Lambda_{\mathbb{R}}/\Lambda'_{\mathbb{R}}}$ .

This definition makes sense thanks to the discreteness of the quotient lattice  $\Lambda/\Lambda'$  in the real vector space  $\Lambda_{\mathbb{R}}/\Lambda'_{\mathbb{R}}$ .



**Figure 2.** The  $\Lambda_2$ -nearest colattice  $v + \Lambda_2$  relative to  $t$ , in green (left). The  $\Lambda_1$ -nearest colattice  $v + \Lambda_1$  relative to  $t$  (right).

**Example.** To illustrate this definition, we give two examples in dimension 3, of rank 1 and 2 nearest colattices. Set  $\Lambda$  to be a rank 3 lattice, and fix  $\Lambda_1$  and  $\Lambda_2$  to be two pure sublattices of respective ranks 1 and 2. Denote by  $\pi_i$  the canonical projection onto the quotient  $\Lambda/\Lambda_i$ , which is of dimension  $3 - i$  for  $i \in \{1, 2\}$ . The  $\Lambda_i$ -closest colattice to  $t$ , denoted by  $v_i + \Lambda_i$ , is such that  $\pi_i(v_i)$  is a closest vector to  $\pi_i(t)$  in the corresponding quotient lattice. Figure 2 (left) and (right), respectively, depict these situations.

**Remark 3.2.** A computational insight into Definition 3.1 is given by viewing a nearest colattice as a solution to an instance of exact-CVP in the quotient lattice  $\Lambda/\Lambda'$ .

Taking the same notation as in Definition 3.1, let us project  $t$  orthogonally onto the affine space  $v + \Lambda'_\mathbb{R}$ , and take  $w$  to be a closest vector to this projection. The vector  $w$  is then relatively close to  $t$ . Let us quantify its defect of closeness towards an actual closest vector to  $t$ :

**Proposition 3.3.** *With the same notation as above:  $\|t - w\|^2 \leq \mu(\Lambda/\Lambda')^2 + \mu(\Lambda')^2$ .*

*Proof.* This is clear by Pythagoras' theorem. □

By definition of the covering radius, we then have:

**Corollary 3.4** (subadditivity of the covering radius over short exact sequences). *Let*

$$0 \rightarrow \Lambda' \rightarrow \Lambda \rightarrow \Lambda/\Lambda' \rightarrow 0$$

*be a short exact sequence of lattices. Then we have  $\mu(\Lambda)^2 \leq \mu(\Lambda/\Lambda')^2 + \mu(\Lambda')^2$ .*

This inequality is tight, and is an equality when there exists a sublattice  $\Lambda''$  such that  $\Lambda' \oplus \Lambda'' = \Lambda$  and  $\Lambda'' \subseteq \Lambda'_\perp$ .



**3.2. Recursion along a filtration.** Let us now consider a filtration  $\Lambda_0 \subset \Lambda_1 \subset \cdots \subset \Lambda_k = \Lambda$  and a target vector  $t \in \Lambda_{\mathbb{R}}$ . Repeatedly applying [Corollary 3.4](#) along the subfiltrations  $0 \subset \Lambda_i \subset \Lambda_{i+1}$ , yields a sequence of inequalities  $\mu(\Lambda_{i+1})^2 - \mu(\Lambda_i)^2 \leq \mu(\Lambda_{i+1}/\Lambda_i)^2$ . The telescoping sum now gives the relation  $\mu(\Lambda)^2 \leq \sum_{i=1}^k \mu(\Lambda_{i+1}/\Lambda_i)^2$ . This formula has a very natural algorithmic interpretation as a recursive oracle for approx-CVP:

- (1) Starting from the target vector  $t$ , we solve the CVP instance corresponding to  $\pi(t)$  in the quotient  $\Lambda_k/\Lambda_{k-1}$  with  $\pi$  the canonical projection onto this quotient to find  $v + \Lambda_{k-1}$ , the nearest  $\Lambda_{k-1}$ -colattice to  $t$ .
- (2) We then project  $t$  orthogonally onto  $v + (\Lambda_{k-1} \otimes_{\mathbb{Z}} \mathbb{R})$ . Call this vector  $t'$ .
- (3) A recursive call to the algorithm on the instance  $(t' - v, \Lambda_0 \subset \cdots \subset \Lambda_{k-1})$  yields a vector  $w \in \Lambda_2$ .
- (4) Return  $w + v$ .

Its translation in pseudo-code is given in an iterative manner in the algorithm `Nearest-Colattice`.

---

**Algorithm 2:** `Nearest-Colattice`

---

Input: A filtration  $\{0\} = \Lambda_0 \subset \Lambda_1 \subset \cdots \subset \Lambda_k = \Lambda$ , a target  $t \in \Lambda_{\mathbb{R}}$ .

Result: A vector in  $\Lambda$  close to  $t$ .

```

1  $s \leftarrow -t$ 
2 for  $i = k$  downto 1 do
3    $s \leftarrow s - \text{Lift}(\text{argmin}_{h \in \Lambda_i/\Lambda_{i-1}} \|v - h\|)$ 
4 return  $t + s$ 
```

---

**Proposition 3.5.** *Let  $B$  be a basis of a lattice  $\Lambda$  of rank  $n$ . Given a target  $t \in \Lambda_{\mathbb{R}}$ , the algorithm `Nearest-Colattice` finds a vector  $x \in \Lambda$  such that  $\|x - t\|^2 \leq \sum_{i=1}^k \mu(\Lambda_{i+1}/\Lambda_i)^2$  in time*

$$T_{\text{CVP}}(\beta)(n + \log \|t\| + \log \|B\|)^{O(1)},$$

where  $\beta$  is the largest gap of rank in the filtration  $\beta = \max_i (\text{rk}(\Lambda_{i+1}) - \text{rk}(\Lambda_i))$ .

*Proof.* The bound on the quality of the approximation is a direct consequence of the previous discussion. The running time bound derives from the definition of  $T_{\text{CVP}}$  and the fact that the `Lift` operations can be conducted in polynomial time.  $\square$

**Remark 3.6** (retrieving Babai's algorithm). In the specific case where the filtration is complete, that is to say that  $\text{rk}(\Lambda_i) = i$  for each  $1 \leq i \leq n$ , the `Nearest-Colattice` algorithm coincides with the so-called *Babai's nearest plane* algorithm. In particular, it recovers a vector at distance

$$\sqrt{\sum_{i=1}^n \mu(\Lambda_i/\Lambda_{i-1})^2} = \frac{1}{2} \sqrt{\sum_{i=1}^n \text{covol}(\Lambda_i/\Lambda_{i-1})^2},$$

since for each index  $i$ , we have  $\mu(\Lambda_i/\Lambda_{i-1}) = \frac{1}{2} \text{covol}(\Lambda_i/\Lambda_{i-1})$  as these quotients are one-dimensional.

The bound given in [Proposition 3.5](#) is not easily instantiable as it requires having access to the covering radius of the successive quotients of the filtration. However, under a mild heuristic on random lattices, we now exhibit a bound which only depends on the parameter  $\beta$  and the covolume of  $\Lambda$ .

**3.3. On the covering radius of a random lattice.** In this section we prove that the covering radius of a random lattice behaves essentially in  $\sqrt{\text{rk}(\Lambda)}$ .

In 1945, Siegel [\[34\]](#) proved that the projection of the Haar measure of  $\text{SL}_n(\mathbb{R})$  over the quotient  $\text{SL}_n(\mathbb{R})/\text{SL}_n(\mathbb{Z})$  is of finite mass, yielding a natural probability distribution  $\nu_n$  over the moduli space  $\mathcal{L}_n$  of unit-volume lattices. By construction this distribution is translation-invariant, that is, for any measurable set  $\mathcal{S} \subseteq \mathcal{L}_n$  and all  $U \in \text{SL}_n(\mathbb{Z})$ , we have  $\nu_n(\mathcal{S}) = \nu_n(SU)$ . A *random lattice* is then defined as a unit-covolume lattice in  $\mathbb{R}^n$  drawn under the probability distribution  $\nu_n$ .

We first recall an estimate due to Rogers [\[32\]](#), giving the expectation<sup>1</sup> of the number of lattice points in a fixed set.

**Theorem 3.7** (Rogers' average). *Let  $n \leq 4$  be an integer and  $\rho$  be the characteristic function of a Borel set  $C$  of  $\mathbb{R}^n$  whose volume is  $V$ , centered at 0. Then:*

$$0 \leq \int_{\mathcal{L}_n} \rho(\Lambda \setminus \{0\}) d\nu_n(\Lambda) - 2e^{-V/2} \sum_{r=0}^{\infty} \frac{r}{r!} (V/2)^r \leq (V+1) \left( 6 \left( \sqrt{\frac{3}{4}} \right)^n + 105 \cdot 2^{-n} \right).$$

This allows us to prove that the first minimum of a random lattice is greater than a multiple of  $\sqrt{n}$ .

**Lemma 4.** *Let  $\Lambda$  be a random lattice of rank  $n$ . Then, with probability  $1 - 2^{-\Omega(n)}$ ,  $\lambda_1(\Lambda) > c\sqrt{n}$  for a universal constant  $c > 0$ .*

*Proof.* Consider the ball  $C$  of volume  $V = 0.99^n$ . Its radius is equal to  $0.99\pi^{-1/2}\Gamma(\frac{n}{2} + 1)^{1/n}$ , which is lower bounded by  $c\sqrt{n}$  for a constant  $c > 0$ , using for instance Stirling's estimate. By [Theorem 3.7](#), the expectation of the number of lattice points in  $C$  is at most

$$128 \left( \frac{3}{4} \right)^{\frac{n}{2}} (V+1) + V \in (1 + o(1))V.$$

This estimate upper bounds the probability that there exists a nonzero lattice vector in  $C$  by  $2^{-\Omega(n)}$ , using Markov's inequality on the positive random variable  $|\Lambda \cap C|$ .  $\square$

Using the transference theorem, we then derive the following estimate on the covering radius of a random lattice:

**Theorem 4.1.** *Let  $\Lambda$  be a random lattice of rank  $n$ . Then, with probability  $1 - 2^{-\Omega(n)}$ ,  $\mu(\Lambda) < d\sqrt{n}$  for a universal constant  $d$ .*

*Proof.* First note that the dual lattice  $\Lambda^\vee$  follows the same distribution as  $\Lambda$ . Hence, using the estimate of [Lemma 4](#), we know that with probability  $1 - 2^{-\Omega(n)}$ ,  $\lambda_1(\Lambda^\vee) > c\sqrt{n}$ . Banaszczyk's transference

<sup>1</sup>The result proved by Rogers is actually more general and bounds all the moments of the enumerator of lattice points. For the purpose of this work, only the first moment is actually required.

theorem indicates that in this case,

$$\mu(\Lambda) \leq \frac{n}{\lambda_1(\Lambda^\vee)} \leq \frac{\sqrt{n}}{c},$$

concluding the proof.  $\square$

This justifies the following heuristic:

**Heuristic 4.2.** In algorithm `Nearest-Colattice`, for any index  $i$ , we have  $\mu(\Lambda_{i+1}/\Lambda_i) \leq c\lambda_1(\Lambda_{i+1}/\Lambda_i)$  for some universal constant  $c$ .

The Gaussian heuristic suggests that “almost all” targets  $t$  are at distance  $(1 + o(1))\lambda_1(\Lambda)$ , so that for practical purposes in the analysis we can take  $c = 1$  in [Heuristic 4.2](#).

#### 4.1. Quality of the algorithm on random lattices.

**Theorem 4.3.** Let  $\beta > 0$  be a positive integer and  $B$  be a basis of a lattice  $\Lambda$  of rank  $n > 2\beta$ . After precomputations using a time bounded by  $T(\beta)(n + \log \|B\|)^{O(1)}$ , given a target  $t \in \Lambda_{\mathbb{R}}$  and under [Heuristic 4.2](#), the algorithm `Nearest-Colattice` finds a vector  $x \in \Lambda$  such that

$$\|x - t\| \leq \Theta(\beta)^{\frac{n}{2\beta}} \text{covol}(\Lambda)^{\frac{1}{n}}$$

in time  $T_{\text{CVP}}(\beta) \text{Poly}(n, \log \|t\|, \log \|B\|)$ .

*Proof.* We start by reducing the basis  $B$  of  $\Lambda$  using the DBKZ algorithm, and collect the vectors in blocks of size  $\beta$ , giving a filtration

$$\{0\} = \Lambda_0 \subset \Lambda_1 \subset \cdots \subset \Lambda_k = \Lambda,$$

for  $k = \lceil \frac{n}{\beta} \rceil$  and  $\text{rk}(\Lambda_{i+1}/\Lambda_i) = \beta$  for each index  $i$  except the penultimate one, of rank  $n - \beta \lfloor \frac{n}{\beta} \rfloor$ . We define  $l_i$  as  $\text{rk}(\Lambda_{i+1}/\Lambda_i)$ . By [Theorem 2.10](#) and finite induction in each block using the multiplicativity of the covolume over short exact sequences, we have for  $i < k - 1$ ,

$$\begin{aligned} \text{covol}(\Lambda_{i+1}/\Lambda_i)^{\frac{1}{l_i}} &\approx \text{covol}(\Lambda)^{\frac{1}{n}} \left( \prod_{j=i\beta}^{i\beta+l_i-1} \Theta(\beta)^{\frac{n+1-2j}{2(\beta-1)}} \right)^{\frac{1}{l_i}} \\ &= \Theta(\beta)^{\frac{n+2-2i\beta-l_i}{2(\beta-1)}} \text{covol}(\Lambda)^{\frac{1}{n}}. \end{aligned}$$

We also have

$$\Theta(\sqrt{\beta}) \text{covol}(\Lambda_k/\Lambda_{k-1})^{1/\beta} \approx \Theta(\beta)^{\frac{n+1-2(n-\beta)}{2(\beta-1)}} \text{covol}(\Lambda)^{\frac{1}{n}}$$

so that the previous approximation is also true for  $i = k - 1$ . Using [Heuristic 4.2](#) and Minkowski’s first theorem, we can estimate the covering radius of this quotient as

$$\mu(\Lambda_{i+1}/\Lambda_i) \leq \Theta(\sqrt{l_i})\Theta(\beta)^{\frac{n+2-2i\beta-l_i}{2(\beta-1)}} \text{covol}(\Lambda)^{\frac{1}{n}}.$$

**Proposition 3.5** now asserts that `Nearest-Colattice` returns a vector at distance from  $t$  bounded by

$$\text{covol}(\Lambda)^{\frac{1}{n}} \sum_{i=0}^k \Theta(\sqrt{l_i}) \Theta(\beta)^{\frac{n+2-2i\beta-l_i}{2(\beta-1)}} = \Theta(\beta)^{\frac{n}{2\beta-2}} \text{covol}(\Lambda)^{\frac{1}{n}}$$

where the last equality stems from the condition  $n \geq 2\beta$ , so that only the first term is significant.  $\square$

Note that in the algorithm, all lattices depend only on  $\Lambda$ , not on the targets. Therefore, it is possible to use CVP algorithms after precomputations. These algorithms are significantly faster; we refer to [13] for heuristic ones and to [10; 35] for proven approximation algorithms.

### 5. Proven APPROX-CVP algorithm with precomputation

In all of this section, let us fix an oracle  $\mathcal{O}$ , solving the  $\gamma$ -HSVP. We solve APPROX-CVP with preprocessing from the oracle  $\mathcal{O}$ .

**Theorem 5.1** (APPROX-CVPP oracle from HSVP oracle). *Let  $\Lambda$  be a lattice of rank  $n$ . Then one can solve the  $(n^{3/2}\gamma^3)$ -closest vector problem in  $\Lambda$ , using  $2n^2$  calls to the oracle  $\mathcal{O}$  during precomputation, and polynomial time computations.*

The first step of this reduction consists in proving that we can find a lattice point at a distance roughly  $\lambda_n(\Lambda)$ .

**Theorem 5.2.** *Let  $\Lambda$  be a lattice of rank  $n$  and  $t \in \Lambda \otimes \mathbb{R}$  a target vector; then one can find a lattice vector  $c \in \Lambda$  satisfying  $\|c - t\| \leq \frac{1}{2}\sqrt{n}\gamma\lambda_n(\Lambda)$ , using  $n$  calls to the oracle  $\mathcal{O}$  during precomputation, and polynomial time computations.*

*Proof.* We aim to construct a complete filtration  $\{0\} \subset \Lambda_1 \subset \dots \subset \Lambda_n = \Lambda$  of the input lattice  $\Lambda$  such that for any index  $1 \leq i \leq n-1$ , we have  $\text{covol}(\Lambda_i/\Lambda_{i-1}) \leq \gamma\lambda_n(\Lambda)$ . We proceed inductively:

- By a call to the oracle  $\mathcal{O}$  on the lattice  $\Lambda$ , we find a vector  $b_1$ . Set  $\Lambda_1 = b_1\mathbb{Z}$  to be the corresponding sublattice.
- Suppose that the filtration is constructed up to index  $i$ . Then we call the oracle  $\mathcal{O}$  on the quotient sublattice  $\Lambda/\Lambda_i$  (or equivalently on the projection of  $\Lambda$  orthogonally to  $\Lambda_i$ ), and lift the returned vector using the `Lift` function in  $v \in \Lambda$ . Eventually we set  $\Lambda_{i+1} = \Lambda_i \oplus v\mathbb{Z}$ .

At each index, we have by construction  $\lambda_{n-i+1}(\Lambda/\Lambda_i) \leq \lambda_n(\Lambda)$ . As such,  $\text{covol}(\Lambda/\Lambda_i) \leq \lambda_n(\Lambda)^{n-i+1}$ , and, eventually, we have, for each index  $i$ ,

$$\text{covol}(\Lambda_i/\Lambda_{i-1}) \leq \gamma \cdot \lambda_n(\Lambda).$$

As stated in [Remark 3.6](#), Babai's algorithm on the point  $t$  returns a lattice vector  $c \in \Lambda$  such that  $\|c - t\| \leq \sqrt{\sum_{i=1}^n \mu(\Lambda_i/\Lambda_{i-1})^2} \leq \frac{1}{2}(\sqrt{n}\gamma\lambda_n(\Lambda))$ .  $\square$

**Remark 5.3** (on the quality of this decoding). For a random lattice, we expect  $\lambda_n(\Lambda) \approx \sqrt{n} \operatorname{covol}(\Lambda)^{1/n}$ , so that the distance between the decoded vector and the target is only a factor  $\gamma$  times larger than the guaranteed output of the oracle.

We can now complete the reduction:

*Proof of Theorem 5.1.* Let  $\Lambda$  be a rank  $n$  lattice. Without loss of generality, we might assume that the norm  $\|\cdot\|$  of  $\Lambda$  coincides with its dual norm, so that the dual  $\Lambda^\vee$  can be isometrically embedded in  $\Lambda_\mathbb{R}$ . We first find a nonzero vector in the dual lattice  $c \in \Lambda^\vee$ , where  $\|c\| \leq \gamma^2 \lambda_1(\Lambda^\vee)$  using Lovász's reduction stated in Theorem 2.8 on the oracle  $\mathcal{O}$ . Define  $v \in \Lambda$  and  $e \in \Lambda \otimes \mathbb{R}$  to satisfy  $t = v + e$  with  $\|e\|$  minimal. We now have two cases, depending on how large the error term  $e$  is:

*Case  $\|c\|\|e\| \geq \frac{1}{2}$  (large case):* Then, by plugging Banaszczyk's transference inequality to the bound on  $\|c\|$ , we get

$$\|e\| \geq \frac{1}{2\gamma^2 \lambda_1(\Lambda^\vee)} \geq \frac{\lambda_n(\Lambda)}{2n\gamma^2}.$$

Thus, we can use Theorem 5.2 to solve APPROX-CVP with approximation factor equal to

$$\frac{\sqrt{n}\gamma}{2} \left( \frac{1}{2n\gamma^2} \right)^{-1} = n^{\frac{3}{2}} \gamma^3.$$

*Case  $\|c\|\|e\| < \frac{1}{2}$  (small case):* Then, we have by linearity,  $\langle c, t \rangle = \langle c, v \rangle + \langle c, e \rangle$ . Hence, by the Cauchy–Schwarz inequality and the assumption on  $\|c\|\|e\|$  we can assert that

$$\lfloor \langle c, t \rangle \rfloor = \langle c, v \rangle.$$

Let  $\Lambda'$  be the projection of  $\Lambda$  over the orthogonal space to  $c$  and denote by  $\pi$  the corresponding orthogonal projection.

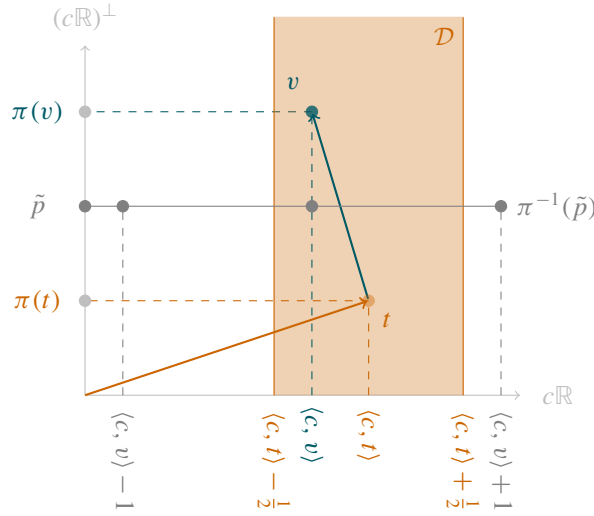
Let us prove that  $\pi(v)$  is a closest vector of  $\pi(t)$  in  $\Lambda'$ . To do so, let us take  $\tilde{p}$  a shortest vector  $\pi(t)$  in  $\Lambda$ . We now look at the fiber (in  $\Lambda$ ) above  $\tilde{p}$  and take the closest element  $p$  to  $t$  in this set. Then by Pythagoras' theorem,  $p$  is an element of the intersection of  $\pi^{-1}(\tilde{p})$  with the convex body  $\mathcal{D} = \{x \mid |\langle c, x \rangle| < \frac{1}{2}\}$ . As the vector  $c$  belongs to the dual of  $\Lambda$ , we have that for any  $p_1, p_2 \in \pi^{-1}(\tilde{p})$ ,  $\langle p_1 - p_2, c \rangle \in \mathbb{Z}$ , so that  $\pi^{-1}(\tilde{p}) \cap \mathcal{D}$  is of cardinality one. Write  $p$  for this point. Then,  $\langle p, c \rangle = \langle v, c \rangle$ , as  $|\langle p - v, c \rangle| < \frac{1}{2}$  and is an integer. Now remark that by minimality of  $\|v - t\|$ , we have by Pythagoras' theorem that  $v = p$ , implying that  $\pi(v) = \tilde{p}$ .

By induction, we find  $w \in \Lambda$  such that  $\|\pi(w - t)\| \leq n^{3/2} \gamma^3 \|\pi(v - t)\|$  and since  $\langle c, w - t \rangle = \langle c, v - t \rangle$  we obtain  $\|w - t\| \leq n^{3/2} \gamma^3 \|v - t\|$ .  $\square$

Overall, we get the following corollary by using the Micciancio-Voulgaris algorithm for the oracle  $\mathcal{O}$ :

**Corollary 5.4.** *We can solve  $\beta^{O(n/\beta)}$ -APPROX-CVP deterministically in time bounded by  $2^\beta$  times the size of the input.*

**Remark 5.5.** Using exactly the same proof scheme, we can refine the approximation factor to an  $n^{3/2} \gamma_S \gamma$  by using a separate  $\gamma_S$ -SVP oracle instead of using  $\gamma$ -HSVP as a  $\gamma^2$ -SVP oracle.



**Figure 3.** Illustration of the situation depicted in the proof, in the two-dimensional case.

## 6. Cryptographic perspectives

In cryptography, the bounded distance decoding (BDD) problem<sup>2</sup> has a lot of importance, as it directly relates to the celebrated learning with error (LWE) problem [31]. This latter problem can be reduced to APPROX-CVP, but our theoretical reduction with HSVP has a loss which is too large to be competitive.

In the so-called GPV framework [18], instantiated in the DLP cryptosystem [14] and its follow-ups FALCON [16], MODFALCON [9], a valid signature is a point close to a target, which is the hash of the message. Hence, forging a signature boils down to finding a close vector to a random target. Our first (heuristic) result implies that, once a reduced basis has been found, forging a message is relatively easy. Previous methods such as in [16] used Kannan’s embedding [24] so that the cost given only applies for one forgery, whereas a batch forgery is possible for roughly the same cost.

The same remark applies for practically solving the BDD problem, and indeed the LWE problem. Once a highly reduced basis is found, it is enough to compute a CVP on the tail of the basis, and finish with Babai’s algorithm. More precisely, by using the same notation and exploiting the proof of Theorem 4.3, a sufficient condition for decoding will be

$$\|\pi(e)\| \leq \theta(\beta)^{\frac{2\beta-n}{2\beta}} \text{covol}(\Lambda)^{\frac{1}{n}},$$

where,  $\pi$  is the orthogonal projection onto  $\Lambda/\Lambda_k$  and  $\beta$  is the rank of this latter lattice.

This trick seems to have been in the folklore for some time, and is the reason given by NEWHOPE [4] designers for selecting a random “ $a$ ”, which corresponds to a random lattice (where the authors of [4] claim that Babai’s algorithm is enough, but it seems to be practically true in general for an extremely well reduced basis, i.e., with more precomputations performed).

<sup>2</sup>This problem being defined as finding the closest lattice vector of a target, provided it is within a fraction of  $\lambda_1(\Lambda)$ .

## Acknowledgments

This work was done while the authors were visiting the Simons Institute for the theory of computing in February 2020. They also thanks the anonymous reviewers for their insightful comments on this work.

## References

- [1] D. Aggarwal, D. Dadush, and N. Stephens-Davidowitz. Solving the closest vector problem in  $2^n$  time - the discrete Gaussian strikes again! In *56th FOCS*. IEEE Computer Society Press, 2015.
- [2] D. Aggarwal, J. Li, P. Q. Nguyen, and N. Stephens-Davidowitz. Slide reduction, revisited—filling the gaps in SVP approximation. *arXiv preprint arXiv:1908.03724*, 2019.
- [3] M. Ajtai, R. Kumar, and D. Sivakumar. Sampling short lattice vectors and the closest lattice vector problem. In *Proceedings 17th IEEE Annual Conference on Computational Complexity*. IEEE, 2002.
- [4] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe. Post-quantum key exchange - A new hope. In *USENIX Security 2016*.
- [5] L. Babai. On Lovász’ lattice reduction and the nearest lattice point problem. *Combinatorica*, 6(1), 1986.
- [6] W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296(1), 1993.
- [7] A. Becker, L. Ducas, N. Gama, and T. Laarhoven. New directions in nearest neighbor searching with applications to lattice sieving. In *27th SODA*. ACM-SIAM, 2016.
- [8] J. Blömer and S. Naewe. Sampling methods for shortest vectors, closest vectors and successive minima. *Theoretical Computer Science*, 410(18) 2009.
- [9] C. Chuengsatiansup, T. Prest, D. Stehlé, A. Wallet, and K. Xagawa. Modfalcon: compact signatures based on module NTRU lattices. *IACR Cryptology ePrint Archive*, 2019.
- [10] D. Dadush, O. Regev, and N. Stephens-Davidowitz. On the closest vector problem with a distance guarantee. In *2014 IEEE 29th Conference on Computational Complexity (CCC)*, IEEE, 2014.
- [11] I. Dinur, G. Kindler, and S. Safra. Approximating-CVP to within almost-polynomial factors is np-hard. In *Proceedings 39th Annual Symposium on Foundations of Computer Science*. IEEE, 1998.
- [12] C. Dubey, and T. Holenstein. Approximating the closest vector problem using an approximate shortest vector oracle Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques. 2011
- [13] L. Ducas, T. Laarhoven, and W. P. van Woerden. The randomized slicer for CVPP: sharper, faster, smaller, batchier. *Cryptology ePrint*, Report 2020/120.
- [14] L. Ducas, V. Lyubashevsky, and T. Prest. Efficient identity-based encryption over NTRU lattices. In *ASIACRYPT 2014*. Springer 2014.
- [15] F. Eisenbrand, N. Hähnle, and M. Niemeier. Covering cubes and the closest vector problem. In *the 27th symposium on Computational geometry*, 2011.
- [16] P.-A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Prest, T. Ricosset, G. Seiler, W. Whyte, and Z. Zhang. Falcon: Fast-Fourier lattice-based compact signatures over NTRU. *Submission to the NIST’s post-quantum cryptography standardization process*, 2018.
- [17] N. Gama and P. Q. Nguyen. Finding short lattice vectors within Mordell’s inequality. In *40th ACM STOC*. ACM Press, 2008.
- [18] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *40th ACM STOC*. ACM Press, 2008.
- [19] O. Goldreich, D. Micciancio, S. Safra, and J.-P. Seifert. Approximating shortest lattice vectors is not harder than approximating closest lattice vectors. *Information Processing Letters*, 71(2) 1999.
- [20] G. Hanrot, X. Pujol, and D. Stehlé. Analyzing blockwise lattice algorithms using dynamical systems. In *CRYPTO 2011*. Springer, 2011.

- [21] G. Hanrot and D. Stehlé. Improved analysis of Kannan’s shortest lattice vector algorithm. In *CRYPTO 2007*. Springer, 2007.
- [22] I. Haviv and O. Regev. Tensor-based hardness of the shortest vector problem to within almost polynomial factors. In *39th ACM STOC*. ACM Press, 2007.
- [23] G. Herold, E. Kirshanova, and T. Laarhoven. Speed-ups and time-memory trade-offs for tuple lattice sieving. In *PKC 2018*. Springer, 2018.
- [24] R. Kannan. Minkowski’s convex body theorem and integer programming. *Mathematics of operations research*, 12(3) 1987.
- [25] T. Laarhoven, M. Mosca, and J. Van De Pol. Finding shortest lattice vectors faster using quantum search. *Designs, Codes and Cryptography*, 77(2-3) 2015.
- [26] A. K. Lenstra, H. W. J. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261 1982.
- [27] L. Lovász. *An algorithmic theory of numbers, graphs, and convexity*. SIAM, 1986.
- [28] D. Micciancio and P. Voulgaris. Faster exponential time algorithms for the shortest vector problem. In *21st SODA*. ACM-SIAM, 2010.
- [29] D. Micciancio and M. Walter. Practical, predictable lattice basis reduction. In *EUROCRYPT 2016*. Springer, 2016.
- [30] P. Q. Nguyen and B. Vallée. *The LLL algorithm*. Springer, 2010.
- [31] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6) 2009.
- [32] C. A. Rogers et al. Mean values over the space of lattices. *Acta mathematica*, 94 1955.
- [33] C. Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. *Theor. Comput. Sci.*, 53 1987.
- [34] C. L. Siegel. A mean value theorem in Geometry of Numbers. *Annals of Mathematics*, 46(2) 1945.
- [35] N. Stephens-Davidowitz. A time-distance trade-off for GDD with preprocessing—instantiating the DLW heuristic. *preprint arXiv:1902.08340*, 2019.
- [36] W. Wei, M. Liu, and X. Wang. Finding shortest lattice vectors in the presence of gaps. In *CT-RSA 2015*. Springer, 2015.

Received 28 Feb 2020. Revised 28 Feb 2020.

THOMAS ESPITAU: [t.espitau@gmail.com](mailto:t.espitau@gmail.com)  
NTT Corporation, Tokyo, Japan

PAUL KIRCHNER: [paul.kirchner@irisa.fr](mailto:paul.kirchner@irisa.fr)  
Rennes University, Rennes, France



# Cryptanalysis of the generalised Legendre pseudorandom function

Novak Kaluđerović, Thorsten Kleinjung, and Dušan Kostić

Linear Legendre pseudorandom functions were introduced in 1988 by Damgård, and higher degree generalisations were introduced by Russell and Shparlinski in 2004. We present new key recovery methods that improve the state of the art for both cases. For degree  $r \geq 3$  we give an attack that runs in time  $O(p^{r-3})$  after  $O(p^3)$  precomputation for the most relevant high degree case; it is based on the action of the group of Möbius transformations on degree  $r$  polynomials. For  $r < 3$  we give an  $O(p^{r/2})$  attack with  $O(p^{r/4})$  oracle queries. In the linear case we recovered the keys for the 64, 74 and 84-bit prime Ethereum challenges, being the first to solve the 84-bit case.

## 1. Introduction

The usage of Legendre symbols in a pseudorandom function (PRF) is an idea originally proposed by Damgård [3]. Further generalisations with higher degree polynomials were proposed by Russell and Shparlinski [9]. In both cases a prime  $p$  is given and the Legendre PRF is modelled as an oracle  $\mathcal{O}$  that on input  $x$  outputs the Legendre symbol  $\left(\frac{f(x)}{p}\right)$ , where  $f(x) \in \mathbb{F}_p[x]$  is a secret key. Damgård conjectured that when  $f$  is linear, given a sequence of Legendre symbols of consecutive elements it is hard to predict the next one. Similar problems conjectured to be hard were also proposed [7], such as finding the secret polynomial while being given access to  $\mathcal{O}$  and distinguishing  $\mathcal{O}$  from a random function. So far no polynomial time algorithms have been found for either of these problems and it is believed that they are hard. Until recently, practical applications have been limited, primarily due to availability of much faster alternatives.

A recent result by Grassi et al. [7] sparked an interest in the linear Legendre PRF because it was found suitable as a multiparty computation (MPC) friendly pseudorandom generator. This is mainly due to the homomorphic property of the Legendre symbol and the possibility of evaluating it with only three modular multiplications in arithmetic circuit multiparty computations, which makes it a very efficient MPC friendly PRF candidate.

There are plans to use this construction as a PRF for a proof of custody scheme in the Ethereum blockchain [6]. The proof of custody scheme requires a *mix* function, i.e., a pseudorandom function

MSC2010: 11T71.

Keywords: Legendre symbol, Legendre PRF, cryptanalysis, group action, pseudorandom.

that produces one bit of output. The Legendre PRF was shown to be a great candidate for this purpose because of its efficiency. In comparison, SHA256 requires tens of thousands of multiplications while AES needs 290 in the MPC setting [6].

In order to raise interest in this construction, a number of Ethereum research challenges have been posted [6]. The goal is to recover the secret key given  $2^{20}$  consecutive Legendre symbols, for primes of size varying from 64 to 148 bits.

**1A. Contribution.** In this paper we analyse the action of the group of Möbius transformations on monic polynomials of degree  $r$ , and we use it to give an improved attack on the Legendre pseudorandom function. For polynomials of degree  $r \geq 3$  modulo a prime  $p$  we distinguish three types of polynomials and for the most relevant case we give an  $O(p^{r-3})$  attack after an  $O(p^3)$  precomputation with  $p$  oracle queries. For degree  $r < 3$  an  $O(p^{r/2})$  attack is given with  $p^{r/4}$  queries. If the number of queries  $M$  is limited, we give an  $O(p^r \log p/M^2)$  attack. These are improvements with respect to the previous algorithms [2; 8] of factor from  $p$  up to  $p^3$  in the general case, and even higher for a new family of *bad* keys. In the linear and limited query case a factor of  $\log p$  fewer trials in the search phase are needed.

We also give the solutions to challenges 0, 1 and 2 of the Ethereum research linear Legendre PRF for 64, 74 and 84-bit primes. In all cases we were given access to  $2^{20}$  Legendre symbols.

## 2. Background

Let  $p$  be an odd prime. Throughout the paper we suppose that the prime is public.<sup>1</sup> We denote with  $\mathbb{F}_p$  the field of cardinality  $p$ .

### 2A. Notation.

**Definition 2.1** (pseudorandom functions). A pseudorandom function family  $\{\mathcal{O}_k\}_k$  is a set of functions with the same domain and codomain indexed by a set of keys  $k$  such that a function  $\mathcal{O}_k$  chosen randomly over the set of  $k$ -values cannot be distinguished from a random function.

**Definition 2.2** (Legendre symbol). We define the Legendre symbol by setting

$$\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } x \in \mathbb{F}_p \text{ is a square mod } p, \\ -1 & \text{if } x \in \mathbb{F}_p \text{ is not a square mod } p. \end{cases}$$

In general the Legendre symbol is defined by setting  $\left(\frac{0}{p}\right) = 0$ , which makes the symbol multiplicative. However this comes at a cost of increasing the size of the codomain. In practice  $\left(\frac{0}{p}\right) = 1$  is used.

We will assume that the multiplicative property of the Legendre symbol stands. This is a nonproblem and the reader should be easily convinced that the algorithms we give terminate in the same expected time and with the same probability.

<sup>1</sup>Originally, as proposed by Damgård, the prime was considered secret. We chose only to pursue the case of a public prime, as in the MPC use case.

**Definition 2.3** (Legendre sequence). We define a Legendre sequence with starting point  $a$  and length  $L$  to be the sequence of Legendre symbols evaluated at  $L$  consecutive elements starting from  $a$ . We denote it with  $\{a\}_L$ :

$$\{a\}_L := \left(\frac{a}{p}\right), \left(\frac{a+1}{p}\right), \left(\frac{a+2}{p}\right), \dots, \left(\frac{a+L-1}{p}\right).$$

Every  $a$  fully determines its sequence of length  $L$ , but not vice versa — that property depends on  $L$ . In general, these sequences are as well distributed as one can hope them to be. We know already that when  $L = 1$  half of the  $a$ -values give 1, and the other half give  $-1$ . Similar properties are true for larger  $L$ , and in general, following a theorem of Davenport, around one in  $2^L$  elements of  $\mathbb{F}_p$  is a starting point of a given sequence of length  $L$ .

**Theorem 2.4** (Davenport, 1933 [4]). *Let  $S$  be a finite sequence of  $\pm 1$ 's of length  $L$ . Then the number of elements of  $\mathbb{F}_p$  whose sequence is equal to  $S$  satisfies*

$$\#\{a \in \mathbb{F}_p \mid \{a\}_L = S\} = \frac{p}{2^L} + O(p^\varepsilon)$$

where  $0 < \varepsilon < 1$  is a constant depending only on  $L$ .

Throughout the paper we assume that  $L$  is such that  $\{a\}_L$  uniquely defines  $a$ , i.e., that

$$\{a\}_L = \{b\}_L \text{ if and only if } a = b. \quad (2-1)$$

It is easy to see that if we want this property to hold, we need  $L = \Omega(\log_2 p)$ . The only provable upper bound we have comes from the Weil bound [10] and is  $L = O(\sqrt{p} \log p)$  which is exponential.

Our computational results, together with other statistical data on the distribution of Legendre sequences [3], indicate that on average over all sequences  $S$  of length  $L$ , there are  $p/2^L + O(1)$  elements whose Legendre sequences are equal to  $S$ . In other words, for a random  $S$  and a random  $j$  we have  $\{j\}_L = S$  with probability  $1/2^L$ . A good estimate of  $L$  in terms of  $p$  is  $L = \lceil 2 \log_2 p \rceil$ .

**2B. The Legendre pseudorandom function.** In this section we define the Legendre pseudorandom function and its higher degree generalisation.

**Definition 2.5** (Legendre PRF). The Legendre pseudorandom functions are functions  $\mathcal{O}_k$  from  $\mathbb{F}_p$  to  $\{-1, 1\}$  indexed by  $k \in \mathbb{F}_p$  and defined as

$$\mathcal{O}_k(x) = \left(\frac{x+k}{p}\right).$$

**Definition 2.6** (higher degree Legendre PRF). The Legendre pseudorandom functions of degree  $r$  are a family of functions  $\mathcal{O}_f$  from  $\mathbb{F}_p$  to  $\{-1, 1\}$  indexed by  $f = k_r x^r + \dots + k_1 x + k_0 \in \mathbb{F}_p[x]$  and defined as

$$\mathcal{O}_f(x) = \left(\frac{f(x)}{p}\right).$$

The degree  $r$  is assumed to be polylogarithmic in  $p$ .

Two oracles  $\mathcal{O}_f(x)$  and  $\mathcal{O}_{f/k_r}(x)$  are the same up to multiplication by  $\left(\frac{k_r}{p}\right)$  and therefore we can assume the polynomial  $f$  to be monic. The case of linear  $f(x)$  reduces to the standard Legendre PRF which we thus from now on refer to as the linear Legendre PRF.

The polynomial  $f(x)$  is considered up to multiplication by a square since the Legendre symbol is invariant under square factors of  $f(x)$ . This is not entirely true as a square linear factor introduces a zero and may change the output of the oracle at one point, but the reader should be convinced that this can be safely ignored.

The secret key space, i.e., the space from which we choose  $f(x)$  is the space of monic polynomials modulo squares. The number of such polynomials equals  $p^r - p^{r-1}$  for  $r > 1$  (see [1], problem 3.3) and  $p$  for  $r = 1$ .

**Definition 2.7** (generalised Legendre sequence). The length  $L$  Legendre sequence of a polynomial  $f(x)$  is denoted by  $\{f\}_L$  and defined as

$$\{f\}_L := \left(\frac{f(0)}{p}\right), \left(\frac{f(1)}{p}\right), \left(\frac{f(2)}{p}\right), \dots, \left(\frac{f(L-1)}{p}\right).$$

As a generalisation to Theorem 2.4 and property (2-1) we assume that  $L$  is such that  $\{f\}_L$  uniquely defines  $f$ , i.e., that

$$\{f\}_L = \{g\}_L \text{ if and only if } f = g. \quad (2-2)$$

With  $r$  the degree of  $f$  we have  $L = \Omega(r \log p)$ . We assume that property (2-2) holds for  $L = \Theta(r \log p)$ . A reasonable estimate is  $L = \lceil 2r \log p \rceil$ . Throughout the paper we include the dependence on  $L$  in the complexity of our algorithms.

**2C. Hard problems.** There are three main problems conjectured to be hard, and on which the security of the Legendre PRF is based.

**Definition 2.8** (generalised Legendre symbol problem – GLSP). Let  $f$  be a uniformly random monic square-free polynomial. Given access to an oracle  $\mathcal{O}$  that on input  $x \in \mathbb{F}_p$  computes  $\mathcal{O}(x) = \left(\frac{f(x)}{p}\right)$ , find  $f$ .

**Definition 2.9** (decisional generalised Legendre symbol problem – DGLSP). Let  $f$  be a uniformly random monic square-free polynomial. Let  $\mathcal{O}_0$  be an oracle that on input  $x \in \mathbb{F}_p$  computes  $\mathcal{O}_0(x) = \left(\frac{f(x)}{p}\right)$ , and let  $\mathcal{O}_1$  be an oracle that on input  $x$  outputs a random value in  $\{-1, +1\}$ . Given access to  $\mathcal{O}_b$  where  $b$  is an unknown random bit, find  $b$ .

**Definition 2.10** (next symbol problem – NSP). Given a Legendre sequence  $\{f\}_M$  of  $M = \text{polylog}(p)$  symbols, find  $\left(\frac{f(M)}{p}\right)$ , or equivalently find  $\{f\}_{M+1}$ .

It is easy to see that the GLSP and NSP are at least as hard as DGLSP. In the other direction, following a theorem of Yao [11] on general pseudorandom functions, predicting the next bit of a pseudorandom function is as hard as distinguishing it from a truly random one. Therefore  $\text{NSP} = \text{DGLSP} \leq \text{GLSP}$ , under polynomial time reductions.

### 3. Group action on polynomials

Möbius transformations act naturally on rational functions of  $\mathbb{P}^1$ , changing the argument and preserving their degrees. We show how this action can be exploited in order to connect oracles of monic polynomials that are in the same orbit.

**3A. Möbius transformations.** Let  $\mathcal{M}$  be the group of  $\mathbb{F}_p$ -rational automorphisms of  $\mathbb{P}^1$ . It is known that  $\mathcal{M}$  is isomorphic to  $\text{PGL}_2(\mathbb{F}_p)$  and that this group has order  $p^3 - p$ . The elements of  $\mathcal{M}$  are Möbius transformations. Given a matrix  $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{PGL}_2(\mathbb{F}_p)$  there is a unique Möbius transformation  $\varphi_m$  given by

$$\varphi_m : \mathbb{P}^1 \rightarrow \mathbb{P}^1, \quad [x : y] \mapsto [ax + by : cx + dy],$$

and function composition satisfies  $\varphi_{m_1} \circ \varphi_{m_2} = \varphi_{m_1 m_2}$ . We drop the notation of  $\varphi_m$  and only use  $m$  from now on.

**3B. Action of  $\mathcal{M}$  on monic polynomials.** The action of a Möbius transformation  $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}$  on a polynomial  $f$  is denoted by  $m \cdot f = f_m$  and defined as

$$m \cdot f = f_m(x) := f\left(\frac{ax + b}{cx + d}\right) \frac{(cx + d)^r}{f\left(\frac{a}{c}\right)c^r}. \quad (3-1)$$

The corrective factors  $(cx + d)^r$  and  $f\left(\frac{a}{c}\right)c^r$  are introduced in order to make  $f_m$  a polynomial and to make it monic correspondingly.

There is another way to look at this action — if  $\alpha$  is a root of  $f$  then  $m^{-1}(\alpha)$  is a root of  $f_m$ , where  $m^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$  is the inverse of the Möbius transformation  $m$ . Thus, if  $f(x) = \prod_{i=1}^r (x - \alpha_i)$  then

$$f_m(x) = \prod_{i=1}^r (x - m^{-1}\alpha_i) = \prod_{i=1}^r \left(x - \frac{d\alpha_i - b}{-c\alpha_i + a}\right). \quad (3-2)$$

Therefore the group  $\mathcal{M}$  of Möbius transformations has left (covariant) action on the roots of polynomials in  $\mathbb{F}_p[x]$  and right (contravariant) action on polynomials.

**3C. Obtaining oracles of polynomials in the orbit.** Suppose we are given access to  $\mathcal{O}$ , the oracle of  $f$ . Following (3-1) we can mimic the oracle of  $f_m$  with

$$\left(\frac{f_m(x)}{p}\right) = \mathcal{O}\left(\frac{ax + b}{cx + d}\right) \left(\frac{cx + d}{p}\right)^r \mathcal{O}\left(\frac{a}{c}\right) \left(\frac{c}{p}\right)^r.$$

Therefore we can obtain  $\{f_m\}_L$  by computing  $L + 1$  Legendre symbols and querying the oracle  $L + 1$  times. If  $c = 0$  then  $\mathcal{O}\left(\frac{a}{c}\right)\left(\frac{c}{p}\right)^r$  is substituted with  $\left(\frac{a}{p}\right)^r$ . If  $cx + d = 0$  for some  $x \in [0, L)$ , then we substitute  $\mathcal{O}\left(\frac{ax+b}{cx+d}\right)\left(\frac{cx+d}{p}\right)^r$  by  $\left(\frac{ax+b}{p}\right)^r$ .

**3D. Polynomial types.** We divide the key space into three sets based on reducibility of the polynomials and the size of their orbit given by the action of  $\mathcal{M}$ . The following lemma helps characterise these sets.

**Lemma 3.1.** *Let  $\mathcal{M} = \text{PGL}_2(\mathbb{F}_p)$  and  $f \in \mathbb{F}_p[x]$  be an irreducible polynomial of degree  $r$  with  $3 \leq r < p$ . Then, the stabiliser of  $f$  is a cyclic group of order  $r'$  for some  $r' \mid r$ . Furthermore  $r' \mid p^2 - 1$ .*

*Proof.* Let  $\text{Stab}(f) = \{m \in \mathcal{M} \mid f = f_m\}$  be the stabiliser of  $f$ , and let  $m \in \text{Stab}(f)$ . By property (3-2) the roots of  $f_m$  are  $m^{-1}\alpha_i$  implying that  $m$  permutes the roots of  $f$ . Let  $\text{Gal}(f) = \{F_i := x \mapsto x^{p^i} \mid i \in \mathbb{Z}/r\}$  be the Galois group of  $f$ , and let  $\alpha$  be any root of  $f$ . Then  $m\alpha = F_i(\alpha)$  for some  $i \in \mathbb{Z}/r$ . Furthermore  $m(F_j(\alpha)) = F_j(m\alpha) = F_j(F_i(\alpha)) = F_i(F_j(\alpha))$  since  $m$  is rational and it commutes with the Frobenius. Therefore each element of the stabiliser acts on the roots as an element of  $\text{Gal}(f)$ . This gives rise to a homomorphism from  $\text{Stab}(f)$  to  $\text{Gal}(f)$  which is injective since two Möbius transformations with the same action on a set of  $r \geq 3$  points have to be equal. Therefore  $\text{Stab}(f)$  is a subgroup of  $\text{Gal}(f) \cong \mathbb{Z}/r$ , so it is isomorphic to  $\mathbb{Z}/r'$  for some  $r' \mid r$ . The stabiliser is naturally a subgroup of  $\mathcal{M}$ , so its order divides  $\#\mathcal{M} = p(p^2 - 1)$ . Since  $r' < p$  we have  $r' \mid p^2 - 1$ .  $\square$

**Definition 3.2.** We call irreducible polynomials with a trivial stabiliser *good*, irreducible polynomials with a stabiliser of size  $r' > 1$  are called *bad*, and reducible polynomials are called *ugly*.

## 4. Algorithm

We give an algorithm for solving the generalised Legendre symbol problem. We start by querying the oracle  $\mathcal{O}(x)$  at all  $x \in \mathbb{F}_p$ , and computing  $\left(\frac{x}{p}\right)$  for all  $x \in \mathbb{F}_p$ . These results are then saved in a table and whenever we need an oracle query or a Legendre symbol we read them instead of computing an expensive symbol or querying the oracle multiple times.

The general idea is to do a table-based collision search. We make a table containing  $\{f_m\}_L$  for some  $m \in \mathcal{M}$ , and we try random  $g$  until  $\{g\}_L = \{f_m\}_L$  for some  $m$ . This gives us  $f = g_{m^{-1}}$ . The tables and the trials differ for different polynomial types, so we give three separate algorithms for *good*, *bad* and *ugly* polynomials. The comparisons with previous algorithms are given in Table 1.

**4A. Good polynomials algorithm.** We recall that  $f$  is *good* if it is an irreducible polynomial of degree  $r \geq 3$  and the stabiliser of  $f$  is trivial.

**4A1. Precomputation.** In the precomputation stage we generate a table  $T$  containing  $\{f_m\}_L$  and a description of  $m$  for all Möbius transformations  $m$  as described in Section 3C. Since  $f$  is *good*, the table  $T$  contains  $p^3 - p$  different sequences.

**4A2. Search.** The search is done by trying random  $g(x)$  of degree  $r$  and computing  $\{g\}_L$  until we find a hit, which we expect to find after  $O(p^{r-3})$  trials. For each trial,  $g$  is evaluated at  $L$  points, and  $L$  Legendre symbols are extracted, so the run time can be measured in the number of Legendre symbols extracted, which is  $O(p^{r-3}L)$ .

**4B. Bad polynomials algorithm.** We recall that  $f$  is *bad* if it is an irreducible polynomial of degree  $r \geq 3$  and the stabiliser of  $f$  is nontrivial. It follows from Lemma 3.1 that  $\text{Stab}(f)$  is isomorphic to  $\mathbb{Z}/r'$ .

**4B1. Precomputation.** We start by finding  $\text{Stab}(f)$ , the stabiliser of  $f$ . A straightforward way to find it in  $O(p^3)$  is by enumerating  $\mathcal{M}$  and isolating the matrices that fix  $f$ . The [Appendix](#) describes a nontrivial way to find it in  $O(p^2 \log r)$  steps.

Call  $m$  any generator of  $\text{Stab}(f)$ . The matrix  $m$  is rational so it has a Jordan canonical form of one of the following three types:

$$\begin{array}{ccc} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} & \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} & \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} \\ \text{Type 1} & \text{Type 2} & \text{Type 3} \end{array}$$

where  $a, b \in \mathbb{F}_p \setminus \{0\}$  and  $\lambda, \mu \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$  are conjugates of each other. We can exclude Type 3 matrices since they have order  $p$ , while  $m$  has order  $r' < p$ .

Let  $D$  be a diagonal matrix of order  $r'$  and  $P$  a change of basis matrix (these can be chosen uniquely from a set of representatives given in the [Appendix](#)) such that

$$m = P D P^{-1}.$$

Following from  $D \cdot f_P = (PD) \cdot f = (mP) \cdot f = P \cdot f_m = P \cdot f = f_P$ , the polynomial  $f_P$  is stabilised by  $D$ . Therefore  $f_P$  satisfies  $f_P\left(\frac{r}{s}x\right)\left(\frac{s}{r}\right)^r = f_P\left(\frac{r}{s}x\right) = f_P(x)$  where  $(r, s) = (a, b)$  or  $(\lambda, \mu)$ . This sets the following constraints on the coefficients of  $f_P$ :

$$\begin{aligned} f_P(x) &= x^r + k_{r-1}x^{r-1} + \cdots + k_2x^2 + k_1x + k_0 = x^r + \sum_{i=0}^{r-1} k_i x^i, \\ (D \cdot f_P)(x) &= x^r + k_{r-1} \left(\frac{r}{s}\right)^{r-1} x^{r-1} + \cdots + k_1 \left(\frac{r}{s}\right)x + k_0 = x^r + \sum_{i=0}^{r-1} k_i \left(\frac{r}{s}\right)^i x^i \end{aligned}$$

from which it follows that

$$k_i = k_i \left(\frac{r}{s}\right)^i \text{ for } i = 0, 1, \dots, r-1. \quad (4-1)$$

Since  $\frac{r}{s}$  has order  $r'$  we have  $k_i = 0$  for all  $i$  that are not multiples of  $r'$ .

We create a table  $T$  of size  $O(p)$  containing polynomials  $t$  in the orbit of  $f$  with  $t_P$  satisfying (4-1). The process differs for the two types of matrices so we treat them separately.

**Type 1.** When  $D$  is rational,  $P$  is rational too, so the polynomial  $f_P$  is in the orbit of  $f$ . If  $C$  is a rational diagonal matrix,  $C \cdot f_P$  is another polynomial in the orbit of  $f$  satisfying (4-1). The total number of such polynomials is  $(p-1)/r'$  since matrices  $C$  can be chosen up to stabiliser of  $f_P$  which is  $\langle D \rangle$ . A set of representatives is

$$\mathcal{C}_1 = \left\{ \begin{pmatrix} g^i & 0 \\ 0 & 1 \end{pmatrix} \mid g \text{ a generator of } \mathbb{F}_p^*, 0 \leq i < \frac{p-1}{r'} \right\}.$$

The table  $T$  contains  $\{P C P^{-1} \cdot f\}_L$  together with a description of  $C$  for all  $C$  in  $\mathcal{C}_1$ . It has  $(p-1)/r'$  elements, and for all polynomials  $t$  in the table,  $t_P$  satisfies (4-1).

**Type 2.** When  $D$  is irrational,  $P$  is too, so  $f_P$  is not in the orbit of  $f$ . There are additional constraints on  $f_P$  following from the rationality of  $m$ :

$$m = P \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} P^{-1} = \bar{m} = \bar{P} \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} \bar{P}^{-1} = \bar{P} \begin{pmatrix} \mu & 0 \\ 0 & \lambda \end{pmatrix} \bar{P}^{-1}.$$

Let  $A_P := P^{-1} \bar{P}$ . From the definition of  $A_P$  and the above formulas it follows that

$$A_P^{-1} = \bar{A}_P, \\ \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} A_P = A_P \begin{pmatrix} \mu & 0 \\ 0 & \lambda \end{pmatrix}.$$

These constraints imply that  $A_P = \begin{pmatrix} 0 & \alpha \\ 1/\bar{\alpha} & 0 \end{pmatrix}$  for some  $\alpha \in \mathbb{F}_{p^2}$ . The action of  $A_P$  is the same as the action of  $\begin{pmatrix} 0 & s \\ 1 & 0 \end{pmatrix}$  where  $s = \alpha\bar{\alpha} \in \mathbb{F}_p$ . Note that  $s$  can be computed and, up to choosing a different representative for  $P$ , can be set to be equal to 1. We further have

$$A_P \cdot f_P(x) = f_{PA_P}(x) = f_{\bar{P}}(x) = \bar{P} \cdot f(x) = \bar{P} \cdot \overline{f(x)} = \overline{P \cdot f(x)} = \overline{f_P(x)},$$

which gives new constraints on the coefficients of  $f_P(x)$ :

$$\overline{f_P(x)} = x^r + \bar{k}_{r-1}x^{r-1} + \cdots + \bar{k}_2x^2 + \bar{k}_1x + \bar{k}_0 = x^r + \sum_{i=0}^{r-1} \bar{k}_i x^i, \\ (A_P \cdot f_P)(x) = x^r + \frac{k_1 s}{k_0} x^{r-1} + \cdots + \frac{k_{r-1} s^{r-1}}{k_0} x + \frac{s^r}{k_0} = x^r + \sum_{i=0}^{r-1} \frac{k_{r-i} s^{r-i}}{k_0} x^i.$$

This translates to

$$k_0^{p+1} = s^r, \quad k_{r-i} = \frac{k_0 \bar{k}_i}{s^{r-i}}, \quad k_{r/2}^{p-1} = \frac{s^{r/2}}{k_0} \text{ if } r \text{ is even.} \quad (4-2)$$

The polynomial  $f_P$  is not the only polynomial satisfying (4-1) and (4-2). Certainly (4-1) is satisfied for every  $C \cdot f_P$  where  $C$  is a diagonal matrix. In order for  $C \cdot f_P$  to satisfy (4-2) we need  $A_P \cdot f_{PC} = \overline{f_{PC}}$ , which implies

$$(CA_P \bar{C}^{-1}) \cdot f_P(x) = \overline{f_P(x)}.$$

This condition, together with  $C$  being diagonal implies that  $C$  is contained in

$$\left\{ \begin{pmatrix} c & 0 \\ 0 & \bar{c} \end{pmatrix} \mid c \in \mathbb{F}_{p^2}^* \right\}.$$

Multiplying  $C$  on the right by a rational scalar matrix or by an element of  $\text{Stab}(f_P) = \langle D \rangle$  does not change the polynomial  $C \cdot f_P$ . Therefore  $C$  can be chosen from a reduced set of representatives, for example,

$$\mathcal{C}_2 = \left\{ \begin{pmatrix} g^i & 0 \\ 0 & \bar{g}^i \end{pmatrix} \mid g \text{ a generator of } \mathbb{F}_{p^2}^*, \ 0 \leq i < \frac{p+1}{r''} \right\},$$

where  $(p+1)/r'' = \gcd(p+1, (p^2-1)/r')$ , in other words  $r'' = r' / (\gcd(r', p-1))$ . The choice of  $r''$



follows from the exponents of  $g$  being chosen modulo  $p + 1$  (action of  $\mathbb{F}_p^*$ ) and modulo  $(p^2 - 1)/r'$  (action of  $r'$ -th roots of unity).

The table  $T$  contains  $\{PCP^{-1} \cdot f\}_L$  together with a description of  $C$  for all  $C$  in  $\mathcal{C}_2$  (note that  $PCP^{-1}$  is rational). It has  $(p + 1)/r''$  elements, and for all polynomials  $t$  in the table,  $t_P$  satisfies (4-1) and (4-2).

**4B2. Search.** In the search phase we go over  $g(x) = x^r + \sum_{i=0}^{r/r'-1} g_i x^i$  that satisfy (4-1) and compute  $\{g_{P^{-1}}\}_L$  until we find a hit in  $T$ . In that case,  $f = g_{(PC)^{-1}}$ .

For Type 1, the coefficients  $g_i$  are in  $\mathbb{F}_p$ . The total number of polynomials  $g$  is  $p^{r/r'}$  and we expect to find a hit after  $O(p^{r/r'-1}r')$  trials.

For Type 2, the coefficients  $g_i$  are in  $\mathbb{F}_{p^2}$  and they satisfy (4-2). Therefore there are  $p + 1$  choices for  $g_0$ , the  $g_i$  with  $1 \leq i < r/2$  can be chosen freely, giving  $p^2$  choices each, and the  $g_j$  for  $r/2 < j$  are constrained to one value for each choice of the previous coefficients. If  $r$  is even,  $g_{r/2}$  has  $p - 1$  choices. The total number of polynomials  $g$  is  $O(p^{r/r'})$  and we expect to find a hit after  $O(p^{r/r'-1}r'')$  trials.

**4C. Ugly polynomials algorithm.** We recall that  $f$  is *ugly* if it is a reducible polynomial of degree  $r \geq 3$ . Write  $f(x) = l(x)h(x)$  where  $r_h = \deg(h(x)) \geq r/2$ .

The Legendre symbol is multiplicative, and Möbius transformations are homomorphic with respect to polynomial multiplication, so we have  $\{f_m\}_L = \{l_m\}_L \{h_m\}_L$ , where the multiplication is element-wise. It follows that  $\{f_m\}_L \{l_m\}_L = \{h_m\}_L$ .

**4C1. Precomputation.** We create two tables,  $T_1$  containing  $\{f_m\}_L$  for all  $m \in \mathcal{M}$ , and  $T_2$  containing sequences of all polynomials  $g(x)$  of degree  $r - r_h$  (the candidates for  $l_m(x)$ ). The main table  $T$  is a product of  $T_1$  and  $T_2$ , i.e., a table of size  $O(p^{r-r_h+3})$  containing  $\{f_m\}_L \{g\}_L$  for all  $m \in \mathcal{M}$  and all  $g$ .

**4C2. Search.** The search phase consists of trying random polynomials  $t(x)$  of degree  $r_h$  until we find a hit in  $T$ . This gives  $\{t\}_L = \{f_m\}_L \{g\}_L$ , and implies that  $t(x) = h_m(x)$ ,  $g(x) = l_m(x)$ , and finally  $f(x) = g_{m^{-1}}(x)t_{m^{-1}}(x)$ . We expect to find a solution in  $O(p^{r_h-3})$  trials.

The above description glosses over a number of minor details that one needs to be careful about. The run time is actually  $p^{r_h}$  divided by the size of the orbit of  $h(x)$ .

If  $h$  is *good*, then its orbit is maximal and we are done.

If  $h$  is *bad*, we can test all *bad*  $h$  in time  $O(p^{r_h/r'_h}L)$  for each  $r'_h \mid r_h$ , so in total  $O(p^{r_h/2}L)$ . For both Type 1 and Type 2 we can enumerate all polynomials  $h$  in time  $O(p^{r_h/r'_h-1}r''_hL)$  with  $r''_h$  defined as in Section 4B.

If  $h$  is *ugly*, we analyse two cases:

- (1)  $h$  has an irreducible factor of degree at least 3: Suppose  $h = h_1h_2$  of degrees  $r_1$  and  $r_2$ . We select a set of  $O(p^{r_1-3})$  representatives for  $h_1$ , multiply them with polynomials of degree  $r_2$  and search for  $\{h\}_L = \{h_1\}_L \{h_2\}_L$  in  $T$ , achieving an  $O(p^{r_h-3})$  run time.
- (2)  $h$  has all factors of degree  $\leq 2$ : There are three subcases to consider:
  - $h$  is divisible by a product of three linear polynomials. Then at least one  $h_m$  is divisible by  $x(x-1)(x-2)$ , so we test for  $h = x(x-1)(x-2)h_2$  where  $h_2$  are of degree  $r_h - 3$ .

- $h$  is divisible by a linear and quadratic polynomial. Then one of  $h_m$  is divisible by  $x(x^2 - u)$  where  $u$  is a chosen nonsquare, so we test for  $h = x(x^2 - u)h_2$  where  $h_2$  are of degree  $r_h - 3$ .
- $h$  is divisible by two quadratic polynomials. Then one of them can be considered to be  $x^2 - u$  where  $u$  is a nonsquare, and the other one has only 1 degree of freedom. We test for  $h = (x^2 - u)h_1h_2$  where  $h_1$  is selected from  $O(p)$  quadratic polynomials and  $h_2$  is of degree  $r_h - 4$ .

Therefore if  $f$  is *ugly* we can find it in  $O(p^{r_h-3})$  trials irrespective of the type of  $h$ .

<i>good</i> polynomials	search	precomputation	memory
Khovratovich [8]	$p^{r-1}r \log p$	$r \log p$	$r \log p$
Beullens et al. [2]	$p^{r-2}r^2 \log^2 p$	$p^2$	$p^2$
Our algorithm	$p^{r-3}r \log p$	$p^3r \log p$	$p^3r \log p$
<i>bad</i> polynomials	search	precomputation	memory
Khovratovich [8]	$p^{r-1}r \log p$	$r \log p$	$r \log p$
Beullens et al. [2]	$p^{r-2}r^2 \log^2 p$	$p^2$	$p^{r-r_h}r \log p$
Our algorithm	$p^{r/r'-1}r''r \log p$	$p^2r \log p$	$(p/r'')r \log p$
<i>ugly</i> polynomials	search	precomputation	memory
Khovratovich [8]	$p^{r-1}r \log p$	$r \log p$	$r \log p$
Beullens et al. [2]	$p^{r_h}r \log p$	$p^{r-r_h}r \log p$	$p^{r-r_h}r \log p$
Our algorithm	$p^{r_h-3}r \log p$	$p^{r-r_h+3}r \log p$	$p^{r-r_h+3}r \log p$

**Table 1.** Comparison of the best known algorithms for solving the degree  $r \geq 3$  Legendre PRF, in big- $O$ 's. The size of the stabiliser of  $f$  is denoted with  $r'$ , and  $r'' = r'$  if  $r' \mid p-1$  and  $r'' = r'/\gcd(r', p-1)$  otherwise. We denote with  $r_h$  the degree of a factor of  $f$  which is at least  $r/2$ . Complexity is given in the number of Legendre symbols computed/extracted. In all cases we need  $p$  queries.

**4D. Time-memory tradeoff for low degrees.** The run time of the algorithm depends mainly on the search stage. However for some low degree polynomials, the precomputation may take longer than the search stage. In some cases a time-memory tradeoff allows us to reduce the complexity further.

**4D1. Good polynomials.** For  $r \geq 6$ , the table-based collision search with an  $O(p^3)$  table and  $O(p^{r-3})$  trials is optimal. For  $3 \leq r \leq 5$ , a tradeoff with an  $O(p^{r/2})$  table and  $O(p^{r/2})$  trials is better.

**4D2. Bad polynomials.** If  $r/r' - 1 < 2$  then the bottleneck is the precomputation phase that takes  $O(p^2 \log r)$  steps. This can happen when  $r' = r/c$  for  $c = 1, 2$ . Not much can be done to reduce the precomputation cost since testing *badness* costs  $O(p^2 \log r)$ . For  $r = 3$  we can lower the attack complexity to  $O(p^{1.5})$  with a table-based collision search for *good* polynomials.

**4D3. Ugly polynomials.** We test if  $f$  is ugly by trying to find it using the *ugly* polynomials algorithm for each  $r_h = \lceil r/2 \rceil, \dots, r-1$ . The precomputation cost is  $O(p^{r-r_h+3})$  and the search cost is  $O(p^{r_h-3})$ .

If  $r - r_h + 3 > r_h - 3$ , i.e.,  $r_h < r/2 + 3$ , then we can do a tradeoff. Call  $\varepsilon := r_h - r/2 < 3$ . We compute only the action of  $p^\varepsilon$  matrices on  $f$ , and after multiplying with the table  $T_2$  of  $p^{r-r_h}$  sequences, obtain

a table of size  $p^{r/2}$ . We expect to finish the search phase in  $O(p^{r_h-\varepsilon}) = O(p^{r/2})$  if a collision exists. Otherwise we assume that  $f$  does not have a factor of degree  $r_h$  and move to  $r_h + 1$ .

**4E. Security recommendations.** Following our argumentation, the most secure PRFs are the ones coming from *good* polynomials. While we can test for irreducibility in polynomial time, the only way to distinguish *good* and *bad* polynomials is by means of the  $O(p^2 \log r)$  algorithm from the [Appendix](#). The number of *bad* polynomials is small, and can be shown to be bounded from above by

$$\sum_{\substack{r' \mid \gcd(r, p^2-1) \\ r' > 1}} -\mu(r') p^{r/r'+1} r' = O(p^{r/2+1} r).$$

The easiest way to assure our secret polynomial is not *bad* is to choose  $p$  and  $r$  such that  $\gcd(r, p^2-1) = 1$ .

**4F. Degree  $r = 2$ .** If  $r = 2$  all polynomials are *bad* or *ugly*. There is a deterministic  $O(p)$  algorithm for finding  $f$  in this case — we first precompute the action of  $\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{F}_p \right\}$  on the polynomial  $f$ , which ensures that the precomputed table contains the Legendre sequence of a polynomial of the form  $x^2 - c$ :

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot (x^2 - tx + n) = x^2 - (t - 2a)x + (n + a^2 - ta).$$

Then we test all  $p$  such polynomials until we find  $f$ .

## 5. Limited query case and the linear Legendre PRF

In [Section 4](#) we query the oracle at all elements of  $\mathbb{F}_p$  and then extract up to  $p^3 - p$  sequences. The reader should be convinced that the same argumentation works with  $p - o(p/L)$  queries, as we still have access to  $\Omega(p^3)$  sequences. When the secret polynomial is linear doing more than  $O(p^{1/2}L)$  queries is wasteful. Indeed creating a table with  $O(p^{1/2})$  sequences by doing  $L$  queries per sequence allows us to find the secret polynomial after  $O(p^{1/2})$  trials. This is essentially the algorithm in [\[8\]](#), where the author further provides a memoryless approach.

The main difference in the linear case with respect to the higher degree case is that we are allowed  $M \leq \sqrt{p}L$  queries to the oracle. How many different group actions can we obtain from only  $M$  queries? The same question can be asked in the higher degree case, and the algorithm we provide can be directly applied in that scenario. One would expect a cubic increase, as with full access to the oracle, but this seems to be out of reach.

**5A. Linear shifts subgroup.** Let  $G$  be the subgroup of  $\mathcal{M}$  consisting only of linear Möbius transformations,

$$G = \left\{ \begin{pmatrix} d & i \\ 0 & 1 \end{pmatrix} \mid d \in \mathbb{F}_p^*, i \in \mathbb{F}_p \right\} \leq \text{PGL}_2(\mathbb{F}_p).$$

An element  $(i, d) := \begin{pmatrix} d & i \\ 0 & 1 \end{pmatrix}$  sends  $f(x)$  to  $f_{i,d}(x)$ . In order to extract  $\{f_{i,d}(x)\}_L$  from the oracle  $\mathcal{O}$  of  $f$ ,

we compute

$$\left(\frac{f_{i,d}(x)}{p}\right) = \mathcal{O}\left(\frac{dx+i}{0x+1}\right)\left(\frac{0x+1}{p}\right)^r \left(\frac{d}{p}\right)^r = \mathcal{O}(dx+i)\left(\frac{d}{p}\right)^r$$

for all  $x \in [0, L)$ . If  $\mathcal{O}$  is queried in  $[0, M)$ , then we can extract all  $f_{i,d}$  such that  $dx+i \in [0, M)$  for all  $x \in [0, L)$ . This creates the following constraints on  $i, d$ :

$$\begin{cases} d = 1, 2, \dots, \lfloor \frac{M-1}{L-1} \rfloor, \\ i = 0, 1, \dots, M-1 - (L-1)d, \end{cases} \quad \text{or} \quad \begin{cases} d = -1, -2, \dots, -\lfloor \frac{M-1}{L-1} \rfloor, \\ i = (L-1)(-d), \dots, M-1. \end{cases}$$

The total number of eligible  $(i, d) \in G$  is

$$\sum_{d=1}^{\lfloor \frac{M-1}{L-1} \rfloor} 2(M - (L-1)d) = \frac{M^2}{L-1} - M + O(L)$$

with the constant in  $O(L)$  being at most 2.

The limited query algorithm works as follows:

**5A1. Precomputation.** Query  $\mathcal{O}$  at  $[0, M)$ . Extract  $O(\frac{M^2}{L})$  Legendre sequences  $\{f_{i,d}\}_L$  and save them in a table  $T$  together with descriptions of  $(i, d)$ .

**5A2. Search.** The search is done by trying random polynomials until we find a hit in the table, which is expected after  $O(\frac{p'L}{M^2})$  trials, in particular  $O(\frac{p'L}{M^2})$  for the linear PRF.

**5A3. Further improvements.** The cost of the precomputation is  $M$  queries and  $O(\frac{M^2}{L})$  sequence extractions. The cost of the search is  $O(\frac{p'L}{M^2})$  trials. A straightforward way to do a sequence extraction is to read the presaved queries  $L$  times. Due to the nature of the sequences, this cost can be amortised to  $O(1)$  per sequence. Doing a trial consists of evaluating the polynomial in  $L$  places and computing  $L$  Legendre symbols. Again, this cost can be amortised to  $O(\log L)$  per trial. These implementational improvements are not within the scope of this paper, and they are explained in detail in [5].

**5B. Algorithm comparison.** The first algorithm by Khovratovich [8] computes sequences with on-the-go queries, and directly computes Legendre symbols. The main benefit of this approach is that it is memoryless. This was improved on in [2] by extracting sequences rather than querying/computing symbols, and increasing the sequence yield to  $M^2/L^2$ . In our terminology, the authors of [2] use the same group  $G$  but only elements  $(i, d)$  such that  $i < d$ , leading them to a table which is a factor of  $L$  smaller with respect to ours. Using the full group  $G$  as in Section 5A comes with cheaper sequence extraction in the precomputation stage, but more expensive sequence extraction in the search stage and thus the  $\log \log p$  factor in Table 2. A more detailed analysis is given in [5].

**5C. Experiments.** A number of Ethereum research challenges [6] were posted for breaking the linear Legendre PRF. In each challenge we are given a prime  $p$  of size varying from 64 to 148 bits, and  $M = 2^{20}$  bits of the sequence  $\{k\}_M$  as defined in Definition 2.3. The challenge is to recover the key  $k$ . Our results

algorithm	search	precomputation	memory	optimal run time
Khovratovich [8]	$\frac{pt \log^2 p}{M}$	$M$	$\log p$	$\sqrt{pt} \log p$
Beullens et al. [2]	$\frac{p \log^2 p}{M^2}$	$M^2$	$\frac{M^2}{\log p}$	$\sqrt{p} \log p$
our algorithm	$\frac{p \log p \log \log p}{M^2}$	$\frac{M^2}{\log p}$	$M^2$	$\sqrt{p \log \log p}$

**Table 2.** Comparison of the best known algorithms for the linear Legendre PRF challenge, in big- $O$ 's and  $\Theta(\log p)$ -bit word operations. We denote with  $t$  the time to compute a Legendre symbol.

are shown in Table 3. For each challenge, we were able to precompute a table with  $\sim 2^{34}$  sequences. The most interesting is of course challenge #2 since it had not been solved before. The actual number of trials performed in challenge #2 is  $2^{46.97} = 1.38e14$  which is far less than expected. This can be explained by large variance and by sheer luck. The two most difficult challenges (#3 and #4) are out of reach with the proposed attack and its implementation. An in-depth explanation of the experiments is given in [5]. The code and the keys of the first three challenges can be found at <https://github.com/nKolja/LegendrePRF>.

challenge	prime bit size	expected # trials	observed # trials	expected core-hours	observed core-hours
0	64	$2^{30}$	$2^{30.78}$	290 sec	490 sec
1	74	$2^{40}$	$2^{39.53}$	82	59
2	84	$2^{50}$	$2^{46.97}$	1.4e5	1.72e4
3	100	$2^{66}$	-	9.1e9	-
4	148	$2^{114}$	-	2.5e24	-

**Table 3.** Results and estimates for solving the Legendre PRF challenges [6].

### Appendix: Computing the stabiliser $\text{Stab}(f)$ of $f$

Let  $m \in \text{Stab}(f)$  be a matrix of order  $r'$ . Following the same argumentation from Section 4B there exists a change of coordinate matrix  $P$  such that  $D = P^{-1}mP$  is a diagonal matrix. We give a set of representatives for matrices  $D$  and  $P$  such that for each  $m$  there is a single pair  $D, P$  in that set satisfying

$$m = P D P^{-1}.$$

This property can be used to argue that we need only to find one  $m_r$  of order  $p_r$  for any prime divisor  $p_r \mid r'$ . Given  $m_r$ , an element  $m_i$  of order  $p_r^i$  is simply  $P D^{1/p_r^{i-1}} P^{-1}$ , and an element  $m_q$  of order  $q_r$  for some other divisor  $q_r \mid r'$  is  $P D_q P^{-1}$  for the corresponding matrix  $D_q$  of order  $q_r$ . Furthermore, an element of order  $p_r q_r$  can be found by computing  $m_r^u m_q^v$  with  $up_r + vq_r = 1$ . Therefore in order to find the full stabiliser group we need only to find one element of prime order. This is done by searching for elements of order  $q$  in the stabiliser, for each prime  $q \mid r$ , so we assume that we know  $r'$ .

The search for  $m$  is done by going through the conjugacy class of a matrix  $D$  of order  $r'$ , until we find a matrix that stabilises  $f$ . The conjugacy class has size  $\Theta(p^2)$  so we expect to find  $m$  in  $p^2$  steps, but we have to be careful and go through the whole class without repetitions.

The process is explained separately for Type 1 and Type 2 matrices.

**Matrices of Type 1.** If  $m$  is of Type 1 then for some  $P \in \text{GL}_2(\mathbb{F}_p)$ ,

$$m = P \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} P^{-1}$$

with  $a, b \in \mathbb{F}_p$  nonzero such that  $\xi := a/b$  has order  $r'$ . Since  $m$  is defined up to scalar multiplication in  $\mathbb{F}_p^*$ , we may suppose that  $a = \xi$  and  $b = 1$ , so  $D = \begin{pmatrix} \xi & 0 \\ 0 & 1 \end{pmatrix}$  for some  $\xi$  primitive  $r'$ -th root of unity in  $\mathbb{F}_p$ . There are in total  $\varphi(r')$  different  $\xi$  values to consider, however each one will give rise to a different generator of the stabiliser of  $f$ , so the choice of  $\xi$  does not matter.

The search for  $m$  is done by enumerating  $PDP^{-1}$ , where matrices  $P$  are chosen from  $\text{GL}_2(\mathbb{F}_p)$  up to right multiplication by an element of  $Z(D) = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid ab \neq 0 \right\}$ , the centraliser of  $D$ . In total there are  $p^2 + p$  elements in  $\text{GL}_2(\mathbb{F}_p)/Z(D)$ . One set of representatives can be chosen to be

$$\left\{ \begin{pmatrix} 0 & 1 \\ 1 & d \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ c & d \end{pmatrix} \mid c, d \in \mathbb{F}_p \text{ such that the determinants are nonzero} \right\}.$$

When  $r' = 2$ , so  $D = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ , the set of representatives is halved because  $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in Z(D)$  after projecting on  $\text{PGL}_2(\mathbb{F}_p)$ . In that case we give the following  $(p^2 + p)/2$  representatives for the matrices  $P$ :

$$\left\{ \begin{pmatrix} 0 & 1 \\ 1 & d \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ c & d \end{pmatrix} \mid c < d \in \mathbb{F}_p \right\}$$

where the ordering of elements of  $\mathbb{F}_p$  is induced from the lift to  $\{0, 1, \dots, p-1\}$ .

**Matrices of Type 2.** If  $m$  is of Type 2 then for some  $P \in \text{GL}_2(\mathbb{F}_{p^2})$ ,

$$m = P \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} P^{-1}$$

where  $\lambda, \mu \in \mathbb{F}_{p^2}$  are conjugate roots of an irreducible second degree polynomial such that  $\xi := \lambda/\mu$  is a primitive  $r'$ -th root of unity.

**Lemma A.1.** *The diagonal matrix  $D$  defined above is unique in  $\text{GL}_2(\mathbb{F}_{p^2})/\mathbb{F}_p^*$ .*

*Proof.* Since  $\xi = \bar{\mu}/\mu = \mu^{p-1}$  we have  $\xi^{p+1} = 1$ . Due to the primitivity of  $\xi$  it follows that  $r' \mid p+1$ .

If  $\xi \in \mathbb{F}_p$  then  $\xi^2 = 1$  so  $\xi = -1$  and  $r' = 2$ . In that case  $\lambda = -\mu$ , so the minimal polynomial of  $\lambda$  is  $x^2 - c$  for some nonsquare  $c$ . Up to multiplying  $D$  by a constant in  $\mathbb{F}_p^*$ , we may suppose  $\lambda = \sqrt{u}$  for a fixed nonsquare  $u$ , and therefore there is only one such matrix.

If  $\xi$  is not rational, then  $\bar{\xi} = \xi^p = 1/\xi$ , so  $\xi\bar{\xi} = 1$ . From  $\lambda = \xi\mu$  we have  $D = \begin{pmatrix} \xi\mu & 0 \\ 0 & \mu \end{pmatrix}$ . The determinant and the trace of  $D$  are the same as those of  $m$ , so in particular they are rational. This means that

$$\mu(\xi + 1) \in \mathbb{F}_p, \quad \xi\mu^2 \in \mathbb{F}_p$$

from which it follows that  $\mu = a/(\xi + 1)$  and  $\lambda = \xi a/(\xi + 1)$  for some  $a \in \mathbb{F}_p$ . For any choice of  $a$ , the second condition follows from  $\xi\bar{\xi} = 1$ . Multiplying  $\lambda$  and  $\mu$  by any nonzero rational constant does not

change the property of  $D$  being conjugate to  $m \in \text{PGL}_2(\mathbb{F}_p)$ , to them being irrational conjugates of each other or to their quotient being equal to  $\xi$ . Therefore we may suppose  $\lambda = \xi/(\xi + 1)$  and  $\mu = 1/(\xi + 1)$ .  $\square$

We start by computing a primitive root of unity  $\xi$  of order  $r'$ , and set  $D$  as above. As before, the choice of  $\xi$  does not matter.

The search for  $m$  follows by going through  $PDP^{-1}$  where the matrices  $P$  are chosen such that  $PDP^{-1}$  is rational and up to right multiplication by  $Z(D)$ , the centraliser of  $D$ .

*Rational  $PDP^{-1}$ .* If  $PDP^{-1}$  is rational we have  $PDP^{-1} = \overline{P} \overline{D} \overline{P}^{-1}$ , so

$$(P^{-1} \overline{P}) \begin{pmatrix} \mu & 0 \\ 0 & \lambda \end{pmatrix} = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} (P^{-1} \overline{P}).$$

Define  $A_P := P^{-1} \overline{P}$ . The matrix  $A_P$  satisfies  $A_P^{-1} = \overline{A_P}$ , so it has to satisfy

$$A_P = \begin{pmatrix} 0 & \alpha \\ 1/\overline{\alpha} & 0 \end{pmatrix}$$

for some nonzero  $\alpha$  in  $\mathbb{F}_{p^2}$ . From  $\overline{P} = PA_P$  we have some constraints on  $P$ :

$$P \in \left\{ \begin{pmatrix} q & \overline{q\alpha} \\ r & \overline{r\alpha} \end{pmatrix} \mid q, r \in \mathbb{F}_{p^2}, qr \neq 0, q^{p-1} \neq r^{p-1} \right\}.$$

*The centraliser  $Z(D)$ .* The matrix  $D$  is diagonal with different eigenvalues, so

$$Z(D) = \left\{ \begin{pmatrix} x & 0 \\ 0 & \overline{y} \end{pmatrix} \mid x, y \in \mathbb{F}_{p^2}, xy \neq 0 \right\}.$$

Multiplying a  $P$  on the right by an element of the centraliser gives

$$\begin{pmatrix} q & \overline{q\alpha} \\ r & \overline{r\alpha} \end{pmatrix} \begin{pmatrix} x & 0 \\ 0 & \overline{y} \end{pmatrix} = \begin{pmatrix} qx & \overline{q\alpha\overline{y}} \\ rx & \overline{r\alpha\overline{y}} \end{pmatrix} = \begin{pmatrix} qx & \overline{qx} \left( \frac{\overline{\alpha y}}{x} \right) \\ rx & \overline{rx} \left( \frac{\overline{\alpha y}}{x} \right) \end{pmatrix},$$

which sends  $(q, r)$  to  $(qx, rx)$  and  $\alpha$  to  $\alpha y/x$ , so we may assume that  $q = \alpha = 1$ . A set of  $p^2 - p$  representatives for matrices  $P$  is

$$\left\{ \begin{pmatrix} 1 & 1 \\ r & \overline{r} \end{pmatrix} \mid r \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p \right\}.$$

When  $r' = 2$ , so  $D = \begin{pmatrix} \sqrt{u} & 0 \\ 0 & -\sqrt{u} \end{pmatrix}$  for some rational nonsquare  $u$ , the set of representatives is halved because  $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in Z(D)$  after projecting on  $\text{GL}_2(\mathbb{F}_p^2)/\mathbb{F}_p^*$ . In that case we give the following  $(p^2 - p)/2$  representatives for matrices  $P$ :

$$\left\{ \begin{pmatrix} 1 & 1 \\ r & \overline{r} \end{pmatrix} \mid r = a\sqrt{u} + b, \quad 1 \leq a \leq \frac{p-1}{2}, \quad 0 \leq b < p \right\}.$$

## References

- [1] Elwyn R. Berlekamp, *Algebraic coding theory - revised edition*, World Scientific Publishing Co., Inc., USA, 2015.
- [2] Ward Beullens, Tim Beyne, Aleksei Udovenko, and Giuseppe Vito, *Cryptanalysis of the Legendre PRF and generalizations*, Cryptology ePrint Archive, Report 2019/1357, 2019, <https://eprint.iacr.org/2019/1357>.
- [3] Ivan Damgård, *On the randomness of Legendre and Jacobi sequences*, Proceedings of the 8th Annual International Cryptology Conference on Advances in Cryptology (London, UK), CRYPTO '88, Springer-Verlag, 1990, pp. 163–172.
- [4] H. Davenport, *On the distribution of quadratic residues (mod p)*, Journal of the London Mathematical Society **s1-8** (1933), no. 1, 46–52.
- [5] Novak Kaluđerović, Thorsten Kleinjung, and Dušan Kostić, *Improved key recovery on the Legendre PRF*, Cryptology ePrint Archive, Report 2020/098, 2020, <https://eprint.iacr.org/2020/098>.
- [6] Dankard Feist, *Legendre pseudo-random function*, 2019, <https://legendreprf.org/bounties>.
- [7] Lorenzo Grassi, Christian Rechberger, Dragos Rotaru, Peter Scholl, and Nigel P. Smart, *MPC-friendly symmetric key primitives*, Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (New York, NY, USA), CCS '16, ACM, 2016, pp. 430–443.
- [8] Dmitry Khovratovich, *Key recovery attacks on the Legendre PRFs within the birthday bound*, Cryptology ePrint Archive, Report 2019/862, 2019, <https://eprint.iacr.org/2019/862>.
- [9] Alexander Russell and Igor E. Shparlinski, *Classical and quantum function reconstruction via character evaluation*, Journal of Complexity **20** (2004), no. 2-3, 404–422 (English).
- [10] André Weil, *On some exponential sums*, Proceedings of the National Academy of Sciences **34** (1948), no. 5, 204–207.
- [11] Andrew C. Yao, *Theory and application of trapdoor functions*, Proceedings of the 23rd Annual Symposium on Foundations of Computer Science (USA), SFCS '82, IEEE Computer Society, 1982, p. 80–91.

Received 27 Feb 2020. Revised 31 Jul 2020.

NOVAK KALUĐEROVIĆ: [novak.kaluderovic@epfl.ch](mailto:novak.kaluderovic@epfl.ch)

Laboratory for cryptologic algorithms, École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland

THORSTEN KLEINJUNG: [thorsten.kleinjung@epfl.ch](mailto:thorsten.kleinjung@epfl.ch)

Laboratory for cryptologic algorithms, École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland

DUŠAN KOSTIĆ: [dusan.kostic@epfl.ch](mailto:dusan.kostic@epfl.ch)

Laboratory for cryptologic algorithms, École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland



# Counting Richelot isogenies between superspecial abelian surfaces

Toshiyuki Katsura and Katsuyuki Takashima

Castoryck, Decru, and Smith used superspecial genus-2 curves and their Richelot isogeny graph for basing genus-2 isogeny cryptography, and recently, Costello and Smith devised an improved isogeny path-finding algorithm in the genus-2 setting. In order to establish a firm ground for the cryptographic construction and analysis, we give a new characterization of *decomposed Richelot isogenies* in terms of *involutive reduced automorphisms* of genus-2 curves over a finite field, and explicitly count such decomposed (and nondecomposed) Richelot isogenies between *superspecial* principally polarized abelian surfaces. As a corollary, we give another algebraic geometric proof of Theorem 2 in the paper of Castoryck et al.

## 1. Introduction

Isogenies of supersingular elliptic curves are widely studied as one candidate for postquantum cryptography, e.g., [3; 5; 10; 2]. Recently, several authors have extended the cryptosystems to higher genus isogenies, especially the genus-2 case [17; 6; 1; 4].

Castoryck, Decru, and Smith [1] showed that *superspecial* genus-2 curves and their isogeny graphs give a correct foundation for constructing genus-2 isogeny cryptography. The recent cryptanalysis by Costello and Smith [4] employed the subgraph whose vertices consist of decomposed principally polarized abelian varieties, hence it is important to study the subgraph in cryptography.

Castoryck et al. also presented concrete algebraic formulas for computing  $(2, 2)$ -isogenies by using the Richelot construction. In the genus-2 case, the isogenies may have decomposed principally polarized abelian surfaces as codomain, and we call them decomposed isogenies. In [1], the authors gave explicit formulas for the decomposed isogenies and a theorem stating that the number of decomposed Richelot isogenies outgoing from the Jacobian  $J(C)$  of a superspecial curve  $C$  of genus 2 is *at most six* [1, Theorem 2], but they *do not precisely determine* this number. Moreover, their proof is *computer-aided*, that is, using the Gröbner basis computation.

Therefore, we revisit the isogeny counting based on an intrinsic algebraic geometric characterization. In 1960, Igusa [9] classified the curves of genus 2 with given reduced groups of automorphisms,

*MSC2010:* primary 14K02; secondary 14G50, 14H37, 14H40.

*Keywords:* Richelot isogenies, superspecial abelian surfaces, reduced group of automorphisms, genus-2 isogeny cryptography.

and in 1986, Ibukiyama, Katsura, and Oort [7] explicitly counted such superspecial curves according to the classification. Based on the classical results, we first count the number of Richelot isogenies from a superspecial Jacobian to decomposed surfaces (Cases (0)–(6) in Section 5) in terms of *involutive* (i.e., of order 2) *reduced automorphisms* which are called long elements. As a corollary, we give an algebraic geometric proof of Theorem 2 in [1] together with a *precise count of decomposed Richelot isogenies* (Remark 5.1). Moreover, by extending the method, we also count the total number of (decomposed) Richelot isogenies up to isomorphism outgoing from irreducible superspecial curves of genus 2 (resp. decomposed principally polarized superspecial abelian surfaces) in Theorem 6.2 (resp. Theorem 6.4).

Our paper is organized as follows: Section 2 gives mathematical preliminaries including the Igusa classification and the Ibukiyama–Katsura–Oort curve counting. Section 3 presents an abstract description of Richelot isogenies and Section 4 gives the main characterization of decomposed Richelot isogenies in terms of reduced groups of automorphisms. Section 5 counts the number of long elements of order 2 in reduced groups of automorphisms based on the results in Section 4. Section 6 gives the total numbers of (decomposed) Richelot isogenies outgoing from the irreducible superspecial curves of genus 2 and products of two elliptic curves, respectively. Section 7 gives some examples in small characteristic. Finally, Section 8 gives a concluding remark.

We use the following notation: For an abelian surface  $A$ ,  $A[n]$  denotes the group of  $n$ -torsion points of  $A$ ,  $A'$  the dual of  $A$ ,  $\text{NS}(A)$  the Néron–Severi group of  $A$ , and  $T_v$  the translation by an element  $v$  of  $A$ . For a nonsingular projective variety  $X$ ,  $D \sim D'$  (resp.  $D \approx D'$ ) denotes linear equivalence (resp. numerical equivalence) for divisors  $D$  and  $D'$  on  $X$ , and  $\text{id}_X$  the identity morphism of  $X$ .

## 2. Preliminaries

Let  $k$  be an algebraically closed field of characteristic  $p > 5$ . An abelian surface  $A$  defined over  $k$  is said to be superspecial if  $A$  is isomorphic to  $E_1 \times E_2$  with  $E_i$  supersingular elliptic curves ( $i = 1, 2$ ). Since for any supersingular elliptic curves  $E_i$  ( $i = 1, 2, 3, 4$ ) we have an isomorphism  $E_1 \times E_2 \cong E_3 \times E_4$  (see Shioda [15, Theorem 3.5], for instance), this notion does not depend on the choice of supersingular elliptic curves. For a nonsingular projective curve  $C$  of genus 2, we denote by  $(J(C), C)$  the canonically polarized Jacobian variety of  $C$ . The curve  $C$  is said to be superspecial if  $J(C)$  is superspecial as an abelian surface. We denote by  $\text{Aut}(C)$  the group of automorphisms of  $C$ . Since  $C$  is hyperelliptic,  $C$  has the hyperelliptic involution  $\iota$  such that the quotient curve  $C/\langle \iota \rangle$  is isomorphic to the projective line  $\mathbb{P}^1$ :

$$\psi : C \rightarrow \mathbb{P}^1.$$

There exist 6 ramification points on  $C$ . We denote them by  $P_i$  ( $1 \leq i \leq 6$ ). Then, the  $Q_i = \psi(P_i)$  are the branch points of  $\psi$  on  $\mathbb{P}^1$ . The group  $\langle \iota \rangle$  is a normal subgroup of  $\text{Aut}(C)$ . We put  $\text{RA}(C) \cong \text{Aut}(C)/\langle \iota \rangle$  and we call it the reduced group of automorphisms of  $C$ . We call an element of  $\text{RA}(C)$  a reduced automorphism of  $C$ . For  $\sigma \in \text{RA}(C)$ ,  $\tilde{\sigma}$  is an element of  $\text{Aut}(C)$  such that  $\tilde{\sigma} \bmod \langle \iota \rangle = \sigma$ .

**Definition 2.1.** An element  $\sigma \in \text{RA}(C)$  of order 2 is said to be long if  $\tilde{\sigma}$  is of order 2. Otherwise, an element  $\sigma \in \text{RA}(C)$  of order 2 is said to be short (see [12, Definition 7.15]).

This definition does not depend on the choice of  $\tilde{\sigma}$ .

**Lemma 2.2.** If an element  $\sigma \in \text{RA}(C)$  of order 2 acts freely on 6 branch points, then  $\sigma$  is long.

*Proof.* By a suitable choice of coordinate  $x$  of  $\mathbb{A}^1 \subset \mathbb{P}^1$ , taking 0 as a fixed point of  $\sigma$ , we may assume  $\sigma(x) = -x$ , and  $Q_1 = 1, Q_2 = -1, Q_3 = a, Q_4 = -a, Q_5 = b, Q_6 = -b$  ( $a \neq 0, \pm 1; b \neq 0, \pm 1; a \neq \pm b$ ). Then, the curve is defined by

$$y^2 = (x^2 - 1)(x^2 - a^2)(x^2 - b^2),$$

and  $\tilde{\sigma}$  is given by  $x \mapsto -x, y \mapsto \pm y$ . Therefore,  $\tilde{\sigma}$  is of order 2.  $\square$

**Lemma 2.3.** If  $\text{RA}(C)$  has an element  $\sigma$  of order 2, then there exists a long element  $\tau \in \text{RA}(C)$  of order 2.

*Proof.* If  $\sigma$  acts freely on 6 branch points, then by Lemma 2.2,  $\sigma$  itself is a long element of order 2. We assume that the branch point  $Q_1 = \psi(P_1)$  is a fixed point of  $\sigma$ . Since  $\sigma$  is of order 2, it must have one more fixed point among the branch points, say  $Q_2 = \psi(P_2)$ . By a suitable choice of coordinate  $x$  of  $\mathbb{A}^1 \subset \mathbb{P}^1$ , we may assume  $Q_1 = 0$  and  $Q_2 = \infty$ . We may also assume  $Q_3 = 1$ . Then,  $\sigma$  is given by  $x \mapsto -x$  and the six branch points are  $0, 1, -1, a, -a, \infty$  ( $a \neq \pm 1$ ). The curve  $C$  is given by

$$y^2 = x(x^2 - 1)(x^2 - a^2) \quad (a \neq 0, \pm 1).$$

We consider an element  $\tau \in \text{Aut}(\mathbb{P}^1)$  defined by  $x \mapsto a/x$ . Then, we have an automorphisms  $\tilde{\tau}$  of  $C$  defined by  $x \mapsto a/x, y \mapsto a\sqrt{a}y/x^3$ . Therefore, we see  $\tau \in \text{RA}(C)$ . Since  $\tilde{\tau}$  is of order 2,  $\tau$  is long.  $\square$

$\text{RA}(C)$  acts on the projective line  $\mathbb{P}^1$  as a subgroup of  $\text{PGL}_2(k)$ . The structure of  $\text{RA}(C)$  is classified as follows (see [9, page 644] and [7, page 130]):

$$(0) 0, \quad (1) \mathbb{Z}/2\mathbb{Z}, \quad (2) S_3, \quad (3) \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad (4) D_{12}, \quad (5) S_4, \quad (6) \mathbb{Z}/5\mathbb{Z}.$$

We denote by  $n_i$  the number of superspecial curves of genus 2 whose reduced group of automorphisms is isomorphic to the group (i). Then, the  $n_i$  are given as follows (see [7, Theorem 3.3]):

$$\begin{aligned} (0) \quad n_0 &= \frac{(p-1)(p^2-35p+346)}{2880} - \frac{\{1 - (\frac{-1}{p})\}}{32} - \frac{\{1 - (\frac{-2}{p})\}}{8} - \frac{\{1 - (\frac{-3}{p})\}}{9} + \begin{cases} 0 & \text{if } p \equiv 1, 2 \text{ or } 3 \pmod{5}, \\ -\frac{1}{5} & \text{if } p \equiv 4 \pmod{5}. \end{cases} \\ (1) \quad n_1 &= \frac{(p-1)(p-17)}{48} + \frac{\{1 - (\frac{-1}{p})\}}{8} + \frac{\{1 - (\frac{-2}{p})\}}{2} + \frac{\{1 - (\frac{-3}{p})\}}{2}. \\ (2) \quad n_2 &= \frac{(p-1)}{6} - \frac{\{1 - (\frac{-2}{p})\}}{2} - \frac{\{1 - (\frac{-3}{p})\}}{3}. \\ (3) \quad n_3 &= \frac{(p-1)}{8} - \frac{\{1 - (\frac{-1}{p})\}}{8} - \frac{\{1 - (\frac{-2}{p})\}}{4} - \frac{\{1 - (\frac{-3}{p})\}}{2}. \\ (4) \quad n_4 &= \frac{\{1 - (\frac{-3}{p})\}}{2}. \end{aligned}$$

$$(5) \ n_5 = \frac{\{1 - (\frac{-2}{p})\}}{2}.$$
$$(6) \ n_6 = \begin{cases} 0 & \text{if } p \equiv 1, 2 \text{ or } 3 \pmod{5}, \\ 1 & \text{if } p \equiv 4 \pmod{5}. \end{cases}$$

Here, for a prime number  $q$  and an integer  $a$ ,  $(\frac{a}{q})$  is the Legendre symbol. The total number  $n$  of superspecial curves of genus 2 is given by

$$\begin{aligned} n &= n_0 + n_1 + n_2 + n_3 + n_4 + n_5 + n_6 \\ &= \frac{(p-1)(p^2+25p+166)}{2880} - \frac{\{1 - (\frac{-1}{p})\}}{32} + \frac{\{1 - (\frac{-2}{p})\}}{8} + \frac{\{1 - (\frac{-3}{p})\}}{18} + \begin{cases} 0 & \text{if } p \equiv 1, 2 \text{ or } 3 \pmod{5}, \\ \frac{4}{5} & \text{if } p \equiv 4 \pmod{5}. \end{cases} \end{aligned}$$

For an abelian surface  $A$ , we have  $A^t = \text{Pic}^0(A)$  (Picard variety of  $A$ ), and for a divisor  $D$  on  $A$ , there exists a homomorphism

$$\begin{aligned} \varphi_D : A &\rightarrow A^t \\ v &\mapsto T_v^* D - D. \end{aligned}$$

If  $D$  is ample, then  $\varphi_D$  is surjective, i.e., an isogeny. We know  $(D \cdot D)^2 = 4 \deg \varphi_D$ . We set  $K(D) = \text{Ker } \varphi_D$ . If  $D$  is ample, then  $K(D)$  is finite and there is a nondegenerate alternating bilinear form  $e^D(v, w)$  on  $K(D)$  (see Mumford [14, Section 23]). Let  $G$  be an isotropic subgroup scheme of  $K(D)$  with respect to  $e^D(v, w)$ . In case  $D$  is ample,  $G$  is finite and we have an isogeny

$$\pi : A \rightarrow A/G.$$

The following theorem is due to Mumford [14, Section 23, Theorem 2, Corollary]:

**Theorem 2.4.** *Let  $G$  be an isotropic subgroup scheme of  $K(D)$ . Then, there exists a divisor  $D'$  on  $A/G$  such that  $\pi^* D' \sim D$ .*

Let  $n$  be a positive integer which is prime to  $p$ . Then, we have the Weil pairing  $e_n : A[n] \times A^t[n] \rightarrow \mu_n$ . Here,  $\mu_n$  is the multiplicative group of order  $n$ . By Mumford [14, Section 23 “Functorial properties of  $e^L$  (5)”], we have the following.

**Lemma 2.5.** *For  $v \in A[n]$  and  $w \in \varphi_D^{-1}(A^t[n])$ , we have*

$$e_n(v, \varphi_D(w)) = e^{nD}(v, w).$$

If  $D$  is a principal polarization, the homomorphism  $\varphi_D : A \rightarrow A^t$  is an isomorphism. Therefore, by this identification we can identify the pairing  $e^{nD}$  with the Weil pairing  $e_n$ .

3. Richelot isogenies

We recall the abstract description of Richelot isogenies. (For the concrete construction of Richelot isogenies, see Smith [16] or Castryck, Decru and Smith [1, Section 3], for instance.)

Let  $A$  be an abelian surface with a principal polarization  $C$ . Then, we may assume that  $C$  is effective, and we have the self-intersection number  $C^2 = 2$ . It is easy to show (or as was shown by A. Weil) that there are two cases for effective divisors with self-intersection 2 on an abelian surface  $A$ :

(1) There exists a nonsingular curve  $C$  of genus 2 such that  $A$  is isomorphic to the Jacobian variety  $J(C)$  of  $C$  and that  $C$  is the divisor with self-intersection 2. In this case,  $(J(C), C)$  is said to be nondecomposed.

(2) There exist two elliptic curves  $E_1, E_2$  with  $(E_1 \cdot E_2) = 1$  such that  $E_1 \times \{0\} + \{0\} \times E_2$  is a divisor with self-intersection 2 and that  $A \cong E_1 \times E_2$ . In this case,  $(A, E_1 \times \{0\} + \{0\} \times E_2)$  is said to be decomposed.

Since  $\varphi_C$  is an isomorphism by the fact that  $C$  is a principal polarization, we have  $K(2C) = \text{Ker } \varphi_{2C} = \text{Ker } 2\varphi_C = A[2]$ . Let  $G$  be a maximal isotropic subgroup of  $K(2C) = A[2]$  with respect to the pairing  $e^{2C}$ . Since we have  $|G|^2 = |A[2]| = 2^4$  (see Mumford [14, Section 23, Theorem 4]), we have  $|G| = 4$  and  $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . We have a quotient homomorphism

$$\pi : A \rightarrow A/G.$$

By Theorem 2.4, there exists a divisor  $C'$  on  $A/G$  such that  $2C \sim \pi^*C'$ . Since  $\pi$  is a finite morphism and  $2C$  is ample, we see that  $C'$  is also ample. We have the self-intersection number  $(2C \cdot 2C) = 8$ , and we have

$$8 = (2C \cdot 2C) = (\pi^*C' \cdot \pi^*C') = \deg \pi(C' \cdot C') = 4(C' \cdot C').$$

Therefore, we have  $(C' \cdot C') = 2$ , that is,  $C'$  is a principal polarization on  $A/G$ . By the Riemann–Roch theorem of an abelian surface for ample divisors, we have

$$\dim H^0(A/G, \mathcal{O}_{A/G}(C')) = (C' \cdot C')/2 = 1.$$

Therefore, we may assume  $C'$  is an effective divisor.

Using these facts, we see that  $C'$  is either a nonsingular curve of genus 2 or  $E_1 \cup E_2$  with elliptic curves  $E_i$  ( $i = 1, 2$ ) which intersect each other transversely. In this situation, the correspondence from  $(A, C)$  to  $(A/G, C')$  is called a Richelot isogeny. We consider a triple  $(A, C, G)$  with maximal isotropic subgroup  $G \subset A[2]$  with respect to the pairing  $e^{2C}$ , and the corresponding Richelot isogeny  $\pi$  from  $(A, C, G)$  to  $(A/G, C', G')$  with maximal isotropic subgroup  $G' = \pi(A[2])$ . Then, it is easy to see that for the Richelot isogeny  $\pi' : (A/G, C') \rightarrow ((A/G)/G', C'')$ , the principally polarized abelian surface  $((A/G)/G', C'', G'')$  with maximal isotropic subgroup  $G'' = \pi'((A/G)[2])$  is isomorphic to the original  $(A, C, G)$ .

Now, we consider the case where  $A$  is a superspecial abelian surface. Then, since  $\pi$  is separable,  $A/G$  is also a superspecial abelian surface. We will use this fact freely.

From here on, for abelian surface  $E_1 \times E_2$  with elliptic curves  $E_i$  ( $i = 1, 2$ ) we denote by  $E_1 + E_2$  the divisor  $E_1 \times \{0\} + \{0\} \times E_2$ , if no confusion occurs. We sometimes call  $E_1 \times E_2$  a principally polarized abelian surface. In this case, the principal polarization on  $E_1 \times E_2$  is given by  $E_1 + E_2$ .

**Definition 3.1.** Let  $(A, C)$ ,  $(A', C')$  and  $(A'', C'')$  be principally polarized abelian surfaces with principal polarizations  $C, C', C''$ , respectively. The Richelot isogeny  $\pi : A \rightarrow A'$  is said to be isomorphic to the Richelot isogeny  $\varpi : A \rightarrow A''$  if there exist an automorphism  $\sigma \in A$  with  $\sigma^*C \approx C$  and an isomorphism  $g : A' \rightarrow A''$  with  $g^*C'' \approx C'$  such that the following diagram commutes:

$$\begin{array}{ccc} A & \xrightarrow{\sigma} & A \\ \pi \downarrow & & \downarrow \varpi \\ A' & \xrightarrow{g} & A'' \end{array}$$

#### 4. Decomposed Richelot isogenies

In this section, we use the same notation as in [Section 3](#).

**Definition 4.1.** Let  $A$  and  $A'$  be abelian surfaces with principal polarizations  $C, C'$ , respectively. A Richelot isogeny  $A \rightarrow A'$  is said to be decomposed if  $C'$  consists of two elliptic curves. Otherwise, the Richelot isogeny is said to be nondecomposed.

**Example 4.2.** Let  $C_{a,b}$  be a nonsingular projective model of the curve of genus 2 defined by the equation

$$y^2 = (x^2 - 1)(x^2 - a)(x^2 - b) \quad (a \neq 0, 1; b \neq 0, 1; a \neq b).$$

Let  $\iota$  be the hyperelliptic involution defined by  $x \mapsto x, y \mapsto -y$ .  $\text{RA}(C_{a,b})$  has an element of order 2 defined by

$$\sigma : x \mapsto -x, y \mapsto y.$$

We put  $\tau = \iota \circ \sigma$ . We have two elliptic curves  $E_\sigma = C_{a,b}/\langle \sigma \rangle$  and  $E_\tau = C_{a,b}/\langle \tau \rangle$ . The elliptic curve  $E_\sigma$  is isomorphic to an elliptic curve  $E_\lambda : y^2 = x(x-1)(x-\lambda)$  with

$$\lambda = (b-a)/(1-a) \tag{4-1}$$

and the elliptic curve  $E_\tau$  is isomorphic to an elliptic curve  $E_\mu : y^2 = x(x-1)(x-\mu)$  with

$$\mu = (b-a)/b(1-a). \tag{4-2}$$

The map given by (4-1) and (4-2) yields a bijection

$$\begin{aligned} \{(a, b) \mid a, b \in k; a \neq 0, 1; b \neq 0, 1; a \neq b, \text{ and } J(C_{a,b}) \text{ is superspecial}\} \\ \rightarrow \{(\lambda, \mu) \mid \lambda, \mu \in k; \lambda \neq \mu; E_\lambda, E_\mu \text{ are supersingular}\} \end{aligned}$$

(for the details, see Katsura and Oort [13, page 259]). We have a natural morphism  $C_{a,b} \rightarrow E_\sigma \times E_\tau$  and this morphism induces an isogeny

$$\pi : J(C_{a,b}) \rightarrow E_\sigma \times E_\tau.$$

By [9, page 648], we know  $\text{Ker } \pi \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  and  $\text{Ker } \pi$  consists of  $P_1 - \sigma(P_1)$ ,  $P_3 - \sigma(P_3)$ ,  $P_5 - \sigma(P_5)$  and the zero point. Here,  $P_1 = (1, 0)$ ,  $P_3 = (a, 0)$ ,  $P_5 = (b, 0)$ . Since  $P_i - \sigma(P_i)$  is a divisor of order 2, we have  $P_i - \sigma(P_i) \sim \sigma(P_i) - P_i$ .

Comparing the calculation in [1, Proposition 1(2)] with the one in [13, Lemma 2.4], we see that  $\pi : J(C_{a,b}) \rightarrow E_\sigma \times E_\tau$  is a decomposed Richelot isogeny with  $C'_{a,b} = E_\sigma + E_\tau$  (also see [12, Proof of Proposition 7.18 (iii)]). We will use the bijection above to calculate decomposed Richelot isogenies.

**Proposition 4.3.** *Let  $C$  be a nonsingular projective curve of genus 2. Then, the following three conditions are equivalent:*

- (i)  $C$  has a decomposed Richelot isogeny outgoing from  $J(C)$ .
- (ii)  $\text{RA}(C)$  has an element of order 2.
- (iii)  $\text{RA}(C)$  has a long element of order 2.

*Proof.* (i)  $\Rightarrow$  (ii). By assumption, we have a Richelot isogeny

$$\pi : J(C) \rightarrow J(C)/G \quad (4-3)$$

such that  $G$  is an isotropic subgroup of  $J(C)[2]$  with respect to  $2C$ , and that  $C'$  is a principal polarization consisting of two elliptic curves  $E_i$  ( $i = 1, 2$ ) on  $J(C)/G$  with  $2C \sim \pi^*(E_1 + E_2)$ . Since  $C$  is a principal polarization, we have an isomorphism  $\varphi_C : J(C) \cong J(C)^t$ . In a similar way, we have  $J(C)/G \cong (J(C)/G)^t$ . Dualizing (4-3), we have

$$\eta = \pi^t : J(C)/G \rightarrow J(C)$$

with  $J(C)/G \cong E_1 \times E_2$ ,  $C' = E_1 + E_2$  and  $\eta^*(C) \sim 2(E_1 + E_2)$ . The kernel  $\text{Ker } \eta$  is an isotropic subgroup of  $(E_1 \times E_2)[2]$  with respect to the divisor  $2(E_1 + E_2)$ .

Denoting by  $\iota_{E_1}$  the inversion of  $E_1$ , we set

$$\bar{\tau} = \iota_{E_1} \times \text{id}_{E_2}.$$

Then,  $\bar{\tau}$  is an automorphism of order 2 which is not the inversion of  $E_1 \times E_2$ . By the definition, we have

$$\bar{\tau}^*(E_1 + E_2) = E_1 + E_2.$$

Moreover, since  $\text{Ker } \eta$  consists of elements of order 2 and  $\bar{\tau}$  fixes the elements of order 2,  $\bar{\tau}$  preserves  $\text{Ker } \eta$ . Therefore,  $\bar{\tau}$  induces an automorphism  $\tau$  of  $J(C) \cong (J(C)/G)/\text{Ker } \eta \cong (E_1 \times E_2)/\text{Ker } \eta$ . Therefore, we have the following diagram:

$$\begin{array}{ccc} E_1 \times E_2 & \xrightarrow{\bar{\tau}} & E_1 \times E_2 \\ \eta \downarrow & & \downarrow \eta \\ J(C) & \xrightarrow{\tau} & J(C) \end{array}$$

We have

$$\eta^* \tau^* C = \bar{\tau}^* \eta^* C \sim \bar{\tau}^*(2(E_1 + E_2)) = 2(E_1 + E_2).$$

On the other hand, we have

$$\eta^* C \sim 2(E_1 + E_2).$$

Since  $\eta^*$  is an injective homomorphism from  $\text{NS}(J(C))$  to  $\text{NS}(E_1 \times E_2)$ , we have  $C \approx \tau^* C$ . Therefore,  $\tau^* C - C$  is an element of  $\text{Pic}^0(J(C)) = J(C)^t$ . Since  $C$  is ample, the homomorphism

$$\begin{aligned} \varphi_C : J(C) &\rightarrow J(C)^t \\ v &\mapsto T_v^* C - C \end{aligned}$$

is surjective. Therefore, there exists an element  $v \in J(C)$  such that

$$T_v^* C - C \sim \tau^* C - C,$$

that is,  $T_v^* C \sim \tau^* C$ . Since  $T_v^* C$  is a principal polarization, we see

$$\dim H^0(J(C), \mathcal{O}_{J(C)}(T_v^* C)) = 1.$$

Therefore, we have  $T_v^* C = \tau^* C$ , that is,  $T_{-v}^* \tau^* C = C$ . Since  $\tau$  is of order 2, we have  $(\tau \circ T_{-v})^2 = T_{-v-\tau(v)}$ , a translation. Therefore, we have  $T_{-v-\tau(v)}^* C = C$ . However, since  $C$  is a principal polarization, we have  $\text{Ker } \varphi_C = \{0\}$ . Therefore, we have  $T_{-v-\tau(v)} = \text{id}$ . This means  $\tau \circ T_{-v}$  is an automorphism of order 2 of  $C$ . By definition, this is not the inversion  $\iota$ . Hence, this gives an element of order 2 in  $\text{RA}(C)$ .

(ii)  $\Rightarrow$  (iii) This follows from [Lemma 2.3](#).

(iii)  $\Rightarrow$  (i) This follows from [Lemma 2.2](#) and [Example 4.2](#). □

**Remark 4.4.** In the proof of the proposition, the automorphism  $\tau \circ T_{-v}$  really gives a long element of order 2 in  $\text{RA}(C)$ .

By [\[1, Section 3.3\]](#), if the curve  $C$  of genus 2 is obtained from a decomposed principally polarized abelian surface by a Richelot isogeny, then the curve  $C$  has a long reduced automorphism of order 2. As is well-known, for a curve  $C$  of genus 2, the Jacobian variety  $J(C)$  has 15 Richelot isogenies (see [\[1, Section 3.2\]](#), for instance). If we have a Richelot isogeny  $(A, C) \rightarrow (A', C')$ , then we also have a Richelot isogeny  $(A', C') \rightarrow (A, C)$ . Therefore, we have the following proposition.

**Proposition 4.5.** *Let  $C$  be a nonsingular projective curve of genus 2. Among the 15 Richelot isogenies outgoing from  $J(C)$ , the number of decomposed Richelot isogenies is equal to the number of long elements of order 2 in  $\text{RA}(C)$ .*

In this proposition, we consider that a different isotropic subgroup gives a different Richelot isogeny. However, two different Richelot isogenies may be isomorphic to each other by a suitable automorphism (see [Definition 3.1](#)). From the next section, we will compute the number of Richelot isogenies up to isomorphism.



## 5. The number of long elements of order 2

In this section, we count the number of long elements of order 2 in  $\text{RA}(C)$ . For an element  $f \in \text{RA}(C)$ , we express the reduced automorphism by

$$f : x \mapsto f(x)$$

with a suitable coordinate  $x$  of  $\mathbb{A}^1 \subset \mathbb{P}^1$ . We will give the list of  $f(x)$  corresponding to elements of order 2. Here, we denote by  $\omega$  a primitive cube root of unity, by  $i$  a primitive fourth root of unity, and by  $\zeta$  a primitive sixth root of unity:

Case 0:  $\text{RA}(C) \cong \{0\}$ .

- There exist no long elements of order 2.

Case 1:  $\text{RA}(C) \cong \mathbb{Z}/2\mathbb{Z}$ .

- The curve  $C$  is given by  $y^2 = (x^2 - 1)(x^2 - a^2)(x^2 - b^2)$ .
- There exists only one long element of order 2 given by  $f(x) = -x$ .

Case 2:  $\text{RA}(C) \cong S_3$ .

- The curve  $C$  is given by  $y^2 = (x^3 - 1)(x^3 - a^3)$ .
- There exist three long elements of order 2 given by  $f(x) = a/x, \omega a/x, \omega^2 a/x$ .

Case 3:  $\text{RA}(C) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .

- The curve  $C$  is given by  $y^2 = x(x^2 - 1)(x^2 - a^2)$ .
- There exist two long elements of order 2 given by  $f(x) = a/x, -a/x$ .
- There exists one short element of order 2 given by  $f(x) = -x$ .

Case 4:  $\text{RA}(C) \cong D_{12}$ .

- The curve is given by  $y^2 = x^6 - 1$ .
- There exist four long elements of order 2 given by  $f(x) = -x, \zeta/x, \zeta^3/x, \zeta^5/x$ .
- There exist three short elements of order 2 given by  $f(x) = 1/x, \zeta^2/x, \zeta^4/x$ .

Case 5:  $\text{RA}(C) \cong S_4$ .

- The curve  $C$  is given by  $y^2 = x(x^4 - 1)$ .
- There exist six long elements of order 2 given by  $f(x) = (x+1)/(x-1), -(x-1)/(x+1), i(x+i)/(x-i), i/x, -i/x, -i(x-i)/(x+i)$ .
- There exist three short elements of order 2 given by  $f(x) = -x, 1/x, -1/x$ .

Case 6:  $\text{RA}(C) \cong \mathbb{Z}/5\mathbb{Z}$ .

- The curve is given by  $y^2 = x^5 - 1$ .
- There exist no long elements of order 2.

**Remark 5.1.** By [Proposition 4.5](#) and the calculation above, we see that for a curve  $C$  of genus 2, the number of outgoing decomposed Richelot isogenies from  $J(C)$  is at most six. This result coincides with the one given in [\[1, Theorem 2\]](#).

## 6. Counting Richelot isogenies

**6A. Richelot isogenies from Jacobians of irreducible genus-2 curves.** Let  $C$  be a nonsingular projective curve of genus 2, and let  $J(C)$  be the Jacobian variety of  $C$ . For a fixed  $C$ , we consider the set  $\{(J(C), G)\}$  of pairs of  $J(C)$  and an isotropic subgroup  $G$  for the polarization  $2C$ . The group  $\text{Aut}(C)$  acts on the ramification points of  $C \rightarrow \mathbb{P}^1$ . Using this action,  $\text{Aut}(C)$  induces the action on the set  $\{(J(C), G)\}$ . Since the inversion  $\iota$  of  $C$  acts on  $J(C)[2]$  trivially, the reduced group  $\text{RA}(C)$  of automorphisms acts on the set  $\{(J(C), G)\}$  which consists of 15 elements.

Let  $P_i$  ( $i = 1, 2, \dots, 6$ ) be the ramification points of  $\psi : C \rightarrow \mathbb{P}^1$ . A division into the sets of 3 pairs of these 6 points gives an isotropic subgroup  $G$ , that is,

$$\{P_{i_1} - P_{i_2}, P_{i_3} - P_{i_4}, P_{i_5} - P_{i_6}, \text{ the identity}\}$$

gives an isotropic subgroup of  $J(C)[2]$ . The action of  $\text{RA}(C)$  on the set  $\{(J(C), G)\}$  is given by the action of  $\text{RA}(C)$  on the set

$$\{((P_{i_1}, P_{i_2}), (P_{i_3}, P_{i_4}), (P_{i_5}, P_{i_6}))\},$$

which contains 15 sets. Here, the pair  $(P_i, P_j)$  is unordered. In this section, we count the number of orbits of this action for each case.

Let  $C$  be a curve of genus 2 with  $\text{RA}(C) \cong \mathbb{Z}/2\mathbb{Z}$ . Such a curve is given by the equation

$$y^2 = (x^2 - 1)(x^2 - a)(x^2 - b)$$

with suitable conditions for  $a$  and  $b$ . The branch points  $Q_i = \psi(P_i)$  are given by

$$Q_1 = 1, \quad Q_2 = -1, \quad Q_3 = \sqrt{a}, \quad Q_4 = -\sqrt{a}, \quad Q_5 = \sqrt{b}, \quad Q_6 = -\sqrt{b}.$$

The generator of the reduced group  $\text{RA}(C)$  of automorphisms is given by

$$\sigma : x \mapsto -x.$$

Since the inversion  $\iota$  acts trivially on the ramification points,  $\text{RA}(C)$  acts on the set of the ramification points  $\{P_1, P_2, P_3, P_4, P_5, P_6\}$ , and the action of  $\sigma$  on the ramification points is given by

$$P_{2i-1} \mapsto P_{2i}, P_{2i} \mapsto P_{2i-1} \quad (i = 1, 2, 3).$$

The isotropic subgroup which corresponds to  $\langle (P_1, P_2), (P_3, P_4), (P_5, P_6) \rangle$  gives a decomposed Richelot isogeny and the other isotropic subgroups give nondecomposed isogenies. Moreover,  $\langle (\sigma(P_{i_1}), \sigma(P_{i_2})), (\sigma(P_{i_3}), \sigma(P_{i_4})), (\sigma(P_{i_5}), \sigma(P_{i_6})) \rangle$  gives the Richelot isogeny isomorphic to the one given by  $\langle (P_{i_1}, P_{i_2}), (P_{i_3}, P_{i_4}), (P_{i_5}, P_{i_6}) \rangle$ . We denote  $P_i$  by  $i$  for the sake of simplicity. Then, the action  $\sigma$  is given by the

permutation  $(1, 2)(3, 4)(5, 6)$ , and by the action of  $\text{RA}(C)$ , the set  $\{(P_{i_1}, P_{i_2}), (P_{i_3}, P_{i_4}), (P_{i_5}, P_{i_6})\}$  of 15 elements is divided into the following 11 loci:

$$\begin{aligned} & \{(1, 2), (3, 4), (5, 6)\}, \{(1, 2), (3, 5), (4, 6)\}, \{(1, 2), (3, 6), (4, 5)\}, \\ & \{(1, 3), (2, 4), (5, 6)\}, \{(1, 3), (2, 5), (4, 6)\}, \{(1, 6), (2, 4), (3, 5)\}, \\ & \{(1, 3), (2, 6), (4, 5)\}, \{(1, 5), (2, 4), (3, 6)\}, \{(1, 4), (2, 3), (5, 6)\}, \\ & \{(1, 4), (2, 5), (3, 6)\}, \{(1, 6), (2, 3), (4, 5)\}, \{(1, 4), (2, 6), (3, 5)\}, \{(1, 5), (2, 3), (4, 6)\}, \\ & \{(1, 5), (2, 6), (3, 4)\}, \{(1, 6), (2, 5), (3, 4)\}. \end{aligned}$$

The reduced automorphism  $\sigma$  is a long one of order 2 and the element  $[(1, 2), (3, 4), (5, 6)]$  is fixed by  $\sigma$ . Therefore, the element  $[(1, 2), (3, 4), (5, 6)]$  gives a decomposed isogeny. The other 10 loci give nondecomposed isogenies. In the same way, we have the following proposition.

**Proposition 6.1.** *Under the notation above, the number of Richelot isogenies up to isomorphism in each case and the number of elements in each orbit are listed as follows. Here, in the list, for example,  $(1 \times 6, 2 \times 4)(1 \times 1)$  means that there exist 6 orbits which contain 1 element and 4 orbits which contain 2 elements for nondecomposed Richelot isogenies, and there exists 1 orbit which contains 1 element for decomposed Richelot isogenies:*

- (0)  $\text{RA}(C) \cong \{0\}$  15 Richelot isogenies, no decomposed ones:  $(1 \times 15)(0)$ .
- (1)  $\text{RA}(C) \cong \mathbb{Z}/2\mathbb{Z}$  11 Richelot isogenies, 1 decomposed one:  $(1 \times 6, 2 \times 4)(1 \times 1)$ .
- (2)  $\text{RA}(C) \cong S_3$  7 Richelot isogenies, 1 decomposed one:  $(1 \times 3, 3 \times 3)(3 \times 1)$ .
- (3)  $\text{RA}(C) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  8 Richelot isogenies, 2 decomposed ones:  $(1 \times 1, 2 \times 4, 4 \times 1)(1 \times 2)$ .
- (4)  $\text{RA}(C) \cong D_{12}$  5 Richelot isogenies, 2 decomposed ones:  $(2 \times 1, 3 \times 1, 6 \times 1)(1 \times 1, 3 \times 1)$ .
- (5)  $\text{RA}(C) \cong S_4$  4 Richelot isogenies, 1 decomposed one:  $(1 \times 1, 4 \times 2)(6 \times 1)$ .
- (6)  $\text{RA}(C) \cong \mathbb{Z}/5\mathbb{Z}$  3 Richelot isogenies, no decomposed ones:  $(5 \times 3)(0)$ .

**Theorem 6.2.** *The total number of Richelot isogenies up to isomorphism outgoing from the irreducible superspecial curves of genus 2 is equal to*

$$\frac{(p-1)(p+2)(p+7)}{192} - \frac{3\{1 - (\frac{-1}{p})\}}{32} + \frac{\{1 - (\frac{-2}{p})\}}{8}.$$

*The total number of decomposed Richelot isogenies up to isomorphism outgoing from the irreducible superspecial curves of genus 2 is equal to*

$$\frac{(p-1)(p+3)}{48} - \frac{\{1 - (\frac{-1}{p})\}}{8} + \frac{\{1 - (\frac{-3}{p})\}}{6}. \quad (6-1)$$

*Proof.* The total number of Richelot isogenies up to isomorphism outgoing from the irreducible superspecial curves of genus 2 is equal to

$$15n_0 + 11n_1 + 7n_2 + 8n_3 + 5n_4 + 4n_5 + 3n_6$$

and the total number of decomposed Richelot isogenies up to isomorphism outgoing from the irreducible superspecial curves of genus 2 is equal to

$$n_1 + n_2 + 2n_3 + 2n_4 + n_5.$$

The results follow from these facts. □

**6B. Richelot isogenies from elliptic curve products.** Let  $E, E'$  be supersingular elliptic curves, and we consider a decomposed principal polarization  $E + E'$  and a Richelot isogeny  $(E \times E', E + E') \rightarrow (J(C), C)$ . For a principally polarized abelian surface  $(E \times E', E + E')$ , we denote by  $\text{Aut}(E \times E')$  the group of automorphisms of  $E \times E'$  which preserve the polarization  $E + E'$ . Let  $\{P_1, P_2, P_3\}$  (resp.  $\{P_4, P_5, P_6\}$ ) be the 2-torsion points of  $E'$  (resp.  $E$ ). Then, the six points  $P_i$  ( $1 \leq i \leq 6$ ) on  $E \times E'$  play the role of ramification points of irreducible curves of genus 2, and  $\text{Aut}(E \times E')$  acts on the set  $\{P_1, P_2, P_3, P_4, P_5, P_6\}$ . The subgroup  $\langle \iota_E \times \text{id}_{E'}, \text{id}_E \times \iota_{E'} \rangle$  acts on the set  $\{P_1, P_2, P_3, P_4, P_5, P_6\}$  trivially. In this section, let  $E_2$  be the elliptic curve defined by  $y^2 = x^3 - x$  and  $E_3$  the elliptic curve defined by  $y^2 = x^3 - 1$ . We know  $\text{Aut } E_2 \cong \mathbb{Z}/4\mathbb{Z}$  and  $\text{Aut } E_3 \cong \mathbb{Z}/6\mathbb{Z}$ . The elliptic curve  $E_2$  is supersingular if and only if  $p \equiv 3 \pmod{4}$  and  $E_3$  is supersingular if and only if  $p \equiv 2 \pmod{3}$ . In this section, the abelian surface  $E \times E'$  means an abelian surface  $E \times E'$  with principal polarization  $E + E'$ .

Now, let  $E, E'$  be supersingular elliptic curves which are neither isomorphic to  $E_2$  nor to  $E_3$ . We also assume  $E$  is not isomorphic to  $E'$ . Using these notations, we have the following list of orders of the groups of automorphisms:

$$\begin{aligned} |\text{Aut}(E \times E')| &= 4, & |\text{Aut}(E \times E)| &= 8, & |\text{Aut}(E \times E_2)| &= 8, & |\text{Aut}(E \times E_3)| &= 12, \\ |\text{Aut}(E_2 \times E_2)| &= 32, & |\text{Aut}(E_3 \times E_3)| &= 72, & |\text{Aut}(E_2 \times E_3)| &= 24. \end{aligned}$$

The isotropic subgroups for the polarization  $2(E + E')$  are determined in [1, Section 3.3]. Using their results and the same method as in Section 6A, we have the following proposition.

**Proposition 6.3.** *Let  $E, E'$  be supersingular elliptic curves which are neither isomorphic to  $E_2$  nor to  $E_3$  with  $E_2$  and  $E_3$  defined as above. We also assume that  $E$  is not isomorphic to  $E'$ . The number of Richelot isogenies up to isomorphism outgoing from a decomposed principally polarized superspecial abelian surface in each case and the number of elements in each orbit are listed as follows. Here, in the list, for example,  $(1 \times 3, 2 \times 1)(1 \times 4, 2 \times 3)$  means that there exist 3 orbits which contain 1 element and 1 orbit which contains 2 elements for nondecomposed Richelot isogenies, and there exist 4 orbits which contain 1 element and 3 orbits which contain 2 elements for decomposed Richelot isogenies:*

- (i)  $\underline{E \times E'}$  15 Richelot isogenies, 6 nondecomposed ones:  $(1 \times 6)(1 \times 9)$ .
- (ii)  $\underline{E \times E}$  11 Richelot isogenies, 4 nondecomposed ones:  $(1 \times 3, 2 \times 1)(1 \times 4, 2 \times 3)$ .
- (iii)  $\underline{E \times E_2}$  9 Richelot isogenies, 3 nondecomposed ones ( $p \equiv 3 \pmod{4}$ ):  $(2 \times 3)(1 \times 3, 2 \times 3)$ .
- (iv)  $\underline{E \times E_3}$  5 Richelot isogenies, 2 nondecomposed ones ( $p \equiv 2 \pmod{3}$ ):  $(3 \times 2)(3 \times 3)$ .
- (v)  $\underline{E_2 \times E_2}$  5 Richelot isogenies, 1 nondecomposed one ( $p \equiv 3 \pmod{4}$ ):  $(4 \times 1)(1 \times 1, 2 \times 1, 4 \times 2)$ .

(vi)  $E_3 \times E_3$  3 Richelot isogenies, 1 nondecomposed one ( $p \equiv 2 \pmod{3}$ ):  $(3 \times 1)(3 \times 1, 9 \times 1)$ .

(vii)  $E_2 \times E_3$  3 Richelot isogenies, 1 nondecomposed one ( $p \equiv 11 \pmod{12}$ ):  $(6 \times 1)(3 \times 1, 6 \times 1)$ .

*Proof.* We give a proof for the case (iv). For the other cases, the arguments are quite similar. Since the elliptic curve  $E_3$  is defined by  $y^2 = x^3 - 1$ , the 2-torsion points  $(x, y)$  of  $E_3$  are given by  $P_1 = (1, 0)$ ,  $P_2 = (\omega, 0)$  and  $P_3 = (\omega^2, 0)$ . Here,  $\omega$  is a primitive cube root of unity. We denote by  $P_4, P_5$  and  $P_6$  the 2-torsion points of  $E$ . We have an automorphism  $\sigma$  of order 3 of  $E_3$  defined by  $\sigma : x \mapsto \omega x, y \mapsto y$ . As in the case of [Section 6A](#), we describe the isotropic subgroups  $G$ . We know that a division into the sets of 3 pairs of these 6 points  $P_i$  ( $1 \leq i \leq 6$ ) on  $E \times E_3$  gives an isotropic subgroup  $G$ , that is,  $\{P_{i_1} - P_{i_2}, P_{i_3} - P_{i_4}, P_{i_5} - P_{i_6}, \text{ the identity}\}$  gives an isotropic subgroup of  $(E \times E_3)[2]$ . Here, we consider  $P_i$  ( $1 \leq i \leq 3$ ) as the point  $(0, P_i)$  on  $E \times E_3$ , and  $P_i$  ( $4 \leq i \leq 6$ ) as the point  $(P_i, 0)$  on  $E \times E_3$ . This set contains 15 elements. In the case (iv), we have  $E \not\cong E_3$ . Therefore, by [\[1, Section 3.3\]](#), among the 15 isotropic subgroups the 9 cases such that  $P_{i_1}, P_{i_2}, P_{i_3} \in E$  and  $P_{i_4}, P_{i_5}, P_{i_6} \in E_3$  give the decomposed Richelot isogenies and the rest gives the nondecomposed Richelot isogenies. For the abbreviation, we denote by  $P_i$  by  $i$ . Then, on the set  $\{1, 2, 3, 4, 5, 6\}$ ,  $\text{id}_E \times \sigma$  acts as the cyclic permutation  $(1, 2, 3)$ . The isotropic subgroup  $G$  is determined by the set of 3 pairs of 2-torsion points:

$$\{(i_1, i_2), (i_3, i_4), (i_5, i_6)\},$$

and the group  $\text{Aut}(E \times E_3)$  induces the action on the set of the 15 isotropic subgroups. Since the action of the subgroup  $\langle \iota_E \times \text{id}_{E_3}, \text{id}_E \times \iota_{E_3} \rangle$  is trivial on the set of the 15 isotropic subgroups, we see that the action is given by the group  $\text{Aut}(E \times E_3) / \langle \iota_E \times \text{id}_{E_3}, \text{id}_E \times \iota_{E_3} \rangle \cong \langle \text{id}_E \times \sigma \rangle$ . By this action, the set of the 15 isotropic subgroups is divided into the following 5 orbits:

$$\begin{aligned} & \{[(1, 2), (3, 4), (5, 6)], [(2, 3), (1, 4), (5, 6)], [(1, 3), (2, 4), (5, 6)]\}, \\ & \{[(1, 2), (3, 5), (4, 6)], [(2, 3), (1, 5), (4, 6)], [(1, 3), (2, 5), (4, 6)]\}, \\ & \{[(1, 2), (3, 6), (4, 5)], [(2, 3), (1, 6), (4, 5)], [(1, 3), (2, 6), (4, 5)]\}, \\ & \{[(1, 4), (2, 5), (3, 6)], [(1, 6), (2, 4), (3, 5)], [(1, 5), (2, 6), (3, 5)]\}, \\ & \{[(1, 4), (2, 6), (3, 5)], [(1, 5), (2, 4), (3, 6)], [(1, 6), (2, 5), (3, 4)]\}. \end{aligned}$$

By the criterion above, the first 3 sets correspond with the decomposed Richelot isogenies, and the last 2 sets correspond with the nondecomposed Richelot isogenies.  $\square$

We denote by  $h$  the number of supersingular elliptic curves defined over  $k$ . Then, we know

$$h = \frac{p-1}{12} + \frac{\left\{1 - \left(\frac{-3}{p}\right)\right\}}{3} + \frac{\left\{1 - \left(\frac{-1}{p}\right)\right\}}{4}$$

(see Igusa [\[8\]](#), for instance). We denote by  $h_1$  the number of supersingular elliptic curves  $E$  with  $\text{Aut}(E) \cong \mathbb{Z}/2\mathbb{Z}$ ,  $h_2$  the number of supersingular elliptic curves  $E_2$  with  $\text{Aut}(E_2) \cong \mathbb{Z}/4\mathbb{Z}$ ,  $h_3$  the number of supersingular elliptic curves  $E_3$  with  $\text{Aut}(E_3) \cong \mathbb{Z}/6\mathbb{Z}$ . We have  $h = h_1 + h_2 + h_3$  and  $h_2 = \left\{1 - \left(\frac{-1}{p}\right)\right\}/2$  and  $h_3 = \left\{1 - \left(\frac{-3}{p}\right)\right\}/2$ .

**Theorem 6.4.** *The total number of nondecomposed Richelot isogenies up to isomorphism outgoing from decomposed principally polarized superspecial abelian surfaces is equal to*

$$\frac{(p-1)(p+3)}{48} - \frac{\left\{1 - \left(\frac{-1}{p}\right)\right\}}{8} + \frac{\left\{1 - \left(\frac{-3}{p}\right)\right\}}{6}. \quad (6-2)$$

*The total number of decomposed Richelot isogenies up to isomorphism outgoing from decomposed principally polarized superspecial abelian surfaces is equal to*

$$\frac{(p-1)(3p+17)}{96} + \frac{(p+6)\left\{1 - \left(\frac{-1}{p}\right)\right\}}{16} + \frac{\left\{1 - \left(\frac{-3}{p}\right)\right\}}{3}.$$

*Proof.* The total number of nondecomposed Richelot isogenies up to isomorphism outgoing from decomposed principally polarized superspecial abelian surfaces is equal to

$$6 \left\{ \frac{h_1(h_1-1)}{2} \right\} + 4h_1 + 3h_2h_1 + 2h_3h_1 + h_2 + h_3 + h_2h_3.$$

The total number of decomposed Richelot isogenies up to isomorphism outgoing from decomposed principally polarized superspecial abelian surfaces is equal to

$$9 \left\{ \frac{h_1(h_1-1)}{2} \right\} + 7h_1 + 6h_2h_1 + 3h_3h_1 + 4h_2 + 2h_3 + 2h_2h_3.$$

Since  $\left\{1 - \left(\frac{-1}{p}\right)\right\}^2 = 2\left\{1 - \left(\frac{-1}{p}\right)\right\}$  and  $\left\{1 - \left(\frac{-3}{p}\right)\right\}^2 = 2\left\{1 - \left(\frac{-3}{p}\right)\right\}$ , the result follows from these facts.  $\square$

**Remark 6.5.** Since the total number of *decomposed* Richelot isogenies up to isomorphism outgoing from the *irreducible* superspecial curves of genus 2 is equal to the total number of *nondecomposed* Richelot isogenies up to isomorphism outgoing from *decomposed* principally polarized superspecial abelian surfaces, (6-1) and (6-2) give the same number.

## 7. Examples

By [7, Section 1.3], we have the following normal forms of curves  $C$  of genus 2 with given reduced group  $\text{RA}(C)$  of automorphisms:

- (1) For  $S_3 \subset \text{RA}(C)$ , the normal form is  $y^2 = (x^3 - 1)(x^3 - \alpha)$ . This curve is superspecial if and only if  $\alpha$  is a zero of the polynomial

$$g(z) = \sum_{l=0}^{[p/3]} \binom{(p-1)/2}{((p+1)/6)+l} \binom{(p-1)/2}{l} z^l.$$

- (2) For  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \subset \text{RA}(C)$ , the normal form is  $y^2 = x(x^2 - 1)(x^2 - \beta)$ . This curve is superspecial if and only if  $\beta$  is a zero of the polynomial

$$h(z) = \sum_{l=0}^{[p/4]} \binom{(p-1)/2}{((p+1)/4)+l} \binom{(p-1)/2}{l} z^l.$$

- (3) For  $\text{RA}(C) \cong D_{12}$ , the normal form is  $y^2 = x^6 - 1$ . This curve is superspecial if and only if  $p \equiv 5 \pmod{6}$  (see [7, Proposition 1.11]).
- (4) For  $\text{RA}(C) \cong S_4$ , the normal form is  $y^2 = x(x^4 - 1)$ . This is superspecial if and only if  $p \equiv 5$  or  $7 \pmod{8}$  (see [7, Proposition 1.12]).

Finally, the elliptic curve  $E$  defined by  $y^2 = x(x-1)(x-\lambda)$  is supersingular if and only if  $\lambda$  is a zero of the Legendre polynomial

$$\Phi(z) = \sum_{l=0}^{(p-1)/2} \binom{(p-1)/2}{l}^2 z^l.$$

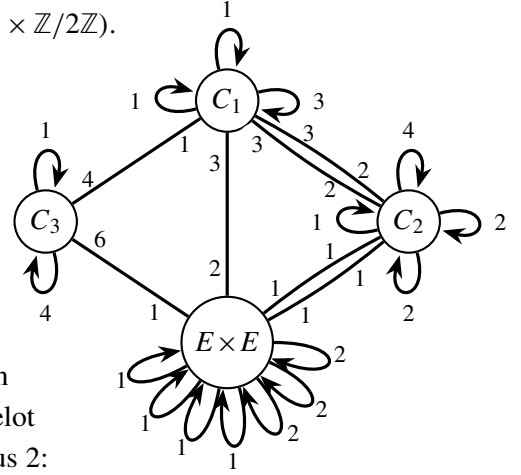
Using these results, we construct some examples.

**7A. Examples in characteristic 13.** Assume the characteristic is  $p = 13$ . Over  $k$  we have only one supersingular elliptic curve  $E$ , and three superspecial curves  $C_1, C_2$  and  $C_3$  of genus 2 with  $\text{RA}(C_1) \cong S_3$ ,  $\text{RA}(C_2) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  and  $\text{RA}(C_3) = S_4$ , respectively (see [7, Remark 3.4]). In characteristic 13, we know  $h(z) = 7z^3 + 12z^2 + 12z + 7$ , and the zeros are  $-1$  and  $-5 \pm \sqrt{6}$ . We also know  $g(z) = 2z^4 + 3z^3 + 4z^2 + 3z + 2$ , and one of the zeros is  $-4 + \sqrt{2}$ . The Legendre polynomial is given by  $\Phi(z) = z^6 + 10z^5 + 4z^4 + 10z^3 + 4z^2 + 10z + 1$ , and one of the zeros is  $3 - 2\sqrt{2}$ . Using these facts, we know that the curves above are given by the following equations:

- (1)  $E: y^2 = x(x-1)(x-3+2\sqrt{2})$  ( $\text{RA}(E) = \text{Aut}(E)/\langle \iota_E \rangle \cong \{0\}$ ).
- (2)  $C_1: y^2 = (x^3-1)(x^3+4-\sqrt{2})$  ( $\text{RA}(C_1) \cong S_3$ ).
- (3)  $C_2: y^2 = x(x^2-1)(x^2+5+2\sqrt{6})$  ( $\text{RA}(C_2) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ).
- (4)  $C_3: y^2 = x(x^4-1)$  ( $\text{RA}(C_3) \cong S_4$ ).

Therefore, outgoing from superspecial curves of genus 2, we have, in total,  $1 + 2 + 1 = 4$  decomposed Richelot isogenies up to isomorphism by Proposition 6.1. On the other hand, outgoing from the unique decomposed principally polarized abelian surface  $(E \times E, E + E)$ , we have 5 nondecomposed Richelot isogenies (not up to isomorphism) (see [8] and [1, Figure 1]). Using the method in [1, Section 3.3], as the images of 5 nondecomposed Richelot isogenies, we have the following superspecial curves of genus 2:

- (a)  $C_a: y^2 = (x^2-1)(x^2-4+7\sqrt{2})(x^2-6+6\sqrt{2})$  ( $\text{RA}(C_a) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ).
- (b)  $C_b: y^2 = (x^2-1)(x^2+3-2\sqrt{2})(x^2-4-\sqrt{2})$  ( $\text{RA}(C_b) \cong S_4$ ).
- (c)  $C_c: y^2 = (x^2-1)(x^2+3-4\sqrt{2})(x^2+1+3\sqrt{2})$  ( $\text{RA}(C_c) \cong S_3$ ).
- (d)  $C_d: y^2 = (x^2-1)(x^2-3)(x^2+3-4\sqrt{2})$  ( $\text{RA}(C_d) \cong S_3$ ).
- (e)  $C_e: y^2 = (x^2-1)(x^2-6-6\sqrt{2})(x^2-2+2\sqrt{2})$  ( $\text{RA}(C_e) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ).



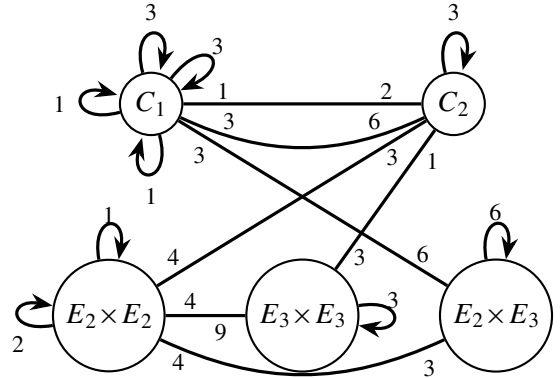
We see that  $C_a \cong C_e \cong C_2$ ,  $C_c \cong C_d \cong C_1$  and  $C_b \cong C_3$ . As Richelot isogenies,  $(E \times E, E + E) \rightarrow (J(C_e), C_e)$  is isomorphic to  $(E \times E, E + E) \rightarrow (J(C_d), C_d)$ , but  $(E \times E, E + E) \rightarrow (J(C_a), C_a)$  is not isomorphic to  $(E \times E, E + E) \rightarrow (J(C_e), C_e)$ . Compare our graph with Figure 1 of [1]. In the graph the numbers along the edges are the multiplicities of Richelot isogenies outgoing from the nodes.

**7B. Examples in characteristic 11.** Assume the characteristic is  $p = 11$ . Over  $k$  we have two supersingular elliptic curves  $E_2, E_3$  and two superspecial curves  $C_1, C_2$  of genus 2 with  $\text{RA}(C_1) \cong S_3$ ,  $\text{RA}(C_2) \cong D_{12}$ , respectively (see [7, Remark 3.4]). In characteristic 11, we know

$$g(z) = 10(z^3 + 5z^2 + 5z + 1),$$

and the roots are  $-1, 3$  and  $4$ . Using this fact, we know that the curves above are given by the following equations:

- (1)  $E_2: y^2 = x^3 - x$  ( $\text{RA}(E_2) \cong \mathbb{Z}/2\mathbb{Z}$ ).
- (2)  $E_3: y^2 = x^3 - 1$  ( $\text{RA}(E_3) \cong \mathbb{Z}/3\mathbb{Z}$ ).
- (3)  $C_1: y^2 = (x^3 - 1)(x^3 - 3)$  ( $\text{RA}(C_1) \cong S_3$ ).
- (4)  $C_2: y^2 = x^6 - 1$  ( $\text{RA}(C_2) \cong D_{12}$ ).

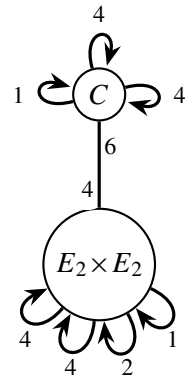


We have three decomposed principally polarized abelian surfaces:  $E_2 \times E_2$ ,  $E_3 \times E_3$ ,  $E_2 \times E_3$ . Therefore, from the superspecial curves of genus 2 we have, in total,  $1 + 2 = 3$  decomposed Richelot isogenies up to isomorphism by Proposition 6.1. On the other hand, from the decomposed principally polarized abelian surfaces, we have  $1 + 1 + 1 = 3$  nondecomposed Richelot isogenies up to isomorphism by Proposition 6.3. For the decomposed principally polarized abelian surface  $E_2 \times E_2$  the image of the only one nondecomposed Richelot isogeny is given by  $C_2$ . For the decomposed principally polarized abelian surface  $E_3 \times E_3$  the image of the only one nondecomposed Richelot isogeny is also given by  $C_2$ . For the decomposed principally polarized abelian surface  $E_2 \times E_3$  the image of the only one nondecomposed Richelot isogeny is given by  $C_1$ . See also Jordan and Zaytman [11, Section 5.1].

**7C. Examples in characteristic 7.** Assume the characteristic is  $p = 7$ . Over  $k$  we have only one supersingular elliptic curve  $E_2$  and only one superspecial curves  $C$  of genus 2, which has  $\text{RA}(C) \cong S_4$  (see [7, Remark 3.4]). They are given by the following equations:

- (1)  $E_2: y^2 = x^3 - x$  ( $\text{RA}(E_2) \cong \mathbb{Z}/2\mathbb{Z}$ ).
- (2)  $C: y^2 = x(x^4 - 1)$  ( $\text{RA}(C) \cong S_4$ ).

We have only one decomposed principally polarized abelian surface  $E_2 \times E_2$ . Therefore, outgoing from the superspecial curves of genus 2 we have only one decomposed Richelot isogeny up to isomorphism. From the decomposed principally polarized abelian surface, we also have only one nondecomposed Richelot isogeny up to isomorphism





(see [1, Sections 3.2 and 3.3]). For the decomposed principally polarized abelian surface  $E_2 \times E_2$  the image of the only one nondecomposed Richelot isogeny is given by  $C$ .

## 8. Concluding remark

Our results answered a question about the number of decomposed Richelot isogenies and improved our understanding of the isogeny graph for genus-2 isogeny cryptography. Further applications (or implications) of our results to cryptography are left as an open problem.

For example, a very recent cryptanalytic algorithm by Costello and Smith [4] is considered as an interesting target. They reduced the isogeny path-finding algorithm in the superspecial Richelot isogeny graph to the elliptic curve path-finding problem, thus improving the complexity. A key ingredient of the reduction is a subalgorithm for finding a path connecting a given irreducible genus-2 curve and the (connected) subgraph consisting of elliptic curve products.

Proposition 4.3 showed the equivalence of existence of a decomposed Richelot isogeny outgoing from  $J(C)$  and that of a (long) element of order 2 in the reduced group of automorphisms of  $C$ . It implies that the subgraph of elliptic curve products are adjacent to genus-2 curves having involutive reduced automorphisms in the superspecial graph. We hope that this new characterization can be applied to analyzing and/or improving the Costello–Smith attack.

## Acknowledgements

The authors would like to thank anonymous reviewers of ANTS-XIV for their careful reading and useful suggestions for revising our paper, and E. Florit and B. Smith for their useful comments, in particular, for the correction of the figure in the case of  $p = 11$  in Section 7B. Research of Katsura is partially supported by JSPS Grant-in-Aid for Scientific Research (C) No. 20K03530. Research of Takashima is partially supported by JST CREST Grant Number JPMJCR14D6, Japan.

## References

- [1] Wouter Castryck, Thomas Decru, and Benjamin Smith, *Hash functions from superspecial genus-2 curves using Richelot isogenies*, NutMiC 2019: Number-Theoretic Methods in Cryptology, 2019, To appear in J. of Math. Crypt.
- [2] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes, *CSIDH: an efficient post-quantum commutative group action*, ASIACRYPT 2018, Part III, 2018, pp. 395–427.
- [3] Denis X. Charles, Kristin E. Lauter, and Eyal Z. Goren, *Cryptographic hash functions from expander graphs*, J. Crypt. **22** (2009), no. 1, 93–113.
- [4] Craig Costello and Benjamin Smith, *The supersingular isogeny problem in genus 2 and beyond*, PQCrypto 2020, 2020, pp. 151–168.
- [5] Luca De Feo, David Jao, and Jérôme Plût, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, J. Math. Crypt. **8** (2014), no. 3, 209–247.
- [6] E. Victor Flynn and Yan Bo Ti, *Genus two isogeny cryptography*, PQCrypto 2019, 2019, pp. 286–306.
- [7] Tomoyoshi Ibukiyama, Toshiyuki Katsura, and Frans Oort, *Supersingular curves of genus two and class numbers*, Compositio Math. **57** (1986), 127–152.

- [8] Jun-Ichi Igusa, *Class number of a definite quaternion with prime discriminant*, Proc. Nat. Acad. Sci. U.S.A. **44** (1958), 312–314.
- [9] Jun-Ichi Igusa, *Arithmetic variety of moduli for genus two*, Ann of Math. **72** (1960), 612–649.
- [10] David Jao, Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Amir Jalali, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Geovandro Pereira, Joost Renes, Vladimir Soukharev, and David Urbanik, *SIKE: supersingular isogeny key encapsulation*, submission to the NIST’s PQC standardization, round 2, updated version (2020).
- [11] Bruce W. Jordan and Yevgeny Zaytman, *Isogeny graphs of superspecial abelian varieties and generalized Brandt matrices*, preprint, 2020. [arXiv 2005.09031](https://arxiv.org/abs/2005.09031)
- [12] Toshiyuki Katsura and Frans Oort, *Families of supersingular abelian surfaces*, Compositio Math. **62** (1987), 107–167.
- [13] Toshiyuki Katsura and Frans Oort, *Supersingular abelian varieties of dimension two or three and class numbers*, Advanced Studies in Pure Math. **10** (1987), 253–281.
- [14] David Mumford, *Abelian varieties*, Oxford Univ. Press, 1970.
- [15] Tetsuji Shioda, *Supersingular K3 surfaces*, Algebraic Geometry, Proc. Copenhagen 1978 (K. Lønsted, ed.), Lecture Notes in Math. **732**, Springer-Verlag, 1979, pp. 563–591.
- [16] Benjamin Smith, *Explicit endomorphisms and correspondences*, Ph.D. thesis, The University of Sydney, 2005.
- [17] Katsuyuki Takashima, *Efficient algorithms for isogeny sequences and their cryptographic applications*, Mathematical modelling for next-generation cryptography: CREST crypto-math project, Springer-Verlag, 2017, pp. 97–114.

Received 20 Feb 2020. Revised 27 Jul 2020.

TOSHIYUKI KATSURA: [tkatsura@ms.u-tokyo.ac.jp](mailto:tkatsura@ms.u-tokyo.ac.jp)

Graduate School of Mathematical Sciences, The University of Tokyo, Japan

KATSUYUKI TAKASHIMA: [takashima.katsuyuki@aj.mitsubishielectric.co.jp](mailto:takashima.katsuyuki@aj.mitsubishielectric.co.jp)

Information Technology R&D Center, Mitsubishi Electric, Ofuna, Japan

# Algorithms to enumerate superspecial Howe curves of genus 4

Momonari Kudo, Shushi Harashita, and Everett W. Howe

A *Howe curve* is a curve of genus 4 obtained as the fiber product of two genus-1 double covers of  $\mathbf{P}^1$ . We present a simple algorithm for testing isomorphism of Howe curves, and we propose two main algorithms for finding and enumerating superspecial Howe curves: One involves solving multivariate systems coming from Cartier–Manin matrices, while the other uses Richelot isogenies of curves of genus 2. Comparing the two algorithms by implementation and by complexity analyses, we conclude that the latter enumerates superspecial Howe curves more efficiently. Using these algorithms, we show that there exist superspecial curves of genus 4 in characteristic  $p$  for every prime  $p$  with  $7 < p < 20000$ .

## 1. Introduction

**1A. Background and motivation.** Let  $K$  be an algebraically closed field of characteristic  $p > 0$ . A nonsingular curve over  $K$  is called *superspecial* (resp. *supersingular*) if its Jacobian variety is isomorphic (resp. isogenous) to a product of supersingular elliptic curves. Superspecial curves are not only theoretically interesting in algebraic geometry and number theory but also have many applications in coding theory, cryptography, and so on, because they tend to have many rational points and their Jacobian varieties have large endomorphism rings. However, it is not always easy to find such curves, and there are only finitely many superspecial curves for a given genus and characteristic. One method of constructing superspecial curves is to consider fiber products of superspecial curves of lower genera. In this paper, we demonstrate that this method can be efficient by considering the simplest example in which the genus is at least 4: the case of Howe curves. A *Howe curve* (so named by Kudo, Harashita and Senda in [23]) is a curve of genus 4 obtained as the fiber product of two genus-1 double covers  $E_1 \rightarrow \mathbf{P}^1$  and  $E_2 \rightarrow \mathbf{P}^1$ . In [11], Howe studied these curves in order to quickly construct genus-4 curves with many rational points.

**1B. Related works.** The reason that we consider the case of genus  $g \geq 4$  is that the enumeration of the isomorphism classes of superspecial curves with  $g \leq 3$  has already been done, by Deuring [4] for  $g = 1$ , by Ibukiyama, Katsura, and Oort [14] for  $g = 2$ , and by Brock [3] for  $g = 3$ ; see also Ibukiyama [13] and Oort [25] for the existence of such curves for  $g = 3$ . In contrast to the case  $g \leq 3$ , the existence or

MSC2020: primary 11G20; secondary 14G15, 14H45.

Keywords: algebraic curves, superspeciality.

nonexistence of a superspecial curve of genus 4 in general characteristic is an open problem, although some results for specific small  $p$  are known; see [5, Theorem 1.1] for the nonexistence for  $p \leq 3$  and [22, Theorem B] for the nonexistence for  $p = 7$ . As for enumeration, computational approaches have been proposed recently in [21], [22], and [20] in the case of genus 4. The main strategy common to these papers is to parametrize a family of curves (canonical curves in the first two papers, hyperelliptic curves in the third), and then to find the superspecial curves  $X$  in these families by computing the zeros of a multivariate system derived from the condition that the Cartier–Manin matrix of  $X$  is zero. With computer algebra techniques such as Gröbner bases, the authors of these papers enumerated superspecial canonical curves for  $p \leq 11$  in [21] and [22] and superspecial hyperelliptic curves for  $p \leq 23$  in [20]. However, results for larger  $p$  have not been obtained yet due to the cost of solving multivariate systems, and no complexity analysis is given in [21], [22], or [20].

Now we turn our attention to Howe curves. Recently, it was proven in [23] that there exists a supersingular Howe curve in every positive characteristic. In particular, the authors of [23] reduce the existence of such a curve to the existence of a zero of a certain multivariate system, as follows: They study a family of Howe curves realized as  $E_1 : z^2 = f_1(x)$  and  $E_2 : w^2 = f_2(x)$  for cubic polynomials  $f_1$  and  $f_2$  parametrized by elements  $(\lambda : \mu : \nu)$  of  $\mathbf{P}^2$ . Let  $C$  be the genus-2 curve  $y^2 = f_1 f_2$ . The supersingularity of  $H$  is equivalent to that of  $E_1$ ,  $E_2$  and  $C$ , because there exists an isogeny of 2-power degree from the Jacobian  $J(H)$  to  $E_1 \times E_2 \times J(C)$  [11, Theorem 2.1]. Thus, once supersingular isomorphism classes of  $E_1$  and  $E_2$  are given, finding supersingular curves  $H$  is reduced to finding values of the parameter  $(\lambda : \mu : \nu)$  that satisfy a multivariate system derived from the supersingularity of  $C$ . The authors of [23] deduced the existence of such a zero  $(\lambda : \mu : \nu)$  from various algebraic properties of the defining polynomials of the system.

The above reduction is applicable also for the superspecial case, but the method used in [23] to prove the existence of solutions does not carry over well. For this reason, the superspecial case is still open, and we are left to ask: For which primes  $p > 7$  are there superspecial Howe curves in characteristic  $p$ ?

**1C. Our contribution.** We study the existence of superspecial Howe curves by creating efficient algorithms to produce and enumerate them. The following theorems summarize some of what we have found.

**Theorem 1.1.** *For every prime  $p$  with  $7 < p < 20000$  or with  $p \equiv 5 \pmod{6}$ , there exists a superspecial Howe curve in characteristic  $p$ .*

**Theorem 1.2.** *For every prime  $p$  with  $7 < p \leq 199$ , the number of isomorphism classes of superspecial Howe curves in characteristic  $p$  is given in Table 1.*

The upper bounds on  $p$  in these two theorems can easily be increased. For example, on a 2.8 GHz quad-core Intel Core i7 with 16GB RAM, computing the 8351 superspecial Howe curves in characteristic 199 using method (B) below took 124 seconds in Magma. Finding examples of superspecial Howe curves for every  $p$  between 7 and 20000 took 680 minutes on the same machine.

$p$	$n(p)$	ratio	$p$	$n(p)$	ratio	$p$	$n(p)$	ratio
11	4	3.462	67	260	0.996	137	2430	1.089
13	3	1.573	71	742	2.388	139	2447	1.050
17	10	2.345	73	316	0.936	149	3082	1.073
19	4	0.672	79	595	1.390	151	3553	1.189
23	33	3.125	83	655	1.320	157	3427	1.020
29	45	2.126	89	863	1.410	163	3518	0.936
31	59	2.281	97	802	1.012	167	6268	1.550
37	41	0.932	101	1207	1.350	173	4780	1.064
41	105	1.755	103	1151	1.213	179	5771	1.159
43	79	1.145	107	1237	1.163	181	5419	1.053
47	235	2.608	109	1193	1.061	191	9610	1.589
53	167	1.292	113	1323	1.056	193	6298	1.009
59	259	1.453	127	2013	1.132	197	6839	1.030
61	243	1.233	131	2606	1.335	199	8351	1.221

**Table 1.** For each prime  $p$  from 11 to 199, we give the number  $n(p)$  of superspecial Howe curves over  $\overline{\mathbb{F}}_p$  and the ratio of  $n(p)$  to the heuristic prediction  $p^3/1152$  (see [Section 5](#)).

In this paper we discuss two strategies, (A) and (B) below, to find superspecial Howe curves. We also show how isomorphisms between Howe curves can be easily detected from the data that defines them, in (C).

**(A)  $(E_1, E_2)$ -first, using Cartier–Manin matrices.** In this strategy, we use the same realization of Howe curves as in [\[23\]](#), that is, the fiber product of

$$E_1 : z^2 y = x^3 + A_1 \mu^2 x y^2 + B_1 \mu^3 y^3 \quad \text{and} \quad E_2 : w^2 y = (x - \lambda)^3 + A_2 \mu^2 (x - \lambda) y^2 + B_2 \mu^3 y^3$$

over  $\mathbf{P}^1 = \text{Proj } K[x, y]$ . We enumerate pairs  $(E_1, E_2)$  of supersingular elliptic curves so that  $C$  is superspecial. We first discuss the field of definition of superspecial Howe curves (see [Proposition 4.1](#)), which enables us to reduce the size of our search space drastically. Specifically, the coordinates  $A_1, B_1, A_2, B_2, \lambda, \mu, \nu$  belong to  $\mathbb{F}_{p^2}$ , whereas in the supersingular case [\[23\]](#) these coordinates can generate larger subfields of  $\overline{\mathbb{F}}_p$ . For the test of superspeciality, we use the criterion that the Cartier–Manin matrix of  $C$  must be zero [\[14, Lemma 1.1\(i\)\]](#). This reduces the enumeration problem to solving a system of algebraic equations. See [Section 4](#) for the details of this strategy, including a complexity analysis.

**(B)  $C$ -first, using Richelot isogenies.** The second strategy first enumerates superspecial curves  $C : y^2 = f(x)$  of genus 2 with  $f(x)$  of degree 6 and then enumerates decompositions  $f(x) = f_1(x)f_2(x)$  with  $f_i(x)$  of degree 3 so that there is a  $b$  that makes both curves  $E_i : y^2 = (x - b)f_i(x)$  supersingular. The moduli space of curves of genus 2 is of dimension 3. As this dimension is bigger than the space of  $(\lambda : \mu : \nu) \in \mathbf{P}^2$  considered in (A), this strategy, a priori, looks inefficient. But, surprisingly, we conclude that strategy (B) enumerates superspecial Howe curves much more efficiently than does (A). The advantage of (B) comes from making use of Richelot isogenies. Specifically, we construct some superspecial curves of genus 2 by gluing supersingular elliptic curves together along their 2-torsion [\[12, §3\]](#), and then

produce more such curves by applying Richelot isogenies to the curves already produced. This procedure terminates because there are only finitely many superspecial curves of genus 2, and a recent result of Jordan and Zaytman [16, Corollary 18] shows that we obtain all isomorphism classes of superspecial curves of genus 2 in this way.<sup>1</sup>

**(C) A new isomorphism test for Howe curves.** Strategy (A) above produces many not-necessarily-distinct Howe curves, so to prevent overcounting we are left with the task of producing a unique representative for each isomorphism class. As every Howe curve is canonical (see Lemma 2.1), one may check whether two Howe curves are isomorphic by using the isomorphism test for canonical curves given in [22, §6.1], whose implementation is found in [21, §4.3]. This turns out to be very costly, because it uses many Gröbner basis computations. Our Corollary 3.3 gives a much simpler isomorphism test, based on the observation that a Howe curve is completely determined (up to isomorphism) by the degree-2 map to a genus-2 curve it is provided with by virtue of its definition as a fiber product. This isomorphism test is added on as a separate step in strategy (A), but is baked into the algorithm we use for strategy (B).

## 2. Howe curves and their superspeciality

In this section, we recall the definition of Howe curves, show that they are canonical, and give a computational criterion for their superspeciality.

Let  $K$  be an algebraically closed field of characteristic  $p \neq 2$ . A *Howe curve* over  $K$  is a curve which is isomorphic to the desingularization of the fiber product  $E_1 \times_{\mathbf{P}^1} E_2$  of two genus-1 double covers  $E_i \rightarrow \mathbf{P}^1$  ramified over  $S_i$ , where each  $S_i$  consists of four points and where  $|S_1 \cap S_2| = 1$ .

Given a Howe curve, there is an automorphism of  $\mathbf{P}^1$  that takes the common ramification point of the two genus-1 double covers to infinity. Then the curves  $E_i$  can be written  $w^2 = f_1$  and  $z^2 = f_2$  for separable monic cubic polynomials  $f_i \in K[x]$  that are coprime to one another, where  $x$  generates the function field of  $\mathbf{P}^1$ .

**Lemma 2.1.** *Every Howe curve is a canonical curve of genus 4.*

*Proof.* Let  $H$  be a Howe curve, normalized as above so that it is given as the fiber product of  $w^2 = f_1$  and  $z^2 = f_2$  for coprime separable monic cubic polynomials  $f_1$  and  $f_2$ . For each  $i$ , let  $f_i^{(h)} = y^3 f_i(x/y) \in K[x, y]$  be the homogenous cubic obtained from  $f_i$  and let  $H'$  be the curve defined in  $\mathbf{P}^3 = \text{Proj } K[x, y, z, w]$  by

$$z^2 - w^2 = q(x, y), \quad z^2 y = f_1^{(h)}(x, y),$$

where  $q(x, y)$  is the quadratic form

$$q(x, y) = (f_1^{(h)}(x, y) - f_2^{(h)}(x, y))/y.$$

Note that  $H'$  and  $E_1 \times_{\mathbf{P}^1} E_2$  are isomorphic if the locus  $y = 0$  is excluded. It is straightforward to see that  $H'$  is nonsingular, since  $f_1$  and  $f_2$  are separable and are coprime. Hence  $H$  and  $H'$  are isomorphic to one another (see [26, Proposition II.2.1]).

<sup>1</sup> As this paper was in press, Jordan and Zaytman updated their preprint to indicate that an equivalent result was proven earlier by Ekedahl and Oort.

It is well known that any nonsingular curve defined by a quadratic form and a cubic form in  $\mathbf{P}^3$  is a canonical curve of genus 4 [7, Example IV.5.2.2].  $\square$

To study the superspeciality of Howe curves, we first look at the decomposition of their Jacobians. Let  $f_1$  and  $f_2$  be coprime separable monic cubic polynomials, as above. Let  $f = f_1 f_2$  and consider the hyperelliptic curve  $C$  of genus 2 defined by  $u^2 = f$ . By [11, Theorem 2.1], there exist two isogenies

$$\varphi : J(H) \rightarrow E_1 \times E_2 \times J(C),$$

$$\psi : E_1 \times E_2 \times J(C) \rightarrow J(H),$$

such that  $\varphi \circ \psi$  and  $\psi \circ \varphi$  are both multiplication by 2.

Suppose now that the characteristic  $p$  of  $K$  is an odd prime. Then  $\psi \circ \varphi$  is an automorphism of the  $p$ -kernel of  $J(H)$  and  $\varphi \circ \psi$  is an automorphism of the  $p$ -kernel of  $E_1 \times E_2 \times J(C)$ , so  $J(H)[p]$  and  $E_1[p] \times E_2[p] \times J(C)[p]$  are isomorphic. Hence  $H$  is superspecial if and only if  $E_1$  and  $E_2$  are supersingular and  $C$  is superspecial.

Now we recall a criterion for the superspeciality of  $C$ . Let  $\gamma_i$  be the coefficient of  $x^i$  in  $f^{(p-1)/2}$ , and set

$$a = \gamma_{p-1}, \quad b = \gamma_{2p-1}, \quad c = \gamma_{p-2} \quad \text{and} \quad d = \gamma_{2p-2}.$$

Let  $M$  be the matrix

$$M = \begin{pmatrix} a^p & c^p \\ b^p & d^p \end{pmatrix}. \quad (2-1)$$

Then  $M$  is a Cartier–Manin matrix for  $C$ , that is, there is a basis for  $H^0(C, \Omega_C^1)$  so that left multiplication by  $M$  represents the (semilinear) action of the Cartier operator; here  $\Omega_C^1$  is the sheaf of differential 1-forms on  $C$ . (For information about Cartier–Manin matrices, see [1], which addresses issues with earlier literature, including the standard reference [27, §2].)

**Lemma 2.2.** *Let  $H$  be a Howe curve as above. Then  $H$  is superspecial if and only if  $E_1$  and  $E_2$  are supersingular and  $a = b = c = d = 0$ .*

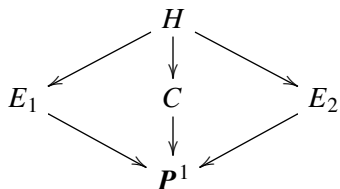
*Proof.* We already noted that  $H$  is superspecial if and only if  $E_1$  and  $E_2$  are supersingular and  $C$  is superspecial. But  $C$  is superspecial if and only if the Cartier operator acts trivially on  $H^0(C, \Omega_C^1)$  [24, Theorem 4.1].  $\square$

### 3. Detecting isomorphisms of Howe curves

In this section, we give an efficient criterion for determining whether two Howe curves are isomorphic or not. This criterion will be used in both the first and the second approach to enumerating superspecial Howe curves over a finite field.

We continue to work over an algebraically closed field of characteristic  $p \neq 2$ . Recall from Section 2 that a Howe curve is the desingularization of the fiber product of two genus-1 double covers of  $\mathbf{P}^1$ , where the ramification loci of the two covers overlap in exactly one point. This means that a Howe curve is

precisely a genus-4 curve  $H$  that fits into a  $V_4$ -diagram of the following form, where  $C$  is a curve of genus 2 and  $E_1$  and  $E_2$  are curves of genus 1:



If  $E_1 \rightarrow \mathbf{P}^1$  ramifies at points  $P, Q_1, Q_2$ , and  $Q_3$ , and if  $E_2 \rightarrow \mathbf{P}^1$  ramifies at  $P, R_1, R_2$ , and  $R_3$ , then the Weierstrass points of  $C$  are the points lying over  $Q_1, Q_2, Q_3, R_1, R_2$ , and  $R_3$ . On the other hand, the point  $P$  splits in the cover  $C \rightarrow \mathbf{P}^1$ , and we let  $P_1$  and  $P_2$  be the points of  $C$  lying over  $P$ .

Thus, to specify a Howe curve, it is enough to provide three pieces of information:

- (1) A genus-2 curve  $C$ .
- (2) An unordered pair of disjoint sets  $\{W_1, W_2\}$ , each consisting of three Weierstrass points of  $C$ .
- (3) An unordered pair of distinct points  $\{P_1, P_2\}$  on  $C$  that are mapped to one another by the hyperelliptic involution.

This data determines the  $V_4$ -diagram above, and hence also determines the double cover  $\eta : H \rightarrow C$ , which we call the *structure map* for the given data. Of course, if  $\alpha$  is an automorphism of  $C$  then  $\{\alpha(W_1), \alpha(W_2)\}$  and  $\{\alpha(P_1), \alpha(P_2)\}$  will give us a double cover  $H \rightarrow C$  that is isomorphic to  $\eta$ , namely,  $\alpha\eta$ .

**Lemma 3.1.** *The data specifying a Howe curve is recoverable (up to automorphisms of  $C$ ) just from the structure map  $\eta : H \rightarrow C$ .*

*Proof.* The map  $C \rightarrow \mathbf{P}^1$  is unique (up to automorphism of  $\mathbf{P}^1$ ), so we recover the entire map  $H \rightarrow C \rightarrow \mathbf{P}^1$  from  $\eta$ . This map is a Galois extension with group  $V_4$ , so we recover the genus-1 curves in the extension, and hence the division of the Weierstrass points of  $C$ . The pair of points  $\{P_1, P_2\}$  is simply the set of ramification points of  $\eta$ .  $\square$

**Theorem 3.2.** *Two structure maps  $\eta_1 : H \rightarrow C_1$  and  $\eta_2 : H \rightarrow C_2$  starting from the same Howe curve  $H$  are isomorphic to one another. That is, there is an isomorphism  $\gamma : C_1 \rightarrow C_2$  and an automorphism  $\delta : H \rightarrow H$  such that the following diagram commutes:*

$$\begin{array}{ccc}
 H & \xrightarrow{\delta} & H \\
 \eta_1 \downarrow & & \downarrow \eta_2 \\
 C_1 & \xrightarrow{\gamma} & C_2
 \end{array}$$

*Proof.* Let  $U_1$  and  $U_2$  be the  $V_4$ -subgroups of  $\text{Aut } H$  specified by  $\eta_1$  and  $\eta_2$ , and let  $S$  be the 2-Sylow subgroup of  $\text{Aut } H$  that contains  $U_1$ . By conjugating  $U_2$  by an automorphism  $\delta$  (and thereby replacing  $\eta_2$  with  $\eta_2\delta$ ) we may assume that  $U_2$  is also contained in  $S$ . Let  $\alpha_1$  and  $\alpha_2$  be the involutions of  $H$  corresponding to the double covers  $\eta_1$  and  $\eta_2$ , and for each  $i$ , let  $\beta_i$  and  $\gamma_i$  be the other nonzero elements of  $U_i$ .



If  $\alpha_1$  and  $\alpha_2$  are conjugate to one another in  $S$  (or even in  $\text{Aut } H$ ), we are done. So assume, to get a contradiction, that  $\alpha_1$  and  $\alpha_2$  lie in different conjugacy classes of  $S$ .

We know that the quotient of  $H$  by the subgroup  $\langle \alpha_i \rangle$  has genus 2, while the quotients of  $H$  by  $\langle \beta_i \rangle$  and by  $\langle \gamma_i \rangle$  have genus 1. The same is true for all of the conjugates of  $\alpha_i$ ,  $\beta_i$ , and  $\gamma_i$  in  $S$ . More generally, if we have two commuting involutions in  $S$  that generate a  $V_4$ -subgroup, we obtain a diagram

$$\begin{array}{ccccc}
 & & H & & \\
 & \swarrow & \downarrow & \searrow & \\
 Y_1 & & Y_2 & & Y_3 \\
 & \searrow & \downarrow & \swarrow & \\
 & & X & & 
 \end{array} \tag{3-1}$$

We know that none of the curves  $Y_i$  can have genus 0 (by Lemma 2.1), so the only possibilities are that either all of the  $Y_i$  have genus 2 and  $X$  has genus 1, or one of the  $Y_i$  has genus 2, the other two have genus 1, and  $X$  has genus 0. (This follows from the fact that in any diagram such as (3-1), the genus of  $H$  is the sum of the genera of the  $Y_i$  minus twice the genus of  $X$ ; see [17, Theorem B].) Thus, given two commuting involutions in  $S$ , if we know the genera of the quotients of  $H$  they produce, we can deduce the genus of the quotient of  $H$  by their product.

Our strategy, then, will be to enumerate all possible 2-groups  $S$  that occur as the 2-Sylow subgroup of the automorphism group of a nonhyperelliptic curve  $H$  of genus 4, along with all possible pairs  $U_1$  and  $U_2$  of  $V_4$ -subgroups of  $S$  that contain elements  $\alpha_1$  and  $\alpha_2$  that are not conjugate in  $S$ . We will assume that  $\alpha_1$  and  $\alpha_2$  generate genus-2 curves, while the other involutions in  $U_1$  and  $U_2$  generate genus-1 curves. Given these assumptions, we deduce, for as many involutions as we can, the genera of the curves associated to these involutions.

Suppose  $\delta$  is an involution in  $S$  for which we know that the quotient  $Y = H/\langle \delta \rangle$  has genus 2. Let  $T$  be the centralizer of  $\delta$  in  $S$ . Then the quotient  $T/\langle \delta \rangle$  is contained in the automorphism group of the genus-2 curve  $Y$ . Using Igusa's classification of the automorphism groups of genus-2 curves [15, §8], we can show that there are only eight 2-groups that appear as subgroups of the automorphism groups of genus-2 curves. If  $T/\langle \delta \rangle$  is not one of these groups, then we have shown that the values of  $U_1$ ,  $U_2$ ,  $\alpha_1$ , and  $\alpha_2$  cannot correspond to two different realizations of  $H$  as a Howe curve.

In order to use this strategy, we need a good bound on the sizes of automorphism groups of nonhyperelliptic curves of genus 4 in characteristic not 2. A result of Henn [10, Satz 1] (see also [6]) shows that in characteristic  $p > 2$ , the order of the automorphism group of a curve of genus  $g$  is strictly less than  $8g^3$ , except possibly when the curve is of one of the following types:

- (1)  $x^n + y^m = 1$ , where  $n = 1 + p^a$  for some  $a > 0$  and  $m \mid n$ .
- (2)  $y^p - y = x^n$ , where  $n = 1 + p^a$  for some  $a > 0$ .

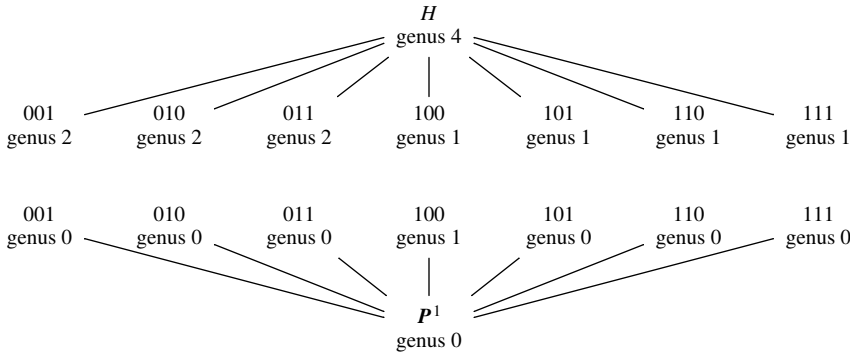
The first type of curve has genus  $(n-2)(m-1)/2$ , and if this is equal to 4 then either we have  $n = 10$  and  $m = 2$  (and  $p = 3$ ) or we have  $n = 6$  and  $m = 3$  (and  $p = 5$ ). In the first case the curve is hyperelliptic; in the second case, as Henn notes, the automorphism group has order 360, which is less than  $8g^3$ . The

second type of curve has genus  $p^a(p-1)/2$ , which is never equal to 4, because  $p$  is odd. Thus, it will suffice for us to look at every 2-group  $S$  of order less than  $8 \cdot 4^3 = 512$ .

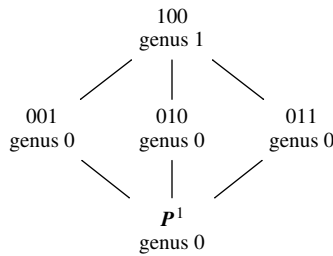
We implemented this computation in Magma; the code is available in the [online supplement](#). We ran our code on all 2-groups of order less than 512, and the only group not eliminated was  $S \cong (\mathbf{Z}/2\mathbf{Z})^3$ .

For this  $S$ , our computation shows that of the seven involutions in  $S$ , three give genus-2 quotients and four give genus-1 quotients, and the three elements that give genus-2 quotients sum to zero. Now consider the seven  $V_4$ -subgroups  $T$  of  $S$ . Each such  $T$  gives us a diagram like (3-1) above. For the  $T$  that contains the three genus-2 involutions, the genus of  $H/T$  is 1, while for the other six  $V_4$ -subgroups  $T$ , the genus of  $H/T$  is 0.

Let us consider the diagram of subextensions between  $H$  and its quotient  $H/S \cong \mathbf{P}^1$ . We label the elements of  $S$  by vectors in  $\mathbb{F}_2^3$ , and we label the  $V_4$ -subgroups in the same way, with the convention that a  $V_4$ -subgroup labeled by  $v$  contains the elements with labels  $g$  such that the dot product of  $v$  and  $g$  is 0. Then the diagram of subextensions, with their genera, is as follows:



(For visual clarity, we have left off the heads of the arrows, and omitted the 21 arrows between the middle layers.) But this configuration of genera is not possible; consider for example the following subdiagram:



This diagram violates the genus property we mentioned below diagram (3-1).

This contradiction shows that the involutions  $\alpha_1$  and  $\alpha_2$  corresponding to the structure maps  $\eta_1$  and  $\eta_2$  lie in the same conjugacy class of  $\text{Aut } H$ , so that  $\eta_1 = \eta_2\delta$  for an automorphism  $\delta$  of  $H$ .  $\square$

**Corollary 3.3.** *Two triples  $(C, \{W_1, W_2\}, \{P_1, P_2\})$  and  $(C', \{W'_1, W'_2\}, \{P'_1, P'_2\})$  give isomorphic Howe curves if and only if there is an isomorphism  $C \rightarrow C'$  that takes  $\{W_1, W_2\}$  to  $\{W'_1, W'_2\}$  and  $\{P_1, P_2\}$  to  $\{P'_1, P'_2\}$ .*

This isomorphism test is very fast; it simply requires determining whether there are any automorphisms of  $\mathbf{P}^1$  that respect the sets of Weierstrass points and their divisions, and that take the  $x$ -coordinate of  $P_1$  and  $P_2$  to that of  $P'_1$  and  $P'_2$ .

#### 4. First approach: reduction to solving multivariate systems

In this section and the next, we present two approaches to solving the problem of enumerating superspecial Howe curves. As we mentioned in [Section 1](#), the first approach, described in this section, enumerates pairs of supersingular elliptic curves  $E_1 : w^2 = f_1$  and  $E_2 : z^2 = f_2$  such that  $C : y^2 = f_1 f_2$  is superspecial. For this, we shall apply a construction of Howe curves given in [\[23\]](#). While this construction is different from the original one of [\[11\]](#), it can easily reduce our problem to finding roots of polynomial systems.

**4A. Reduction to solving multivariate systems over finite fields.** Let  $K$  be an algebraically closed field in characteristic  $p > 3$ . In [\[23\]](#), the authors parametrize the space of all Howe curves by the projective plane  $\mathbf{P}^2$ . We here briefly recall the parametrization; see [\[23, §2\]](#) for more details. Let  $y^2 = x^3 + A_i x + B_i$  ( $i = 1, 2$ ) be two (nonsingular) elliptic curves, where  $A_1, B_1, A_2, B_2 \in K$ . Let  $\lambda, \mu, \nu$  be elements of  $K$  such that  $\mu \neq 0$  and  $\nu \neq 0$ , and such that  $f_1$  and  $f_2$  are coprime, where

$$f_1(x) = x^3 + A_1 \mu^2 x + B_1 \mu^3, \quad (4-1)$$

$$f_2(x) = (x - \lambda)^3 + A_2 \nu^2 (x - \lambda) + B_2 \nu^3. \quad (4-2)$$

A point  $(\lambda : \mu : \nu) \in \mathbf{P}^2(K)$  satisfying these conditions is said to be of *Howe type* in [\[23\]](#). Note that the isomorphism classes of  $E_1$  and  $E_2$  are independent of the choice of  $(\lambda, \mu, \nu)$  provided  $\mu \neq 0$  and  $\nu \neq 0$ . Then the desingularization  $H$  of the fiber product  $E_1 \times_{\mathbf{P}^1} E_2$  is a Howe curve, and vice versa.

This parametrization, together with the criterion of superspeciality in [Section 2](#), enables us to reduce the search for superspecial Howe curves into solving multivariate systems over  $K$ ; it suffices to compute the solutions  $(\lambda : \mu : \nu) \in \mathbf{P}^2(K)$  (of Howe type) to  $a = b = c = d = 0$ , where  $a, b, c$  and  $d$  are the entries of the Cartier–Manin matrix of the hyperelliptic curve  $C : y^2 = f_1 f_2$ . Note that  $a, b, c$  and  $d$  are homogeneous as polynomials in  $\lambda, \mu$  and  $\nu$ , and that  $\text{ord}_*(-) = O(p)$  for  $* = \lambda, \mu, \nu$  and for  $- = a, b, c, d$ .

Note that the multivariate systems above are zero-dimensional, since there are only finitely many points  $(\lambda : \mu : \nu)$  parametrizing supersingular Howe curves (see [\[23\]](#)), whence the same thing holds for superspecial cases. In fact, we may assume that the coordinates  $A_1, B_1, A_2, B_2, \lambda, \mu$  and  $\nu$  belong to  $\mathbb{F}_{p^2}$ :

**Proposition 4.1.** *Any superspecial Howe curve is  $K$ -isomorphic to  $H$  obtained as above for  $A_1, B_1, A_2, B_2, \mu, \nu$  and  $\lambda$  belonging to  $\mathbb{F}_{p^2}$ .*

*Proof.* It suffices to consider the case of  $K = \overline{\mathbb{F}}_{p^2}$ , since every supersingular elliptic curve can be defined over  $\mathbb{F}_{p^2}$  and  $(\lambda, \mu, \nu)$  is a solution of  $a = b = c = d = 0$ . Let  $H'$  be a superspecial Howe curve over  $K = \overline{\mathbb{F}}_{p^2}$ . Choose  $E'_1$  and  $E'_2$  over  $K$  so that  $H'$  is the normalization of  $E'_1 \times_{\mathbf{P}^1} E'_2$ . It is well known that  $H'$  descends to a curve  $H$  over  $\mathbb{F}_{p^2}$  such that the Frobenius map  $F$  (the  $p^2$ -power map) on  $\text{Jac}(H)$

is  $p$  or  $-p$  and all automorphisms of  $H$  are defined over  $\mathbb{F}_{p^2}$  (see the proof of [5, Theorem 1.1]). Let  $E_1$  and  $E_2$  be the quotients of  $H$  corresponding to  $E'_1$  and  $E'_2$ . The quotient  $E_i$  of  $H$  is obtained by an involution  $\iota_i \in \text{Aut}(H)$ , and therefore is defined over  $\mathbb{F}_{p^2}$ . The quotient of  $H$  by the group generated by  $\iota_1$  and  $\iota_2$  is isomorphic to  $\mathbf{P}^1$  over  $\mathbb{F}_{p^2}$ . Let  $S_i$  be the set of the ramified points of  $E_i \rightarrow \mathbf{P}^1$ . Since  $S_1 \cap S_2$  consists of a single point, this point is invariant under the action of the absolute Galois group of  $\mathbb{F}_{p^2}$  and therefore is an  $\mathbb{F}_{p^2}$ -rational point. An element of  $\text{PGL}_2(\mathbb{F}_{p^2})$  sends this point to the infinite point of  $\mathbf{P}^1$ . Since the Frobenius map  $F$  on  $E_i$  is also  $\pm p$ , the other elements  $P$  of  $S_i$  (which are 2-torsion points on  $E_i$ ) are also  $\mathbb{F}_{p^2}$ -rational by  $F(P) = \pm pP = P$ . This implies the desired result.  $\square$

**4B. Concrete algorithm.** Based on the reduction described in the previous subsection, we present a concrete algorithm:

**Algorithm 4.2.** Calculating superspecial Howe curves by reduction to solving multivariate systems.

*Input:* A rational prime  $p > 3$ .

*Output:* A list  $\mathcal{H}(p)$  of superspecial Howe curves, each of which is represented by a pair  $(f_1, f_2)$  of polynomials  $f_1, f_2 \in \mathbb{F}_{p^2}[x]$ .

- (1) Compute the set  $\mathcal{S}(p)$  of representatives of the  $\overline{\mathbb{F}}_p$ -isomorphism classes of supersingular elliptic curves in characteristic  $p$  such that each representative is given in Weierstrass form  $E_{A,B} : y^2 = f_{A,B}(x) = x^3 + Ax + B$  by a pair  $(A, B)$  of elements in  $\mathbb{F}_{p^2}$ .
- (2) Set  $\mathcal{H}_0(p) \leftarrow \emptyset$ . For each pair of  $E_{A_1, B_1}$  and  $E_{A_2, B_2}$  in  $\mathcal{S}(p)$ , possibly choosing  $(A_1, B_1) = (A_2, B_2)$ , conduct Steps (a)–(c) below to compute all  $(\lambda, \mu, \nu) \in (\mathbb{F}_{p^2})^3$  of Howe type such that the desingularization  $H$  of  $E_1 \times_{\mathbf{P}^1} E_2$  is superspecial, where  $E_1 : w^2 = f_1$  (resp.  $E_2 : z^2 = f_2$ ) is an elliptic curve  $\mathbb{F}_{p^2}$ -isomorphic to  $E_{A_1, B_1}$  (resp.  $E_{A_2, B_2}$ ).
  - (a) Compute the Cartier–Manin matrix  $M$  given in (2-1).
  - (b) Compute the set  $\mathcal{V}(A_1, B_1, A_2, B_2)$  of elements  $(\lambda, \mu, \nu) \in (\mathbb{F}_{p^2})^3$  (with  $\nu = 1$ ) such that  $M = 0$ .
  - (c) For each  $(\lambda, \mu, \nu) \in \mathcal{V}(A_1, B_1, A_2, B_2)$ , if  $\mu \neq 0$  and  $\nu \neq 0$ , set  $\mathcal{H}_0(p) \leftarrow \mathcal{H}_0(p) \cup \{(f_1, f_2)\}$ , where  $f_1$  and  $f_2$  are as in (4-1) and (4-2).

*Note:* By Lemma 4.4 and Proposition 4.6 of [23], for each root  $(\lambda, \mu, \nu)$  computed in Step (b), the cubics  $f_1$  and  $f_2$  are coprime if  $\mu \neq 0$  and  $\nu \neq 0$ . Moreover, it suffices to compute elements  $(\lambda, \mu, \nu)$  with  $\nu = 1$ ; see Remark 4.2 of [19] for more details.

- (3) Set  $\mathcal{H}(p) \leftarrow \emptyset$ . For each  $(f_1, f_2) \in \mathcal{H}_0(p)$ , if the Howe curve  $H$  represented by  $(f_1, f_2)$  is not isomorphic to any Howe curve of  $\mathcal{H}(p)$ , set  $\mathcal{H}(p) \leftarrow \mathcal{H}(p) \cup \{H\}$ .

The complexity of this algorithm is estimated as  $\tilde{O}(p^6)$ , as long as  $\#\mathcal{H}_0(p) = O(p^3)$ ; see Section 4C for more details.

**Remark 4.3.** If one would like to search for a single example of a superspecial Howe curve (or determine the nonexistence of such a curve), it suffices to decide the (non-)existence of a root in Step (b). In this case, it will be estimated in the next subsection that the complexity is  $\tilde{O}(p^5)$ .

**4C. Complexity of the first approach.** We here briefly discuss the complexity of [Algorithm 4.2](#) together with several variants of computing the roots of a multivariate system in Step (b). For reasons of space, we give only a summary of the estimation of the complexity, and refer to [\[19, §5.1\]](#) for most of the details. In the following, all time complexity bounds refer to arithmetic complexity, which is the number of operations in  $\mathbb{F}_{p^2}$ . We denote by  $M(n)$  the time to multiply two univariate polynomials over  $\mathbb{F}_{p^2}$  of degree  $n$ .

For Step (1), one can check that its complexity is dominated by the cost of computing all supersingular  $j$ -invariants in characteristic  $p$ . This cost is bounded by  $O(\log^2(p)M(p)) = \tilde{O}(p)$ ; see [\[19, §5.1.1\]](#) for details.

For Step (2), clearly the complexities of Steps (a) and (b) are larger than that of Step (c). In Step (a), we compute the Cartier–Manin matrix  $M$  from  $f = f_1 f_2$  with indeterminates  $\lambda$  and  $\mu$ . The cost of computing  $M$  is bounded by  $\tilde{O}(p^3)$ ; see [Remark 4.4](#) below. In Step (b), there are three variants (i)–(iii) to compute all  $(\lambda, \mu, \nu) \in (\mathbb{F}_{p^2})^3$  with  $\nu = 1$  such that  $M = 0$ , where  $M$  is the Cartier–Manin matrix as in (2-1) with entries  $a, b, c$  and  $d$ :

- (i) Use brute force to enumerate all  $(\lambda, \mu) \in (\mathbb{F}_{p^2})^2$  to check whether  $M$  is equal to 0 or not.
- (ii) Regard one of  $\lambda$  and  $\mu$ , say  $\lambda$ , as a variable. For each  $\mu \in \mathbb{F}_{p^2}$ , compute the roots in  $\mathbb{F}_{p^2}$  of  $G = \gcd(a, b, c, d) \in \mathbb{F}_{p^2}[\lambda]$ .
- (iii) Regarding both  $\lambda$  and  $\mu$  as variables, use an approach based on resultants.

It is estimated that the complexity of (i) is  $O(p^5)$ , and that those of (ii) and (iii) are bounded by the same bound  $\tilde{O}(p^4)$ ; more precisely, the upper-bound of the complexity of (ii) is less than that of (iii) if we consider logarithmic factors; see [\[19, §5.1.2\]](#).

From this, we adopt the fastest variant (ii) with complexity  $\tilde{O}(p^4)$  in our implementation. The number of  $(\lambda, \mu, \nu)$  with  $\nu = 1$  computed in Step (b) is  $\leq p^2 \times \deg(G) = O(p^3)$ . Since the number of possible choices of  $(E_{A_1, B_1}, E_{A_2, B_2})$  is  $\#\mathcal{S}(p) = O(p^2)$ , computing  $(\lambda, \mu, \nu)$  with  $\nu = 1$  for all  $(E_{A_1, B_1}, E_{A_2, B_2})$  is done in  $\#\mathcal{S}(p) \times \tilde{O}(p^4) = \tilde{O}(p^6)$  operations in  $\mathbb{F}_{p^2}$ .

The complexity of Step (3) depends heavily on the number of superspecial Howe curves obtained in Step (2), that is,  $\#\mathcal{H}_0(p)$ . Since each isomorphism test is done in  $O(1)$ , the complexity of Step (3) is  $O((\#\mathcal{H}_0(p))^2)$ . As of this writing, we have not succeeded in finding any sharp bound on  $\#\mathcal{H}_0(p)$ . We can naively estimate  $\#\mathcal{H}_0(p) = O(p^5)$  from the complexity analysis of Step (2), whereas we expect  $\#\mathcal{H}_0(p) = O(p^3)$  from the practical behavior [\[19, §4.2, Table 1\]](#). Thus, the complexity of Step (3) is naively  $O(p^{10})$ , but in practice  $O(p^6)$  which does not exceed the complexity of Steps (1)–(2).

Note that to determine the (non-)existence of a superspecial Howe curve, it is not necessary to compute a root in Step (b), but it suffices to compute the gcd  $G$  only. Since each gcd can be computed in time  $\tilde{O}(p)$  by fast gcd algorithms, one can verify that the total complexity of this variant of [Algorithm 4.2](#) is  $\tilde{O}(p^5)$ .

**Remark 4.4.** In Step (a), we compute a Cartier–Manin matrix over  $\mathbb{F}_{p^2}[\lambda, \mu]$ . Bostan, Gaudry, and Schost showed that in general, computing the Cartier–Manin matrix  $M$  of a hyperelliptic curve  $y^2 = f(x)$

defined over a field  $K$  can be accomplished by multiplying matrices obtained from recurrences for the coefficients of  $f(x)^n$ ; see [2, §8] or [9, §2] for details. The algorithm of Harvey and Sutherland [9], which is an improvement of their earlier algorithm [8] presented at ANTS XI, is also based on this reduction, and it is the fastest algorithm to compute  $M$  for the case of  $K = \mathbb{F}_p$ . From this, we suspect that one of the best ways to compute  $M$  in Step (a) would be to extend the Harvey–Sutherland algorithm [9] to the case of  $\mathbb{F}_{p^2}(\lambda, \mu)$ . However, since we have not yet succeeded in making this extension, we compute  $M$  using the reduction mentioned above, or by using formulæ given in [23, §4] for  $M$  specific to Howe curves. It is estimated (to appear in a revised version of [19]) that the complexity of the latter method is bounded by  $\tilde{O}(p^3)$ , which is less than or equal to that of Step (b).

## 5. Second approach: use of Richelot isogenies of genus-2 curves

In this section we propose another approach to enumerating superspecial Howe curves. As opposed to the approach in Section 4, this second approach *starts* with a superspecial genus-2 curve  $C$ , and then looks to see whether it will fit into a  $V_4$ -diagram with supersingular elliptic curves. While this is precisely the structure of Algorithm 5.7 of [11], the problem remains: How can we *quickly* produce a list of *all* of the superspecial genus-2 curves? We begin by addressing this question.

**5A. Computing superspecial curves of genus 2.** To produce a list  $\mathcal{L}$  of all superspecial genus-2 curves, we use a variant of [11, Algorithm 5.7]. Each superspecial genus-2 curve has a unique model defined over  $\mathbb{F}_{p^2}$  that is maximal over  $\mathbb{F}_{p^2}$ . Given one such curve, all of the curves that are Richelot isogenous to it are also maximal superspecial curves. Thus, given a not-necessarily-complete list of maximal superspecial curves, we can add curves to the list as follows: We go through the list one curve at a time. For each  $C$  we compute the curves that are Richelot isogenous to it, and we add each such curve to the list if it is not already on it. To seed our list, we can use the curves that are  $(2, 2)$ -isogenous to a product of maximal elliptic curves. Then a result of Jordan and Zaytman [16, Corollary 18] shows that this procedure will generate a complete list  $\mathcal{L}$  of all superspecial genus-2 curves.

The exact number of curves on the list  $\mathcal{L}$  is given by a result of Ibukiyama, Katsura, and Oort [14, Theorem 3.3]. The exact answer depends on the congruence class of  $p$  modulo 120, but it follows from their result that for  $p > 3$  we have

$$\#\mathcal{L} = \frac{(p-1)(p^2 + 25p + 166)}{2800} + c, \quad \text{where } \frac{-1}{16} \leq c \leq \frac{209}{180}.$$

**5B. Testing whether a genus-2 curve fits into a  $V_4$ -diagram.** For each  $C \in \mathcal{L}$ , given by an equation

$$y^2 = (x - a_1)(x - a_2)(x - a_3)(x - a_4)(x - a_5)(x - a_6),$$

we would like to try to fit  $C$  into a Howe curve diagram. For each of the ten ways of splitting the Weierstrass points into two groups of three (for example, into  $\{\{a_1, a_2, a_3\}, \{a_4, a_5, a_6\}\}$ ), we could then

ask for the values of  $b$  such that the two genus-1 curves

$$y^2 = (x - b)(x - a_1)(x - a_2)(x - a_3) \quad (5-1)$$

and

$$y^2 = (x - b)(x - a_4)(x - a_5)(x - a_6) \quad (5-2)$$

are both supersingular. (We also consider “ $b=\infty$ ”, corresponding to the curves  $y^2=(x-a_1)(x-a_2)(x-a_3)$  and  $y^2=(x-a_4)(x-a_5)(x-a_6)$ .) Since there are about  $p/12$  supersingular  $j$ -invariants and hence about  $p/2$  supersingular  $\lambda$ -invariants, there are about  $p/2$  values of  $b$  that will make the first curve (5-1) supersingular, and we can compute these values in time  $\tilde{O}(p)$ . For each  $b$ , we then check whether the second curve (5-2) is supersingular. If we were to model this as choosing a random  $\lambda$ -invariant in  $\mathbb{F}_{p^2}$  and asking whether it is supersingular, we would expect success with probability around  $1/(2p)$ .

It is easy to incorporate isomorphism testing into this algorithm so that it produces each superspecial Howe curve exactly once: All we have to do is keep track of how the automorphism group of  $C$  acts on the divisions of its Weierstrass points and on the good values of  $b$ .

Thus, in time  $\tilde{O}(p^4)$ , we can produce unique representatives for each superspecial Howe curve. Heuristically, the number of superspecial Howe curves we find should be the number of superspecial genus-2 curves ( $\approx p^3/2880$ ), times the number of Weierstrass point divisions (10), times the number of values of  $b$  that make the first elliptic curve supersingular ( $\approx p/2$ ), times the probability that the second curve is supersingular ( $\approx 1/(2p)$ ). Heuristically, then, we expect to find about  $p^3/1152$  superspecial Howe curves.

### 5C. Concrete algorithm.

**Algorithm 5.1.** Calculating superspecial Howe curves using Richelot isogenies of genus-2 curves.

*Input:* A rational prime  $p > 3$ .

*Output:* A list  $\mathcal{H}(p)$  of superspecial Howe curves, each of which is represented by a pair  $(f_1, f_2)$  of polynomials  $f_1, f_2 \in \mathbb{F}_{p^2}[x]$ , corresponding to the curve  $y^2 = f_1, z^2 = f_2$ .

- (1) Compute the set  $\text{MaxEll}(p^2)$  of  $\mathbb{F}_{p^2}$ -isomorphism classes of  $\mathbb{F}_{p^2}$ -maximal elliptic curves over  $\mathbb{F}_{p^2}$ . Since every supersingular curve has a unique maximal twist, this can be done as in Step (1) of Algorithm 4.2.
- (2) Set  $\mathcal{L} \leftarrow \emptyset$ . For each pair  $(E, E')$  of elements in  $\text{MaxEll}(p^2)$ , compute the (at most 6) curves  $C$  whose Jacobians are  $(2, 2)$ -isogenous to  $E \times E'$  (see [12, §3]). Adjoin each of these to  $\mathcal{L}$  if it is not isomorphic to an element of  $\mathcal{L}$ .
- (3) Write  $\mathcal{L} = \{C_1, \dots, C_n\}$ . Set  $i = 1$ .
  - (a) For each nonsingular curve  $C'$  which is Richelot isogenous to  $C_i$ , if  $C'$  is not isomorphic to any element of  $\mathcal{L}$ , set  $N \leftarrow |\mathcal{L}|$  and put  $C_{N+1} = C'$  and  $\mathcal{L} \leftarrow \mathcal{L} \cup \{C_{N+1}\}$ .
  - (b) If  $i < |\mathcal{L}|$ , set  $i \leftarrow i + 1$  and go to (a).



- (4) Set  $\mathcal{H}(p) \leftarrow \emptyset$ .
- (5) For each  $C \in \mathcal{L}$ , check whether  $C$  fits into a Howe curve diagram with supersingular double covers  $E_i \rightarrow \mathbf{P}^1$ .
  - (a) For each splitting of the Weierstrass point of  $C$  into two disjoint three-element sets, compute the  $j$ -invariants of the genus-1 curves (5-1) and (5-2), as functions of the indeterminate  $b$ . Find the values of  $b$  that make the first curve supersingular, and for each such value, check to see whether the second curve is supersingular. Record each value of  $b$  for which both curves are supersingular.
  - (b) Using Corollary 3.3, find unique representatives  $y^2 = f_1, z^2 = f_2$  for the curves produced in the previous step, and adjoin  $(f_1, f_2)$  to  $\mathcal{H}(p)$ .

We noted in the previous subsection that Step (5) takes  $\tilde{O}(p^4)$  arithmetic operations over  $\mathbb{F}_{p^2}$ , and the other steps clearly take fewer operations than this.

## 6. Implementations and proofs

In this section, we describe our implementations of the algorithms in the previous sections and our proofs of the main results stated in the Introduction. As we have seen, there are two approaches to enumerating superspecial Howe curves: (A)  $(E_1, E_2)$ -first and (B)  $C$ -first. The arguments in the previous sections show that (B) has an advantage in the complexity analysis. Here we see that (B) is far superior to (A) also when we execute their implementations. Indeed, Theorems 1.1 and 1.2 in the Introduction were obtained by Magma implementations based on (B) that were run on a PC with Ubuntu 16.04 LTS OS at 3.40GHz CPU (Intel Core i7-6700) and 15.6 GB memory. The same result for  $p \leq 53$  was obtained by implementing the method (A) over Magma with an execution by the same PC. Although it took 11871 seconds to obtain Theorem 1.2 for  $p \leq 53$  by (A), the second strategy (B) finishes the enumeration for  $p \leq 199$  in only 924 seconds; see Table 2 for benchmark timing data for small  $p$ .

The code for our implementations is available in the [online supplement](#). In case (A), it is very costly to find Cartier–Manin matrices, and in addition to that there are many pairs  $(E_1, E_2)$  of supersingular elliptic curves. This fact is consistent with the complexity analysis in Section 4C. On the other hand, the method (B) contains few intensive computations and it enables us to find and enumerate superspecial Howe curves very efficiently.

The preceding remarks prove the computational results in Theorems 1.1 and 1.2, and we are left to prove the statement in Theorem 1.1 concerning primes  $p \equiv 5 \pmod{6}$ . This fact is shown by using the Howe curve defined by  $E_1 : z^2y = x^3 + y^3$  and  $E_2 : w^2y = x^3 + ay^3$  with  $a \in \{-1, 1/4\}$ . Indeed, if  $p \equiv 5 \pmod{6}$ , then these two elliptic curves are supersingular and moreover  $y^2 = (x^3 + 1)(x^3 + a)$  is superspecial. This can be checked by observing that the curve has two nonhyperelliptic involutions, given by  $(x, y) \mapsto (a^{1/3}/x, \pm a^{1/2}y/x^3)$ , so that its Jacobian is  $(2, 2)$ -isogenous to a product of elliptic curves. For  $a = -1$  we find that these two curves are both isomorphic to the  $j = 0$  curve with CM by  $-3$ ,



$p$	(A)	(B)	$p$	(A)	(B)	$p$	(A)	(B)
5	0.02	0.08	19	6.14	0.12	41	1118.63	0.71
7	0.01	0.01	23	27.59	0.21	43	1423.26	0.80
11	0.17	0.04	29	114.70	0.31	47	2686.17	1.03
13	0.76	0.05	31	193.82	0.34	53	5678.32	1.46
17	3.92	0.09	37	617.23	0.54			

**Table 2.** Benchmark timing data for (A) [Algorithm 4.2](#) and (B) [Algorithm 5.1](#). All times shown are in seconds.

and for  $a = 1/4$  we find that they are both isomorphic to the  $j = -12288000$  curve with CM by  $-27$ . In both cases, these elliptic curves are supersingular for primes  $p \equiv 5 \pmod{6}$ .

We remark that this curve for  $a = 1/4$  is isomorphic to the curve  $X^3 + Y^3 + W^3 = 2YW + Z^2 = 0$  in  $P^3$  studied by the Kudo in [\[18\]](#), by the correspondence  $x = X$ ,  $y = Y + W$ ,  $z = \sqrt{-3/2}Z$  and  $w = \sqrt{-3/4}(Y - W)$ .

### Acknowledgments

Kudo and Harashita thank Everett Howe for joining as the third author; he told them the second strategy (B), which had not been considered in the earlier version [\[19\]](#). Howe thanks Professors Kudo and Harashita for inviting him to join them in this work. The authors thank the referees for their careful reading and for helpful suggestions and comments. This work was supported by JSPS Grant-in-Aid for Scientific Research (C) 17K05196, JSPS Grant-in-Aid for Research Activity Start-up 18H05836 and 19K21026, and JSPS Grant-in-Aid for Young Scientists 20K14301.

### References

- [1] Jeffrey D. Achter and Everett W. Howe, *Hasse–Witt and Cartier–Manin matrices: a warning and a request*, Arithmetic geometry: computation and applications (Y. Aubry, E. W. Howe, and C. Ritzenthaler, eds.), Contemp. Math., vol. 722, Amer. Math. Soc., Providence, RI, 2019, pp. 1–18. [MR 3896846](#)
- [2] Alin Bostan, Pierrick Gaudry, and Éric Schost, *Linear recurrences with polynomial coefficients and application to integer factorization and Cartier–Manin operator*, SIAM J. Comput. **36** (2007), no. 6, 1777–1806. [MR 2299425](#)
- [3] Bradley Wayne Brock, *Superspecial curves of genera two and three*, Ph.D. thesis, Princeton University, 1993. [MR 2689446](#)
- [4] Max Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272.
- [5] Torsten Ekedahl, *On supersingular curves and abelian varieties*, Math. Scand. **60** (1987), no. 2, 151–178. [MR 914332](#)
- [6] Massimo Giulietti and Gábor Korchmáros, *Nakajima’s remark on Henn’s proof*, Electron. Notes Discrete Math. **40** (2013), 135–138.
- [7] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York–Heidelberg, 1977, Graduate Texts in Mathematics, No. 52. [MR 0463157](#)
- [8] David Harvey and Andrew V. Sutherland, *Computing Hasse–Witt matrices of hyperelliptic curves in average polynomial time*, LMS J. Comput. Math. **17** (2014), suppl. A, 257–273. [MR 3240808](#)
- [9] David Harvey and Andrew V. Sutherland, *Computing Hasse–Witt matrices of hyperelliptic curves in average polynomial time, II*, Frobenius distributions: Lang–Trotter and Sato–Tate conjectures (D. Kohel and I. Shparlinski, eds.), Contemp. Math., vol. 663, Amer. Math. Soc., Providence, RI, 2016, pp. 127–147. [MR 3502941](#)

- [10] Hans-Wolfgang Henn, *Funktionenkörper mit grosser Automorphismengruppe*, J. Reine Angew. Math. **302** (1978), 96–115. [MR 511696](#)
- [11] Everett W. Howe, *Quickly constructing curves of genus 4 with many points*, Frobenius distributions: Lang–Trotter and Sato–Tate conjectures (D. Kohel and I. Shparlinski, eds.), Contemp. Math., vol. 663, Amer. Math. Soc., Providence, RI, 2016, pp. 149–173. [MR 3502942](#)
- [12] Everett W. Howe, Franck Leprévost, and Bjorn Poonen, *Large torsion subgroups of split Jacobians of curves of genus two or three*, Forum Math. **12** (2000), no. 3, 315–364. [MR 1748483](#)
- [13] Tomoyoshi Ibukiyama, *On rational points of curves of genus 3 over finite fields*, Tohoku Math. J. (2) **45** (1993), no. 3, 311–329. [MR 1231559](#)
- [14] Tomoyoshi Ibukiyama, Toshiyuki Katsura, and Frans Oort, *Supersingular curves of genus two and class numbers*, Compositio Math. **57** (1986), no. 2, 127–152. [MR 827350](#)
- [15] Jun-ichi Igusa, *Arithmetic variety of moduli for genus two*, Ann. of Math. (2) **72** (1960), 612–649. [MR 114819](#)
- [16] Bruce W. Jordan and Yevgeny Zaytman, *Isogeny graphs of superspecial abelian varieties and generalized Brandt matrices*, preprint, 2020. [arXiv:2005.09031](#)
- [17] Ernst Kani and Michael Rosen, *Idempotent relations and factors of Jacobians*, Math. Ann. **284** (1989), no. 2, 307–327. [MR 1000113](#)
- [18] Momonari Kudo, *On the existence of superspecial and maximal nonhyperelliptic curves of genera four and five*, Comm. Algebra **47** (2019), no. 12, 5020–5038. [MR 4019321](#)
- [19] Momonari Kudo and Shushi Harashita, *Algorithm to enumerate superspecial Howe curves of genus 4*, preprint, 2020. [arXiv:2003.04153](#)
- [20] Momonari Kudo and Shushi Harashita, *Algorithmic study of superspecial hyperelliptic curves over finite fields*, preprint, 2019. [arXiv:1907.00894](#)
- [21] Momonari Kudo and Shushi Harashita, *Computational approach to enumerate non-hyperelliptic superspecial curves of genus 4*, Tokyo J. Math **43** (2020), no. 1, 259–278. [MR 4121797](#)
- [22] Momonari Kudo and Shushi Harashita, *Superspecial curves of genus 4 in small characteristic*, Finite Fields Appl. **45** (2017), 131–169. [MR 3631358](#)
- [23] Momonari Kudo, Shushi Harashita and Hayato Senda, *The existence of supersingular curves of genus 4 in arbitrary characteristic*, Res. Number Theory **6** (2020), no. 4, article 44. [MR 4170348](#)
- [24] Niels O. Nygaard, *Slopes of powers of Frobenius on crystalline cohomology*, Ann. Sci. École Norm. Sup. (4) **14** (1981), no. 4, 369–401 (1982). [MR 654203](#)
- [25] Frans Oort, *Hyperelliptic supersingular curves*, Arithmetic algebraic geometry (Texel, 1989) (G. van der Geer, F. Oort, and J. Steenbrink, eds.), Progr. Math., vol. 89, Birkhäuser Boston, Boston, MA, 1991, pp. 247–284. [MR 1085262](#)
- [26] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. [MR 2514094](#)
- [27] Noriko Yui, *On the Jacobian varieties of hyperelliptic curves over fields of characteristic  $p > 2$* , J. Algebra **52** (1978), no. 2, 378–410. [MR 491717](#)

Received 25 Feb 2020. Revised 1 Aug 2020.

MOMONARI KUDO: [kudo@mist.i.u-tokyo.ac.jp](mailto:kudo@mist.i.u-tokyo.ac.jp)

Department of Mathematical Informatics, Graduate School of Information Science and Technology, The University of Tokyo, Bunkyo-ku, Tokyo, Japan

SHUSHI HARASHITA: [harasita@ynu.ac.jp](mailto:harasita@ynu.ac.jp)

Graduate School of Environment and Information Sciences, Yokohama National University, Hodogaya-ku, Yokohama, Japan

EVERETT W. HOWE: [however@alumni.caltech.edu](mailto:however@alumni.caltech.edu)

San Diego, CA, United States

# Divisor class group arithmetic on $C_{3,4}$ curves

Evan MacNeil, Michael J. Jacobson Jr., and Renate Scheidler

We present novel explicit formulas for arithmetic in the divisor class group of a  $C_{3,4}$  curve. Our formulas handle all cases of inputs and outputs without having to fall back on a generic method. We also improve on the most commonly occurring case by reducing the number of required field inversions to one at the cost of a small number of additional field operations, resulting in running times that are between 11 and 21% faster than the prior state of the art depending on the field size, and even more for small field sizes when nontypical cases frequently arise.

## 1. Introduction

Computing in the divisor class group of an algebraic curve is a nontrivial component in computing  $L$ -series.  $L$ -series in turn are at the heart of the Sato–Tate conjecture and related conjectures. The Sato–Tate conjecture has been proved for elliptic curves with complex multiplication, but its analogues for other classes of algebraic curves remains open [14]. In order to test these conjectures for other curve families, it is desirable to have efficient algorithms to perform divisor class group arithmetic; see, for example, [7; 6; 13].

The  $C_{3,4}$  curves are a family of genus 3 plane curves. While they are rare among genus 3 curves, such special families of curves make interesting settings in which to study Sato–Tate-related conjectures. Fast explicit formulas exist to perform divisor class group arithmetic for genus 1 and genus 2 curves. However, the picture for genus 3 curves, and  $C_{3,4}$  curves in particular, is incomplete. Existing formulas for arithmetic on  $C_{3,4}$  curves were developed with cryptographic applications in mind, where the curves are defined over very large finite fields of characteristic greater than 3. A  $C_{3,4}$  curve over such a field is isomorphic to one given by a short-form equation (see Section 2), yielding faster arithmetic. Moreover, with very high probability, one will only encounter “typical” divisors (see Section 2) and many degenerate cases need not be considered. When these assumptions are violated, one may fall back on slower divisor addition algorithms that work on any algebraic curve.

---

*MSC2010:* 11R65, 14H45, 14Q05.

*Keywords:* computational number theory, computational algebraic geometry, divisor arithmetic,  $C_{3,4}$  curves, genus 3 nonhyperelliptic curves.

In [2], Arita specialized the algorithm for addition in the class group of a general  $C_{a,b}$  curve in [1] to the  $C_{3,4}$  case. He classified divisors of  $C_{3,4}$  curves into 19 types based on the forms of their Gröbner basis representations. The method allows addition of divisors of any type, although it handles this in a recursive manner that does not terminate for some curves over very small finite fields; Arita was predominantly interested in the cryptographic setting over a large finite field where this does not present a problem. However, number theoretic applications require extensive curve arithmetic over far smaller finite fields.

Other algorithms are less general but much faster. In [8], the most recent of these, Khuri-Makdisi, building upon the work of Flon et al. [4] and Abu Salem and Khuri-Makdisi [11] assumed a  $C_{3,4}$  curve defined by a short-form polynomial equation. In addition to restricting to disjoint divisors without multiple points, they assume that divisors being added or doubled are typical. They represent divisors by a pair of polynomials of minimal degree and obtain sums of divisors by computing kernels of maps between vector spaces. This yields the most efficient explicit formulas, describing the operation as an optimized sequence of field operations instead of via polynomial arithmetic or linear algebra, for the typical case. Thus, prior to our work herein, the state of the art for  $C_{3,4}$  curves was the addition and doubling procedures of [11] and the reduction method of [8]. Both of these are limited to typical divisors, and one had to resort to general arithmetic for all other cases.

Our contribution is to marry the methods of Salem and Khuri-Makdisi — who have the fastest explicit formulas to date — with the methods of Arita — whose formulas are the most general — in order to produce fast and fully general explicit formulas that cover all cases of  $C_{3,4}$  curve arithmetic. This approach is facilitated by the fact that Salem and Khuri-Makdisi’s representation of typical divisors resembles type 31 divisors from Arita’s classification. Our algorithms work in full generality: the curve may be defined over a field of any size and any characteristic, including 0, 2, and 3 (though our implementation only extends to finite fields), the curve equation may be in long or short form (see Section 2), divisors may be typical or atypical, nondisjoint, and have multiple points, and all our algorithms provably terminate.

We extend the approach of [11] for finding the kernel of the aforementioned map to computing its image as well and are thus able to handle atypical and nondisjoint divisors. We also improve on the state of the art of [8; 11] for typical divisors. Fully general algorithms for adding, doubling, and reducing divisors are presented in Sections 3, 4 and 5, respectively. These algorithms are used to develop fast explicit formulas in Section 6 that handle the most typical cases arising in  $C_{3,4}$  curve divisor arithmetic; specifically, adding/doubling disjoint typical divisors on a curve in short form over a field of characteristic greater than 3. The operation counts of these formulas are summarized in Table 1.1, where I, M, S, A refer to the number of field inversions, multiplications, squarings, and additions in the base field of the curve.<sup>1</sup> Our formulas improve on the prior state of the art by requiring only a single field inversion at the cost of a sufficiently small number of other field operations. Experiments confirm an overall running time speed-up by approximately 11–21% depending on the size of the field. Our algorithms are also used to produce explicit formulas for all atypical cases, including nondisjoint or atypical divisors and

<sup>1</sup>Arita did not distinguish between field multiplications and squarings, and neither Arita nor Flon et al. counted field additions in their work.

	Add				Double			
	I	M	S	A	I	M	S	A
Arita [2]	5	204	–	–	5	284	–	–
Flon et al [4]	2	148	15	–	2	165	20	–
Khuri-Makdisi and Salem [8; 11]	2	97	1	132	2	107	3	155
<b>This work</b>	1	111	3	99	1	127	4	112

**Table 1.1.** Comparison of operation counts in prior work.

curves of arbitrary form and in any characteristic. These cases are so numerous that we choose instead to publish them in the form of Sage code on GitHub [9] and present their operation counts in Section 7.

By improving upon the typical case and completing the picture for the atypical cases, our results will have a significant impact on number theoretic computations heavy on arithmetic in the divisor class group of a  $C_{3,4}$  curve. As in [14] for example, one may wish to take a curve over  $\mathbb{Q}$ , reduce it modulo all primes up to some bound, and compute the order of the divisor class group of that reduced curve. The improvement in the typical case remains significant over all the computations, while the completion of the atypical cases becomes more significant over the smaller fields, where one frequently encounters these cases.

## 2. Preliminaries

Let  $K$  be a perfect field. A  $C_{3,4}$  curve is a nonsingular nonhyperelliptic projective curve  $C$  of genus 3 whose affine model is given by  $F(x, y) = 0$  where  $F \in K[x, y]$  is of the form

$$F(x, y) = y^3 + x^4 + c_8xy^2 + c_7x^2y + c_6x^3 + c_5y^2 + c_4xy + c_3x^2 + c_2y + c_1x + c_0.$$

We denote the unique point at infinity on  $C$  by  $P_\infty$ . When  $K$  has characteristic 0 or at least 5, the curve isomorphism  $(x, y) \mapsto (x - a/4, y - (c_8/3)x + (ac_8 - 4c_5)/3)$ ,  $a = (27c_6 - 9c_7c_8 + 2c_8^3)/27$ , over  $K$  transforms the polynomial  $F$  to the short form

$$F(x, y) = y^3 + x^4 + c_7x^2y + c_4xy + c_3x^2 + c_2y + c_1x + c_0.$$

Let  $\text{Div}_K^0(C)$  denote the group of degree zero divisors on  $C$  defined over  $K$ . Elements of  $\text{Div}_K^0(C)$  are of the form

$$D = \sum_{P \in C(\bar{K}) - \{P_\infty\}} \text{ord}_P(D)P - nP_\infty, \quad n = \sum_{P \in C(\bar{K}) - \{P_\infty\}} \text{ord}_P(D),$$

where the sum defining  $D$  is fixed under Galois automorphisms on  $\bar{K}$ . For brevity, we identify  $D$  with its finite part and refer to  $n = \deg(D)$  as its degree. A divisor  $D$  is *effective* if  $\text{ord}_P(D) \geq 0$  for all  $P \in C(\bar{K}) - \{P_\infty\}$  and *reduced* if in addition  $n$  is minimal among the degrees of all the divisors in the linear equivalence class of  $D$ . If  $D$  is reduced, then  $\deg(D) \leq 3$ . Every element of  $\text{Div}_K^0(C)$  is linearly equivalent to an effective divisor and to a unique reduced divisor in  $\text{Div}_K^0(C)$ .

For any two effective divisors  $D, D' \in \text{Div}_K^0(C)$ , define

$$\begin{aligned}\text{lcm}(D, D') &= \sum_{P \in C(\bar{K}) - \{P_\infty\}} \max\{\text{ord}_P(D), \text{ord}_P(D')\}(P - P_\infty), \\ \text{gcd}(D, D') &= \sum_{P \in C(\bar{K}) - \{P_\infty\}} \min\{\text{ord}_P(D), \text{ord}_P(D')\}(P - P_\infty).\end{aligned}$$

Then  $D + D' = \text{gcd}(D, D') + \text{lcm}(D, D')$ .

There is a canonical isomorphism from  $\text{Div}_K^0(C)$  to the group of fractional  $K[C]$ -ideals, written as  $D \mapsto I_D$ , with inverse  $I \mapsto \text{div}(I)$ .  $D$  is effective if and only if  $I_D$  is integral. If  $g_1, g_2, \dots \in K[C]$  are polynomials, then we write  $\text{div}(g_1, g_2, \dots)$  in place of  $\text{div}(\langle g_1, g_2, \dots \rangle)$ .

In [2], Arita described a monomial order on  $K[C]$  induced by the pole orders  $\text{ord}_{P_\infty}(x) = -3$  and  $\text{ord}_{P_\infty}(y) = -4$ . Every ideal  $I$  of  $K[C]$  has a unique reduced Gröbner basis with respect to this ordering that contains the *minimum polynomial* of  $I$ , i.e., the unique polynomial  $f_I$  in any Gröbner basis of  $I$  with the smallest leading monomial and leading coefficient 1. Under this isomorphism, we have the following correspondence between effective divisors and their associated  $K[C]$ -ideals:

Divisors	$D + D'$	$\text{lcm}(D, D')$	$\text{gcd}(D, D')$	$\bar{D}$	$D \leq D'$
Ideals	$I_D I_{D'}$	$I_D \cap I_{D'}$	$I_D + I_{D'}$	$f_{I_D} : I_D$	$I_D \supseteq I_{D'}$

Here,  $f_{I_D} : I_D$  is the unique  $K[C]$ -ideal satisfying  $I_D(f_{I_D} : I_D) = \langle f_{I_D} \rangle$ , the principal ideal generated by  $f_{I_D}$ . The corresponding divisor  $\bar{D} = \text{div}(f_{I_D} : I_D)$  is the *flip* of  $D$ ; it is equivalent to  $-D$  and is reduced. It follows that  $D$  is reduced if and only if  $D = \bar{\bar{D}}$ , and  $\bar{\bar{D}}$  is the *reduction* of  $D$ , i.e., the unique reduced divisor linearly equivalent to  $D$ . This gives rise to the following high-level algorithm for addition in the degree zero divisor class group of a  $C_{3,4}$  curve, found also in [2]. Given two reduced divisors  $D$  and  $D'$ , represented by the reduced Gröbner bases of their respective ideals  $I_D$  and  $I_{D'}$ , perform the following:

- (1) Compute the reduced Gröbner basis of  $J := I_D I_{D'}$ .
- (2) Compute the reduced Gröbner basis of  $J^* := f_J : J$ .
- (3) Compute the reduced Gröbner basis of  $J^{**} := f_{J^*} : J^*$ .

Then  $\text{div}(J^{**})$  is the unique reduced divisor equivalent to  $D + D'$ . In [8], Khuri-Makdisi showed how to combine the last two steps into a single efficient step.

Following [8], an effective divisor  $D$  is said to be *semitypical* if the reduced Gröbner basis of  $I_D$  consists of three polynomials, i.e.,  $I_D = \langle f, g, h \rangle$ . A divisor is *typical* if it is semitypical with  $h \in \langle f, g \rangle$ , where  $h$  is the generator with the largest pole order at infinity. A divisor that is not typical is called *atypical*. All typical divisors are semitypical, but atypical divisors may or may not be semitypical.

In [2], Arita classified all divisors of degree  $\leq 6$  into 19 types according to the leading monomials of their reduced Gröbner bases. Table 2.1 reproduces Arita's classification, along with a 20-th type corresponding to the zero divisor. Note that a divisor of degree  $d \leq 6$  is semitypical if and only if it is of type 31, 41, 51, or 61, and a type 31 divisor  $D$  is typical if and only if  $f_2$ , the coefficient of  $y$  in

Deg	Type	Gröbner Basis
0	0	1
1	11	$x + f_0, \quad y + g_0$
2	21	$y + f_1x + f_0, \quad x^2 + g_1x + g_0$
	22	$x + f_0, \quad y^2 + g_2y + g_0$
3	31	$x^2 + f_2y + f_1x + f_0, \quad xy + g_2y + g_1x + g_0, \quad y^2 + h_2y + h_1x + h_0$
	32	$y + f_1x + f_0, \quad x^3 + g_3x^2 + g_1x + g_0$
	33	$x + f_0$
4	41	$xy + f_3x^2 + f_2y + f_1x + f_0, \quad y^2 + g_3x^2 + g_2y + g_1x + g_0, \quad x^3 + h_3x^2 + h_2y + h_1x + h_0$
	42	$x^2 + f_1x + f_0, \quad xy + g_2y + g_1x + g_0$
	43	$x^2 + f_2y + f_1x + f_0, \quad y^2 + g_4xy + g_2y + g_1x + g_0$
	44	$y + f_1x + f_0$
5	51	$y^2 + f_4xy + f_3x^2 + f_2y + f_1x + f_0, \quad x^3 + g_4xy + g_3x^2 + g_2y + g_1x + g_0, \quad x^2y + h_4xy + h_3x^2 + h_2y + h_1x + h_0$
	52	$xy + f_3x^2 + f_2y + f_1x + f_0, \quad y^2 + g_3x^2 + g_2y + g_1x + g_0$
	53	$xy + f_3x^2 + f_2y + f_1x + f_0, \quad x^3 + g_5y^2 + g_3x^2 + g_2y + g_1x + g_0$
	54	$x^2 + f_2y + f_1x + f_0, \quad xy^2 + g_5y^2 + g_4xy + g_2y + g_1x + g_0$
6	61	$x^3 + f_5y^2 + f_4xy + f_3x^2 + f_2y + f_1x + f_0, \quad x^2y + g_5y^2 + g_4xy + g_3x^2 + g_2y + g_1x + g_0, \quad xy^2 + h_5y^2 + h_4xy + h_3x^2 + h_2y + h_1x + h_0$
	62	$y^2 + f_4xy + f_3x^2 + f_2y + f_1x + f_0, \quad x^3 + g_4xy + g_3x^2 + g_2y + g_1x + g_0$
	63	$y^2 + f_4xy + f_3x^2 + f_2y + f_1x + f_0, \quad x^2y + g_6x^3 + g_4xy + g_3x^2 + g_2y + g_1x + g_0$
	64	$xy + f_3x^2 + f_2y + f_1x + f_0, \quad x^4 + g_6x^3 + g_5y^2 + g_3x^2 + g_2y + g_1x + g_0$
	65	$x^2 + f_2y + f_1x + f_0$

**Table 2.1.** Arita's classification of divisors into types.

$f_{I_D}$ , is nonzero (see [8, Proposition 2.12]). The types of  $\bar{D}$  and  $\bar{\bar{D}}$  are determined by the type of  $D$  as summarized in Table 2.2. Examples of computing the type of  $\bar{D}$  are found in Section 7.3 of [10]. A divisor is reduced if and only if it is of type 0, 11, 21, 22 or 31; in particular, all divisors of degree  $d \leq 2$  are reduced.

Divisor	Type																			
$D$	0	11	21	22	31	32	33	41	42	43	44	51	52	53	54	61	62	63	64	65
$\bar{D}$	0	22	21	11	31	11	0	31	22	21	0	31	22	21	11	31	22	21	11	0
$\bar{\bar{D}}$	0	11	21	22	31	22	0	31	11	21	0	31	11	21	22	31	11	21	22	0

**Table 2.2.** Divisor types and the type of their flip and double flip.



### 3. Addition

In this section, we describe how to add two distinct reduced divisors. Analogous to [11], we make use of certain Riemann–Roch spaces. For any nonzero function  $f \in K[C]$ , denote by  $\text{LM}(f)$  the leading monomial of  $f$ . Let  $m \in K[C]$  be a monomial and  $D$  an effective divisor in  $\text{Div}_K^0(C)$ . Define

$$W^m = \mathcal{L}(-\text{ord}_{P_\infty}(m)P_\infty) = \{f \in K[C] \mid \text{LM}(f) \leq m\},$$

$$W_D^m = \mathcal{L}(-\text{ord}_{P_\infty}(m)P_\infty - D) = \{f \in I_D \mid \text{LM}(f) \leq m\} = W^m \cap I_D.$$

Given a reduced Gröbner basis for  $I_D$ , it is easy to construct an echelon basis for  $W_D^m$  by taking monomial multiples of the basis elements and removing all those that result in duplicate leading monomials. Given an echelon basis for  $W_D^m$  with  $m$  sufficiently large, a reduced Gröbner basis for  $I_D$  can be obtained by removing any basis element whose leading monomial is divisible by that of another basis element.

Now let  $D, D'$  be distinct reduced divisors of respective degrees  $d = \deg(D)$  and  $d' = \deg(D')$ , with  $d \geq d'$ . Let  $m$  be the largest monomial appearing in the reduced Gröbner basis of any ideal  $I$  such that  $\text{div}(I)$  has degree  $d + d'$ . For example, if  $d + d' = 6$ , then the reduced Gröbner basis of an ideal of a type 64 divisor contains a polynomial with leading monomial  $m = x^4$ , and no other degree 6 divisor type has a larger monomial.

Put  $L = \text{lcm}(D, D')$  and  $G = \text{gcd}(D, D')$ . The divisors  $L$  and  $G$  arise from the kernel and image, respectively, of the matrix  $M$  in the diagram below. Here,  $\iota$  denotes inclusion and  $\pi$  is the natural projection:

$$W_L^m \xrightarrow{\ker M} W_D^m \xrightarrow{\quad \quad \quad} W^m \xrightarrow{\quad \quad \quad} \frac{W^m}{W_{D'}^m} \xrightarrow{\text{im } M} \frac{W_G^m}{W_{D'}^m}$$

$\begin{array}{c} \text{---} M \text{---} \\ \nearrow \quad \quad \searrow \\ \iota \quad \quad \quad \pi \end{array}$

A proof of this crucial result can be found in [10, Theorem 8.7]. This is a generalization of the addition procedure of [11], where the authors compute  $\ker M$  for  $m = x^2y$  only. This is sufficient when  $D$  and  $D'$  are disjoint (or equivalently,  $G = 0$ ) and typical, but their approach fails otherwise. A larger bounding monomial  $m$  can handle atypical divisor sums, and computing the image  $\text{im } M$  allows nondisjoint input divisors  $D, D'$ .

The kernel and image of  $M$  are obtained by first computing the reduced row echelon form of  $M$ , denoted  $\text{RREF}(M)$ , which in particular reveals the rank of  $M$  as well as the dimensions of its kernel and image. If  $M$  has full rank, which is typically the case, then  $G = 0$  and  $\ker M$  produces a reduced Gröbner basis for  $I_L = I_{D+D'}$ . If  $M$  has rank 0, then  $D' < D$ , in which case we find the divisor  $A$  such that  $D = D' + A$  and return  $\overline{2D'} + A$  via a call to the doubling algorithm in Section 4. Otherwise, we recursively compute the sum  $\overline{L} + G$ . In this recursive call, one of the input divisors has degree strictly less than  $d'$ , so this recursion terminates. Details of the algorithm and toy examples can be found in [10, Chapter 8].



#### 4. Doubling

Doubling a reduced divisor  $D$  is similar to adding two distinct reduced divisors. Here, we find a (not necessarily reduced) divisor  $A \neq D$  equivalent to  $D$  and compute the reduction  $\overline{A+D} = \overline{2D}$  using the addition algorithm from [Section 3](#). We describe an optimized approach for finding  $A$  that represents a significant improvement over the doubling method presented in [\[10, Chapter 9\]](#).

We begin with the most common case when  $D$  is a type 31 divisor. Let  $\{f, g, h\}$  be a reduced Gröbner basis of its associated ideal  $I_D$ .

**Lemma 4.1.** *Let  $D$  be of type 31. Then there exist polynomials*

$$\begin{aligned} r &= y + r_0, & s &= -(x + s_0), & t &= t_0, \\ r' &= x^2 + r'_2 y + r'_1 x + r'_0, & s' &= s'_0, & t' &= y + t'_0, \\ r'' &= r''_0, & s'' &= y + s''_0, & t'' &= x + t''_0 \end{aligned}$$

in  $K[C]$  such that  $rf + sg + th = 0$ ,  $r'f + s'g + t'h = F$  and  $r''f + s''g + t''h = 0$ .

*Proof.* Explicit formulas for  $r, s, t, r', s', t'$  are given in [Table 6.2](#). The polynomials  $r'' = h_1$ ,  $s'' = y - g_1 + h_2$  and  $t'' = -x - g_2$ , with  $g_1, g_2, h_1, h_2$  as given in [\(6-1\)](#), are easily verified to satisfy the third identity.  $\square$

The quantities  $r'', s'', t''$  are only auxiliary to the proof of [Proposition 4.2](#). Put

$$A = \text{div}(\tilde{f}, \tilde{g}, \tilde{h}) \quad \text{with } \tilde{f} = st' - ts', \quad \tilde{g} = tr' - rt', \quad \tilde{h} = rs' - sr'. \quad (4-1)$$

Then the leading monomials of  $\tilde{f}, \tilde{g}, \tilde{h}$  are  $xy, y^2, x^3$ , respectively, so  $A$  is of type 41 by [Table 2.1](#). It is easy to verify that  $\tilde{f}\tilde{g} = g\tilde{f}$  and  $\tilde{f}\tilde{h} = h\tilde{f}$  in  $K[C]$ . It follows that  $\tilde{f}I_D = \tilde{f}I_A$  and hence  $\text{div } \tilde{f} + A = \text{div } \tilde{f} + D$ , so  $A$  is equivalent to  $D$ .

The following proposition shows that  $A$  and  $D$  are typically disjoint. If not, we have  $D \not\subseteq A$ . Either way, we may add  $D$  and  $A$  using the addition algorithm from the previous section.

**Proposition 4.2.** *Let  $D$  be of type 31 and put  $G = \text{gcd}(D, A)$ . If  $D$  is typical, then  $G = 0$ , otherwise  $G$  has degree 1.*

*Proof.* We have  $\deg(G) \leq \deg(D) = 3$ . Suppose  $\deg(G) \geq 2$ . Then  $D - G$  and  $A - G$  are equivalent divisors of degree  $\leq 2$ . So these two divisors are reduced and hence equal, which is impossible since  $\deg(D) \neq \deg(A)$ . It follows that  $\deg(G) \leq 1$ .

Suppose  $\deg(G) = 1$ . Then  $\deg(D - G) = 2$ ,  $\deg(A - G) = 3$  and  $\overline{D - G} = \overline{A - G}$ , which by [Table 2.2](#) forces  $D - G$  to be of type 22 and  $A - G$  to be of type 32. Let  $x + a$  and  $x + b$  be the minimum polynomials of  $I_G$  and  $I_{D-G}$ , respectively. Then  $f = (x + a)(x + b) \in I_D$ . Appealing to the form of  $I_D$  characterized in [Table 2.1](#),  $f$  is the minimum polynomial of  $I_D$  and has a vanishing  $y$ -coefficient, so  $D$  is atypical.

Conversely, suppose that  $D$  is atypical. Referring to the quantities of [Lemma 4.1](#), we have  $t = -f_2 = 0$ . Put  $I = \langle r, s \rangle$ . Then  $I$  is a prime ideal of degree 1. From [\(4-1\)](#), we see that  $I_A \subseteq I$ . A simple symbolic

computation yields  $f = st''$ ,  $g = rt''$  and  $h = r''s - s''r$ , so  $I_D \subseteq I$ . It follows that  $I_G = I_A + I_D \subseteq I$ , so  $\text{div}(I) \leq G$ , which in turn implies  $\deg(G) \geq 1$ , and hence  $\deg(G) = 1$ .  $\square$

An optimization is possible when computing the kernel of  $M$  in

$$W_L^m \xrightarrow{\ker M} W_A^m \xrightarrow{\iota} W^m \xrightarrow{\pi} \frac{W^m}{W_D^m} \xrightarrow{\text{im } M} \frac{W_G^m}{W_D^m}.$$

$M$

The kernel consists of  $K[C]$ -linear combinations of  $\{\tilde{f}, \tilde{g}, \tilde{h}\}$  that belong to  $W_L^m$ . However, the following theorem shows that when  $D$  is typical, we may instead perform our computations on  $f, g, h$ . The latter have fewer monomials, so the resulting linear combinations are faster to generate.

**Theorem 4.3.** *Let  $D$  be of type 31,  $L = \text{lcm}(D, A)$  and  $G = \text{gcd}(D, A)$ . Let  $a, b, c \in K[C]$ . Then  $af + bg + ch \in I_{2D-G}$  if and only if  $a\tilde{f} + b\tilde{g} + c\tilde{h} \in I_L$ .*

*Proof.* We have  $2D - G + \text{div}(\tilde{f}) = L + D - A + \text{div}(\tilde{f}) = L + \text{div}(f)$ . Since  $f\tilde{g} = g\tilde{f}$  and  $f\tilde{h} = h\tilde{f}$ , the claim follows.  $\square$

If  $D$  is typical, then  $I_{2D-G} = I_{2D}$  by [Proposition 4.2](#).

Next, we provide analogous results for divisors  $D$  of types 11, 21, and 22. Here,  $I_D = \langle f, g \rangle$ .

**Theorem 4.4.** *Let  $D$  be of type 11, 21, or 22, and write  $I_D = \langle f, g \rangle$ . Then there exist nonzero polynomials  $\tilde{f}, \tilde{g} \in K[C]$  such that  $f\tilde{g} + g\tilde{f} = F$  and  $\tilde{f}\langle f, g \rangle = f\langle \tilde{f}, \tilde{g} \rangle$ . The divisor  $A = \text{div}(\tilde{f}, \tilde{g})$  is equivalent to  $D$  and  $\text{gcd}(A, D) = 0$ . Finally, for any  $a, b \in K[C]$ , we have  $af + bg \in I_{2D}$  if and only if  $a\tilde{f} + b\tilde{g} \in I_{A+D}$ .*

*Proof.* The first assertion follows from  $F \in \langle f, g \rangle$ . Since  $f\tilde{g} = -g\tilde{f}$  in  $K[C]$ , we have  $\tilde{f}\langle f, g \rangle = \langle f\tilde{f}, g\tilde{f} \rangle = \langle f\tilde{f}, f\tilde{g} \rangle = f\langle \tilde{f}, \tilde{g} \rangle$ , so  $\text{div}(\tilde{f}) + D = \text{div}(f) + A$ . This identity also yields the last assertion, provided that  $\text{gcd}(A, D) = 0$ .

Suppose first that  $D$  is of type 11. Then the leading monomials of  $f$  and  $g$  are  $x$  and  $y$ , respectively. A solution to  $f\tilde{g} + g\tilde{f} = F$  then requires that the leading monomials of  $\tilde{f}$  and  $\tilde{g}$  are  $y^2$  and  $x^3$ , respectively. Therefore  $A = \text{div}(\tilde{f}, \tilde{g})$  is a type 62 divisor. Suppose  $\text{gcd}(A, D) \neq 0$ . Then  $A - D$  would be a principal divisor of degree 5 which is impossible by [Table 2.1](#).

Likewise, suppose  $D$  is of type 21. Then  $A = \text{div}(\tilde{f}, \tilde{g})$  is of type 43. Suppose  $G = \text{gcd}(A, D) \neq 0$ . Since  $A - G \equiv D - G$ , we either have a degree 3 divisor that is equivalent to a degree 1 divisor, or a degree 2 divisor that is equivalent to 0, depending on the degree of  $G$ . Appealing to [Table 2.1](#), we see that both cases are impossible. The case when  $D$  is of type 22 is similar.  $\square$

Our addition and doubling routines call one another, but this process terminates. The doubling routine terminates on all inputs except atypical type 31 divisors ([Proposition 4.2](#)), in which case we must add  $\bar{L} + G$  where  $\deg G = 1$  and there is no need to subsequently double another type 31 divisor. Furthermore, the addition routine may call itself, but the degree of the smaller divisor strictly decreases, forcing it to eventually terminate.

## 5. Reduction

Reducing a divisor may be accomplished by flipping it twice, as was done in [2; 11]. However, in [8], it was shown that for typical degree 6 divisors, both flips can be combined into a single operation that is more efficient than even just the first flip. Below, we generalize this result to all typical and nonsemityypical divisors (of any degree). The remaining divisors, those that are semityypical but atypical, are addressed in [Theorem 5.2](#).

**Theorem 5.1.** *Let  $D$  be an effective divisor on  $C$  and let  $\{u, v\}$  be any generating set for  $I_D$  such that  $u$  is the minimum polynomial of  $I_D$ . Then there exist polynomials  $f, g \in K[C]$  such that  $fv = gu$  in  $K[C]$  and  $\bar{\bar{D}} = \text{div}(f, g)$ .*

*Proof.* Let  $f$  be the minimum polynomial of the colon ideal  $u : v$ . Then there exists  $g \in K[C]$  such that  $fv = gu$  in  $K[C]$ . The divisor  $A = \text{div}(f, g)$  is equivalent to  $D$  since  $uI_A = \langle fu, gu \rangle = \langle fu, fv \rangle = fI_D$ . The minimality of  $u$  and  $f$  implies that  $A$  is reduced and is hence the reduction of  $D$ .  $\square$

In particular, [Theorem 5.1](#) makes efficient reduction of all divisors listed in [Table 2.1](#) straightforward, except for atypical semityypical divisors, where  $I_D$  might be generated by no two of its Gröbner basis elements. Given  $I_D = \langle u, v \rangle$ , the type of  $\bar{\bar{D}}$  is first read from [Table 2.2](#). Then the leading monomials of  $f, g$ , with  $I_{\bar{\bar{D}}} = \langle f, g \rangle$ , are obtained from [Table 2.1](#). The coefficients of  $f, g$  are now easily computed by equating coefficients in the relation  $fv \equiv gu \pmod{F}$  and solving the resulting system of linear equations.

Reduction of atypical semityypical divisors is done via [Theorem 5.2](#) which represents an improvement for type 41 and 51 divisors over the method presented in [10, Section 10.1].

**Theorem 5.2.** *Let  $D$  be an atypical semityypical divisor, and write  $I_D = \langle f, g, h \rangle$ . Put  $I = \langle f, g \rangle$ . Then there exist  $K$ -rational points  $P, Q$  on  $C$  such that  $\text{div}(I) = D + (P - P_\infty)$  and  $\overline{\text{div}(I)} = Q - P_\infty$ .*

*Proof.* We have  $\deg \text{div}(I) = \dim_K(K[C]/I)$  and  $\deg D = \dim_K(K[C]/I_D)$ . Computing these dimensions for each atypical case using [Table 2.1](#) (the dimensions are determined by the leading coefficients of  $f$  and  $g$ ) yields  $\deg \text{div}(I) = \deg D + 1$  which establishes the existence of  $P$ .

Analogous to [Lemma 4.1](#), there exist polynomials  $r = x + r_0, s = y + s_1x + s_0 \in K[C]$  such that  $fs + gr = F$  when  $D$  is of type 51 and  $fs = gr$  otherwise. Since  $\text{div}(r, s)$  has degree 1, it is reduced and of the form  $Q - P_\infty$ . As in the proof of [Theorem 5.1](#), we see that  $I$  is equivalent to  $\langle r, s \rangle$ , which is hence the reduction of  $\text{div}(I)$ .  $\square$

**Corollary 5.3.**  $\bar{\bar{D}} = (Q - P_\infty) + \overline{P - P_\infty}$ .

*Proof.* By [Theorem 5.2](#),  $D = \text{div}(I) - (P - P_\infty)$  and  $\overline{\text{div}(I)} = Q - P_\infty$ . The reduced divisor equivalent to  $-(P - P_\infty)$  is  $\overline{P - P_\infty}$ . It follows that  $\bar{\bar{D}}$  is equivalent to  $(Q - P_\infty) + \overline{P - P_\infty}$ . Since  $\bar{\bar{D}}$  is reduced and both  $\bar{\bar{D}}$  and  $(Q - P_\infty) + \overline{P - P_\infty}$  have the same degree, they must both be reduced and therefore equal.  $\square$

Obtaining  $P$  amounts to finding polynomials  $p = x + p_0$  and  $q = y + q_1x + q_0$  such that  $hp, hq \in I$ . The polynomials  $r$  and  $s$  of [Theorem 5.2](#) determine  $Q$ .

## 6. Explicit formulas for typical divisors

Here, we derive explicit formulas handling the most typical cases in  $C_{3,4}$  arithmetic: adding disjoint type 31 divisors whose sum is typical, and doubling a typical type 31 divisor whose double is typical. If ever we detect that we are outside these cases, we may fall back on another series of explicit formulas.

Let  $D$  and  $D'$  be typical type 31 divisors, with respective associated ideals and Gröbner bases  $I_D = \langle f, g, h \rangle$  and  $\langle f', g', h' \rangle$ , where

$$\begin{aligned} f &= x^2 + f_2y + f_1x + f_0, & f' &= x^2 + f'_2y + f'_1x + f'_0, \\ g &= xy + g_2y + g_1x + g_0, & g' &= xy + g'_2y + g'_1x + g'_0, \\ h &= y^2 + h_2y + h_1x + h_0, & h' &= y^2 + h'_2y + h'_1x + h'_0. \end{aligned} \quad (6-1)$$

The optimal choice of monomial in the addition and doubling algorithms of [Section 3](#) and [Section 4](#) is  $m = x^2y$ . Bases for the vector spaces  $W_D^{x^2y}$  and  $W_{D'}^{x^2y}$  are  $\{f, g, h, xf, xg\}$  and  $\{f', g', h', xf', xg'\}$ , respectively. The matrix

$$M = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_6 & a_7 & a_8 & a_9 & a_{10} \\ a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \end{pmatrix}$$

for adding  $D$  and  $D'$  is constructed by reducing the former basis modulo the latter; e.g., the reduction of  $f$  modulo  $\{f', g', h', xf', xg'\}$  is  $(f_2 - f'_2)y + (f_1 - f'_1)x + (f_0 - f'_0)$ , so  $a_1 = f_0 - f'_0$ ,  $a_6 = (f_1 - f'_1)$ , etc. Computing the first three columns requires only subtractions (counted as additions). The last two columns are given in terms of the first two by

$$\begin{pmatrix} a_4 & a_5 \\ a_9 & a_{10} \\ a_{14} & a_{15} \end{pmatrix} = \begin{pmatrix} 0 & -f'_0 & -g'_0 \\ 1 & -f'_1 & -g'_1 \\ 0 & -f'_2 & -g'_2 \end{pmatrix} \begin{pmatrix} a_1 & a_2 \\ a_6 & a_7 \\ a_{11} & a_{12} \end{pmatrix}.$$

For doubling  $D$ , we construct the divisor  $A$  defined in [Section 4](#) using the polynomials defined in (4-1) and [Lemma 4.1](#). Then the left three columns of the matrix  $M$  used in the computation of  $D + A$  are the reductions of  $\tilde{f}, \tilde{g}, \tilde{h}$  modulo  $f, g, h$ . Let  $e_1 = -(f_1 + g_2)$  and  $e_2 = r'_2 - f_2$ . Then the left three columns of  $M$  are

$$\begin{pmatrix} t'_0s_0 + s'_0t_0 - g_0 & t'_0r_0 + t_0(f_0 - r'_0) - h_0 & f_0e_1 + g_0e_2 - s'_0r_0 - r'_0s_0 \\ t'_0 - g_1 & t_0(f_1 + f_1) - h_1 & f_1(e_1 + s_0) + g_1e_2 - r'_0 + f_0 \\ s_0 - g_2 & t'_0 - h_2 + r_0 - t_0e_2 & f_2(e_1 - g_2) + r'_2(g_2 - s_0) - s'_0 \end{pmatrix}.$$

The right two columns relate to the first three as above, with  $D$  in place of  $D'$ .

If the first column is zero, then  $D + D'$  (or  $D + A$ ) is atypical and we must fall back on other formulas. Otherwise, we assume  $a_1 \neq 0$  by swapping rows if necessary. Then elementary row operations convert

$M$  into row echelon form:

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_6 & a_7 & a_8 & a_9 & a_{10} \\ a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \end{pmatrix} \longrightarrow \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ 0 & b_1 & b_2 & b_3 & b_4 \\ 0 & 0 & b_5 & b_6 & b_7 \end{pmatrix}.$$

If  $b_1$  or  $b_5$  are zero, then  $D + D'$  (or  $D + A$ ) either contains points of multiplicity exceeding 1 or is atypical. To avoid an expensive inversion operation, we compute a scalar multiple of the reduced row echelon form  $\text{RREF}(M)$  and defer the necessary inversion until later:

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ 0 & b_1 & b_2 & b_3 & b_4 \\ 0 & 0 & b_5 & b_6 & b_7 \end{pmatrix} \longrightarrow \begin{pmatrix} Z & 0 & 0 & A_1 & A_2 \\ 0 & Z & 0 & B_1 & B_2 \\ 0 & 0 & Z & C_1 & C_2 \end{pmatrix}.$$

Now  $\ker(M) = \text{Span}_K\{U, V\}$ , where

$$U = Zxf - C_1h - B_1g - A_1f, \quad V = Zxg - C_2h - B_2g - A_2f.$$

Let

$$U = Zx^3 + U_5y^2 + \cdots + U_0 \quad \text{and} \quad V = Zx^2y + V_5x^2y + \cdots + V_0.$$

Formulas for the coefficients  $U_i, V_i$  are found in [Table 6.3](#), although note that the constant coefficients  $U_0$  and  $V_0$  are not needed and therefore not computed. Let  $u_0, \dots, u_5, v_0, \dots, v_5$  be the coefficients of  $u := U/Z$  and  $v := V/Z$ . To compute  $u_i, v_i$ , we will need the inverse of  $Z$ . However, we will also need the inverse of  $f_2'' = u_5^2 + u_4 - v_5$  later on. We compute both inverses at once with only a single inversion using a variation of Montgomery's Trick. Formulas for  $\zeta := Z^{-1}$  and  $\tau := (f_2'')^{-1}$  are found in [Table 6.3](#). We note that the intermediate value  $z_0$  is equal to  $Z^2 f_2''$ . If this is zero, then the sum is atypical and we fall back on other formulas. Once  $\zeta$  is known, we compute  $u_i = \zeta U_i$  and  $v_i = \zeta V_i$  for  $i = 1, \dots, 5$ .

Now  $I_{D+D'}$  (or  $I_{2D}$ ) is generated by  $\{u, v\}$ . We apply [Theorem 5.1](#) and find polynomials

$$f'' = x^2 + f_2''y + f_1''x + f_0'' \quad \text{and} \quad g'' = xy + g_3''x^2 + g_2''y + g_1''x + g_0''$$

satisfying

$$f''v \equiv g''u \pmod{F}.$$

We would then have to reduce  $g''$  modulo  $f''$  to eliminate the  $x^2$  term in  $g''$ . Since  $g_3'' = u_5$ , this means subtracting  $u_5$  times  $f''$  from  $g''$ . We avoid this by instead finding  $g'' = xy + g_2''y + g_1''x + g_0''$  such that  $f''v \equiv (g'' + u_5 f'')u \pmod{F}$ , thereby saving a multiplication and a few additions.

The third polynomial in the Gröbner basis of  $I_{D+D'}$  (or  $I_{2D}$ ) is

$$h'' = \tau((y + g_1'')f'' - (x + f_1'' - g_2'')g'').$$

Explicit formulas and operation counts for all the quantities above are given in [Tables 6.1, 6.2, and 6.3](#).

Addition	12M+17A
Input: $I_D = \langle f, g, h \rangle, I_{D'} = \langle f', g', h' \rangle$ $f = x^2 + f_2y + f_1x + f_0, f' = x^2 + f'_2y + f'_1x + f'_0$ $g = xy + g_2y + g_1x + g_0, g' = xy + g'_2y + g'_1x + g'_0$ $h = y^2 + h_2y + h_1x + h_0, h' = y^2 + h'_2y + h'_1x + h'_0$ Output: $M_{\text{add}} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_6 & a_7 & a_8 & a_9 & a_{10} \\ a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \end{pmatrix}$	
Compute elements $a_i$ of $M_{\text{add}}$	12M+17A
$a_1 = f_0 - f'_0$ $a_2 = g_0 - g'_0$ $a_3 = h_0 - h'_0$ $a_4 = -f'_0a_6 - g'_0a_{11}$ $a_5 = -f'_0a_7 - g'_0a_{12}$ $a_6 = f_1 - f'_1$ $a_7 = g_1 - g'_1$ $a_8 = h_1 - h'_1$ $a_9 = a_1 - f'_1a_6 - g'_1a_{11}$ $a_{10} = a_2 - f'_1a_7 - g'_1a_{12}$ $a_{11} = f_2 - f'_2$ $a_{12} = g_2 - g'_2$ $a_{13} = h_2 - h'_2$ $a_{14} = -f'_2a_6 - g'_2a_{11}$ $a_{15} = -f'_2a_7 - g'_2a_{12}$ If $a_1 = a_6 = a_{11} = 0$ , then abort. If $a_1 = 0$ is zero but $a_6 \neq 0$ or $a_{11} \neq 0$ , then swap rows so $a_1 \neq 0$ .	

Table 6.1. Construction of matrix  $M$  — typical addition.

## 7. Implementation and testing

A Sage implementation of  $C_{3,4}$  curve arithmetic based on the algorithms in this paper is available at [9]. This implementation includes optimized addition and doubling subroutines `fast_add_31_31`, `fast_add_31_31_high_char`, `fast_double_31`, and `fast_double_31_high_char`. The high characteristic versions assume that the curve equation is given in short form and implement the formulas in Tables 6.1, 6.2, and 6.3. The other versions implement similar formulas with no assumptions on the coefficients  $c_5$ ,  $c_6$ , and  $c_8$ . The optimized subroutines assume the typical cases described in Section 6. When any of these assumptions are violated, an exception is thrown, and a less-optimized subroutine is called instead.

The less-optimized subroutines are nonetheless implemented via explicit formulas. These include addition subroutines for every pair of reduced divisor types (e.g., `add_31_21`), a doubling subroutine for every reduced divisor type (e.g., `double_31`), and a reduction subroutine for every unreduced divisor type (e.g., `reduce_61`).

Addition subroutines, given input divisors  $D$  and  $D'$ , compute  $L = \text{lcm}(D, D')$  and  $G = \text{gcd}(D, D')$  by computing the kernel and image of a matrix as described in Section 3. If  $G = 0$ , then the reduction of  $L$  is computed via the appropriate subroutine and  $\bar{L}$  is returned. Otherwise  $\bar{L}$  and  $G$  are added by calling another addition subroutine. The cost of evaluating  $D + D'$  depends on the type of  $L$ . Costs are given in Table 7.1(A) for the cases when  $G = 0$ . When  $G > 0$ , one or more recursive calls must be made. A full analysis of the cost in these cases was not done, due to the large number of subcases that can occur.

Doubling	28M+1S+41A
Input: $I_D = \langle f, g, h \rangle$ $f = x^2 + f_2y + f_1x + f_0$ , $g = xy + g_2y + g_1x + g_0$ , $h = y^2 + h_2y + h_1x + h_0$ Output: $M_{\text{doub}} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_6 & a_7 & a_8 & a_9 & a_{10} \\ a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \end{pmatrix}$	
Compute polynomials $r = y + r_0$ , $s = -(x + s_0)$ , $t = t_0$ such that $rf + sg + th = 0$	1A
$r_0 = g_1$ $s_0 = f_1 - g_2$ $t_0 = -f_2$	
Compute polynomials $r' = x^2 + r'_2y + r'_1x + r'_0$ , $s' = s'_0$ , $t' = y + t'_0$ such that $r'f + s'g + t'h = F$	2M+1S+7A
$r'_2 = c_7 - f_2$ $r'_1 = -f_1$ $t'_0 = -h_2 - f_2r'_2$ $s'_0 = c_4 - h_1 + f_1(f_2 - r'_2)$ $r'_0 = c_3 + f_1^2 - f_0$	
Compute reductions $\bar{f} = \tilde{f}_2y + \tilde{f}_1x + \tilde{f}_0$ , $\bar{g} = \tilde{g}_2y + \tilde{g}_1x + \tilde{g}_0$ , $\bar{h} = \tilde{h}_2y + \tilde{h}_1x + \tilde{h}_0$	14M+25A
$e_1 = -f_1 - g_2$ $e_2 = r'_2 - f_2$ $\tilde{f}_2 = s_0 - g_2$ $\tilde{f}_1 = t'_0 - g_1$ $\tilde{f}_0 = t'_0s_0 + s'_0t_0 - g_0$ $\tilde{g}_2 = t'_0 - h_2 + r_0 - t_0e_2$ $\tilde{g}_1 = t_0(f_1 + f_1) - h_1$ $\tilde{g}_0 = t'_0r_0 + t_0(f_0 - r'_0) - h_0$ $\tilde{h}_2 = f_2(e_1 - g_2) + r'_2(g_2 - s_0) - s'_0$ $\tilde{h}_1 = f_1(e_1 + s_0) + g_1e_2 - r'_0 + f_0$ $\tilde{h}_0 = f_0e_1 + g_0e_2 - s'_0r_0 - r'_0s_0$	
Compute matrix $M_{\text{doub}}$	12M+8A
$a_1 = \tilde{f}_0$ $a_2 = \tilde{g}_0$ $a_3 = \tilde{h}_0$ $a_4 = -f_0a_6 - g_0a_{11}$ $a_5 = -f_0a_7 - g_0a_{12}$ $a_6 = \tilde{f}_1$ $a_7 = \tilde{g}_1$ $a_8 = \tilde{h}_1$ $a_9 = a_1 - f_1a_6 - g_1a_{11}$ $a_{10} = a_2 - f_1a_7 - g_1a_{12}$ $a_{11} = \tilde{f}_2$ $a_{12} = \tilde{g}_2$ $a_{13} = \tilde{h}_2$ $a_{14} = -f_2a_6 - g_2a_{11}$ $a_{15} = -f_2a_7 - g_2a_{12}$ If $a_1 = a_6 = a_{11}$ , then abort. If $a_1 = 0$ but $a_6 \neq 0$ or $a_{11} \neq 0$ , then swap rows so $a_1 \neq 0$ .	

**Table 6.2.** Construction of matrix  $M$  — typical doubling.

Doubling subroutines, given an input divisor  $D$ , find generators for a divisor  $A$  equivalent to  $D$ , and compute  $G = \gcd(A, D)$  and  $2D - G$  as outlined in [Section 4](#). We recursively compute  $\overline{2D - G} + G$ . The cost depends on the type of  $2D - G$ , if  $G = 0$ , and if a recursive call must be made. [Table 7.1\(B\)](#)

Computing $\ker M$	11+99M+3S+72A
<p>Input: <math>I_D = \langle f, g, h \rangle, M</math></p> $f = x^2 + f_2y + f_1x + f_0, \quad g = xy + g_2y + g_1x + g_0, \quad h = y^2 + h_2y + h_1x + h_0$ $M = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_6 & a_7 & a_8 & a_9 & a_{10} \\ a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \end{pmatrix}$ <p>Output: <math>I_{D+D'} = \langle f'', g'', h'' \rangle</math> (or <math>I_{2D} = \langle f'', g'', h'' \rangle</math>)</p> $f'' = x^2 + f_2''y + f_1''x + f_0'', \quad g'' = xy + g_2''y + g_1''x + g_0'', \quad h'' = y^2 + h_2''y + h_1''x + h_0''$	
Compute row echelon form of $M$	21M+12A
$d_1 = a_1a_{12} - a_2a_{11} \quad d_2 = a_6a_{12} - a_7a_{11}$ $b_1 = a_1a_7 - a_2a_6 \quad b_2 = a_1a_8 - a_3a_6 \quad b_3 = a_1a_9 - a_4a_6$ $b_4 = a_1a_{10} - a_5a_6 \quad b_5 = b_1a_{13} - d_1a_8 + d_2a_3 \quad b_6 = b_1a_{14} - d_1a_9 + d_2a_4$ $b_7 = b_1a_{15} - d_1a_{10} + d_2a_5$	
Compute $Z \cdot \text{RREF}(M)$	18M+6A
$Y = a_1b_1 \quad Z = Yb_5$ $e_1 = b_3b_5 - b_2b_6 \quad e_2 = b_4b_5 - b_2b_7$ $A_1 = b_1(a_4b_5 - b_6a_3) - a_2e_1 \quad B_1 = a_1e_1 \quad C_1 = Yb_6$ $A_2 = b_1(a_5b_5 - b_7a_3) - a_2e_2 \quad B_2 = a_1e_2 \quad C_2 = Yb_7$	
Compute $\ker(M)$	18M+14A
$U_1 = Zf_0 - C_1h_1 - B_1g_1 - A_1f_1 \quad U_2 = -C_1h_2 - B_1g_2 - A_1f_2$ $U_3 = Zf_1 - A_1 \quad U_4 = Zf_2 - B_1 \quad U_5 = -C_1$ $V_1 = Zg_0 - C_2h_1 - B_2g_1 - A_2f_1 \quad V_2 = -C_2h_2 - B_2g_2 - A_2f_2$ $V_3 = Zg_1 - A_2 \quad V_4 = Zg_2 - B_2 \quad V_5 = -C_2$	
Compute $\zeta = Z^{-1}, \tau = (f_2'')^{-1}$	11+5M+2S+3A
$z_0 = U_5^2 + Z(U_4 - V_5) \quad z_1 = Zz_0 \quad z_2 = z_1^{-1} \quad z_3 = Zz_2 \quad \zeta = z_0z_2 \quad \tau = Z^2z_3$	
Compute $u_1, \dots, u_5, v_1, \dots, v_5$	10M
$u_1 = \zeta U_1 \quad u_2 = \zeta U_2 \quad u_3 = \zeta U_3 \quad u_4 = \zeta U_4 \quad u_5 = \zeta U_5$ $v_1 = \zeta V_1 \quad v_2 = \zeta V_2 \quad v_3 = \zeta V_3 \quad v_4 = \zeta V_4 \quad v_5 = \zeta V_5$	
Compute $f'', g'', h''$	27M+1S+37A
$r_0 = u_5(f_2'' + u_4 - c_7) + u_3 - v_4 \quad r_1 = f_2''(f_2'' - u_4)$ $g_0'' = u_5(c_3 - f_0'' - u_1 - f_1''u_3) - g_1''u_3 + f_1''v_3 + v_1$ $g_1'' = r_1 - u_5(u_3 + r_0) + v_3 \quad g_2'' = -u_4u_5 + v_4 - r_0 + \tau(u_4r_0 - u_5g_1'' - u_2)$ $f_0'' = -c_7(r_1 + g_2''u_5) + u_5(f_2''u_3 + f_1''u_4 - c_4 + u_2) + g_2''u_3 + g_1''u_4 - f_2''v_3 - f_1''v_4 + u_1 - v_2$ $f_1'' = r_0 + g_2'' \quad f_2'' = u_5^2 + u_4 - v_5$ $h_0'' = \tau(f_0''g_1'' - g_0''r_0) \quad h_1'' = \tau(g_1''g_2'' - g_0'') \quad h_2'' = g_1'' + \tau(f_0'' - g_2''r_0)$	

Table 6.3. Computing  $\ker M$ .



contains the costs for the cases where  $G = 0$ . Here, “t” and “a” under the type column refer to typical and atypical divisors, respectively.

Our operation counts for the high characteristic formulas compare to the previous state of the art in [8] as follows:

	Addition	Doubling
Khuri-Makdisi [8]	2I+97M+1S+132A	2I+107M+3S+155A
This work	1I+111M+3S+99A	1I+127M+4S+112A

These counts include a trade-off of one inversion for several multiplications. An inversion is generally considered to be as expensive as 80 multiplications, depending on implementation and environment details [3; 5]. Our formulas also significantly decrease the number of additions required, and the total number of field operations in both of our formulas is less than that of [8]. Over large fields such as those considered in [8], additions are generally considered to have negligible cost compared to multiplications and inversions, but in number theoretic computations such as [13] over smaller (typically word-sized) primes, this has been observed not to be the case.

To verify that our results represent an improvement over the previous state-of-the-art, we implemented the formulas from [11] and [8] in Sage and ran benchmark tests as follows. Given a prime  $p$ , choose a random  $C_{3,4}$  curve  $C$  over  $\mathbb{F}_p$  (with defining polynomial in short form) and two random divisors  $D_1$  and  $D_2$  on  $C$ . Details on random divisor generation are given in Section 12.2 of [10]. We counted how many terms in the Fibonacci-like sequence  $D_{i+2} = D_{i+1} + D_i$ ,  $i \geq 1$  (for addition) and the sequence  $D_{i+1} = 2D_i$ ,  $i \geq 1$  (for doubling) each algorithm is able to compute in 10 minutes. We chose to run these tests over the first 23 primes greater than  $2^{28}$ , as primes on this order are of interest in number theoretic applications (see [14], for example), and because degenerate cases are so rare that we can strictly compare our formulas to those of [11] and [8]. Our algorithm computed 126,310,162 additions as compared to 112,041,012 using the algorithm from [8], for a speedup of 12.74%. Similarly, our algorithm computed 120,827,482 doublings as compared to 108,489,487 for a speedup of 11.37%.

This benchmark was repeated over the first 11 primes larger than  $2^{255}$ , where we found a more significant speed-up, likely due to the increasing cost of inverting in large finite fields. Our algorithm computed 63,151,623 additions versus 52,185,141 using the algorithm from [8], for a speedup of 21.01%. Similarly, our algorithm computed 56,795,783 doublings as compared to 48,395,712 for a speedup of 17.36%.

We found the most significant speed-up over very small primes, where atypical cases are frequently encountered and our explicit formulas are much faster than generic arithmetic. Over the ten largest primes below  $2^8$ , we compared our formulas against those of [11] and [8], falling back on Sage’s generic ideal arithmetic for cases not handled by those papers. Our algorithm computed 53,670,222 additions as compared to 31,685,426 using the algorithm from [8], for a speedup of 69.38%, and 48,156,514 doublings as compared to 39,152,564 for a speedup of 23.00%.

It is important to acknowledge the role that the implementation environment plays in these results. The benchmarks were run in the Sage interpreter, which adds significant overhead to the calculations.

Subroutine	Op count				Type of $L$
	I	M	S	A	
add_11_11	1	3	0	4	21
add_11_11	0	1	0	3	22
add_21_11	1	13	0	14	31
add_21_11	0	12	0	17	32
add_21_21	2	68	1	58	41-t
add_21_21	2	67	0	58	41-a
add_21_21	1	27	0	19	42
add_21_21	1	39	0	32	43
add_21_21	0	12	0	9	44
add_21_22	2	40	1	41	41-t
add_21_22	2	39	0	41	41-a
add_21_22	0	2	0	2	42
add_22_11	1	5	0	5	31-a
add_22_11	0	1	0	3	33
add_22_22	1	11	0	17	43
add_31_11	2	43	1	49	41-t
add_31_11	2	22	0	49	41-a
add_31_11	0	6	0	10	42
add_31_11	1	16	0	32	43
add_31_21	2	80	1	77	51-t
add_31_21	2	78	1	74	51-a
add_31_21	1	35	1	33	52
add_31_21	1	57	1	51	53
add_31_21	1	43	1	41	54
add_31_22	2	69	0	64	51-t
add_31_22	2	67	0	61	51-a
add_31_22	1	24	0	20	52
add_31_22	1	46	0	38	53
add_31_22	1	36	0	29	54
fast_add_31_31_high_char	1	111	3	99	61-t
fast_add_31_31	1	114	2	102	61-t
add_31_31	2	127	0	110	61-a
add_31_31	1	69	0	54	62
add_31_31	1	85	0	67	63
add_31_31	1	94	0	75	64
add_31_31	0	32	0	28	65

(A) Addition

Subroutine	Op count				Type of $2D - G$
	I	M	S	A	
double_11	1	15	1	20	21
double_11	0	8	1	13	22
double_21	2	86	1	85	41-t
double_21	2	85	0	85	41-a
double_21	1	50	0	47	42
double_21	1	60	0	60	43
double_21	0	7	0	12	44
double_22	1	22	0	22	42
double_22	1	25	0	29	43
fast_double_31_high_char	1	127	4	112	61
fast_double_31	1	138	2	130	61
double_31	2	159	0	156	61-t
double_31	2	152	0	149	61-a
double_31	1	94	0	90	62
double_31	1	110	0	103	63
double_31	1	119	0	111	64
double_31	0	57	0	64	65

(B) Doubling

Subroutine	Op count			
	I	M	S	A
reduce_32	0	8	0	11
reduce_33	0	0	0	0
reduce_41t	1	23	1	28
reduce_41a	1	22	0	28
reduce_42	0	0	0	1
reduce_43	0	6	0	11
reduce_44	0	0	0	0
reduce_51t	1	24	0	32
reduce_51a	1	22	0	29
reduce_52	0	1	0	3
reduce_53	0	12	0	14
reduce_54	0	7	0	10
reduce_61t	1	35	0	46
reduce_61a	1	28	0	39
reduce_62	0	2	0	5
reduce_63	0	8	0	13
reduce_64	0	12	0	21
reduce_65	0	0	0	0

(C) Reduction

Table 7.1. Operation counts for  $C_{3,4}$  arithmetic.

If implemented in a low level language, such as C/PARI, our improvements over [11; 8] may be more dramatic.

Correctness testing was accomplished by a combination of unit testing and random testing. Unit tests were constructed testing every branch of code in the addition, doubling, and reduction subroutines. These subroutines were also tested via hundreds of thousands of random inputs and the results were compared against Sage's vetted ideal arithmetic.

## 8. Conclusion

By generalizing the techniques of Abu Salem and Khuri-Makdisi [11] to atypical divisors as classified by Arita [2], we provided a fully general framework for efficient divisor arithmetic on  $C_{3,4}$  curves. Taken together with our additional improvements to the setting of typical divisors, we obtain speedups of between 11 and 21% depending on the field size, and even more for small fields were atypical cases arise more frequently.

There is room for further speed advances in  $C_{3,4}$  curve arithmetic, and work on this topic is ongoing. In our formulas for atypical divisors, addition/doubling and reduction are performed separately. Savings could be effected by combining these into a single optimized subroutine, as was done in Section 6 for the typical case. It is also possible to eliminate all inversions using an analogue of projective coordinates, but this would likely not help with number-theoretic computations where frequent equality tests of divisors are required.

Arithmetic on  $C_{3,4}$  curves continues to be significantly more expensive than arithmetic on genus 3 hyperelliptic curves. Preliminary results indicate that Shanks' NUCOMP algorithm [12] achieves significant savings in the latter setting, which raises the question whether a NUCOMP-like idea may be applied to  $C_{3,4}$  curve arithmetic as well.

## References

- [1] Seigo Arita, *Algorithms for computations in Jacobian group of  $C_{a,b}$  curve and their application to discrete-log-based public key cryptosystems*, Conference on the Mathematics of Public Key Cryptography (1999), 165–175.
- [2] Seigo Arita, *An addition algorithm in Jacobian of  $C_{3,4}$  curve*, IEICE Trans. Found. **E88-A** (2005), no. 6, 1589–1598.
- [3] Erik Dahmen, Katsuyuki Okeya, and Daniel Schepers, *Affine precomputation with sole inversion in elliptic curve cryptography*, Information Security and Privacy (Berlin, Heidelberg) (Josef Pieprzyk, Hossein Ghodosi, and Ed Dawson, eds.), Springer Berlin Heidelberg, 2007, pp. 245–258.
- [4] Stéphane Flon, Roger Oyono, and Christophe Ritzenthaler, *Fast addition on non-hyperelliptic genus 3 curves*, Algebraic geometry and its applications, Proceedings of the first SAGA conference, Ser. Number theory and its applications, vol. 4, World Sci. Publ., 2008, pp. 1–28.
- [5] Darrel Hankerson, Alfred Menezes, and Scott Vanstone, *Guide to elliptic curve cryptography*, Springer-Verlag, 2004.
- [6] David Harvey, Maike Massierer, and Andrew S. Sutherland, *Computing  $L$ -series of geometrically hyperelliptic curves of genus three*, LMS J. Comput. Math. **19** (2016), no. suppl. A, 220–234.
- [7] Kiran S. Kedlaya and Andrew V. Sutherland, *Computing  $L$ -series of hyperelliptic curves*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 312–326.
- [8] Kamal Khuri-Makdisi, *On Jacobian group arithmetic for typical divisors on curves*, Research in Number Theory **4** (2018), no. 1.

- [9] Evan MacNeil, *c34-curves*, <https://github.com/emmacneil/c34-curves>, 2019.
- [10] Evan MacNeil, *Divisor class group arithmetic on  $C_{3,4}$  curves*, Master's thesis, University of Calgary, Canada, 2019, <https://prism.ucalgary.ca/handle/1880/111659>.
- [11] Fatima Abu Salem and Kamal Khuri-Makdisi, *Fast Jacobian group operations for  $C_{3,4}$  curves over a large finite field*, LMS J. Comput. Math. **10** (2007), 307–328.
- [12] Daniel Shanks, *On Gauss and composition I, II*, Proc. NATO ASI on Number Theory and Applications, Kluwer Academic Press, 1989, pp. 163–204.
- [13] Andrew V. Sutherland, *Fast Jacobian arithmetic for hyperelliptic curves of genus 3*, Proceedings of the Thirteenth Algorithmic Number Theory Symposium, The Open Book Ser., vol. 2, Math. Sci. Publ., Berkeley, CA, 2019, pp. 425–442.
- [14] Andrew V. Sutherland, *Sato-Tate distributions*, Analytic methods in arithmetic geometry, Contemp. Math., vol. 740, Amer. Math. Soc., Providence, RI, 2019, pp. 197–248.

Received 28 Feb 2020.

EVAN MACNEIL: [macneil.evan@ucalgary.ca](mailto:macneil.evan@ucalgary.ca)

*Department of Mathematics and Statistics, University of Calgary, Calgary AB, Canada*

MICHAEL J. JACOBSON JR.: [jacobs@ucalgary.ca](mailto:jacobs@ucalgary.ca)

*Department of Computer Science, University of Calgary, Calgary AB, Canada*

RENAME SCHEIDLER: [rscheidl@ucalgary.ca](mailto:rscheidl@ucalgary.ca)

*Department of Mathematics and Statistics, University of Calgary, Calgary AB, Canada*

# Reductions between short vector problems and simultaneous approximation

Daniel E. Martin

In 1982, Lagarias showed that solving the approximate shortest vector problem also solves the problem of finding good simultaneous Diophantine approximations (*SIAM J. Comput.*, **14**(1):196–209, 1985)). Here we provide a deterministic, dimension-preserving reduction in the reverse direction. It has polynomial time and space complexity, and it is gap-preserving under the appropriate norms. We also give an alternative to the Lagarias algorithm by first reducing his version of simultaneous approximation to one with no explicit range in which a solution is sought.

## 1. Introduction

Our primary result is to show that a short vector problem reduces deterministically and with polynomial complexity to a single simultaneous approximation problem as presented in the definitions below. We use  $\min^\times$  to denote the nonzero minimum,  $\{\mathbf{x}\} \in (-\frac{1}{2}, \frac{1}{2}]^n$  to denote the fractional part of  $\mathbf{x} \in \mathbb{R}^n$ , and  $[x]$  to denote the set  $\{1, \dots, \lfloor x \rfloor\}$  for  $x \in \mathbb{R}$ .

**Definition 1.1.** A *short vector problem* takes input  $\alpha \in [1, \infty)$  and nonsingular  $M \in M_n(\mathbb{Z})$ . A valid output is  $\mathbf{q}_0 \in \mathbb{Z}^n$  with  $0 < \|M\mathbf{q}_0\| \leq \alpha \min_{\mathbf{q} \in \mathbb{Z}^n}^\times \|M\mathbf{q}\|$ . Let SVP denote an oracle for such a problem.

**Definition 1.2.** A *good Diophantine approximation problem* takes input  $\alpha, N \in [1, \infty)$  and  $\mathbf{x} \in \mathbb{Q}^n$ . A valid output is  $\mathbf{q}_0 \in [\alpha N]$  with  $\|\{q_0 \mathbf{x}\}\| \leq \alpha \min_{q \in [N]} \|\{q \mathbf{x}\}\|$ . Let GDA denote an oracle for such a problem.

Our reduction asserts that if we can find short vectors in a very restricted family of lattices then we can find them in general, since behind a good Diophantine approximation problem is the lattice generated by  $\mathbb{Z}^n$  and one additional vector,  $\mathbf{x}$ .

Literature more commonly refers to a short vector problem as a *shortest vector problem* when  $\alpha = 1$  and an *approximate shortest vector problem* otherwise (often unrestricted to sublattices of  $\mathbb{Z}^n$ , though we have lost no generality). A brief exposition can be found in [26]. See [14] or [24] for a more

comprehensive overview, [27] for a focus on cryptographic applications, [19] for a summary of hardness results, and [6] for relevance and potential applications to post-quantum cryptography.

Regarding simultaneous approximation, Brentjes highlights several algorithms in [7]. For a sample of applications to attacking clique and knapsack-type problems see [13], [20], and [31]. Examples of cryptosystems built on the hardness of simultaneous approximation are [2], [4], and [16]. This version is taken from [9] and [29].

The reduction, given in Algorithm 3, preserves the gap  $\alpha$  when the  $\ell_\infty$ -norm is used for both problems. This means the short vector problem defined by  $\alpha$  and  $M$  is solved by calling  $\text{GDA}(\alpha, \mathbf{x}, N)$  for some  $\mathbf{x} \in \mathbb{Q}^n$  and  $N \in \mathbb{R}$ . It reverses a 1982 result of Lagarias, which reduces a good Diophantine approximation problem to SVP. (See Theorem B in [21], which refers to the problem as *good simultaneous approximation*. We borrow its name from [9] and [29].) Though there is an important contextual distinction: [21] relates simultaneous approximation under the  $\ell_\infty$ -norm to lattice reduction under the  $\ell_2$ -norm, whereas *all reductions in this paper assume a consistent norm*.

Under Lagarias' (and the most common) setup — the  $\ell_\infty$ -norm for GDA and the  $\ell_2$ -norm for SVP — we are not the first to go in this other direction. In a seminar posted online from July 1, 2019, Agrawal presented an algorithm achieving this reduction which was complete apart from some minor details [1]. Tersely stated, he takes an upper triangular basis for a sublattice of  $\mathbb{Z}^n$  and transforms it inductively, using integer combinations and rigid rotations with two basis vectors at a time, into a lattice (a rotated copy of the original) whose short vectors can be found via simultaneous approximation. The short vector problem defined by  $\alpha$  and  $M$  gets reduced to  $\text{GDA}(\alpha/\sqrt{2n}, \mathbf{x}, N)$ , called multiple times in order to account for the unknown minimal vector length which is used to determine  $\mathbf{x}$ .

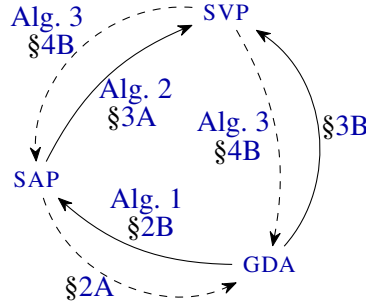
In contrast, the reduction here takes a completely different approach. It finds a sublattice which is nearly scaled orthonormal, so that only one additional vector is needed to generate the original lattice. This extra vector is the input for GDA. We note that when switching between norms, our reduction is also not gap-preserving. To use Algorithm 3 to solve a short vector problem with respect to the  $\ell_2$ -norm via GDA with respect to the  $\ell_\infty$ -norm, the latter must be executed with the parameter  $\alpha/\sqrt{n}$  to account for the maximum ratio of nonzero norms  $\|\mathbf{q}\|_2/\|\mathbf{q}\|_\infty$ .

The relationship between the two problems in Definitions 1.1 and 1.2 will be studied through the following intermediary.

**Definition 1.3.** A *simultaneous approximation problem* takes input  $\alpha \in [1, \infty)$  and  $\mathbf{x} \in \mathbb{Q}^n$ . A valid output is  $q_0 \in \mathbb{Z}$  with  $0 < \|\{q_0\mathbf{x}\}\| \leq \alpha \min_{\mathbf{q} \in \mathbb{Z}} \|\{\mathbf{q}\mathbf{x}\}\|$ . Let SAP denote an oracle for such a problem.

This problem prohibits only the trivial solution, the least common denominator of  $\mathbf{x}$ 's entries, while “ $N$ ” in a good Diophantine approximation problem is generally more restrictive.

Section 2 explores the relationship between the two versions of simultaneous approximation given in Definitions 1.2 and 1.3. Among the results, only Proposition 2.1 in Section 2A is required to verify the final reduction of a short vector problem to either version of simultaneous approximation. Section 2B contains Algorithm 1. It reduces a good Diophantine approximation problem to polynomially many



**Figure 1.** Algorithm and subsection numbers for reductions.

SAP calls, each executed with the parameter  $\alpha/3.06$ . So while this reduction is not gap-preserving, the inflation is independent of the input.

[Section 3](#) reduces both versions of simultaneous approximation to SVP. It begins with [Algorithm 2](#), which solves [Definition 1.3](#)’s version. We remark at the end of [Section 3A](#) how this reduction adapts to the inhomogeneous forms of these problems, meaning the search for  $q_0 \in \mathbb{Z}$  or  $q_0 \in \mathbb{Z}^n$  that makes  $q_0x - y$  or  $Mq_0 - y$  small for some  $y \in \mathbb{Q}^n$ . (In this case the latter is known as the *approximate closest vector problem*, exposted in Chapter 18 of [14], for example.) Then [Section 3B](#) combines Algorithms 1 and 2 to solve [Definition 1.2](#)’s version of simultaneous approximation using SVP. This is our alternative to the Lagarias reduction.

Finally, [Algorithm 3](#) in [Section 4](#) reduces a short vector problem to GDA or SAP. It also adapts to the inhomogeneous versions of SVP and SAP (not GDA, as mentioned at the end of [Section 4C](#)). In [Corollary 4.9](#) we observe that [Algorithm 3](#) facilitates a simpler proof that GDA is NP-hard under an appropriate bound on  $\alpha$ , a result first obtained in [9]. Then we combine Algorithms 2 and 3 in [Section 4B](#) to solve a simultaneous approximation problem with GDA. In particular, we give all six reductions among the defined problems, as shown in [Figure 1](#).

The two reductions in [Figure 1](#) without algorithm numbers are achieved by following the two arrows that combine to give the same source and target. *Dashed arrows indicate a norm restriction. Each must be executed under either the  $\ell_1$ ,  $\ell_2$ , or  $\ell_\infty$ -norm.* However, we show in [Section 4C](#) how the restriction can be alleviated to any  $\ell_p$ -norm provided we accept additional gap inflation by a constant arbitrarily close to 1.

The results are summarized in [Table 1](#). It uses  $m$  and  $d$  to denote the maximal magnitude among input integers and the least common denominator of the input vector, respectively. The matrix or vector dimension is  $n$ , and  $p$  defines the norm. Trivial cases that cause logarithms to equal 0 are ignored. The column descriptions are as follows:

operations: Big- $O$  bound on the number of arithmetic operations per oracle call.

integers: Big- $O$  bound on the length of integers used throughout the reduction.

inflation: Maximum gap inflation. For example, to solve a good Diophantine approximation problem with some  $\alpha$  using [Algorithm 1](#), SAP is called with  $\alpha/3.06$ .

calls: Upper bound on the number of required calls to the oracle.

reduction	operations	integers	inflation	calls
GDA $\rightarrow$ SAP	$n \log m$	$n \log m$	3.06	$\lceil \log_2 d / \alpha N \rceil$
SAP $\rightarrow$ SVP	$(n + \log m)^2$	$n \log m$	1	1
GDA $\rightarrow$ SVP	$(n + \log m)^2$	$n \log m$	3.06	$\lceil \log_2 d / \alpha N \rceil$
SVP $\rightarrow$ GDA	$n^4 \log mn$	$n^4 \log mn$	$n^{1/p}$	1
SVP $\rightarrow$ SAP	$n^4 \log mn$	$n^4 \log mn$	1	1
SAP $\rightarrow$ GDA	$n^5 \log m$	$n^5 \log m$	$n^{1/p}$	1

**Table 1.** Summary of reduction complexities and gap inflations.

## 2. Versions of simultaneous approximation

**2A. SAP to GDA.** Rather than give a complete reduction from a simultaneous approximation problem to GDA, which is postponed until the end of [Section 4B](#), the purpose of this subsection is to observe a condition on the input that makes these two versions of simultaneous approximation nearly equivalent.

**Proposition 2.1.** *Suppose the  $i$ -th coordinate of  $\mathbf{x}$  is of the form  $x_i = 1/d$ , where  $d \in \mathbb{N}$  makes  $d\mathbf{x} \in \mathbb{Z}^n$ . Under an  $\ell_p$ -norm,  $\text{GDA}(\alpha, \mathbf{x}, N)$  solves the simultaneous approximation problem defined by  $\alpha n^{1/p}$  and  $\mathbf{x}$  with  $N = d/2\alpha$ .*

*Proof.* Let  $q_{\min} \in [d/2]$  be such that  $\|\{q_{\min}\mathbf{x}\}\|$  is the nonzero minimum. A vector's fractional part is in  $(-\frac{1}{2}, \frac{1}{2}]^n$ , making its length at most  $n^{1/p}/2$ . So we may assume that  $\|\{q_{\min}\mathbf{x}\}\| < \frac{1}{2}\alpha$ , since otherwise every integer in  $[N] = [d/2\alpha]$  solves the simultaneous approximation problem defined by  $\alpha n^{1/p}$  and  $\mathbf{x}$ .

Under an  $\ell_p$ -norm,  $\|\{q_{\min}\mathbf{x}\}\|$  is an upper bound for its  $i$ -th coordinate,  $q_{\min}/d$ . Combined with the assumption  $\|\{q_{\min}\mathbf{x}\}\| < \frac{1}{2}\alpha$ , this gives  $q_{\min} \in [d/2\alpha] = [N]$ , which implies  $\min_{q \in [N]} \|\{q\mathbf{x}\}\| \leq \min_{q \in \mathbb{Z}}^\times \|\{q\mathbf{x}\}\|$ . And because  $\alpha N < d$ , it is guaranteed that  $\text{GDA}(\alpha, \mathbf{x}, N)$  is not a multiple of  $d$ .  $\square$

Note that without an assumption on  $\mathbf{x}$  like the one used in this proposition, there is no natural choice for  $N$  that makes GDA solve a simultaneous approximation problem. If we set it too small, say with  $N < d/2$ , then  $\min_{q \in [N]} \|\{q\mathbf{x}\}\|$  may be unacceptably larger than  $\min_{q \in \mathbb{Z}}^\times \|\{q\mathbf{x}\}\|$ , potentially making GDA's approximation poor. If we set it too large, say with  $N \geq d/\alpha$ , then GDA may return  $d$ , which is not a valid output for the initial simultaneous approximation problem.

To get around this, our strategy is to first reduce a simultaneous approximation problem to SVP with [Algorithm 2](#). Then in [Algorithm 3](#), which reduces a short vector problem to SAP, we are careful to produce an input vector for the oracle that satisfies the hypothesis of [Proposition 2.1](#) in order to admit GDA.

**2B. GDA to SAP.** Let  $d$  continue to denote the least common denominator of  $\mathbf{x}$ . The problem faced in this reduction is that outputs for a good Diophantine approximation problem are bounded by  $\alpha N$ , which may be smaller than  $d/2$ . This leaves no guarantee that  $\text{SAP}(\alpha, \mathbf{x})$ , call this integer  $d_1 \in [d/2]$ , is a solution. But knowing that  $\mathbf{x}$  is very near a rational vector  $\mathbf{x}_1$  with least common denominator  $d_1$  allows us to call SAP again, now on  $\mathbf{x}_1$  to get  $d_2 \in [d_1/2]$ . This is the least common denominator of some  $\mathbf{x}_2$  near  $\mathbf{x}_1$ , and we continue in this fashion until the output is at most  $\alpha N$ . To get  $d_i \in [d_{i-1}/2]$ , we adopt the convention that modular reduction returns an integer with magnitude at most half the modulus.



---

**Algorithm 1:** A reduction from a good Diophantine approximation problem to multiple calls to SAP under a consistent norm.

---

**input:**  $\alpha, N \in [1, \infty), \mathbf{x} = (x_1, \dots, x_n) \in \mathbb{Q}^n$   
**output:**  $q_0 \in [\alpha N]$  with  $\|\{q_0 \mathbf{x}\}\| \leq \alpha \min_{q \in [N]} \|\{q \mathbf{x}\}\|$

- 1  $d \leftarrow \text{lcd}(x_1, \dots, x_n) > 0$
- 2 **while**  $d > \alpha N$  **do**
- 3      $d \leftarrow |\text{SAP}(\alpha/3.06, \mathbf{x}) \bmod d| \quad \triangleright$  good, but large denominator
- 4      $\mathbf{x} \leftarrow \mathbf{x} - \{d\mathbf{x}\}/d \quad \triangleright$  now  $\text{lcd}(\mathbf{x}) = d$ , at most half of the previous iteration's lcd
- 5 **return**  $d$

---

**Proposition 2.2.** *The output of Algorithm 1 solves the initial good Diophantine approximation problem.*

*Proof.* Let  $d_i$  and  $\mathbf{x}_i$  denote the values of  $d$  and  $\mathbf{x}$  after  $i$  **while** loop iterations have been completed. In particular,  $d_0$  and  $\mathbf{x}_0$  are defined by the input. Also let  $I + 1$  be the total number of iterations executed, so the output is  $d_{I+1}$ .

The triangle inequality gives

$$\|\{d_{I+1} \mathbf{x}\}\| \leq \|\{d_{I+1} \mathbf{x}_I\}\| + d_{I+1} \sum_{i=1}^I \|\mathbf{x}_i - \mathbf{x}_{i-1}\|. \quad (2-1)$$

With  $\lambda_i = \min_{q \in [N]} \|\{q \mathbf{x}_i\}\|$ , the choice of  $d_{I+1}$  bounds the first summand by  $\alpha \lambda_I / c$ , where  $c = 3.06$  in the algorithm but is left undetermined for now. Similarly, the choice of  $d_i = \text{SAP}(\alpha/c, \mathbf{x}_{i-1})$  and the fact that  $d_{i-1} > \alpha N \geq N$  give

$$\|\mathbf{x}_i - \mathbf{x}_{i-1}\| = \frac{\|\{d_i \mathbf{x}_{i-1}\}\|}{d_i} \leq \frac{\alpha \min_{q \in \mathbb{Z}}^\times \|\{q \mathbf{x}_{i-1}\}\|}{c d_i} \leq \frac{\alpha \lambda_{i-1}}{c d_i}. \quad (2-2)$$

So to bound (2-1) it must be checked that the  $\lambda_i$ 's are not too large. To this end, fix some  $i \leq I$  and let  $q_{\min} \in [N]$  satisfy  $\|\{q_{\min} \mathbf{x}_{i-1}\}\| = \lambda_{i-1}$ . Then we have the following upper bound on  $\lambda_i$ , where the three inequalities are due to the triangle inequality, inequality (2-2), and  $q_{\min} \leq N < d_I / \alpha \leq d_i / 2^{I-i} \alpha$ , respectively:

$$\|\{q_{\min} \mathbf{x}_i\}\| \leq \lambda_{i-1} + q_{\min} \|\mathbf{x}_i - \mathbf{x}_{i-1}\| \leq \lambda_{i-1} \left(1 + \frac{\alpha q_{\min}}{c d_i}\right) < \lambda_{i-1} \left(1 + \frac{1}{2^{I-i} c}\right).$$

Inductively, this gives

$$\lambda_i < \lambda_0 \prod_{j=1}^i \left(1 + \frac{1}{2^{I-j} c}\right). \quad (2-3)$$

Now (2-1), (2-2), and (2-3) can be combined to get

$$\|\{d_{I+1} \mathbf{x}\}\| \leq \frac{\alpha d_{I+1}}{c} \sum_{i=0}^I \frac{\lambda_i}{d_{i+1}} \leq \frac{\alpha}{c} \sum_{i=0}^I \frac{\lambda_i}{2^{I-i}} \leq \frac{\alpha \lambda_0}{c} \sum_{i=0}^I \frac{1}{2^{I-i}} \prod_{j=1}^i \left(1 + \frac{1}{2^{I-j} c}\right).$$

Thus the output approximation quality,  $\|d_{l+1}\mathbf{x}\|$ , is at most  $\alpha \min_{q \in [N]} \|q\mathbf{x}\| = \alpha \lambda_0$  provided  $c$  satisfies

$$1 \geq \frac{1}{c} \sum_{i=0}^{\infty} \frac{1}{2^i} \prod_{j=i}^{\infty} \left(1 + \frac{1}{2^j c}\right).$$

This justifies our choice of  $c = 3.06$  in line 3. □

**Proposition 2.3.** *Let  $m > 1$  be the maximum magnitude among integers defining  $\mathbf{x}$ , and let  $d > 1$  be its least common denominator. The reduction in [Algorithm 1](#) requires an initial  $O(n \log m)$  operations plus  $O(n)$  operations for each call to SAP, of which there are at most  $\lceil \log_2(d/\alpha N) \rceil$ , on integers of length  $O(n \log m)$ .*

*Proof.* Repeatedly applying the Euclidean algorithm computes  $d$  with  $O(n \log m)$  operations on integers of length  $O(n \log m)$ . Modular reduction in line 3 decreases each successive least common denominator by at least a factor of  $\frac{1}{2}$ . This bounds the number of **while** loop iterations by  $\lceil \log_2(d/\alpha N) \rceil$ . □

### 3. Reducing to SVP

First we restrict attention to [Definition 1.3](#)'s version of simultaneous approximation (SAP) in [Algorithm 2](#). Then we will compare the combination with [Algorithm 1](#) to Lagarias' reduction in [\[21\]](#) from [Definition 1.2](#)'s version (GDA).

**3A. SAP to SVP.** Here we replace the  $n+1$  vectors associated to simultaneous approximation, namely  $\mathbf{x}$  and a basis for  $\mathbb{Z}^n$ , with  $n$  vectors generating the same lattice. There are algorithms for which this is a byproduct, like Pohst's modified (to account for linearly dependent vector inputs) LLL algorithm [\[23\]](#) or Kannan and Bachem's Hermite normal form algorithm [\[18\]](#). But as a consequence of achieving additional basis properties, they are more complicated and require more operations than necessary. We briefly present an alternative because the improved time complexity is relevant to the next subsection.

---

**Algorithm 2:** A gap-preserving reduction from a simultaneous approximation problem to one call to SVP under a consistent norm.

---

**input:**  $\alpha \in [1, \infty)$ ,  $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{Q}^n$

**output:**  $q_0 \in \mathbb{Z}$  with  $0 < \|\{q_0\mathbf{x}\}\| \leq \alpha \min_{q \in \mathbb{Z}}^\times \|\{q\mathbf{x}\}\|$

1  $d \leftarrow \text{lcd}(x_1, \dots, x_n)$

2  $x_n \leftarrow x_n + a$  with  $a$  an integer that makes

$\gcd(dx_1, \dots, dx_{n-1}, d(x_n + a)) = 1$

▷ make sure  $d\mathbf{x}$  extends to a basis for  $\mathbb{Z}^n$

3  $M \leftarrow$  matrix in  $\text{SL}_n(\mathbb{Z})$  with first column  $d\mathbf{x}$

4  $M \leftarrow M$  with last  $n-1$  columns scaled by  $d$

▷ generates scaled original lattice

5 **return**  $\text{SVP}(\alpha, M)_1$

▷ first coordinate is a solution

---

**Proposition 3.1.** *The output of [Algorithm 2](#) solves the initial simultaneous approximation problem.*

*Proof.* First note that  $a$  in line 2 exists. As  $d$  is the least common denominator,  $\gcd(dx_1, \dots, dx_n)$  and  $d$  are coprime. So take  $a$  to be divisible by those primes which divide  $\gcd(dx_1, \dots, dx_{n-1})$  but not  $dx_n$ . Also, since  $a$  is an integer, the new value of  $\mathbf{x}$  defines the same simultaneous approximation problem as the input.

Coprime entries means  $d\mathbf{x}$  extends to some  $M \in \text{SL}_n(\mathbb{Z})$ . (One method is mentioned in the next proof.) The columns of  $dM$  generate  $d\mathbb{Z}^n$ , so the same is true if we only scale the last  $n - 1$  columns by  $d$ . In particular, the columns of the new  $M$  in line 4 generate  $d\mathbf{x}$  and  $d\mathbb{Z}^n$ , which in turn generate each column. Thus  $M$  defines a basis for the original simultaneous approximation lattice scaled by  $d$ .

Finally, the last  $n - 1$  columns of  $M$  are vectors in  $d\mathbb{Z}^n$ , so that  $M \text{SVP}(\alpha, M) \equiv \text{SVP}(\alpha, M)_1 d\mathbf{x} \pmod{d\mathbb{Z}^n}$ . This verifies that  $\text{SVP}(\alpha, M)_1$  is the integer we seek.  $\square$

**Proposition 3.2.** *Let  $m > 1$  be the maximum magnitude among integers defining  $\mathbf{x}$ . The reduction in [Algorithm 2](#) requires  $O((n + \log m)^2)$  operations on integers of length  $O(n \log m)$ .*

*Proof.* As with [Algorithm 1](#), line 1 requires  $O(n \log m)$  operations on integers of length  $O(n \log m)$ . The integer outputs of these operations also have length  $O(n \log m)$ .

Skipping line 2 for now, the  $i$ -th column (for  $i \geq 2$ ) of  $M$  in line 3 can be set to

$$\left( \frac{b_1 dx_1}{\gcd(dx_1, \dots, dx_{i-1})}, \dots, \frac{b_1 dx_{i-1}}{\gcd(dx_1, \dots, dx_{i-1})}, b_2, 0, \dots, 0 \right)$$

(transposed), where  $b_2 \gcd(dx_1, \dots, dx_{i-1}) - b_1 dx_i = \gcd(dx_1, \dots, dx_i)$ . The determinant of the top-left  $i \times i$  minor is then  $\gcd(dx_1, \dots, dx_i)$  by induction. To find  $b_1$  and  $b_2$  we execute the Euclidean algorithm on  $\gcd(d_i x_1, \dots, d_i x_{i-1})$  and  $d_i x_i$ , where  $d_i = \text{lcd}(x_1, \dots, x_i)$ . But  $\gcd(d_i x_1, \dots, d_i x_{i-1})$  is at most  $m$  times  $\gcd(d_{i-1} x_1, \dots, d_{i-1} x_{i-1})$ , which divides the greatest common divisor of the numerators of  $x_1, \dots, x_{i-1}$ . So for each  $i$  the Euclidean algorithm needs  $O(\log m)$  operations.

Before computing the last column of  $M$ , we find  $a$  in line 2 to ensure a determinant of 1. As discussed in the last proof, we can start with  $a = \gcd(dx_1, \dots, dx_{n-1})$  and replace it with  $a/\gcd(a, dx_n)$  until nothing changes. This requires  $O(\log a) = O(\log m)$  executions of the Euclidean algorithm, each taking  $O(\log m)$  operations.

Scaling all but the first column by  $d$  in line 4 takes  $O(n^2)$  operations.  $\square$

We remark that this algorithm adapts to inhomogeneous forms of these problems. To find  $q_0 \in \mathbb{Z}$  with  $\| \{q_0 \mathbf{x} - \mathbf{y}\} \| \leq \alpha \min_{q \in \mathbb{Z}} \| \{q \mathbf{x} - \mathbf{y}\} \|$  when  $q \mathbf{x} - \mathbf{y} \in \mathbb{Z}^n$  has no solution, we can perform the same reduction and finish by calling an oracle which solves the approximate *closest* vector problem defined by  $\alpha$ ,  $M$ , and  $d\mathbf{y}$ .

**3B. GDA to SVP.** Combining Algorithms 1 and 2 gives an alternative to the Lagarias reduction from good Diophantine approximation to SVP in [21]. We execute [Algorithm 1](#), but use [Algorithm 2](#) to compute  $\text{SAP}(\alpha/3.06, \mathbf{x})$  in line 3. By [Proposition 2.3](#), this requires at most  $\lceil \log_2(d/\alpha N) \rceil$  calls to SVP. And [Proposition 3.2](#) states that each call requires  $O((n + \log m)^2)$  operations on integers of length  $O(n \log m)$ .

Recall that switching from  $\ell_2$  to  $\ell_\infty$  decreases a nonzero norm by at most a factor of  $1/\sqrt{n}$ . In particular, by executing this combination of Algorithms 1 and 2 with respect to the  $\ell_2$ -norm, we get an  $\ell_\infty$  solution to the initial good Diophantine approximation problem provided we use  $\alpha/3.06\sqrt{n}$  for SVP.

Lagarias achieves this reduction with the now well-known trick from [22] of reducing the lattice generated by  $\mathbb{Z}^n$  and  $\mathbf{x}$ , bumped up a dimension by putting 0 in every  $(n+1)$ -th coordinate but  $\mathbf{x}$ 's. The ideal value for the last coordinate of  $\mathbf{x}$ , which is guessed at using  $\lfloor n + \log_2 dN \rfloor$  calls of the form  $\text{SVP}(\alpha/\sqrt{5n}, M)$  for varying  $M$ , is  $\min_{q \in [N]} \|q\mathbf{x}\|/N$ . (The gap inflation approaches  $\sqrt{n}$  as our guesses get better.) The Lagarias reduction requires an initial  $O(n \log m)$  arithmetic operations to compute the least common denominator, then only one additional operation per call. The integers involved have input length  $O(\log m^n N)$ .

Whether the benefit of fewer calls to SVP outweighs the increased operations per call depends on the complexity of the oracle. Ours is an asymptotic improvement when the number of operations performed by SVP exceeds  $O((n + \log m)^2)$ .

#### 4. Reducing to GDA or SAP

We focus first on the reduction to SAP.

**4A. Intuition.** Consider an input matrix  $M \in M_n(\mathbb{Z})$  for a short vector problem. Let  $d = \det M$ , and let  $\mathbf{e}_1, \dots, \mathbf{e}_n$  denote the standard basis vectors for  $\mathbb{Z}^n$ . If there were one vector, call it  $\mathbf{b} \in \mathbb{Z}^n$ , for which the set  $\{M\mathbf{b}, d\mathbf{e}_1, \dots, d\mathbf{e}_n\}$  generated the columns of  $M$ , our reduction would just amount to finding it. This is exactly the setup for simultaneous approximation:  $n+1$  vectors,  $n$  of which are scaled orthonormal. A solution could be obtained by doing simultaneous approximation on  $M\mathbf{b}/d$ , scaling the resulting short vector by  $d$ , and applying  $M^{-1}$  (to comply with Definition 1.1). Unfortunately, unless  $n \leq 2$  or  $d = \pm 1$ , such a  $\mathbf{b}$  does not exist. Indeed, the adjugate matrix,  $\text{adj } M = dM^{-1}$ , has at most rank 1 over  $\mathbb{Z}/p\mathbb{Z}$  for a prime  $p$  dividing  $d$ . So at least  $n-1$  additional vectors are required to have full rank modulo  $p$ , a prerequisite to having full rank over  $\mathbb{Q}$ . But asking that  $M\mathbf{b}$  generate the columns of  $M$  alongside  $d\mathbf{e}_1, \dots, d\mathbf{e}_n$  is equivalent to asking that  $\mathbf{b}$  generate  $\mathbb{Z}^n$  alongside the columns of  $\text{adj } M$ .

What matters is the matrix with columns  $d\mathbf{e}_1, \dots, d\mathbf{e}_n$  being scaled orthonormal. As such, multiplying by it or its inverse has no effect on a vector's relative length. So we plan to find a different set of  $n$  column vectors—a set for which just one additional  $M\mathbf{b}$  is needed to generate the original lattice—which is nearly scaled orthonormal, making the effect of its corresponding matrix multiplication on  $\alpha$  negligible. The initial short vector problem becomes a search for an integer combination of  $M\mathbf{b}$  and these columns, say  $\mathbf{c}_1, \dots, \mathbf{c}_n$ . We can then solve the simultaneous approximation problem defined by  $\alpha$  and  $[\mathbf{c}_1 \cdots \mathbf{c}_n]^{-1} M\mathbf{b}$ . This works as long as multiplying by  $[\mathbf{c}_1 \cdots \mathbf{c}_n]$  changes the ratio between the lengths of the shortest vector and our output by less than whatever is afforded by the fact that lattice norms form a discrete set.

An arbitrary lattice may have all of its scaled orthonormal sublattices contained in  $d\mathbb{Z}^n$ . So as candidates for the matrix  $[\mathbf{c}_1 \cdots \mathbf{c}_n]$ , we look for something of the form  $cd \text{Id} + MA = M(c \text{adj } M + A)$  for

some  $c \in \mathbb{Z}$  and  $A \in M_n(\mathbb{Z})$ . If the entries of  $A$  are sufficiently small, then multiplication by  $cd \text{Id} + MA$  has a similar effect on relative vector norms as multiplying by  $cd \text{Id}$ , which has no effect.

We will tailor our choice of  $c$  and  $A$  so that a coordinate of the simultaneous approximation vector,  $(c \text{adj } M + A)^{-1} \mathbf{b}$ , is  $1/\det(c \text{adj } M + A)$ . This admits [Proposition 2.1](#) and hence GDA.

**4B. SVP to GDA or SAP.** [Algorithm 3](#) uses the following.

**Notation 4.1.** For polynomials  $f_1 = \sum_i f_{1,i} x^i$  and  $f_2 = \sum_i f_{2,i} x^i$  with maximum degree  $d$ , let  $C(f_1, f_2)$  denote the matrix of their coefficients,

$$\begin{bmatrix} f_{1,d} & & 0 & f_{2,d} & & 0 \\ \vdots & \ddots & & \vdots & \ddots & \\ f_{1,1} & \cdots & f_{1,d} & f_{2,1} & \cdots & f_{2,d} \\ f_{1,0} & \cdots & f_{1,d-1} & f_{2,0} & \cdots & f_{2,d-1} \\ & \ddots & \vdots & & \ddots & \vdots \\ 0 & & f_{1,0} & 0 & & f_{2,0} \end{bmatrix}.$$

The matrix above can determine when  $f_1$  and  $f_2$  are coprime over  $\mathbb{Q}(x)$  in lieu of polynomial long division, where coefficient growth is exponential without complicated mitigations as in [\[8\]](#). We demonstrate this now to give some clarity to the meaning behind lines 5 and 6 of [Algorithm 3](#).

**Lemma 4.2.** *Let  $f_1, f_2 \in \mathbb{Z}[x]$ , not both constant. As an ideal in  $\mathbb{Z}[x]$ ,  $(f_1, f_2)$  contains  $\det C(f_1, f_2)$ , which is nonzero if and only if  $f_1$  and  $f_2$  have no common root in the algebraic closure of  $\mathbb{Q}$ .*

*Proof.* Let  $d = \max(\deg f_1, \deg f_2)$ . Consider the vector in  $\mathbb{Z}^{2d}$  whose only (perhaps) nonzero entry is  $\det C(f_1, f_2)$  in the last coordinate. This is the image under  $C(f_1, f_2)$  of some nonzero integer vector. We can split the entries of this vector down the middle to get coefficients for  $g_1, g_2 \in \mathbb{Z}[x]$  that have degree at most  $d - 1$  and satisfy  $\det C(f_1, f_2) = f_1 g_1 + f_2 g_2 \in (f_1, f_2)$ .

Plugging a common root of  $f_1$  and  $f_2$  into this last equation, should one exist, shows  $\det C(f_1, f_2) = 0$ . Conversely, suppose  $f_1 g_1 + f_2 g_2 = 0$  and that  $\deg f_1 = d \geq 1$ . Then  $g_2$  must be nonzero to avoid the same being true of  $g_1$ , contradicting our choice of nonzero coefficient vector. But  $g_2$  has degree at most  $d - 1$ . So  $f_1 g_1 = -f_2 g_2$  implies that at least one of  $f_1$ 's  $d$  roots must be shared by  $f_2$ .  $\square$

**Notation 4.3.** For a matrix  $M$ , let  $M_{i,j}$  denote the entry in its  $i$ -th row and  $j$ -th column, and let  $\check{M}_i$  denote its top-left  $i \times i$  minor.

Line 1 of [Algorithm 3](#) requires knowing the position of a nonzero entry in the input matrix, and line 8 requires knowing the maximum magnitude among entries. For notational convenience, we assume that  $M_{n,1}$  is the nonzero maximum.

Let us turn to the **for** loop, which builds the matrix [Section 4A](#) called  $A$ .

**Lemma 4.4.** *For  $i = 2, \dots, n$ , there is some  $j \leq 2i - 2$  satisfying the criterion of line 5 in the **for** loop iteration corresponding to  $i$ .*

---

**Algorithm 3:** A reduction from a short vector problem with  $n \geq 2$  to one call to SAP (gap-preserving) or GDA under a consistent  $\ell_p$ -norm with  $p \in \{1, 2, \infty\}$ .

---

**input:**  $a \geq b \in \mathbb{N}$  ( $\alpha = a/b$ ),  $M \in M_n(\mathbb{Z})$  with  $0 \neq \det M$  and  $M_{n,1} = \max_{i,j} |M_{i,j}|$   
**output:**  $q_0 \in \mathbb{Z}^n$  with  $0 < \|Mq_0\| \leq \alpha \min_{q \in \mathbb{Z}^n}^\times \|Mq\|$

- 1  $p \leftarrow$  least prime not dividing  $M_{n,1} \det M$
- 2  $M \leftarrow x \operatorname{adj} M + p \operatorname{Id}$   $\triangleright M = M(x)$  has linear polynomial entries
- 3 **for**  $i \leftarrow 2$  **to**  $n$  **do**
- 4      $M_{i,1} \leftarrow M_{i,1} + p$
- 5      $M_{i,i-1} \leftarrow M_{i,i-1} + p^j$  with  $j > 0$  minimal  $\triangleright$  need not compute determinant  
       so  $\det C((\operatorname{adj} \check{M}_i)_{i,1}, (\operatorname{adj} \check{M}_i)_{i,2}) \neq 0$  to test each  $j$ ; see [Theorem 4.8](#)
- 6  $c \leftarrow \det C((\operatorname{adj} M)_{n,1}, (\operatorname{adj} M)_{n,2})$
- 7  $c \leftarrow c/p^j$  with  $j$  maximal or  $p+1$  if  $|c| = p^j$   $\triangleright$  make  $c$  coprime to  $p$
- 8  $M \leftarrow M(c^j)$  with  $j = \lceil \log_{|c|} a^2 (2M_{n,1}n)^{3n} \rceil$   $\triangleright$  substitute for  $x$  so  $M \in M_n(\mathbb{Z})$
- 9  $b_1, b_2 \leftarrow$  integers with  $|b_1|$  minimal  $\triangleright$  that these exist guarantees  
       so  $1 = b_1 (\operatorname{adj} M)_{n,1} + b_2 (\operatorname{adj} M)_{n,2}$   $Mx$  (line 10) and  $M$  generate  $\mathbb{Z}^n$
- 10  $x \leftarrow M^{-1}(b_1, b_2, 0, \dots, 0)$
- 11  $q_0 \leftarrow \text{SAP}(\alpha, x)$  or  $\text{GDA}(\alpha/n^{1/p}, x, N)$   $\triangleright$  GDA works since  $x_n = 1/\det M$ ;  
       with  $N = n^{1/p} \det M/2\alpha$  recall [Proposition 2.1](#)
- 12 **return**  $M\{q_0x\}$

---

*Proof.* When  $i = 2$  we are asked to find  $j$  for which the linear polynomials  $M_{1,1}$  and  $M_{2,1} + p^j$  do not share a root (by [Lemma 4.2](#)). The constant term of  $M_{1,1}$  is  $p$  by line 2, meaning it has at most one root. So asking that  $j \leq 2i - 2 = 2$  gives enough space to avoid the at-most-one value of  $j$  that fails. Now suppose  $i \geq 3$  and that the claim holds for  $i - 1$ . Let  $M$  be its value after line 4 in the **for** loop iteration corresponding to  $i$ , and let

$$f_1 = (\operatorname{adj} \check{M}_{i-1})_{i-1,1} \quad \text{and} \quad f_2 = (\operatorname{adj} \check{M}_{i-1})_{i-1,2}.$$

By assumption there are  $g_1, g_2 \in \mathbb{Z}[x]$  with  $g_1 f_1 + g_2 f_2 = \det C(f_1, f_2) \neq 0$ . Fix an integer  $j$ , and let  $h_1 = (\operatorname{adj} \check{M}_i)_{i,1} - p^j f_1$  and  $h_2 = (\operatorname{adj} \check{M}_i)_{i,2} - p^j f_2$ , the polynomials we hope to make coprime with the appropriate choice of  $j$ . We have

$$\begin{bmatrix} f_2 & -f_1 \\ g_1 & g_2 \end{bmatrix} \begin{bmatrix} h_1 \\ h_2 \end{bmatrix} = \begin{bmatrix} f_2 (\operatorname{adj} \check{M}_i)_{i,1} - f_1 (\operatorname{adj} \check{M}_i)_{i,2} \\ g_1 (\operatorname{adj} \check{M}_i)_{i,1} + g_2 (\operatorname{adj} \check{M}_i)_{i,2} - p^j \det C(f_1, f_2) \end{bmatrix}.$$

In the column on the right, where we now focus our attention,  $p^j$  has been isolated.

For each root of the top polynomial, there is at most one value of  $j$  that makes it a root of the bottom. Thus it suffices to show that  $f_2 (\operatorname{adj} \check{M}_i)_{i,1} - f_1 (\operatorname{adj} \check{M}_i)_{i,2}$  is not the zero polynomial. Then its degree, which is at most  $2i - 3$ , bounds how many values of  $j$  can make the right-side polynomials share a root. As this occurs whenever  $h_1$  and  $h_2$  share a root, [Lemma 4.2](#) would complete the proof.

To show that  $f_2(\text{adj } \check{M}_i)_{i,1} - f_1(\text{adj } \check{M}_i)_{i,2}$  is nonzero, we compute its constant term from the matrix

$$\begin{bmatrix} p & 0 & \cdots & 0 & 0 & 0 \\ p + p^{j_2} & p & & & 0 & 0 \\ p & p^{j_3} & & & 0 & \\ \vdots & & \ddots & & \vdots & \\ p & 0 & & p^{j_{i-1}} & p & 0 \\ p & 0 & \cdots & 0 & p^j & p \end{bmatrix}. \quad (4-1)$$

These are the constants in  $\check{M}_i$  after adding  $p^j$  in the  $i, i-1$  position — the main diagonal comes from line 2, the first column comes from line 4, and the second diagonal comes from line 5. To compute  $h_1$  or  $h_2$ , we use cofactor expansion along the bottom row after deleting the last column and the first or second row. The  $(i-2) \times (i-2)$  minor determinants that are multiplied by the bottom row constant  $p^j$  are exactly  $f_1$  and  $f_2$  up to a sign. What remains sums to  $(\text{adj } \check{M}_i)_{i,1}$  or  $(\text{adj } \check{M}_i)_{i,2}$ . So the constant terms of  $(\text{adj } \check{M}_i)_{i,1}$ ,  $(\text{adj } \check{M}_i)_{i,2}$ , and  $f_2$  are  $p^{i-1}$ , 0, and  $p$  to the power  $1 + j_3 + \cdots + j_{i-1}$ , respectively. This makes  $p$  to the power  $i + j_3 + \cdots + j_{i-1}$  the constant term of  $f_2(\text{adj } \check{M}_i)_{i,1} - f_1(\text{adj } \check{M}_i)_{i,2}$ .  $\square$

We remark that by using a large integer instead of  $x$  in line 2, the **for** loop could successively make pairs of integers coprime rather than polynomials. Then the Euclidean algorithm could test  $j$  in line 5; determinants involving polynomial entries need not be computed. We might expect such an algorithm to require  $O(n^3 \log M_{n,1}n)$  operations (this uses that the average ratio with Euler's phi function,  $\varphi(n)/n$ , is a positive constant), but the provable worst case is bad. The best current asymptotic upper bound on the size of the interval that must be sieved or otherwise searched to find  $j$  is due to Iwaniec [17]. It only limits the algorithm to  $O(n^7 \log M_{n,1}n)$  operations. We favored the polynomial approach because of an easier bound on  $j$  (Lemma 4.4) and a better provable worst case (Theorem 4.8).

The next lemma allows the vector in line 10 to pass as  $\mathbf{b}$  from Section 4A.

**Lemma 4.5.** *With  $M$  denoting its value in line 9,  $\gcd((\text{adj } M)_{n,1}, (\text{adj } M)_{n,2}) = 1$ .*

*Proof.* By Lemma 4.2, it suffices to prove  $\gcd((\text{adj } M)_{n,1}, (\text{adj } M)_{n,2}, c) = 1$  with  $c$  as in line 6. Now let  $c'$  be  $c/p^j$  or  $p+1$  as in line 7. Recall the constant terms displayed in (4-1), which show that  $(\text{adj } M)_{n,2}$  is a power of  $p$  modulo  $c'$ . This implies  $\gcd((\text{adj } M)_{n,1}, (\text{adj } M)_{n,2}, c)$  is a power of  $p$  since  $p \nmid c'$ . But the constants added throughout the **for** loop are multiples of  $p$ . So before substituting for  $x$ , only the leading coefficient of  $(\text{adj } M)_{n,1}$  might have been nonzero modulo  $p$ . With  $M$  now the original input matrix, the leading term is  $M_{n,1} \det M^{n-2} x^{n-1}$ . By line 1 this is coprime to  $p$  whenever the same is true of the integer substituted for  $x$ .  $\square$

**Lemma 4.6.** *Let  $M$  be the input matrix, let  $c^j$  be as in line 8, and let  $A$  be such that  $c^j \text{adj } M + A$  is Algorithm 3's value of  $M$  in line 9. Then  $\|MA\|_{\text{op}} < (2nM_{n,1})^{3n}/5n$  under any  $\ell_p$ -norm.*

*Proof.* The operator norm is  $\max_{\|\mathbf{u}\|=1} \|MA\mathbf{u}\|$ . Using  $\|\mathbf{u}\|_{\infty} \leq 1$  gives

$$\|MA\mathbf{u}\| \leq n \|MA\mathbf{u}\|_{\infty} \leq n^2 \max_{i,j \in [n]} |(MA)_{i,j}|. \quad (4-2)$$

We refer back to (4-1), which displays the entries of  $A$  when  $i = n$ . Lemma 4.4 says  $j_i \leq 2i - 2$ , so the entries of  $MA$  are bounded in magnitude by

$$\max_{i,j \in [n]} |M_{i,j}| \max(np + p^2, p + p^{2n-2}) \leq 2M_{n,1} p^{2n-2} \leq 2M_{n,1}^3 p^{2n-2}. \quad (4-3)$$

(Recall that  $n \geq 2$  for this inequality.) Here  $np + p^2$  comes from the first column of  $A$ , and  $p + p^{2n-2}$  comes from the  $(n-1)$ -th column.

Now we turn to the size of  $p$ . If  $x \in \mathbb{R}$  is such that  $x\#$ , the product of primes not exceeding  $x$ , is larger than  $M_{n,1}|\det M|$ , then it must be that  $p < x$ . Rosser and Schoenfeld's lower bound on Chebyshev's theta function,  $\vartheta(x) = \sum_{p \leq x} \log p$ , gives  $\vartheta(x) > 0.231x$  when  $x \geq 2$  [28]. For the determinant we use Hadamard's bound:  $|\det M| \leq (M_{n,1}\sqrt{n})^n$  [15]. So take  $x = (\log M_{n,1}^3 n^n)/0.462$  (note that  $x \geq 2$  even when  $n = 2$  and  $M_{n,1} = 1$ , allowing for the Rosser–Schoenfeld bound) to get

$$\log x\# = \vartheta(x) > 0.231x = \frac{1}{2} \log M_{n,1}^3 n^n \geq \log M_{n,1}^{n+1} n^{n/2} \geq \log M_{n,1} |\det M|.$$

Combining  $p < x$  with (4-2) and (4-3) gives  $\|MA\|_{\text{op}} < 2M_{n,1}^3 n^2 x^{2n-2}$ . We must show that this is less than the stated bound of  $(2nM_{n,1})^{3n}/5n$ . To do this, raise both expressions to the power  $1/(n-1)$  and use  $(\frac{5}{4})^{1/(n-1)} \leq \frac{5}{4}$ . This simplifies the desired inequality to  $(\log M_{n,1}^3 n)^2 < 1.366M_{n,1}^3 n$ , which is true.  $\square$

**Theorem 4.7.** *Under the  $\ell_1$ ,  $\ell_2$ , or  $\ell_\infty$ -norm, the output of Algorithm 3 solves the initial short vector problem.*

*Proof.* There are two parts to the proof: (1) showing that the algorithm replaces the columns of  $M$  with  $n+1$  vectors that define the same lattice,  $n$  of them being nearly scaled orthonormal, and (2) showing that nearly scaled orthonormal is as good as being scaled orthonormal. Throughout the proof, let  $M$  be the input matrix, let  $c^j$  be as in line 8, let  $M'$  be Algorithm 3's value of  $M$  in line 9, and let  $A = M' - c^j \text{adj } M$  be the matrix of constants added throughout the **for** loop (as used in Lemma 4.6 and as shown in (4-1) when  $i = n$ ).

For part (1), with  $\mathbf{b} = (b_1, b_2, 0, \dots, 0)$  from line 10, Lemma 4.5 gives

$$\mathbf{x} = M'^{-1} \mathbf{b} = \frac{(x_1, x_2, \dots, 1)}{\det M'}. \quad (4-4)$$

By Cramer's rule [10], the 1 in the last coordinate is the determinant after replacing the last column of  $M'$  by  $\mathbf{b}$ , so that these  $n$  columns generate  $\mathbb{Z}^n$ . This in turn shows that the columns of  $MM'$  and  $M\mathbf{b}$  generate the input lattice. Also note by Proposition 2.1, that a coordinate of  $\det M' \mathbf{x}$  being 1 allows for GDA in place of SAP with  $N$  set to  $n^{1/p} \det M' / 2\alpha$  and  $\alpha$  scaled by  $1/n^{1/p}$ .

Instead of finding a short integer combination of  $M\mathbf{b}$  and the columns of

$$MM' = c^j \det M \text{Id} + MA, \quad (4-5)$$

Algorithm 3 uses  $(MM')^{-1}(M\mathbf{b}) = \mathbf{x}$  and the columns of  $(MM')^{-1}(MM') = \text{Id}$ . Then  $MM'\{q_0 \mathbf{x}\}$  is proposed as a short vector. It is indeed an element of the original lattice since the coordinates



of  $M'\{q_0\mathbf{x}\} \equiv q_0\mathbf{b} \bmod \mathbb{Z}^n$  are all integers. But it must be checked is that  $MM'\{q_0\mathbf{x}\}$  is short whenever  $\{q_0\mathbf{x}\}$  is. Part (2) of the proof is to make precise the insignificance of the second matrix summand,  $MA$ , in (4-5). We begin by computing how much multiplication by the full matrix in (4-5) is allowed to inflate the gap without invalidating the output of GDA or SAP.

By Minkowski's theorem [25], the magnitude of the shortest vector in the original lattice with respect to the  $\ell_\infty$ -norm is not more than  $|\det M|^{1/n}$ . So under an  $\ell_p$ -norm with  $p \in \mathbb{N}$ , the shortest vector has some magnitude, say  $\lambda$ , with  $(n^{1/p}|\det M|^{1/n})^p \geq \lambda^p \in \mathbb{Z}$ . In particular,  $n|\det M|^{2/n} \geq \lambda^2 \in \mathbb{Z}$  when  $p \in \{1, 2, \infty\}$ . Now, if  $\mathbf{q} \in \mathbb{Z}^n$  is such that  $\|M\mathbf{q}\|^2 < (a^2\lambda^2 + 1)/b^2$ , then it must be that  $\|M\mathbf{q}\| \leq a\lambda/b$  since there are no integers strictly between  $(a\lambda/b)^2$  and  $(a^2\lambda^2 + 1)/b^2$ . Thus multiplication by  $MM'$  may harmlessly inflate the gap between the norms of our output vector and shortest vector by anything less than

$$\frac{\sqrt{a^2\lambda^2 + 1}}{b\alpha\lambda} = \frac{\sqrt{a^2\lambda^2 + 1}}{a\lambda} \geq \frac{\sqrt{a^2n|\det M|^{2/n} + 1}}{a\sqrt{n}|\det M|^{1/n}}. \quad (4-6)$$

Scaling does not affect the ratio of vector norms, so to determine the effect of multiplication by (4-5) it suffices to consider the matrix

$$\text{Id} + MA/c^j \det M \quad (4-7)$$

instead. If  $\mathbf{q}_{\min}$  is a shortest nonzero vector in the simultaneous approximation lattice generated by  $\mathbb{Z}^n$  and  $\mathbf{x}$ , a shortest vector after applying (4-7) to this lattice has norm at least  $(1 - \|MA\|_{\text{op}}/|c^j \det M|)\|\mathbf{q}_{\min}\|$ . Similarly, the vector  $\{q_0\mathbf{x}\}$  obtained using  $q_0$  from line 11 increases in norm by at most a factor of  $(1 + \|MA\|_{\text{op}}/|c^j \det M|)$ . Combining this with our conclusion regarding (4-6) shows that it suffices to verify the following inequality holds:

$$\frac{1 + \|MA\|_{\text{op}}/|c^j \det M|}{1 - \|MA\|_{\text{op}}/|c^j \det M|} \leq \frac{\sqrt{a^2n|\det M|^{2/n} + 1}}{a\sqrt{n}|\det M|^{1/n}}. \quad (4-8)$$

Now solve for  $|c^j|$  to get a lower bound of

$$\frac{\sqrt{a^2n|\det M|^{2/n} + 1} + a\sqrt{n}|\det M|^{1/n}}{\sqrt{a^2n|\det M|^{2/n} + 1} - a\sqrt{n}|\det M|^{1/n}} \cdot \frac{\|MA\|_{\text{op}}}{|\det M|} < \frac{(5a^2n|\det M|^{2/n})\|MA\|_{\text{op}}}{|\det M|}.$$

Ignoring the powers of  $|\det M|$  on the right-hand side since  $2/n \leq 1$ , we see that  $j$  in line 8 is chosen to make the bound above agree exactly with Lemma 4.6.  $\square$

**Theorem 4.8.** *Let  $m = \max(a^{1/n^3}, M_{n,1})$ . The reduction in Algorithm 3 requires  $O(n^4 \log mn)$  operations on integers of length  $O(n^4 \log mn)$ .*

*Proof.* We will use that finding determinants, adjugates, inverses, or characteristic polynomials of  $n \times n$  matrices with entry magnitudes bounded by  $m$  requires  $O(n^3)$  operations on integers of length  $O(n \log mn)$ . For example, see Danilevsky's method for the characteristic polynomial [11] and the Bareiss algorithm for the others [5]. Note that we may then compute determinants of matrices with linear

polynomial entries in  $O(n^3)$  operations provided the matrix of linear terms or the matrix of constant terms is invertible.

In the proof of [Lemma 4.6](#) we showed that the prime  $p$  from line 1 is less than  $(\log M_{n,1}^{3n} n^n)/0.462$ . So finding it does not contribute to asymptotic complexity.

Now consider the **for** loop, where we must avoid recomputing the determinant in line 5 for each value of  $j$  in order to meet the prescribed bound on operations.

Let  $i \geq 3$  and fix some notation:  $M$  is its value after line 4,  $f_1 = (\text{adj } \check{M}_{i-1})_{i-1,1}$  and  $f_2 = (\text{adj } \check{M}_{i-1})_{i-1,2}$ ,  $g_1$  and  $g_2$  have degree at most  $i - 3$  and  $f_1 g_1 + f_2 g_2 = \det C(f_1, f_2) \neq 0$ , and for some  $j$ ,  $h_1 = (\text{adj } \check{M}_i)_{i,1} - p^j f_1$  and  $h_2 = (\text{adj } \check{M}_i)_{i,2} - p^j f_2$ . Note for computing  $(\text{adj } \check{M}_i)_{i,2}$  that the constant term matrix is not invertible (see (4-1)), which may also be true of the linear term matrix. Because this complicates combining the Bareiss and Danilevsky algorithms, we could find  $(\text{adj } \check{M}_i)_{i,2}$  indirectly by computing  $h_2$  for two values of  $j$  that produce an invertible constant term matrix (recall from (4-1) that  $f_2$  has nonzero constant term), and then solving for it.

Call the polynomials in the resulting column vector below  $h'_1$  and  $h'_2$ :

$$\begin{bmatrix} f_2 + p^j g_1 x^{2i-3} - f_1 + p^j g_2 x^{2i-3} \\ g_1 \qquad \qquad \qquad g_2 \end{bmatrix} \begin{bmatrix} h_1 \\ h_2 \end{bmatrix} = \begin{bmatrix} f_2(\text{adj } \check{M}_i)_{i,1} - f_1(\text{adj } \check{M}_i)_{i,2} - p^j \det C(f_1, f_2) x^{2i-3} \\ g_1(\text{adj } \check{M}_i)_{i,1} + g_2(\text{adj } \check{M}_i)_{i,2} - p^j \det C(f_1, f_2) \end{bmatrix}. \quad (4-9)$$

Remark that if  $j$  makes  $h'_1$  and  $h'_2$  avoid a common root, it does so for  $h_1$  and  $h_2$ .

View  $C(h'_1, h'_2)$  as a matrix with linear polynomial entries where  $p^j$  is the variable. This variable only appears in the leading term of  $h'_1$  and the constant term of  $h'_2$ . So  $p^j$  only occurs on the main diagonal of  $C(h'_1, h'_2)$ , where its coefficient is nonzero. In particular, the polynomial  $\det C(h'_1, h'_2)$  can be found in  $O(n^3)$  operations. Substituting different values of  $p^j$  into this polynomial until one is nonzero avoids repeatedly finding determinants. And note that we still need only test up to  $j = 2i - 2$  as stated in [Lemma 4.4](#) because the determinant of the matrix in (4-9) is a constant (a unit in  $\mathbb{Q}(x)$ ). Thus each **for** loop iteration requires  $O(n^3)$  operations.

The integers composing the linear polynomial matrix entries that begin each **for** loop iteration are small powers of  $p = O(n \log M_{n,1} n)$  and entries in the adjugate of the input matrix,  $M$ . By Hadamard's bound they are thus  $O(n \log M_{n,1} n)$  in length. Hadamard's bound also applies to the coefficients of  $(\text{adj } \check{M}_i)_{i,1}$  and  $(\text{adj } \check{M}_i)_{i,2}$ , making their lengths  $O(n^2 \log M_{n,1} n)$ . And it then applies again to make  $\det C((\text{adj } \check{M}_i)_{i,1}, (\text{adj } \check{M}_i)_{i,2})$  have length  $O(n^3 \log M_{n,1} n)$ . This is our bound on the length of  $c$  in line 6 and hence the length of  $c$  in line 7. The length of  $c^j$  in line 8 is then  $O(\max(\log a^2 (2M_{n,1} n)^{3n}, \log |c|)) = O(n^3 \log mn)$ , with the maximum accommodating the ceiling function. Then a final application of Hadamard's bound for lines 9 and 10 makes integer lengths  $O(n^4 \log mn)$ . This is therefore a bound on the number of operations required by the Euclidean algorithm in line 9.  $\square$

In [12], Dinur proves the NP-hardness of short vector problems under the  $\ell_\infty$ -norm when  $\alpha = n^{c/\log \log n}$  for some  $c > 0$  by giving a direct reduction from the Boolean satisfiability problem (SAT).

As a consequence, Theorems 4.7 and 4.8 prove the same for both good Diophantine approximation and simultaneous approximation problems. (There is no gap inflation for GDA in line 11 under the  $\ell_\infty$ -norm.)

**Corollary 4.9.** *Good Diophantine approximation and simultaneous approximation problems are NP-hard under the  $\ell_\infty$ -norm with  $\alpha = n^{c/\log \log n}$  for some  $c > 0$ .*  $\square$

This result is known for good Diophantine approximation [9], though the reduction  $\text{SAT} \rightarrow \text{SVP} \rightarrow \text{GDA}$  completed here is simpler. Chen and Meng adapt the work of Dinur as well as Rössner and Seifert [30] to reduce SAT to finding short integer vectors that solve a homogeneous system of linear equations (HLS) via an algorithm from [3], which changes the problem to finding pseudo-labels for a regular bipartite graph (PSL). The number of equations in the HLS system is then decreased to one (now called SIR), wherefrom a reduction to GDA is known [29]. Each link,  $\text{SAT} \rightarrow \text{PSL} \rightarrow \text{HLS} \rightarrow \text{SIR} \rightarrow \text{GDA}$ , is gap-preserving under the  $\ell_\infty$ -norm.

Short vector problems are only known to be NP-hard under the  $\ell_\infty$ -norm. But there are other hardness results under a general  $\ell_p$ -norm for which Theorems 4.7 and 4.8 can be considered complementary. See [19] for an exposition.

Another corollary is the reduction from a simultaneous approximation problem to GDA, giving the final row of Table 1. By Proposition 3.2, Algorithm 2 results in one call to SVP with integers of length  $O(n \log m)$ , where we can take  $m$  to be the maximum magnitude among  $a^{1/n^4}$  (still  $\alpha = a/b$ ) and the integers defining  $\mathbf{x}$ . Then Theorem 4.8 implies the reduction to GDA requires  $O(n^4 \log m^n n) = O(n^5 \log m)$  (absorbing the operations required by Algorithm 2) on integers of length  $O(n^5 \log m)$ .

**4C. Further discussion.** The last algorithm was restricted to an  $\ell_p$ -norm for  $p \in \{1, 2, \infty\}$ . So we will discuss what happens with a more general approach.

Multiplication by  $MM'$ , shown in (4-7), may change the gap between the length of the shortest vector in the simultaneous approximation lattice and that of the vector output by GDA or SAP. That this potential inflation does not invalidate our output relies on the set of vector norms being discrete and  $\alpha$  being rational — facts that were exploited to produce the expression in (4-6). The idea behind the paragraph preceding (4-6) is to find a nonempty interval  $(\alpha\lambda, \alpha'\lambda)$ , where  $\lambda = \min_{\mathbf{q} \in \mathbb{Z}^n}^\times \|\mathbf{M}\mathbf{q}\|$ , that contains no norms from the lattice defined by  $M$  (or even  $\mathbb{Z}^n$  for the interval tacitly given in the proof). This creates admissible inflation,  $\alpha'/\alpha$ , which equals (4-6).

The purpose of restricting to  $\ell_1$ ,  $\ell_2$ , or  $\ell_\infty$  is to facilitate finding this interval. Knowing that  $(b\alpha\lambda)^2 \in \mathbb{Z}$  for some  $b \in \mathbb{Z}$  simplifies the search for  $\alpha'$ . The same is true for any  $\ell_p$ -norm with  $p \in \mathbb{N}$ . But the immediate analogs of (4-6), (4-7), and (4-8) lead to a replacement for the very last bound used in the proof of the form

$$\frac{(5pa^pn|\det M|^{p/n})\|\mathbf{M}\mathbf{A}\|_{\text{op}}}{2|\det M|}.$$

This makes the number of operations needed to execute line 9 depend exponentially on the input length  $\log p$  (though it is still polynomial for any fixed  $p$ ). We have not taken into account, however, the possibility of a nontrivial lower bound for the difference between large consecutive integers which are

sums of  $n$  perfect  $p$ -th powers. Such a bound would allow for a longer interval,  $(\alpha\lambda, \alpha'\lambda)$ , that provably contains no lattice norms.

These arguments are all in effort to perfectly preserve the gap when reducing to SAP or, when  $p = \infty$ , GDA. The situation clarifies if a small amount of inflation is allowed. To solve a short vector problem with gap  $\alpha$  using SAP with gap  $\alpha' < \alpha$ , inequality (4-8) becomes

$$\frac{1 + \|MA\|_{\text{op}}/|c^j \det M|}{1 - \|MA\|_{\text{op}}/|c^j \det M|} \leq \frac{\alpha}{\alpha'}.$$

We still need to substitute a power of  $c$  for  $x$  in line 8 for the purpose of Lemma 4.5. Given these two constraints, it is sufficient to take  $M \leftarrow M(c^j)$  for

$$j = \left\lceil \log_{|c|} \frac{(\alpha + \alpha')\|MA\|_{\text{op}}}{(\alpha - \alpha')|\det M|} \right\rceil,$$

which can be made more explicit with Lemma 4.6. There is no need to insist that  $\alpha$  is rational or impose a restriction on  $p \in [1, \infty]$  defining the norm.

As a final note, the reduction to SAP again adapts to inhomogeneous forms of these problems while the reduction to GDA does not. If  $\mathbf{y} \in \mathbb{Q}^n$ , then the algorithm (which now reduces the *closest* vector problem) can end by solving the simultaneous approximation problem of finding  $q_0 \in \mathbb{Z}$  with  $\|q_0 \mathbf{x} - (MM')^{-1} \mathbf{y}\| \leq \alpha \min_{q \in \mathbb{Z}} \|q \mathbf{x} - (MM')^{-1} \mathbf{y}\|$ , using the matrix from (4-7). But unless we know that the last coordinate (where the 1 is located in (4-4)) of  $(MM')^{-1} \mathbf{y}$  is an integer, there is no clear modification to Proposition 2.1 that permits the use of GDA.

## References

- [1] M. Agrawal. [Simultaneous Diophantine approximation and short lattice vectors](#), 2019. Accessed: 2019-12-01.
- [2] F. Armknecht, C. Elsner, and M. Schmidt. Using the inhomogeneous simultaneous approximation problem for cryptographic design. In *Africacrypt*, pages 242–259. Springer, 2011.
- [3] S. Arora, L. Babai, J. Stern, and E. Sweedyk. The hardness of approximate optima in lattices, codes, and systems of linear equations. *J. Comput. System Sci.*, 54(2):317–331, 1997.
- [4] W. Baocang and H. Yupu. Public key cryptosystem based on two cryptographic assumptions. *IEE Proc. Comms.*, 152(6):861–865, 2005.
- [5] E. H. Bareiss. Sylvester’s identity and multistep integer-preserving Gaussian elimination. *Math. Comp.*, 22(103):565–578, 1968.
- [6] D. J. Bernstein and T. Lange. Post-quantum cryptography. *Nature*, 549(7671):188–194, 2017.
- [7] A. J. Brentjes. Multi-dimensional continued fraction algorithms. *MC Tracts*, 1981.
- [8] W. S. Brown. On Euclid’s algorithm and the computation of polynomial greatest common divisors. *J. ACM*, 18(4):478–504, 1971.
- [9] W. Chen and J. Meng. An improved lower bound for approximating Shortest Integer Relation in  $\ell_\infty$ -norm ( $\text{SIR}_\infty$ ). *Inform. Process. Lett.*, 101(4):174–179, 2007.
- [10] G. Cramer. *Introduction à l’analyse des lignes courbes algébriques*. Cramer & Cl. Philibert, 1750.
- [11] A. Danilevsky. On the numerical solution of the secular equation. *Mat. Sb.*, 44(2):169–172, 1937.
- [12] I. Dinur. Approximating  $\text{SVP}_\infty$  to within almost-polynomial factors is NP-hard. *Theor. Comput. Sci.*, 285(1):55–71, 2002.

- [13] A. Frank and É. Tardos. An application of simultaneous Diophantine approximation in combinatorial optimization. *Combinatorica*, 7(1):49–65, 1987.
- [14] S. D. Galbraith. *Mathematics of public key cryptography*. Cambridge University Press, 2012.
- [15] J. S. Hadamard. Résolution d’une question relative aux déterminants. *B. Sc. Math.*, 2:240–246, 1893.
- [16] H. Inoue, S. Kamada, and K. Naito. Simultaneous approximation problems of  $p$ -adic numbers and  $p$ -adic knapsack cryptosystems—Alice in  $p$ -adic numberland. *p-Adic Numbers Ultrametric Anal. Appl.*, 8(4):312–324, 2016.
- [17] H. Iwaniec. On the problem of Jacobsthal. *Demonstr. Math.*, 11(1):225–232, 1978.
- [18] R. Kannan and A. Bachem. Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix. *SIAM J. Comput.*, 8(4):499–507, 1979.
- [19] R. Kumar and D. Sivakumar. Complexity of SVP. *SIGACT News*, 32(3):40–52, 2001.
- [20] J. C. Lagarias. Knapsack public key cryptosystems and Diophantine approximation. In *Eurocrypt*, pages 3–23. Springer, 1984.
- [21] J. C. Lagarias. The computational complexity of simultaneous Diophantine approximation problems. *SIAM J. Comput.*, 14(1):196–209, 1985.
- [22] H. W. Lenstra, A. K. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 264(4):515–534, 1982.
- [23] M. Pohst. A modification of the LLL reduction algorithm. *J. Sym. Comp.*, 4(1):123–127, 1987.
- [24] D. Micciancio and S. Goldwasser. *Complexity of lattice problems: a cryptographic perspective*, volume 671. Springer Science & Business Media, 2012.
- [25] H. Minkowski. *Geometrie der zahlen*, volume 40. R. G. Teubner: Leipzig/Berlin, 1910.
- [26] P. Nguyen. Lattice reduction algorithms: Theory and practice. In *Eurocrypt*, pages 2–6. Springer, 2011.
- [27] C. Peikert. A decade of lattice cryptography. *Found. Trends Theor. Comput. Sci.*, 10(4):283–424, 2016.
- [28] J. B. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. Math.*, 6(1):64–94, 1962.
- [29] C. Rössner and J.-P. Seifert. Approximating good simultaneous Diophantine approximations is almost NP-hard. In *MFCS*, pages 494–505. Springer, 1996.
- [30] C. Rössner and J.-P. Seifert. On the hardness of approximating shortest integer relations among rational numbers. *Theor. Comput. Sci.*, 209(1-2):287–297, 1998.
- [31] A. Shamir. A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem. In *FOCS*, pages 145–152. IEEE, 1982.

Received 28 Feb 2020. Revised 1 Aug 2020.

DANIEL E. MARTIN: [daniel.e.martin@colorado.edu](mailto:daniel.e.martin@colorado.edu)

Department of Mathematics, University of Colorado, Boulder, CO, United States



# Computation of paramodular forms

Gustavo Rama and Gonzalo Tornara

We develop an algorithm to compute paramodular forms of weight 3 as orthogonal modular forms attached to positive definite quinary quadratic forms. For square-free levels we expect that every paramodular form of weight 3 arises in this way.

## Introduction

There are many efficient algorithms to compute classical (elliptic) modular forms (the Eichler–Selberg trace formula [Wad71], the method of modular symbols [Cre97], quaternion algebras and Brandt matrices [Piz80; Koh01], ternary quadratic forms [Bir91; Tor05; Ram14; HTV20], etc.) These have been used to compute extensive tables of modular forms [BK75; Cre97; Ste12; Cre19; LMF20].

Paramodular forms are Siegel modular forms for the paramodular group  $K(N)$  (see [PY15]). They have gained attention in recent years due to the paramodular conjecture of Brumer and Kramer [BK14; BK19] which relates them to abelian surfaces (see [BPP<sup>+</sup>19; BK17; BCGP18; CCG19] for recent progress on this conjecture). Poor and Yuen computed in [PY15] paramodular forms of weight 2 for  $K(p)$  for primes  $p < 600$ , and for square-free levels in [PSY17]. These methods compute Fourier coefficients of paramodular forms; from those one can recover the Hecke eigenvalues, although a large number of Fourier coefficients are needed. It is possible to compute Hecke eigenvalues without computing Fourier coefficients by the method of specialization as done in [BPP<sup>+</sup>19] but this is still expensive.

In this paper we develop an alternative algorithm to compute (Hecke eigenvalues of) paramodular forms of weight 3 using positive definite quinary quadratic forms. This is a generalization of a method of Birch to compute classical modular forms using ternary quadratic forms [Bir91; Hei16; HTV20]. Our method is based on a conjecture of Ibukiyama [Ibu07] which generalizes Eichler correspondence to paramodular forms. In principle it should be possible to extend this method for arbitrary weights  $\geq 3$ .

For prime levels, Ladd shows in his thesis [Lad18] that Ibukiyama conjecture implies that every orthogonal modular form corresponds to a paramodular form, in the sense that computing orthogonal modular forms of level  $O(\Lambda)$  for a well chosen lattice  $\Lambda$  recovers the Hecke eigenvalues of paramodular forms.

MSC2020: 11F55.

Keywords: paramodular forms, orthogonal modular forms.

However, not every paramodular form of prime level comes from an orthogonal modular form with trivial representation, as we show in [Example 13](#). In fact only the forms with sign  $+1$  in the functional equation seem to arise in this way. We overcome this limitation in [Section 3](#) by using orthogonal modular forms with a nontrivial character for the spinor norm (this idea has been proposed for ternary quadratic forms in [\[Tor05; Ram14\]](#), and completed in [\[HTV20\]](#)). Based on the dimension formulas of Ibukiyama [\[Ibu07\]](#) and on our computations of spaces of orthogonal modular forms we are led to conjecture that every paramodular form of prime level corresponds to some orthogonal modular form (see [Theorem 14](#) and [Conjecture 15](#)). We expect the same holds for composite square-free levels although we do not have as much evidence for composite levels as we do for prime levels.

An interesting feature of the space  $\mathcal{M}(\mathrm{O}(\hat{\Lambda}))$  of orthogonal modular forms with trivial character is the existence of a map  $\Theta$  from  $\mathcal{M}(\mathrm{O}(\hat{\Lambda}))$  to the space of elliptic modular forms of weight  $\frac{5}{2}$ . Because of properties of this map with respect to Hecke operators, when  $f$  is an eigenform in the cuspidal subspace  $\mathcal{S}(\mathrm{O}(\hat{\Lambda}))$  with  $\Theta(f) \neq 0$ , the Shimura lift of  $\Theta(f)$  is a modular form of weight 4 whose Gritsenko lift corresponds to  $f$ , as in the following diagram:

$$\begin{array}{ccc}
 \mathcal{S}(\mathrm{O}(\hat{\Lambda})) & \xrightarrow{\Theta} & S_{5/2}(4N) \\
 \uparrow \text{Ibukiyama} \downarrow & & \downarrow \text{Shimura} \\
 S_3(K(N)) & \xleftarrow{\text{Gritsenko}} & S_4(N)
 \end{array}$$

For prime level Hein, Ladd and Tornaría conjectured that, conversely, if  $\Theta(f) = 0$  then  $f$  corresponds to a paramodular form which is not a Gritsenko lift (see [\[Hei16, Conjecture 3.5.6\]](#)). The analogue of this conjecture for composite levels fails as shown in [Example 10](#), due to the occurrence of eigenforms of Yoshida type. We propose [Conjecture 12](#) as an alternative.

With respect to computations, Hein [\[Hei16\]](#) computed, in the case of trivial representation, the orthogonal modular forms with rational eigenvalues for quinary lattices of prime discriminant with  $p < 200$ , which (conjecturally) correspond to paramodular forms with  $+1$  in the functional equation. This was extended by Ladd [\[Lad18\]](#) for  $p < 400$ . Using our proposed algorithm we computed the orthogonal modular forms, with the different characters of the spinor norm, for quinary lattices of square-free discriminant  $D < 1000$ . We expect to have a complete list of all paramodular forms for those levels. This computations can be found in [\[RT20\]](#).

This article is organized as follows. In [Section 1](#) we recall the basic notions of neighbor lattices and orthogonal modular forms over  $\mathbb{Q}$ . In [Section 2](#) we consider quinary orthogonal modular forms over  $\mathbb{Q}$  and define the  $L$ -functions associated to a Hecke-eigenform in  $\mathcal{M}(\mathrm{O}(\hat{\Lambda}))$ . We also generalize the conjecture of Hein, Ladd and Tornaría to square-free levels.

In [Section 3](#) we introduce a family of nontrivial representations for  $\mathrm{O}(5)$  using characters of the spinor norm. We conjecture that with this representation we can obtain all paramodular form of prime level. In [Section 4](#) we study the orthogonal modular forms of discriminant  $5 \cdot 61$ , classify all the irreducible Hecke-submodules and conjecture that  $S_3(K(5 \cdot 61))$  is spanned by orthogonal modular forms. In [Section 5](#) we



consider the standard representation and compare the dimensions of spaces of orthogonal modular forms with this representation and the dimension of spaces of paramodular forms of weight 4.

In [Section 6](#) we match some hypergeometric motives with spaces of orthogonal modular forms with not square-free discriminant. In [Section 7](#) we mention the algorithms used to carry out our computations. Finally, in [Section 8](#) we include tables of orthogonal modular forms for prime levels  $p$ , with  $p < 500$ .

## 1. Neighbor lattices and orthogonal modular forms

In this section we follow the article of Greenberg and Voight [\[GV14\]](#) and the Ph.D. thesis of Hein [\[Hei16\]](#).

**1.1. Neighbor lattices.** We fix  $(V, Q)$ , a positive definite  $\mathbb{Q}$ -quadratic space.

**Definition.** Let  $\Lambda \subset V$  be a  $\mathbb{Z}$ -lattice, and  $k \geq 1$  an integer. We say that the  $\mathbb{Z}$ -lattice  $\Pi$  is a  $p^k$ -neighbor of  $\Lambda$  if  $\Lambda_q = \Pi_q$  for all primes  $q \neq p$  and there exist  $\mathbb{Z}$ -module isomorphisms

$$\Lambda/(\Lambda \cap \Pi) \cong \Pi/(\Lambda \cap \Pi) \cong (\mathbb{Z}/p\mathbb{Z})^k.$$

**Remark 1.** For  $k = 1$  the previous definition agrees with the classical definition of  $p$ -neighbors; see for example [\[Bir91\]](#).

**Lemma 2.** Let  $\Lambda, \Pi \subset V$  be two  $\mathbb{Z}$ -lattices both locally unimodular at a prime  $p$ . Then,  $\Lambda$  and  $\Pi$  are  $p^k$ -neighbors if and only if  $\Lambda_q = \Pi_q$  for all primes  $q \neq p$  and there exists a basis of  $V_p$

$$e_1, \dots, e_k, g_1, \dots, g_{n-2k}, f_1, \dots, f_k,$$

such that

- (1)  $\langle e_i, e_j \rangle = \langle f_i, f_j \rangle = 0$ ,
- (2)  $\langle e_i, f_j \rangle = \delta_{ij}$ ,
- (3)  $\langle e_i, g_j \rangle = \langle f_i, g_j \rangle = 0$ ,
- (4)  $e_1, \dots, e_k, g_1, \dots, g_{n-2k}, f_1, \dots, f_k$  is a  $\mathbb{Z}_p$ -basis of  $\Lambda_p$ , and
- (5)  $pe_1, \dots, pe_k, g_1, \dots, g_{n-2k}, p^{-1}f_1, \dots, p^{-1}f_k$  is a  $\mathbb{Z}_p$ -basis of  $\Pi_p$ .

If  $\Lambda$  is unimodular at  $p$ , we say that a basis that satisfies conditions (1)–(4) of the previous lemma is a  $p^k$ -standard basis for  $\Lambda_p$ . Consider a hyperbolic lattice  $H_p = \mathbb{Z}_p e \oplus \mathbb{Z}_p f$  with  $\langle e, e \rangle = \langle f, f \rangle = 0$ , and  $\langle e, f \rangle = 1$ . With respect to this basis, we consider  $\omega = \begin{pmatrix} p & 0 \\ 0 & p^{-1} \end{pmatrix} \in \mathrm{O}(H_p \otimes \mathbb{Q}_p)$ . We extend  $\omega$  to

$$\omega^{\oplus k} = \underbrace{\omega \oplus \dots \oplus \omega}_k \in \mathrm{O}(V_p),$$

where the  $i$ -th entry in the direct sum acts upon the hyperbolic component  $\{e_i, f_i\}$  given by a  $p^k$ -standard basis of  $\Lambda_p$ . We have that  $\Pi$  is a  $p^k$ -neighbor of  $\Lambda$  if and only if there exists  $\hat{\sigma}$  in  $\mathrm{O}(\hat{\Lambda})$  such that  $\hat{\Pi} = \hat{\sigma} \hat{\omega}^{\oplus k} \hat{\Lambda}$ . Also we have the following double coset decomposition

$$\mathrm{O}(\hat{\Lambda}) \hat{\omega}^{\oplus k} \mathrm{O}(\hat{\Lambda}) = \bigsqcup_m \hat{p}_m \mathrm{O}(\hat{\Lambda}), \quad (3)$$

where each  $\hat{p}_m$  corresponds to a  $p^k$ -neighbor of  $\Lambda$ .

**Lemma 4.** *Lattices (locally unimodular at  $p$ ) in the same genus have the same number of  $p^k$ -neighbors.*

The lemma allows us to define the integers  $N(\Lambda; p, k) = \#\text{Neighbors}(\Lambda; p, k)$ , which are genus invariants. By [Hei16, Equation 5.3.8] we have  $N(\Lambda; p, k) = O(p^{k(n-k-1)})$ . When  $n = 5$  we have a more precise formula,  $N(\Lambda; p, k) = p^{k-1}(p^3 + p^2 + p + 1)$  for  $k = 1, 2$  and  $\Lambda$  unimodular at  $p$ . When  $\Lambda$  is not unimodular at  $p$ , and  $p \parallel \text{disc}(\Lambda)$ , then  $N(\Lambda; p, 1) = (p^3 + p^2 + p) \pm p^2$ .

**1.2. Orthogonal modular forms.** Let  $\Lambda \subset V$  be a  $\mathbb{Z}$ -lattice with  $\text{disc}(\Lambda) = D$ , let  $W$  a finite-dimensional  $\mathbb{Q}$ -vector space, and let  $\rho : O(V) \rightarrow GL(W)$  a finite-dimensional representation. We define the space of orthogonal modular forms with level  $O(\hat{\Lambda})$  and weight  $W$  to be the finite dimensional  $\mathbb{Q}$ -vector space

$$\mathcal{M}(O(\hat{\Lambda}), W) = \{f : O(\hat{V}) \rightarrow W \mid f(\sigma \hat{g} \hat{k}) = \rho(\sigma)f(\hat{g}) \text{ for all } \sigma \in O(V), \hat{g} \in O(\hat{V}), \hat{k} \in O(\hat{\Lambda})\}.$$

The class set of  $\Lambda$  is in bijection with  $O(V) \backslash O(\hat{V}) / O(\hat{\Lambda})$  and we have the double coset decomposition

$$O(\hat{V}) = \bigsqcup_{i=1}^h O(V) \hat{x}_i O(\hat{\Lambda}),$$

where  $h$  is the class number of  $\Lambda$ , so the values of a modular form  $f \in \mathcal{M}(O(\hat{\Lambda}), W)$  are determined by the values  $f(\hat{x}_i)$ , for  $i = 1, \dots, h$ , and the representation  $\rho$ . We also have the following isomorphism

$$\begin{aligned} \mathcal{M}(O(\hat{\Lambda}), W) &\xrightarrow{\sim} \bigoplus_{i=1}^h W^{O(\Lambda_i)} \\ f &\longmapsto (f(\hat{x}_1), f(\hat{x}_2), \dots, f(\hat{x}_h)) \end{aligned}$$

where  $\Lambda_i = \hat{x}_i \hat{\Lambda} \cap V$ , for  $i = 1, 2, \dots, h$ , are representatives of the class set of  $\Lambda$ .

If  $p$  is a prime such that  $\Lambda$  is unimodular at  $p$ , and  $k \geq 1$ , we define the  $p^k$ -Hecke operator on  $\mathcal{M}(O(\hat{\Lambda}), W)$  given by

$$(T_{p,k} f)(\hat{g}) = \sum_m f(\hat{g} \hat{p}_m),$$

where the  $\hat{p}_m$  are given by the coset decomposition in (3). The Hecke operators  $T_{p,k}$  and  $T_{q,k'}$  commute for all  $p \neq q$  primes.

We can define an inner product in  $\mathcal{M}(O(\hat{\Lambda}), W)$  by

$$\langle\langle f, g \rangle\rangle = \sum_{i=1}^h \frac{f(\hat{x}_i)g(\hat{x}_i)}{\#O(\Lambda_i)},$$

note that  $\#O(\Lambda_i)$  is finite because  $V$  is positive definite. The Hecke operators  $T_{p,k}$  on  $\mathcal{M}(O(\hat{\Lambda}), W)$  are self-adjoint with respect to  $\langle\langle -, - \rangle\rangle$ .

We define the Eisenstein subspace, denoted by  $\mathcal{E}(O(\hat{\Lambda}), W) \subset \mathcal{M}(O(\hat{\Lambda}), W)$ , to be the subspace of constant functions of  $\mathcal{M}(O(\hat{\Lambda}), W)$ . The cuspidal subspace, denoted by  $\mathcal{S}(O(\hat{\Lambda}), W) \subset \mathcal{M}(O(\hat{\Lambda}), W)$ , is the subspace orthogonal to  $\mathcal{E}(O(\hat{\Lambda}), W)$ . The following lemma is clear.

**Lemma 5.** *If  $\rho : \mathrm{O}(V) \rightarrow \mathrm{GL}(W)$  is a nontrivial irreducible representation, then  $\mathcal{M}(\mathrm{O}(\hat{\Lambda}), W) = \mathcal{S}(\mathrm{O}(\hat{\Lambda}), W)$ .*

We denote by  $\mathcal{M}(\mathrm{O}(\hat{\Lambda}))$  the space of orthogonal modular forms when  $W = \mathbb{Q}$  and  $\rho$  the trivial representation, and the cuspidal subspace by  $\mathcal{S}(\mathrm{O}(\hat{\Lambda}))$ . Let  $f_1, \dots, f_h$  be the indicator basis of  $\mathcal{M}(\mathrm{O}(\hat{\Lambda}))$ , so that  $f_j(\hat{x}_i) = \delta_{ij}$ . We have

$$(T_{p,k} f_j)(\hat{x}_i) = \sum_m f_j(\hat{x}_i \hat{p}_m) = \sum_m f_j(\hat{x}_{m_*}) = \sum_m \delta_{jm_*},$$

where  $\hat{x}_i \hat{p}_m \hat{\Lambda} = \sigma \hat{x}_{m_*} \hat{\Lambda}$  for some  $\sigma \in \mathrm{O}(V)$  and some  $m_*$ . Let  $N_{ij}(\Lambda; p, k) = (T_{p,k} f_j)(\hat{x}_i)$ , the number of  $p^k$ -neighbors of  $\Lambda_i$  which are isomorphic to  $\Lambda_j$ . Then, we can compute  $T_{p,k}$  in the basis  $f_1, \dots, f_h$  by the formula

$$T_{p,k} f_j = \sum_{i=1}^h N_{ij}(\Lambda; p, k) f_i.$$

By Lemma 4 we have

$$N(\Lambda; p, k) = \sum_{j=1}^h N_{ij}(\Lambda; p, k),$$

for all  $i = 1, \dots, h$ , and  $f_1 + \dots + f_h$  is an eigenvector of  $\mathcal{M}(\mathrm{O}(\hat{\Lambda}))$  with eigenvalue  $N(\Lambda; p, k)$ . Also,  $f_1 + \dots + f_h$  is a generator of  $\mathcal{E}(\mathrm{O}(\hat{\Lambda}))$ , and we conclude that  $\dim \mathcal{M}(\mathrm{O}(\hat{\Lambda})) = \dim \mathcal{S}(\mathrm{O}(\hat{\Lambda})) + 1$ .

We want to define  $T_{p,1}$  for  $\mathcal{M}(\mathrm{O}(\hat{\Lambda}))$  when  $p \parallel D$ . Since  $\Lambda$  is not unimodular at  $p$ , we cannot use Lemma 2, so we define it in the indicator basis

$$T_{p,1} f_j = f_j + \sum_{i=1}^h N_{ij}(\Lambda; p, 1) f_i.$$

This operator is well defined because  $N_{ij}(\Lambda; p, 1)$  is well defined in all cases; see [Tor05, Theorem 3.5].

Sometimes it will be convenient to use the dual basis of  $\mathcal{M}(\mathrm{O}(\hat{\Lambda}))$ , such that  $e_j = (1/\#\mathrm{O}(\Lambda_i)) f_j$ . We define the theta series map as the linear map

$$\Theta : \mathcal{M}(\mathrm{O}(\hat{\Lambda})) \rightarrow M_{5/2}(4D),$$

given in the dual basis by

$$\Theta(e_i) = \Theta(\Lambda_i) = \sum_{v \in \Lambda_i} q^{Q(v)}.$$

## 2. Orthogonal modular forms for $\mathrm{O}(5)$

We consider now positive definite  $\mathbb{Q}$ -quadratic spaces  $(V, Q)$  with  $\dim V = 5$ . In 2014 Hein, Ladd, and Tornara conjectured that, if  $f \in \mathcal{M}(\mathrm{O}(\hat{\Lambda}))$  is a Hecke-eigenform, with  $\mathrm{disc}(\Lambda) = p$  a prime, and  $\Theta(f) = 0$ , then the  $L$ -function associated to  $f$  is attached to a paramodular form of weight 3 which is not a Gritsenko lift. This can be found in [Hei16, Conjecture 3.5.6]. Also, Hein [Hei16] computed the

good Euler factors for primes less than 100 for all the forms with rational eigenvalues for prime levels up to 200, and Ladd [Lad18] computed the good Euler factors for odd primes up to 31 for all the forms with rational eigenvalues for prime levels up to 400.

As  $\dim V = 5$  we only have  $p^k$ -neighbors for  $k = 1, 2$ . Given  $f \in \mathcal{M}(\mathrm{O}(\hat{\Lambda}))$  a Hecke-eigenform and  $p$  prime, let  $\lambda_{p,1}$  and  $\lambda_{p,2}$  be the eigenvalues of  $T_{p,1}$  and  $T_{p,2}$  for  $f$ . We define its (spin)  $L$ -function by the Euler product

$$L(f, s) := \prod_{p \text{ prime}} L_p(f, p^{-s})^{-1},$$

where the local Euler factors are given by

$$L_p(f, X) := 1 - \lambda_{p,1}X + (\lambda_{p,2} + 1 + p^2)pX^2 - \lambda_{p,1}p^3X^3 + p^6X^4, \quad \text{if } p \nmid D. \tag{6}$$

This is obtained by considering the Satake polynomial on  $\mathrm{SO}(5)$ , found in Murphy [Mur13, page 76], with a suitable change of variable. And

$$L_p(f, X) := (1 + \epsilon_p pX)(1 - (\lambda_{p,1} + \epsilon_p p)X + p^3X^2), \quad \text{if } p \parallel D, \tag{7}$$

where the local root number  $\epsilon_p = c(V_p)$ . Here  $c(V_p)$  is the Witt invariant of  $V$  at  $p$  as defined by Lam in [Lam05, page 117]. Note that for  $\dim V = 5$  it coincides for all odd  $p$  with the Hasse invariant as defined in Cassels [Cas78, Chapter 4], but is the opposite for  $p = 2$  (see [Lam05, Proposition 3.20]). The last polynomial is similar to the one found in [Ibu07, Theorem 4.1]. We define it this way, along  $T_{p,1}$  for  $p \parallel D$  so that the analogue formula for  $L_p$  in the next section, in which we use a nontrivial one dimensional representation, is symmetrical to this one.

When  $D$  is square-free it is conjectured that the  $L$ -functions satisfy the functional equation

$$\tilde{L}(f, s) = \tilde{L}(f, 4 - s),$$

where

$$\tilde{L}(f, s) = \left(\frac{D}{\pi^2}\right)^{s/2} \Gamma\left(\frac{s-1}{2}\right) \Gamma\left(\frac{s}{2}\right)^2 \Gamma\left(\frac{s+1}{2}\right) L(f, s). \tag{8}$$

**Example 9** ( $D = 61$ ). Let the quadratic space  $V = \mathbb{Q}^5$ , and  $Q = x^2 + xy - xt + y^2 - yt + z^2 + 2w^2 - wt + 3t^2$  a quadratic form of discriminant 61, and let  $\Lambda = \mathbb{Z}^5$ . This is the first example of prime discriminant in  $\mathrm{O}(5)$  for which the theta series map on the genus has a nontrivial kernel, of dimension 1. As noted in [Hei16], there exists a Hecke-eigenform  $f \in \mathcal{M}(\mathrm{O}(\hat{\Lambda}))$  such that  $\Theta(f) = 0$ . Also the  $L$  factors of  $f$  for 2, 3, 5 match those of the nonlift paramodular form of level 61 as computed by Ash, Gunnels and McConnell in [AGM08, Section 4] (see also Poor and Yuen [PY15, Section 8]).

By the formulas of Ibukiyama [Ibu07] we have

$$\dim S_3(K(61)) = \dim S(\mathrm{O}(\hat{\Lambda})) = \dim S_4^-(61) + \dim \ker \Theta.$$

Therefore we expect the correspondence from  $S(\mathrm{O}(\hat{\Lambda}))$  to  $S_3(K(61))$  is a bijection.

**Example 10** ( $D = 55$ ). We consider the quadratic space  $V = \mathbb{Q}^5$ ,  $Q = x^2 + xy + y^2 + z^2 + 2t^2 + yw + zw + tw + 3w^2$ , and  $\Lambda = \Lambda_1 = \mathbb{Z}^5$ . The Hasse invariant of the genus at 5 is +1, and at 11 is -1. There are 3 other  $\mathbb{Z}$ -lattices in the genus of  $\Lambda$ , namely  $\Lambda_2, \Lambda_3, \Lambda_4$ . The quadratic forms associated to the bases of  $\Lambda_i$ , for  $i = 2, 3, 4$ , are

$$Q_2 = x^2 + xy + y^2 + xz + z^2 + 3t^2 + zw + 2tw + 3w^2,$$

$$Q_3 = x^2 + xy + y^2 + xz + z^2 + yt + 3t^2 + zw + 3w^2,$$

$$Q_4 = x^2 + y^2 + 2z^2 + yt + 2zt + 2t^2 + xw + yw + zw + tw + 2w^2.$$

Let  $f = 2e_1 - 2e_2 + e_3 - e_4 \in \mathcal{M}(\mathcal{O}(\hat{\Lambda}))$ , which is a Hecke-eigenform, where  $\{e_1, e_2, e_3, e_4\}$  is the dual basis of  $\mathcal{M}(\mathcal{O}(\hat{\Lambda}))$ . It is easy to see that  $\Theta(f) = 2\Theta(\Lambda_1) - 2\Theta(\Lambda_2) + \Theta(\Lambda_3) - \Theta(\Lambda_4) = 0$ . This is because the Sturm bound for the space  $M_{5/2}(4 \cdot 55)$  is 90 (note that the Sturm bound of half-integral weight is the same as the integral case; see for example [GK13, Lemma 3.1]), and the first 90 coefficients of  $\Theta(f)$  are 0.

By [IK17] we know that  $\dim S_3(K(55)) = 3$ . On the other hand the space of classical cusp forms of weight 4, level 55 and sign -1 has dimension 3, this can be found in [LMF20]. There are two such forms, one of dimension 1, and one of dimension 2. We conclude that the space  $S_3(K(55))$  is spanned by Gritsenko lifts. We verified that  $f$  is not a Gritsenko lift by looking at its eigenvalues, and we conclude that the conjecture mentioned is no longer valid when  $D$  is not prime.

We computed the eigenvalues of  $T_{p,1}$  of  $f$  for  $p < 300$ , also the eigenvalues of  $T_{p,2}$  for  $p < 50$ , and we conclude.

**Theorem 11.** For  $p < 50$ ,  $p \neq 5, 11$

$$L_p(f, X) = (1 - pa_pX + p^3X^2)(1 - b_pX + p^3X^2),$$

where  $a_p$  is the  $p$ -th Fourier coefficient of the Hecke-eigenform of weight 2 and level 11,  $g_{11}$ , and  $b_p$  is the  $p$ -th Fourier coefficient of the Hecke-eigenform of weight 4 and level 5,  $g_5$ .

Also, for  $p < 300$

$$L_p(f, X) = 1 - (pa_p + b_p)X + O(X^2).$$

The above theorem leads us to conjecture that  $L(f, s) = L(g_{11}, s - 1)L(g_5, s)$ , so that  $f$  should correspond to some Siegel modular form of Yoshida type. By the previous reasoning  $f$  cannot correspond to a form in  $S_3(K(55))$ .

**Conjecture 12.** Let  $f \in \mathcal{M}(\mathcal{O}(\hat{\Lambda}))$  be a Hecke-eigenform, with  $D$  square-free and  $\Theta(f) = 0$ . Then  $f$  corresponds either to a paramodular form of weight 3 which is not a Gritsenko lift or to a modular form of Yoshida type as in the example above.

**Example 13.** ( $D = 167$ ) Let  $V = \mathbb{Q}^5$  and

$$Q_{167} = x^2 + xy + y^2 + z^2 + xt + zt + t^2 + tw + 34w^2,$$

a quinary quadratic form with discriminant 167. The genus of  $\Lambda = \mathbb{Z}^5$  has 19 isometry classes, so we have that  $\dim \mathcal{S}(\mathcal{O}(\hat{\Lambda})) = 18$ . On the other hand we have  $\dim S_3(K(167)) = 19$ , and we see that the correspondence from  $\mathcal{S}(\mathcal{O}(\hat{\Lambda}))$  into  $S_3(K(167))$  is not surjective. According to [GPY19, Table 1] this is the first known case of a paramodular newform of weight 3 with sign  $-1$  in the functional equation. See also [AGM10, Table 4].

### 3. The missing forms

As seen in the previous example, for a prime  $p$ , not all forms in  $S_3(K(p))$  correspond to forms in  $\mathcal{S}(\mathcal{O}(\hat{\Lambda}))$ , with  $\text{disc}(\Lambda) = p$ . Moreover, the forms in  $\mathcal{S}(\mathcal{O}(\hat{\Lambda}))$  have sign  $+1$  in their associated  $L$ -function. To find the remaining paramodular forms we introduce a representation using the spinor norm. With this representation, we can obtain orthogonal modular forms with sign  $-1$  in their associated  $L$ -function. See [HTV20] for a more detailed presentation of this idea in the case of ternary quadratic forms.

If  $d \mid D$ , we define the character  $\nu_d : \mathbb{Q}_{>0}^\times / \mathbb{Q}_{>0}^{\times 2} \rightarrow \{\pm 1\}$ , defined in primes by

$$\nu_d(p) = \begin{cases} -1 & \text{if } p \mid d, \\ 1 & \text{otherwise.} \end{cases}$$

We define the representation  $\rho_d : \mathcal{O}(V) \rightarrow \{\pm 1\} \subset \mathbb{Q}^\times \cong \text{GL}(\mathbb{Q})$  by

$$\rho_d(\sigma) = \nu_d(\theta(\pm\sigma)) \text{ if } \sigma \in \mathcal{O}^\pm(V),$$

where  $\theta : \mathcal{O}^+(V) \rightarrow \mathbb{Q}^\times / (\mathbb{Q}^\times)^2$  is the spinor norm. We denote the space of orthogonal modular forms for this representation  $\mathcal{M}_d(\mathcal{O}(\hat{\Lambda}))$ , and the cuspidal subspace by  $\mathcal{S}_d(\mathcal{O}(\hat{\Lambda}))$ . In this case

$$\mathcal{M}_d(\mathcal{O}(\hat{\Lambda})) \cong \bigoplus_{i=1}^h \mathbb{Q}^{\mathcal{O}(\Lambda_i)},$$

where  $\mathbb{Q}^{\mathcal{O}(\Lambda_i)} = \mathbb{Q}$  if and only if  $\nu_d(\sigma) = 1$  for all  $\sigma \in \mathcal{O}^+(\Lambda_i)$ .

Let  $\{t_1 < \dots < t_{h_d}\} = \{t : \mathbb{Q}^{\mathcal{O}(\Lambda_t)} = \mathbb{Q}\}$ , and  $f_{t_j} \in \mathcal{M}_d(\mathcal{O}(\hat{\Lambda}))$  such that  $f_{t_j}(\hat{x}_i) = \delta_{t_j i}$ , so  $\{f_{t_1}, \dots, f_{t_{h_d}}\}$  is a basis of  $\mathcal{M}_d(\mathcal{O}(\hat{\Lambda}))$ .

If  $p$  is a prime such that  $\Lambda$  is unimodular at  $p$ , and  $k \geq 1$ , by definition of the Hecke operator we have

$$(T_{p,k} f_{t_j})(\hat{x}_i) = \sum_m f_{t_j}(\hat{x}_i \hat{p}_m) = \sum_m \rho_d(\sigma) f_{t_j}(\hat{x}_{m_*}) = \sum_m \rho_d(\sigma) \delta_{t_j m_*},$$

where  $\hat{x}_i \hat{p}_m \hat{\Lambda} = \sigma \hat{x}_{m_*} \hat{\Lambda}$ . Henceforth, to compute  $(T_{p,k} f_{t_j})(\hat{x}_i)$ , we sum  $\rho_d(\sigma)$  over  $\sigma \in \mathcal{O}(V)$  such that  $\sigma \Pi_m = \Lambda_{t_j}$ , where the  $\Pi_m$  are the  $p^k$ -neighbors of  $\Lambda_i$ , and we define that sum as  $N_{i t_j}^d(\Lambda; p, k)$ . We get the formula

$$T_{p,k} f_{t_j} = \sum_{i=1}^{h_d} N_{i t_j}^d(\Lambda; p, k) f_{t_i}.$$

We define  $T_{p,1}$  for  $\mathcal{M}_d(\mathcal{O}(\hat{\Lambda}))$  when  $p \parallel D$  by

$$T_{p,1} f_{t_j} = v_d(p) \left( f_{t_j} + \sum_{s=1}^{h_d} N_{t_i t_j}^d(\Lambda; p, 1) f_{t_i} \right).$$

Given a Hecke-eigenform  $f \in \mathcal{S}_d(\mathcal{O}(\hat{\Lambda}))$  we want to define its (spin)  $L$ -function. As before, we define it by the Euler product

$$L(f, s) = \prod_p L_p(f, p^{-s})^{-1}$$

where  $L_p$  is defined with the same equation as (6), if  $p \nmid D$ . When  $p \parallel D$  we use (7), where the local root number is  $\epsilon_p = v_d(p) c(V_p)$ . When  $D$  is square-free we conjecture that the  $L$ -function satisfy the functional equation

$$\tilde{L}(f, s) = v_d(D) \tilde{L}(f, 4 - s),$$

where  $\tilde{L}$  is defined as (8).

**Example 13** ( $D = 167$ , continued). For  $d = p$  we have  $\dim \mathcal{S}_{167}(\mathcal{O}(\hat{\Lambda})) = 1$ , and

$$\dim \mathcal{S}_3(K(167)) = \dim \mathcal{S}(\mathcal{O}(\hat{\Lambda})) + \dim \mathcal{S}_{167}(\mathcal{O}(\hat{\Lambda})).$$

Let  $f \in \mathcal{S}_{167}(\mathcal{O}(\hat{\Lambda}))$ ,  $f \neq 0$ . It is a Hecke-eigenform because the dimension of the space is 1. In Table 1 we show the Hecke-eigenvalues of  $T_{p,1}$  for  $f$  with  $p < 500$ . And in Table 2 the Hecke-eigenvalues of  $T_{p,2}$  for  $f$  with  $p < 50$ . With the previous data we constructed an  $L$ -function in PARI/GP [PAR18] using the routine `lfuncreate` providing the first 502 Dirichlet coefficients, and verified by the `lfuncheckfeq` routine, returning a verification accuracy of 90 bits of precision.

**3.1. A conjecture for prime level.** Let  $p$  prime, and  $\Lambda_p$  be a lattice in the unique genus of quinary quadratic forms of discriminant  $p$ . We verified computationally the following theorem.

**Theorem 14.** For  $p < 7000$

$$\dim \mathcal{S}_3(K(p)) = \dim \mathcal{S}(\mathcal{O}(\hat{\Lambda}_p)) + \dim \mathcal{S}_p(\mathcal{O}(\hat{\Lambda}_p)).$$

Which leads us to the following conjecture.

**Conjecture 15.** For prime  $p$  there is a Hecke-equivariant isomorphism

$$\mathcal{S}_3(K(p)) \cong \mathcal{S}(\mathcal{O}(\hat{\Lambda}_p)) \oplus \mathcal{S}_p(\mathcal{O}(\hat{\Lambda}_p)).$$

Also,  $\mathcal{S}(\mathcal{O}(\hat{\Lambda}_p))$  correspond to the forms of  $\mathcal{S}_3(K(p))$  such that their associated  $L$ -function has sign  $+1$  in its functional equation, and  $\mathcal{S}_p(\mathcal{O}(\hat{\Lambda}_p))$  correspond to the forms such that their associated  $L$ -function has sign  $-1$  in its functional equation.

$p$	$\lambda_{p,1}$	$p$	$\lambda_{p,1}$	$p$	$\lambda_{p,1}$	$p$	$\lambda_{p,1}$	$p$	$\lambda_{p,1}$
2	-8	71	-481	167	-2707	271	2954	389	5316
3	-10	73	-744	173	-182	277	-8334	397	4324
5	-4	79	927	179	2568	281	-2942	401	-4679
7	-14	83	-632	181	-2804	283	6360	409	-3476
11	-22	89	-297	191	-3035	293	-856	419	-910
13	-4	97	2	193	583	307	3548	421	3552
17	-47	101	-992	197	2276	311	-6322	431	-4878
19	-12	103	-1222	199	6754	313	-9443	433	15213
23	41	107	1436	211	360	317	108	439	-6909
29	50	109	-954	223	3569	331	1596	443	-7130
31	-504	113	19	227	-3346	337	-2129	449	12908
37	-102	127	516	229	2220	347	1856	457	-4005
41	174	131	-258	233	-2780	349	480	461	-7334
43	30	137	1080	239	-3878	353	1704	463	-77
47	42	139	1030	241	-819	359	4601	467	12248
53	156	149	-974	251	6112	367	6298	479	6447
59	-252	151	-1119	257	-5343	373	-4998	487	-14197
61	472	157	1152	263	-808	379	7706	491	1960
67	106	163	108	269	3592	383	-18293	499	3288

**Table 1.** Hecke-eigenvalues of  $T_{p,1}$  for  $f \in \mathcal{S}_{167}(\mathrm{O}(\hat{\Lambda}))$ ,  $p < 500$ .

4. Composite levels

When  $D$  is composite, as already seen in [Example 10](#), the space of orthogonal modular forms includes Yoshida lifts, which do not correspond to paramodular forms.

In this section we investigate orthogonal modular forms for  $D = 305 = 5 \cdot 61$ . We have two genera of quintic positive definite quadratic forms, namely, let  $\Lambda_1$  and  $\Lambda_2$  be lattices of dimension 5 such that  $\mathrm{disc}(\Lambda_i) = 5 \cdot 61$  and

$$\begin{aligned} \epsilon_5(\Lambda_1) &= -1 & \epsilon_5(\Lambda_2) &= +1 \\ \epsilon_{61}(\Lambda_1) &= +1 & \epsilon_{61}(\Lambda_2) &= -1 \end{aligned}$$

We computed  $\mathcal{S}_d(\mathrm{O}(\hat{\Lambda}_i))$ , for  $d \in \{1, 5, 61, 5 \cdot 61\}$ ,  $i = 1, 2$ , as well as  $T_{p,1}$  and  $T_{p,2}$  for  $p$  prime  $p < 20$ , with the convention that

$$\mathcal{S}_1(\mathrm{O}(\hat{\Lambda}_i)) := \mathcal{S}(\mathrm{O}(\hat{\Lambda}_i)).$$

$p$	$\lambda_{p,2}$	$p$	$\lambda_{p,2}$	$p$	$\lambda_{p,2}$	$p$	$\lambda_{p,2}$	$p$	$\lambda_{p,2}$
2	10	7	-9	17	260	29	-187	41	800
3	11	11	-67	19	41	31	2744	43	442
5	-44	13	-158	23	-198	37	-730	47	-5052

**Table 2.** Hecke-eigenvalues of  $T_{p,2}$  for  $f \in \mathcal{S}_{167}(\mathrm{O}(\hat{\Lambda}))$ ,  $p < 50$ .



		A-L		Dim		$\subset \ker \Theta$		Traces				
		$\epsilon_5$	$\epsilon_{61}$					$\lambda_{2,1}$	$\lambda_{3,1}$	$\lambda_{5,1}$	$\lambda_{7,1}$	$\lambda_{11,1}$
$\mathcal{S}_1(\mathcal{O}(\hat{\Lambda}_1))$	$A_1$	−	+	8	Yes	1	−21	12	−28	−10		
	$A_2$	−	+	9	No	57	119	69	505	1338		
	$A_3$	−	+	13	No	73	129	455	647	1660		
$\mathcal{S}_{61}(\mathcal{O}(\hat{\Lambda}_1))$	$B_1$	−	−	1		−4	−12	−4	9	−13		
$\mathcal{S}_{5,61}(\mathcal{O}(\hat{\Lambda}_1))$	$C_1$	+	−	1		−2	2	−2	−19	21		
	$C_2$	+	−	1		2	−6	10	−3	29		
	$C_3$	+	−	8		3	−27	−6	−58	−54		
	$C_4$	+	−	13		81	157	325	669	1652		
$\mathcal{S}_1(\mathcal{O}(\hat{\Lambda}_2))$	$D_1$	+	−	1	No	2	14	25	62	164		
	$D_2$	+	−	1	Yes	−7	−3	28	−9	−4		
	$D_3$	+	−	1	Yes	−2	2	−2	−19	21		
	$D_4$	+	−	1	Yes	2	−6	10	−3	29		
	$D_5$	+	−	3	Yes	−10	12	−20	−3	239		
	$D_6$	+	−	6	No	29	59	314	309	612		
	$D_7$	+	−	8	Yes	3	−27	−6	−58	−54		
	$D_8$	+	−	13	No	81	157	325	669	1652		
$\mathcal{S}_5(\mathcal{O}(\hat{\Lambda}_2))$	$E_1$	−	−	1		−7	−3	−22	−9	−4		
	$E_2$	−	−	1		−4	−12	−4	9	−13		
$\mathcal{S}_{61}(\mathcal{O}(\hat{\Lambda}_2))$	$F_1$	+	+	1		−6	−4	−20	13	−23		
$\mathcal{S}_{5,61}(\mathcal{O}(\hat{\Lambda}_2))$	$G_1$	−	+	8		1	−21	12	−28	−10		
	$G_2$	−	+	13		73	129	455	647	1660		

**Table 3.** Decomposition of  $\mathcal{S}_d(\mathcal{O}(\hat{\Lambda}_i))$ , with  $\text{disc}(\Lambda_i) = 5 \cdot 61$ .

The decomposition of these spaces is shown in Table 3. We show the dimensions of the subspaces, the local root numbers, for  $d = 1$  whether they are in the kernel of the theta map, and the traces of the eigenvalues  $\lambda_{p,1}$  for  $p \leq 11$ .

The subspaces  $A_2$  and  $D_1$  correspond to the classical modular forms of weight 4 and sign + of levels 61 and 5 respectively (61.4.a.b and 5.4.a.a in [LMF20]). By this we mean that  $\lambda_{p,1} = a_p + p + p^2$  where  $a_p$  is the eigenvalue of the classical modular form, just as for Gritsenko lifts, but since the sign is + they do not lift to  $\mathcal{S}_3(K(D))$ .

The subspaces  $D_5$  and  $F_1$  are of Yoshida type as in Example 10 ( $D_5$  corresponds to the pair 61.2.a.b and 5.4.a.a, and  $F_1$  corresponds to the pair 61.2.a.a and 5.4.a.a). By [Sch18] they also do not lift to  $\mathcal{S}_3(K(D))$ .

The subspaces  $A_3$ ,  $C_4$ ,  $D_6$ ,  $D_8$  and  $G_2$  correspond to classical modular forms of weight 4 and sign − of level 61 (for  $D_6$ ) and 305 (for the other four), so they appear as Gritsenko lifts in  $\mathcal{S}_3(K(D))$ . Also  $A_3$  and  $G_2$ ,  $C_4$  and  $D_8$  lift from the same space.

The subspaces  $D_2$  and  $E_1$  come from the nonlift orthogonal modular form in  $\mathcal{S}(\mathrm{O}(\hat{\Lambda}_{61}))$  (see [Example 9](#)). The subspace  $D_2$  has sign  $-$ , and  $E_1$  has sign  $+$ , and the eigenvalues  $\lambda_{5,1}$  are different, and they have the same eigenvalues otherwise. The subspaces  $A_1, B_1, C_1, C_2, C_3, D_3, D_4, D_7, E_2$  and  $G_1$  are nonlifts. Also, we conjecture that  $A_1$  and  $G_1, B_1$  and  $E_2, C_1$  and  $D_3, C_2$  and  $D_4$ , and  $C_3$  and  $D_7$  are isomorphic as Hecke-modules.

By the formulas found in [\[IK17\]](#)  $\dim S_3(5 \cdot 61) = 53$ . By counting dimensions and the previous descriptions, we conjecture

$$S_3(K(5 \cdot 61)) \cong A_1 \oplus B_1 \oplus C_1 \oplus C_2 \oplus C_3 \oplus D_2 \oplus E_1 \oplus A_3 \oplus C_4 \oplus D_6$$

We expect that, for square-free  $D$ , the space  $S_3(K(D))$  is always spanned, as Hecke module, by orthogonal modular forms corresponding to quinary lattices of discriminant  $D$  as in this example, which would give a nice algorithm to compute (the eigenvalues of) all paramodular forms of square-free level.

## 5. Paramodular forms of higher dimension

Prompted by a question of Eran Assaf we consider the proper standard representation of  $\mathrm{O}(5)$

$$\mathrm{std}^+ : \mathrm{O}(V) \rightarrow \mathrm{GL}(V)$$

$$\sigma \mapsto \det(\sigma)\sigma$$

If  $\mathrm{disc}(V) = p$ , for a prime  $p$ , we also consider the representation  $\mathrm{std}_p^+ := \mathrm{std}^+ \otimes \rho_p$ . We computed the dimensions of  $\mathcal{S}(\mathrm{O}(\hat{\Lambda}_p), \mathrm{std}_p^+)$  and  $\mathcal{S}(\mathrm{O}(\hat{\Lambda}_p), \mathrm{std}^+)$ , for primes  $p < 100$ , as seen in [Table 4](#). We can see that

$$\dim S_4(K(p)) = \mathcal{S}(\mathrm{O}(\hat{\Lambda}_p), \mathrm{std}_p^+) + \mathcal{S}(\mathrm{O}(\hat{\Lambda}_p), \mathrm{std}^+).$$

As before we have the Gritenko lift from  $S_6^-(p)$  to  $S_4(K(p))$ . We note that the first prime such that the difference of the dimensions of the mentioned spaces is 1 is  $p = 31$ . We conjecture that there is an eigenform in  $\mathcal{S}(\mathrm{O}(\hat{\Lambda}_{31}), \mathrm{std}_{31}^+)$  corresponding to a nonlift paramodular form in  $S_4(K(31))$ , with sign  $+$  in the functional equation of its spin  $L$ -function.

We also note that the first  $p$  where  $\dim \mathcal{S}(\mathrm{O}(\hat{\Lambda}_p), \mathrm{std}^+) > 0$  is 83. We conjecture that the eigenform in  $\mathcal{S}(\mathrm{O}(\hat{\Lambda}_{83}), \mathrm{std}^+)$  correspond to a nonlift paramodular form in  $S_4(K(83))$ , with sign  $-$  in the functional equation of its spin  $L$ -function.

In future work we plan to compute the decomposition of these spaces for weights higher than 4.

## 6. Hypergeometric motives

Hypergeometric motives with Hodge vector  $(1, 1, 1, 1)$  are geometric objects which are (conjecturally) expected to correspond to Siegel modular forms of weight 3. For an introduction to hypergeometric motives see [\[Rob15\]](#). David Roberts (personal communication, 2018) has computed a list of some such hypergeometric motives with conductors at most 400. David Yuen and Chris Poor have found matching

$p$	2	3	5	7	11	13	17	19	23	29	31	37
$\dim(\mathcal{S}(\hat{\Lambda}_p), \text{std}_p^+)$	0	0	0	1	1	2	2	3	3	3	6	8
$\dim(\mathcal{S}(\hat{\Lambda}_p), \text{std}^+)$	0	0	0	0	0	0	0	0	0	0	0	0
$\dim S_4(K(p))$	0	0	0	1	1	2	2	3	3	3	6	8
$\dim S_6^-(p)$	0	0	0	1	1	2	2	3	3	3	5	7
$p$	43	47	53	59	61	67	71	73	79	83	89	97
$\dim(\mathcal{S}(\hat{\Lambda}_p), \text{std}_p^+)$	9	8	10	11	16	17	15	21	22	18	23	32
$\dim(\mathcal{S}(\hat{\Lambda}_p), \text{std}^+)$	0	0	0	0	0	0	0	0	0	1	0	0
$\dim S_4(K(p))$	9	8	10	11	16	17	15	21	22	19	23	32
$\dim S_6^-(p)$	8	7	9	9	11	13	11	14	14	14	15	19

**Table 4.** Dimensions of spaces of orthogonal modular forms for  $\text{std}_p^+$  and  $\text{std}^+$ , paramodular forms  $S_4(K(p))$  and modular forms  $S_6^-(p)$  for  $p < 100$

Siegel modular forms for four cases with square-free conductor: 182, 205, 255, and 257. Also, Ladd [Lad18, page 24] found an orthogonal modular form such that the odd Euler factors of its  $L$ -function coincides with the Euler factors of the  $L$ -series of the hypergeometric motive of conductor 257.

The remaining four cases provided by Roberts have not square-free conductors 128, 378, 384 and 256. For the first three we have found Hecke-eigenvectors  $f$  in  $\mathcal{S}(\text{O}(\hat{\Lambda}))$ , such that the first 50 coefficients of the  $L$ -function of  $f$  coincide with the coefficients of the  $L$ -function of  $H$ . The coefficients of the  $L$ -function of  $H$  were computed using MAGMA [BCP97] as in [Rob15]. For the local Euler factors with  $p^2 \mid \text{disc}(Q)$  we used the one given by the  $L$ -function of the hypergeometric motive.

- (1) For the hypergeometric motive  $H$  of conductor 128, with data  $A = [2, 2, 8]$ ,  $B = [1, 1, 4, 4]$ ,  $t = 1$ , and  $L_2(x) = 1 + 2x + 8x^2$ . The quadratic space is  $\mathbb{Q}^5$  with

$$Q = x^2 + xy + y^2 + z^2 + xt + zt + t^2 + zw + 26w^2, \quad \text{disc}(Q) = 128 = 2^7, \quad \text{and} \quad \Lambda = \mathbb{Z}^5.$$

- (2) For the hypergeometric motive  $H$  of conductor 378, with data  $A = [3, 2, 2]$ ,  $B = [1, 1, 6]$ ,  $t = 64$ , and  $L_3 = 1 + 3x$ . The quadratic space is  $\mathbb{Q}^5$  with

$$Q = x^2 + xy + y^2 + z^2 + xt + zt + t^2 + zw + 76w^2, \quad \text{disc}(Q) = 378 = 2 \cdot 3^3 \cdot 7, \quad \text{and} \quad \Lambda = \mathbb{Z}^5.$$

- (3) For the hypergeometric motive  $H$  of conductor 384, with data  $A = [2, 2, 2, 2]$ ,  $B = [1, 1, 1, 1]$ ,  $t = 1/4$ , and  $L_2 = 1$ . The quadratic space is  $\mathbb{Q}^5$  with

$$Q = x^2 + xy + y^2 + xz + 2z^2 + xt + 2t^2 + 12w^2, \quad \text{disc}(Q) = 384 = 2^7 \cdot 3, \quad \text{and} \quad \Lambda = \mathbb{Z}^5.$$

We have not been able to find matching Hecke-eigenvectors in  $\mathcal{S}(\text{O}(\hat{\Lambda}))$  for the hypergeometric motive of conductor 256, with data

$$A = [2, 2, 2, 2, 4], \quad B = [1, 1, 8], \quad t = 1, \quad \text{and} \quad L_2 = 1 - 2x.$$

The Euler factors for this motive can be computed from the given data using MAGMA:

```
> R<x> := PolynomialRing(Integers());
> L:=LSeries(HypergeometricData([2, 2, 2, 2, 4], [1, 1, 8]), 1:
> BadPrimes:=[<2, 8,1-2*x>]);
> EulerFactor(L, 3);
729*x^4 - 54*x^3 - 2*x^2 - 2*x + 1
```

As a reference, the first Euler factors are

$$\begin{aligned} L_2 &= 1 - 2x, \\ L_3 &= 1 - 2x - 2x^2 - 54x^3 + 729x^4, \\ L_5 &= 1 + 12x + 142x^2 + 1500x^3 + 15625x^4. \end{aligned}$$

## 7. Algorithms

To carry out the computations mentioned throughout the article we relied on [Hei16], and Greenberg and Voight [GV14]. Hein gives a very detailed description to compute spaces of orthogonal modular forms over totally real number fields, as well as their Hecke-operators for good primes.

We implemented the algorithms to compute  $\mathcal{M}(\mathcal{O}(\hat{\Lambda}))$  and  $\mathcal{M}_d(\mathcal{O}(\hat{\Lambda}))$ , as well as  $T_{p,k}$  for  $k = 1, 2$ , in Sage [Sag19]. One of the most important parts of the algorithm to compute  $T_{p,k}$  relies on isomorphism testing of quadratic forms, for which Sage uses PARI [PAR18], which implements an algorithm of Plesken and Souvignier [PS97]. To compute the representation given in Section 3, we implemented a function to compute the spinor norm based in Example 8 in [Cas78, page 30]. Cassels give an algorithm to decompose an autometry  $A$  of a positive definite quadratic space  $V$  of dimension  $n$  as a product of at most  $n$  transpositions  $\tau_{v_i}$ ,  $v_i \in V$ . The spinor norm is computed as the product of the norm of  $v_i$  modulo squares. In our case, any proper autometry is a product of at most 4 transpositions. The implemented code can be found in [Ram20].

To do the computations of Theorem 14, we did a random search of quinary positive definite quadratic forms of prime discriminant. For each prime  $p < 7000$  we found a representative of the unique genus of discriminant  $p$ . To find the matches of hypergeometric motives of Section 6, we used tables of Nipp of reduced regular primitive positive-definite quinary quadratic forms over  $\mathbb{Z}$  [Nip].

## 8. Tables

In Tables 5 and 6 we show the orthogonal modular forms from  $\mathcal{S}(\mathcal{O}(\hat{\Lambda}_p))$ ,  $\mathcal{S}_p(\mathcal{O}(\hat{\Lambda}_p))$  for  $p < 300$  that are not Gritsenko lifts. These tables can be found in [RT20], as well as for squarefree  $D < 1000$ . We include the dimension and the traces of  $\lambda_{p,1}$  for  $p \leq 13$  and  $\lambda_{p,2}$  for  $p \leq 5$ . The rational ones for  $d = 1$  and  $p < 200$  were first computed by Hein [Hei16], and for  $p < 400$  by Ladd [Lad18].

$p$	$d$	label	dim	$\lambda_{2,1}$	$\lambda_{3,1}$	$\lambda_{5,1}$	$\lambda_{7,1}$	$\lambda_{11,1}$	$\lambda_{13,1}$	$\lambda_{2,2}$	$\lambda_{3,2}$	$\lambda_{5,2}$
61	1	61a	1	-7	-3	3	-9	-4	-3	7	-9	-9
73	1	73a	1	-6	-2	0	7	-66	16	6	-9	0
79	1	79a	1	-5	-5	3	15	26	-15	2	4	-10
89	1	89a	1	-4	-6	16	-17	-2	-46	2	-6	27
97	1	97a	2	-9	-4	-4	16	-64	24	6	-14	4
101	1	101a	2	-7	-11	22	-32	46	-54	2	0	-21
103	1	103a	2	-9	-2	-15	26	-9	29	5	-10	-30
109	1	109a	3	-10	-15	-7	37	27	20	-3	7	-20
113	1	113a	1	-3	-4	8	4	-4	-40	2	-4	-4
127	1	127a	3	-9	-9	-12	45	18	69	0	6	-12
131	1	131a	2	-6	-4	8	-10	64	-84	4	-8	-4
137	1	137a	2	-4	-10	12	0	16	-8	0	8	12
139	1	139a	4	-14	-4	-22	14	-6	76	4	-10	-26
149	1	149a	4	-6	-23	16	-17	77	-9	-6	12	-15
151	1	151a	5	-12	-17	-33	57	81	75	-9	12	-28
157	1	157a	2	6	2	-14	8	-36	46	2	-22	-12
	1	157b	5	-15	-12	0	-11	9	217	3	16	-78
163	1	163a	4	-10	-4	-16	38	4	84	2	-8	-12
167	167	167a	1	-8	-10	-4	-14	-22	-4	10	11	-44
	1	167b	1	-2	0	-2	2	-14	-34	2	-17	16
	1	167c	2	-3	-9	2	3	92	-41	-3	12	-28
173	173	173a	1	-8	-9	-10	-4	-4	-72	10	7	-3
	1	173b	1	-2	-1	0	-16	-24	2	0	-23	-9
	1	173c	4	-7	-15	14	-27	92	43	-2	22	-90
179	1	179a	4	-6	-10	-6	2	134	-134	-2	-8	-32
181	1	181a	10	-27	-16	-14	-38	59	249	0	-24	-91
191	1	191a	2	-3	-6	-7	-23	93	-19	-5	12	-10
	1	191b	4	-6	-10	8	10	126	-136	2	-12	-52
193	1	193a	10	-15	-26	-38	56	-78	200	-11	-2	26
197	197	197a	1	-7	-10	-8	5	2	-66	7	14	-2
	1	197b	1	1	-8	9	23	-12	-38	1	6	-24
	1	197c	2	-4	-4	0	-20	78	-10	-4	-6	-42
	1	197d	3	-2	-13	0	-19	25	101	-5	14	-6
199	1	199a	10	-27	-8	-43	41	33	170	1	-22	-120

**Table 5.** Forms in  $\mathcal{S}_d(\mathcal{O}(\hat{\Lambda}_p))$  for  $d = 1$ ,  $p$  and  $p < 200$ .

$p$	$d$	label	dim	$\lambda_{2,1}$	$\lambda_{3,1}$	$\lambda_{5,1}$	$\lambda_{7,1}$	$\lambda_{11,1}$	$\lambda_{13,1}$	$\lambda_{2,2}$	$\lambda_{3,2}$	$\lambda_{5,2}$
211	1	211a	10	-18	-16	-48	38	24	118	-12	-8	16
223	223	223a	1	-6	-11	6	-28	8	-42	6	13	-33
	1	223b	1	-2	1	-8	-6	-30	36	-2	-17	5
	1	223c	10	-22	-4	-47	72	40	175	2	-6	-74
227	227	227a	2	-13	-18	-14	-22	-56	-15	13	12	16
	1	227b	6	-7	-8	-6	-14	92	-85	-3	-12	-46
229	1	229a	1	-2	-1	-9	-2	-13	24	-5	-12	-18
	1	229b	1	0	-5	17	-40	57	10	-1	-4	30
	1	229c	14	-33	-18	-17	7	-64	316	2	-20	-136
233	233	233a	1	-6	-10	-7	4	-22	-40	5	10	22
	1	233b	1	0	-2	8	-6	-38	32	2	-14	-6
	1	233c	4	-4	-12	-4	-28	24	-96	0	0	-8
	1	233d	5	-2	-16	-9	-10	72	76	-6	14	-18
239	239	239a	1	-6	-9	-8	10	-49	7	6	13	-13
	1	239b	10	-5	-30	-14	-9	266	-164	-14	1	-75
241	1	241a	18	-31	-32	-38	-14	-146	302	-14	-54	-88
251	251	251a	1	-6	-8	-11	6	-63	2	6	3	-15
	1	251b	1	-2	-2	9	-20	39	18	-4	3	17
	1	251c	10	-14	-4	-4	-36	222	-202	6	-28	-62
257	1	257a	1	-1	0	-4	-8	24	12	-2	-8	-52
	257	257b	2	-13	-13	-26	-16	-9	-51	14	0	18
	1	257c	12	-13	-23	24	-82	1	-23	-5	-28	-6
263	263	263a	2	-11	-20	-15	-3	-10	-23	7	26	-2
	1	263b	11	-7	-25	-8	-10	206	-78	-10	6	-14
269	269	269a	1	-7	-4	-20	-4	4	49	8	0	23
	269	269b	1	-5	-10	-8	20	-60	-75	4	12	-25
	1	269c	1	-1	2	-1	8	21	30	1	6	-10
	1	269d	15	-20	-28	67	-145	114	14	-3	-52	-77
271	271	271a	1	-5	-10	2	-10	-27	-25	5	13	-25
	1	271b	19	-35	-19	-70	81	-20	245	-13	-25	-83
277	277	277a	1	-5	-10	-1	-10	38	-94	4	13	0
	1	277b	22	-25	-35	-44	48	-104	438	-19	-7	-56
281	281	281a	1	-6	-6	-16	6	-26	14	6	2	29
	1	281b	18	-4	-50	8	-116	142	-96	-23	-20	-42
283	283	283a	1	-6	-6	-6	-29	15	-47	7	-4	-24
	283	283b	1	-4	-14	8	-17	-15	-33	1	22	8
	1	283c	1	-2	-2	6	-7	-11	33	-5	0	-24
	1	283d	17	-26	2	-74	85	-95	213	1	-36	-82
293	293	293a	4	-24	-27	-57	-14	-7	-94	21	13	36
	1	293b	17	-13	-36	49	-117	37	99	-14	-11	-80

**Table 6.** Forms in  $S_d(\mathcal{O}(\hat{\Lambda}_p))$  for  $d = 1$ ,  $p$  and  $200 < p < 300$ .

## References

- [AGM08] Avner Ash, Paul Gunnells, and Mark McConnell, *Cohomology of congruence subgroups of  $SL(4, \mathbb{Z})$ . II*, J. Number Theory **128** (2008), no. 8, 2263–2274. [MR 2394820](#)
- [AGM10] Avner Ash, Paul Gunnells, and Mark McConnell, *Cohomology of congruence subgroups of  $SL_4(\mathbb{Z})$ . III*, Math. Comp. **79** (2010), no. 271, 1811–1831. [MR 2630015](#)
- [BCGP18] George Boxer, Frank Calegari, Toby Gee, and Vincent Pilloni, *Abelian surfaces over totally real fields are potentially modular*, preprint, 2018. [arXiv 1812.09269](#)
- [BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3–4, 235–265, Computational algebra and number theory (London, 1993). [MR 1484478](#)
- [Bir91] Bryan John Birch, *Hecke actions on classes of ternary quadratic forms*, Computational number theory (Debrecen, 1989), de Gruyter, Berlin, 1991, pp. 191–212. [MR 1151865](#)
- [BK75] Bryan John Birch and Willem Kuyk (eds.), *Modular functions of one variable. IV*, Lecture Notes in Mathematics, Vol. 476, Springer-Verlag, Berlin-New York, 1975. [MR 0376533](#)
- [BK14] Armand Brumer and Kenneth Kramer, *Paramodular abelian varieties of odd conductor*, Trans. Amer. Math. Soc. **366** (2014), no. 5, 2463–2516. [MR 3165645](#)
- [BK17] Tobias Berger and Krzysztof Klosin, *Deformations of Saito-Kurokawa type and the paramodular conjecture*, preprint, 2017, With an appendix by Cris Poor, Jerry Shurman, and David S. Yuen. [arXiv 1710.10228](#)
- [BK19] Armand Brumer and Kenneth Kramer, *Corrigendum to “Paramodular abelian varieties of odd conductor”*, Trans. Amer. Math. Soc. **372** (2019), no. 3, 2251–2254. [MR 3976591](#)
- [BPP<sup>+</sup>19] Armand Brumer, Ariel Pacetti, Cris Poor, Gonzalo Tornaría, John Voight, and David S. Yuen, *On the paramodularity of typical abelian surfaces*, Algebra Number Theory **13** (2019), no. 5, 1145–1195. [MR 3981316](#)
- [Cas78] John William Scott Cassels, *Rational quadratic forms*, London Mathematical Society Monographs, vol. 13, Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1978. [MR 522835](#)
- [CCG19] Frank Calegari, Shiva Chidambaram, and Alexandru Ghitza, *Some modular abelian surfaces*. [arXiv 1906.10939](#)
- [Cre97] John Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997. [MR 1628193](#)
- [Cre19] John Cremona, *ecdata: 2019-10-29*, October 2019, <http://doi.org/10.5281/zenodo.3522235>.
- [GK13] Sanoli Gun and Narasimha Kumar, *A note on Fourier-Jacobi coefficients of Siegel modular forms*, Arch. Math. (Basel) **101** (2013), no. 6, 519–524. [MR 3133725](#)
- [GPY19] Valery Gritsenko, Cris Poor, and David S Yuen, *Antisymmetric paramodular forms of weights 2 and 3*, International Mathematics Research Notices (2019).
- [GV14] Matthew Greenberg and John Voight, *Lattice methods for algebraic modular forms on classical groups*, Computations with modular forms, Contrib. Math. Comput. Sci., vol. 6, Springer, Cham, 2014, pp. 147–179. [MR 3381452](#)
- [Hei16] Jeffery Hein, *Orthogonal modular forms: An application to a conjecture of Birch, algorithms and computations*, Ph.D. thesis, Dartmouth College, 2016. [MR 3553638](#)
- [HTV20] Jeffery Hein, Gonzalo Tornaría, and John Voight, *Hilbert modular forms as orthogonal modular forms*, preprint (2020).
- [Ibu07] Tomoyoshi Ibukiyama, *Paramodular forms and compact twist*, Automorphic Forms on  $GSp(4)$ , Proceedings of the 9th Autumn Workshop on Number Theory, (ed. M. Furusawa), 2007, pp. 37–48.
- [IK17] Tomoyoshi Ibukiyama and Hidetaka Kitayama, *Dimension formulas of paramodular forms of squarefree level and comparison with inner twist*, J. Math. Soc. Japan **69** (2017), no. 2, 597–671. [MR 3638279](#)
- [Koh01] David R. Kohel, *Hecke module structure of quaternions*, Class field theory—its centenary and prospect (Tokyo, 1998), Adv. Stud. Pure Math., vol. 30, Math. Soc. Japan, Tokyo, 2001, pp. 177–195. [MR 1846458](#)

- [Lad18] Watson Bernard Ladd, *Algebraic modular forms on  $\mathrm{so}_5(\mathbb{Q})$  and the computation of paramodular forms*, Ph.D. thesis, University of California, Berkeley, 2018.
- [Lam05] Thomas Lam, *Introduction to quadratic forms over fields*, Graduate Studies in Mathematics, vol. 67, American Mathematical Society, Providence, RI, 2005. [MR 2104929](#)
- [LMF20] The LMFDB Collaboration, *The L-functions and modular forms database*, <http://www.lmfdb.org>, 2020, [Online; accessed 10 February 2020].
- [Mur13] Daniel Kim Murphy, *Algebraic modular forms on definite orthogonal groups*, Ph.D. thesis, Stanford University, 2013.
- [Nip] Gordon L. Nipp, *Tables of quinary quadratic forms*, <http://www.math.rwth-aachen.de/Gabriele.Nebe/LATTICES/nipp5.html>.
- [PAR18] The PARI Group, Univ. Bordeaux, *Pari/gp version 2.11.0*, 2018, <http://pari.math.u-bordeaux.fr/>.
- [Piz80] Arnold Pizer, *An algorithm for computing modular forms on  $\Gamma_0(N)$* , J. Algebra **64** (1980), no. 2, 340–390. [MR 579066](#)
- [PS97] Wilhelm Plesken and Bernd Souvignier, *Computing isometries of lattices*, vol. 24, 1997, Computational algebra and number theory (London, 1993), pp. 327–334. [MR 1484483](#)
- [PSY17] Cris Poor, Jerry Shurman, and David S. Yuen, *Siegel paramodular forms of weight 2 and squarefree level*, Int. J. Number Theory **13** (2017), no. 10, 2627–2652. [MR 3713095](#)
- [PY15] Cris Poor and David S. Yuen, *Paramodular cusp forms*, Math. Comp. **84** (2015), no. 293, 1401–1438. [MR 3315514](#)
- [Ram14] Gustavo Rama, *Módulo de Brandt generalizado*, M.Sc., Universidad de la República, 2014.
- [Ram20] Gustavo Rama, *Quinary orthogonal modular forms code repository*, preprint, 2020.
- [Rob15] David P. Roberts, *Hypergeometric motives I*, lecture notes, 2015.
- [RT20] Gustavo Rama and Gonzalo Tornaría, *Quinary orthogonal modular forms*, preprint, 2020.
- [Sag19] *Sagemath, the Sage Mathematics Software System (Version 8.7)*, 2019, <https://www.sagemath.org>.
- [Sch18] Ralf Schmidt, *Packet structure and paramodular forms*, Trans. Amer. Math. Soc. **370** (2018), no. 5, 3085–3112. [MR 3766842](#)
- [Ste12] William Stein, *The Modular Forms Database*, 2012, <http://wstein.org/Tables>.
- [Tor05] Gonzalo Tornaría, *The Brandt module of ternary quadratic lattices*, Ph.D. thesis, The University of Texas at Austin, 2005. [MR 2717378](#)
- [Wad71] Hideo Wada, *Tables of Hecke operations. I*, Seminar on Modern Methods in Number Theory (Inst. Statist. Math., Tokyo, 1971), Paper No. 39, 1971, p. 10. [MR 0379377](#)

Received 28 Feb 2020.

GUSTAVO RAMA: [grama@fing.edu.uy](mailto:grama@fing.edu.uy)

Facultad de Ingeniería, Universidad de La República, Montevideo, Uruguay

GONZALO TORNARÍA: [tornaria@cmat.edu.uy](mailto:tornaria@cmat.edu.uy)

Centro de Matemática, Universidad de la República, Montevideo, Uruguay



# An algorithm and estimates for the Erdős–Selfridge function

Brianna Sorenson, Jonathan Sorenson, and Jonathan Webster

Let  $p(n)$  denote the smallest prime divisor of the integer  $n$ . Define the function  $g(k)$  to be the smallest integer  $> k + 1$  such that  $p\left(\binom{g(k)}{k}\right) > k$ . We present a new algorithm to compute the value of  $g(k)$ , and use it to both verify previous work and compute new values of  $g(k)$ , with our current limit being

$$g(375) = 12\,86399\,96537\,88432\,18438\,16804\,13559.$$

We prove that our algorithm runs in time sublinear in  $g(k)$ , and under the assumption of a reasonable heuristic, its running time is

$$g(k) \exp[-c(k \log \log k)/(\log k)^2(1 + o(1))] \quad \text{for } c > 0.$$

## 1. Introduction

Let  $p(n)$  denote the smallest prime divisor of the integer  $n$ , and define the function  $g(k)$  to be the smallest integer  $> k + 1$  such that  $p\left(\binom{g(k)}{k}\right) > k$ . So we have  $g(2) = 6$  and  $g(3) = g(4) = 7$ .

We begin with a discussion of previous work on  $g(k)$ , then state our new results, and finally outline the rest of this paper.

**1.1. Previous work.** Paul Erdős introduced the problem of estimating the function  $g(k)$  in 1969 [4]. He, along with Ecklund and Selfridge [2] showed that  $g(k) > k^{1+c}$  for a small constant  $c$ , showed that  $g(k) < e^{k(1+o(1))}$ , and tabulated  $g(k)$  up to  $k = 40$ , plus  $g(42)$ ,  $g(46)$ , and  $g(52)$ .

Scheidler and Williams [15] described how to use Kummer’s theorem to construct a sieving problem to compute  $g(k)$ , and they proceeded to find  $g(k)$  for all  $k \leq 140$ . Five years later, Lukes, Scheidler, and Williams [11] improved their sieve, used special-purpose hardware, and computed  $g(k)$  for all  $k \leq 200$ .

Successive analytic improvements on lower bounds of  $g(k)$  have been proved by [3; 6; 10], where the strongest result known, due to Konyagin, is

$$g(k) > k^{c \log k} \quad \text{for } c > 0.$$

We are aware of no further results on  $g(k)$  that postdate 1999.

MSC2010: 11Y16.

Keywords: Erdos–Selfridge function, elementary number theory, analytic number theory, binomial coefficients.

**1.2. Definitions and new results.** In computing  $g(k)$  for  $k \leq 200$ , the authors of [15; 11] used Kummer's theorem to construct a sieving problem.

**Theorem 1.1** (Kummer). *Let  $k < n$  be positive integers, and let  $p$  be a prime  $\leq k$ . Let  $t$  be a positive integer with  $t \geq \lfloor \log_p n \rfloor$ . Write*

$$k = \sum_{i=0}^t a_i p^i \quad \text{and} \quad n = \sum_{i=0}^t b_i p^i$$

*as the base- $p$  representations of  $k$  and  $n$ , respectively. Then  $p$  does not divide  $\binom{n}{k}$  if and only if  $b_i \geq a_i$  for  $i = 0, \dots, t$ .*

For each prime  $p \leq k$ , this theorem gives congruences  $g(k)$  must satisfy. Our approach is similar to [15; 11], but we selectively choose enough prime power moduli so that we expect  $g(k)$  to be among the residues. This approach is a search for a least residue and avoids explicit sieving. We accomplish this by using the space-saving wheel which was described in [16]. This wheel data structure has been successfully used in other sieving problems [17; 18; 19] but we omit the “sieving” part that occurs after the residue is constructed. Our resulting algorithm has, so far, verified all previous computations for  $g(k)$ , and extended them for all  $k \leq 375$ . A complete table of all currently computed  $g(k)$  values can be found in the Online Encyclopedia of Integer Sequences entry A003458.

Let  $M_k := \prod_{p \leq k} p^{\lfloor \log_p k \rfloor + 1}$  and let  $R_k$  denote the number of acceptable residues, under Kummer's theorem, modulo  $M_k$ . Then  $g(k)$  is the least residue (greater than  $k + 1$ ) among the  $R_k$  residues. Our *uniform distribution heuristic* (UDH) states that the  $R_k$  residues are, in a sense, uniformly distributed. Under this assumption, we expect  $g(k)$  to be roughly  $M_k/R_k$ . In fact, we define  $\hat{g}(k) := M_k/R_k$ . The authors of [11] studied this approximating function; it plays a central role in the analysis of our algorithm, but not in its correctness.

Assuming the UDH implies that with high probability, we have

$$\log g(k) = \log \hat{g}(k) + O(\log k).$$

Let  $G(x, k)$  count the number of  $n \leq x$  such that  $p\left(\binom{n}{k}\right) > k$ . We show unconditionally that, for  $x > x_0(k)$ ,

$$G(x, k) = (x/\hat{g}(k))(1 + o(1)).$$

These results imply that  $\hat{g}(k)$  should approximate  $g(k)$  reasonably well. We then show that

$$0.530684 + o(1) \leq \frac{\log \hat{g}(k)}{k/\log k} \leq 1 + o(1).$$

We prove a running time for our algorithm of

$$g(k) \exp \left[ -c \frac{k \log \log k}{(\log k)^2} \right]$$

for a constant  $c > 0$ . We also sketch a more general argument showing our algorithm's running time is sublinear in  $g(k)$ , unconditionally.

**1.3. Outline.** Our paper is organized as follows. In [Section 2](#) we present our algorithm, including a description of the space-saving wheel data structure. In [Section 3](#) we discuss the knapsack subproblem and techniques for splitting prime rings when deciding the sieving modulus for the algorithm. In [Section 4](#) we demonstrate each of the above steps to compute  $g(10) = 46$ . In [Section 5](#) we provide some statistical evidence for the credibility of the UDH, show that  $g(k)$  is roughly  $\hat{g}(k)$  with high probability, and we give an easy proof of our estimate for  $G(x, k)$ . In [Section 6](#), we show  $\log \hat{g}(k)$  is proportional to  $k/\log k$  and bound the running time of our algorithm. In [Section 7](#), we conclude with some computational notes.

## 2. The algorithm

The naive approach is to search through all the  $R_k$  admissible residues modulo  $M_k$  to find the smallest residue greater than  $k + 1$ . However,  $R_k$  is typically too large for this, making this algorithm practical only for very small  $k$ .

Instead, we enumerate residues that satisfy the requirements of Kummer’s theorem modulo  $N$ , where  $N$  is a divisor of  $M_k$  that is larger than, but near to  $\hat{g}(k)$ , as follows:

- (1) Compute  $M_k$ ,  $R_k$ , and  $k\hat{g}(k) = kM_k/R_k$ .
- (2) Choose a divisor  $N$  of  $M_k$  just above our estimate  $k\hat{g}(k)$  with the property that there is a minimal number of residues to check. Details of how to do this are discussed in [Section 3](#).
- (3) Build a *ring* data structure for each prime power dividing  $N$ , which is a list of admissible residues as defined by Kummer’s theorem.
- (4) Construct a *wheel* data structure<sup>1</sup> with jump tables to generate the residues modulo  $N$ ; see [\[16\]](#). A jump entry is the minimum amount to add that preserves the residue class modulo earlier rings, and jumps to an admissible residue for the current ring.<sup>2</sup>
- (5) Rings for the remaining prime powers are also created, but not a wheel (the jumps are not needed). We refer to these rings as *filters*.<sup>2</sup> A residue passes the filter if, when reduced modulo the ring size, the corresponding admissible bit is set to one. The smallest residue generated from the wheel that also passes all the filters is  $g(k)$ .

Any prime power ring that is part of the wheel, where that prime power also fully divides  $M_k$ , is not needed as a filter. Or in other words, if a prime divides  $N$  but not  $M_k/N$ , its prime power is not needed as a filter.

- (6) Now that our data structures are initialized, we generate each residue modulo  $N$  from the wheel to see if it passes the filters. As we go, we maintain the value of the minimum residue, so far, that passed all the filters. Once every residue from the wheel is generated, this minimum is  $g(k)$ .

<sup>1</sup>Any data structure that can access residues in constant time will suffice. An anonymous referee kindly pointed out that doubly-focused enumeration [\[1\]](#) will work here as well. It will require more space and the early abort strategy described in [Section 4](#) is a little harder to implement.

<sup>2</sup>The ordering of the rings does not matter for correctness. For speed, it is best to put the ring with the most jump entries last, and to put the best filters first.

If we run the whole algorithm and fail to find a residue that passes the filters, this means  $g(k) > N$ . In this case, we simply multiply our previous estimate for  $g(k)$  by  $k$ , choose a new, larger  $N$ , and try again.

Note that the problem of finding a solution below a given bound to a system of pairwise coprime modular congruences is known to be NP-complete; see [5; 12].

### 3. Prime splitting and knapsack

The purpose of this section is to look at how to choose  $N$ , a divisor of  $M_k$  that is just larger than  $k\hat{g}(k)$ . The analysis in Section 6 shows that it is sufficient, for asymptotic purposes, to choose  $N$  to be a product of consecutive primes greater than  $k/2$  until the product exceeds  $k\hat{g}(k)$ . In practice we can do much better than what the asymptotic argument shows. We discuss a few ways we do this in the context of a knapsack problem.

**3.1. Knapsack problem setup.** We want to choose  $N$  so that the prime powers dividing  $N$  give a very low filter rate, thereby giving fewer residues to enumerate, which makes the algorithm faster. Note that selecting prime power moduli based on filter rate alone is not optimal. The size of the modulus matters as well; a smaller modulus with a higher but still good filter rate can be preferable to a large modulus with a better filter rate.

Let  $t_p := \lfloor \log_p k \rfloor + 1$  be the number of digits required to write  $k$  in base  $p$ , with the  $a_{ip}$  representing these digits, so that  $k = \sum_{i=0}^{t_p-1} a_{ip} p^i$ . We have  $t_p \geq 2$ , and for most primes  $t_p = 2$ . Define  $T_p$  to be the maximum exponent of  $p$  so that  $p^{T_p} \mid N$ . This implies  $0 \leq T_p \leq t_p$ , and  $N = \prod_{p \leq k} p^{T_p}$ .

Let  $r_{ip} := p - a_{ip}$ , and let  $R_{xp} := \prod_{i < x} r_{ip}$ . Then the number of acceptable residues modulo  $p^{T_p}$  is  $R_{T_p p}$ . The running time of the algorithm is proportional to the number of residues modulo  $N$ , which, by the Chinese remainder theorem, is

$$\prod_{p \leq k} R_{T_p p} = \prod_{p \leq k} p^{T_p} \frac{R_{T_p p}}{p^{T_p}} = N \cdot \prod_{p \leq k} \frac{R_{T_p p}}{p^{T_p}}.$$

We want to minimize the product of the filtering rates for primes included in  $N$ , which is equivalent to maximizing the reciprocal, which we write as

$$\prod_{p \leq k} \frac{p^{T_p}}{R_{T_p p}} = \exp \sum_{p \leq k} \log \frac{p^{T_p}}{R_{T_p p}}.$$

This allows us to set up a *knapsack problem* [9] for choosing prime powers to include in  $N$  by setting the overall capacity of the knapsack to  $\log N$ , and the size and value of prime powers are set as follows:

$$\text{size}(p^T) := \log p^T = T \log p,$$

$$\text{value}(p^T) := \log(\text{modulus}/\# \text{ residues}) = \log(p^T / R_T) = T \log p - \log R_T.$$

The question, then, is how to set  $T$  for each prime  $p$  to give a good selection of items to include in the knapsack. Also, we must ensure that the same prime  $p$  is not chosen more than once, with different  $T$  values, for inclusion in the knapsack.

**3.2. Prime splitting.** In practice, we can often get better results by including prime powers. So our approach is, for each prime  $p \leq k$ , to compute an optimal value for  $T$  based on filter rate, and then use a greedy algorithm to fill our knapsack. We call computing this value for  $T$  *splitting* the prime power, and label this split point  $s_p$ . We then allow for up to three possible choices in the knapsack for each prime  $p$ : set  $T = 0$  (that is, omit  $p$  from  $N$  entirely), use  $T = s_p$  (use the optimal split point), or use  $T = t_p$ , the maximum (note that  $s_p = t_p$  is possible).

Maximizing the value-to-size ratio, we get

$$\frac{\text{value}}{\text{size}} = \frac{T \log p - \log R_{Tp}}{T \log p} = 1 - \frac{\log R_{Tp}}{T \log p}.$$

So, in time linear in  $t_p$ , we can try all possible  $T$  values and quickly find the optimum,  $s_p$ . Since 1 and  $\log p$  do not change, it suffices to compute  $(1/T) \log R_{Tp}$  for each  $T$  to find the optimum.

**3.3. The greedy knapsack algorithm.** After splitting, we have a list of candidate prime powers to include in  $N$ . We sort the list based on value-to-size ratio, and choose enough to include in  $N$  based on the value of  $\hat{g}(k)$ . In practice, this simple and fast algorithm to construct  $N$  worked very well.

**3.4. A dynamic programming approach.** An anonymous referee pointed out an elegant way to find  $N$ .

Start with  $(N = 1, R = 1)$ , where  $N$  is the modulus, and  $R$  the number of admissible residues. For each prime power  $p^i$  appearing in  $M_k$ , and for each  $(N, R)$  value found so far, form new values  $(N \cdot p^i, R \cdot R_{ip})$  for  $0 \leq i \leq t$ , where  $R_{ip}$  is the number of admissible residues modulo  $p^i$ . Sort the new  $(N, R)$  values by increasing value of  $R$ . For each  $(N, R), (N', R')$  with  $R < R'$ , discard  $(N', R')$  if  $N' < N$ , since  $(N, R)$  is always better. Also discard values  $(N', R')$  if  $N' \geq N \geq k \hat{g}(k)$ .

This clever algorithm will produce an optimal solution for  $N$ . Although we have not implemented it (yet), it seems likely to be fast enough that in practice it is a better choice than our own approach. Indeed, informal timing results from the aforementioned referee bear this out.

## 4. Example for $g(10)$

As an example computation, we present each of the steps described above to compute  $g(10) = 46$ .

We write  $10 = 1010_2 = 101_3 = 20_5 = 13_7$ . Kummer's theorem then says that

$$g(10) \equiv 1010_2, 1011_2, 1110_2, 1111_2 \pmod{16}.$$

Similarly, there are 12 residues modulo  $3^3$ , 15 residues modulo  $5^2$ , and 24 residues modulo  $7^2$ . In total, there are  $R_{10} = 4 \cdot 12 \cdot 15 \cdot 24 = 17280$  admissible residues modulo  $M_{10} = 16 \cdot 27 \cdot 25 \cdot 49 = 529200$ . We compute  $10 \cdot \hat{g}(10) = 306.25$  for use in our knapsack problem.

Considering the powers of 2 first, we compute  $r_{02} = 2$ ,  $r_{12} = 1$ ,  $r_{22} = 2$ , and  $r_{32} = 1$ . This gives  $R_{12} = 2$ ,  $R_{22} = 2$ ,  $R_{32} = 4$ , and  $R_{42} = 4$ . We get value-to-size ratios of 0,  $1/2$ ,  $1/3$ , and  $1/2$ . This implies  $s_2 = 2$  or 4. In practice, we normally use the largest value for  $s_p$  when several values give the same ratio, since it implies a better filter rate.

$p$	$T$	value	size	ratio
2	4	$\log(2^4/4)$	$\log(2^4)$	0.5
3	1	$\log(3/2)$	$\log 3$	0.4009...
7	1	$\log(7/4)$	$\log 7$	0.287...
3	3	$\log(3^3/12)$	$\log(3^3)$	0.246...
7	2	$\log(7^2/24)$	$\log(7^2)$	0.183...
5	2	$\log(5^2/20)$	$\log(5^2)$	0.069...

**Table 1.** Knapsack items for  $g(10)$ .

For  $p = 3$ , we have  $k = 101_3$ . We have  $r_{03} = 2$ ,  $r_{13} = 3$ , and  $r_{23} = 2$ . This gives  $R_{13} = 2$ ,  $R_{23} = 6$ , and  $R_{33} = 12$ . The successive  $(1/T) \log R$  values are  $\log 2$ ,  $(1/2) \log 6$ , and  $(1/3) \log 12$ . Of these,  $\log 2$  is the smallest, giving  $s_3 = 1$ . In a similar fashion, we obtain  $s_5 = 2$  and  $s_7 = 1$ .

Table 1 shows the resulting knapsack items (using the natural log), ordered by value-to-size ratio. We greedily choose items to include in our knapsack of size  $\log 306$ . We first choose  $2^4 = 16$ , leaving  $306/16 \approx 20$  “room” in our knapsack; then 3 is chosen next. This leaves about  $20/3 \approx 7$  room. The choice of 7 fills all remaining room, and gives  $N = 2^4 \cdot 3 \cdot 7$ .

Using  $N$ , we set up the space-saving wheel with rings that encode  $g(10) \equiv 10, 11, 14, 15 \pmod{16}$ ,  $g(10) \equiv 1, 2 \pmod{3}$ , and  $g(10) \equiv 3, 4, 5, 6 \pmod{7}$ . If  $N$  is large enough, we expect  $g(10)$  to be among these 32 residues.

The jump tables are:

Ring 16:	residue	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	admissible	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	1
	jump	+10	+9	+8	+7	+6	+5	+4	+3	+2	+1	+1	+3	+2	+1	+1	+11

Ring 3:	residue	0	1	2
	admissible	0	1	1
	jump	+16	+16	+32

Ring 7:	residue	0	1	2	3	4	5	6
	admissible	0	0	0	1	1	1	1
	jump	+48	+96	+144	+192	+48	+48	+48

We also build filters for the prime power congruences not used in the jump tables (9, 25, 49), but omit their explicit construction for the sake of brevity.

The smallest possible starting point is  $k + 2$ , or 12 in our example. Since 12 is not admissible modulo 16, we apply the jump (+2) to get 14. We pass up to the next ring. We find  $14 \bmod 3 \equiv 2$  is admissible. We pass to the next ring. Since  $14 \bmod 7 \equiv 0$  is not admissible, we jump (+48) to get 62. There are 4 total residues in the 7 ring, so we also generate  $62 + 48 = 110$ ,  $110 + 48 = 158$ , and  $158 + 48 = 206$ . All residues produced by the 7 ring are filtered:

$$62 \bmod 27 \equiv 8 = 22_3 : \text{fail}, \qquad 110 \bmod 27 \equiv 2_3 : \text{fail},$$
$$158 \bmod 25 \equiv 8 = 13_5 : \text{fail}, \qquad 206 \bmod 25 \equiv 6 = 11_5 : \text{fail}.$$

We then backtrack to ring 3 at 14, and generate  $14 + 32 = 46$ . We pass to ring 7. The initial value

in this ring,  $46 \bmod 7 \equiv 4$ , is already admissible and is generated first. These get filtered and 46 passes all filters. We record this value as a candidate for  $g(10)$  and continue the computation to see if a smaller value exists. Since,  $g(10) = 46$ , no such value will be found. From this point on, the wheel will not generate a residue for filtering if it exceeds 46. And nothing larger than  $N$  can ever be generated.

After 4 residues in the 7 ring, we drop down to the 3 ring, where we have already done 2 residues, so we drop back to the 16 ring. At the 16 ring, we generate the next residue  $14 + 1 = 15$ , which is passed up to the 3 ring.

This implies that, at each ring, we need to keep track of the next residue to generate, and how many have been generated so far so that we know when to back up to a previous ring.

And so it goes. The amortized cost is a constant number of arithmetic operations per residue generated by the outermost ring where they are filtered. If we apply the filters in decreasing order of filter rate, on average, a residue is only tested against a constant number of filters, and so again, the cost is a constant number of arithmetic operations per residue modulo  $N$ .

By keeping track of the minimum residue that passes the filters, we do not have to generate any residues larger than this minimum. In our example, once 46 passes the filters, we don't even generate the rest of ring 7—an “early abort” strategy, if you will. This optimization can make a big difference in practice.

## 5. Uniform distribution heuristic

The *uniform distribution heuristic* (UDH) states that the admissible residues modulo  $M_k$  behave as if they are chosen at random from a uniform distribution over the interval  $[1, M_k - 1]$ . It is not entirely dissimilar to Cramér's random model; the heuristic that integers near  $x$  are prime with probability  $1/\log x$ , and our intention is that these two models be treated similarly, in that we know they are not, strictly speaking, true, yet seem to have good predictive behavior under the right circumstances.

With the help of Rasitha Jayasekare, a statistician at Butler University, we ran statistical tests on the residues for  $5 \leq k \leq 15$ . For each  $k$ , we generated all  $R_k$  admissible residues and applied the Anderson–Darling and Kolmogorov–Smirnov tests to measure uniformity. Both tests confirm with a high probability that the data comes from a uniform distribution.

**Theorem 5.1.** *The UDH implies that, with probability  $1 - o(1)$ , we have*

$$\hat{g}(k)/k \leq g(k) \leq k\hat{g}(k).$$

*Proof.* Without loss of generality, we ignore residues  $\leq k + 1$  because  $k$  is asymptotically negligible compared to  $M_k$  and  $R_k$ . We have

$$\Pr(g(k) \leq x) = 1 - \Pr(\text{all residues are greater than } x) = 1 - \left(\frac{M_k - x}{M_k}\right)^{R_k} = 1 - \left(1 - \frac{x}{M_k}\right)^{R_k}.$$

For an upper bound, set  $x = (kM_k)/R_k$ , to obtain

$$\Pr(g(k) \leq (kM_k)/R_k) = 1 - \left(1 - \frac{k}{R_k}\right)^{R_k} \sim 1 - e^{-k} = 1 - o(1)$$

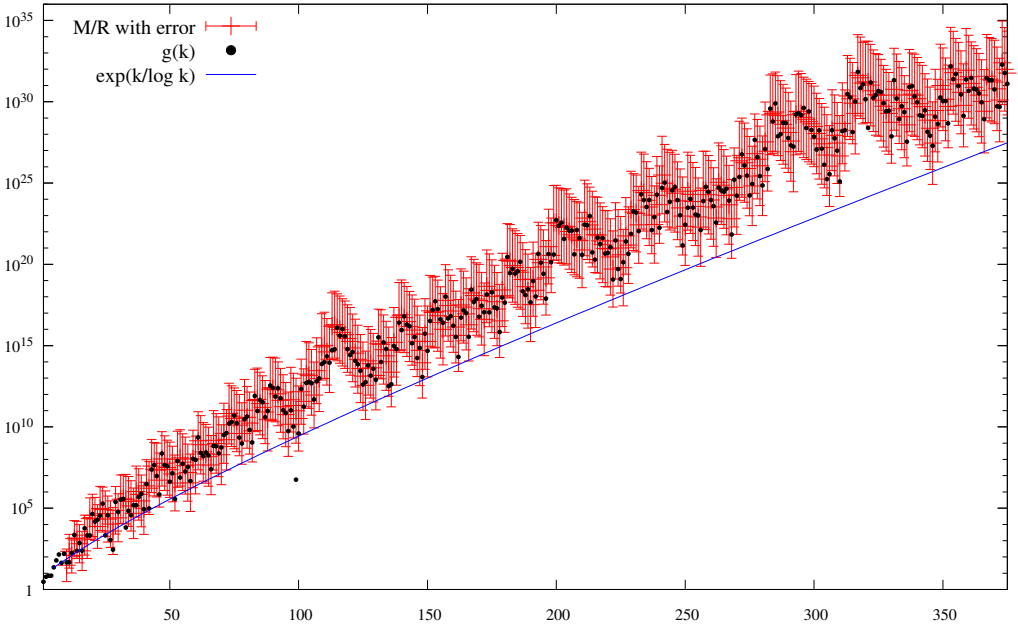


Figure 1. Comparing  $g(k)$  to  $M/R$  with error  $k$ .

for large  $R_k$  (and  $R_k$  does get quite large). For a lower bound, set  $x = M_k/(kR_k)$  to obtain

$$\Pr(g(k) \leq M_k/(kR_k)) = 1 - \left(1 - \frac{1}{kR_k}\right)^{R_k} \sim 1 - e^{-1/k} = o(1).$$

This completes the proof. □

So we have that, with high probability,

$$\log g(k) = \log \hat{g}(k) + O(\log k)$$

if we assume the uniform distribution heuristic. This has worked well in practice; the inequality in [Theorem 5.1](#) is satisfied by all computed  $g(k)$  (excepting  $k = 99$ ).

In [Figure 1](#), we have empirical data comparing actual values of  $g(k)$  (the black dots) to  $\hat{g}(k)$  plotted as intervals from  $\hat{g}(k)/k$  up to  $k\hat{g}(k)$  as red error bars. The plot uses a logarithmic scale.

Recall that  $G(x, k)$  counts the integers  $n \leq x$  such that  $p\left(\binom{n}{k}\right) > k$ . We conclude this section with the following.

**Theorem 5.2.** *If  $x$  is sufficiently large, then  $G(x, k) = (x/\hat{g}(k))(1 + o(1))$ .*

*Proof.* Write  $x = q \cdot M_k + r$  using the division algorithm, with integers  $q, r > 0$  and  $r < M_k$ . A contiguous interval of length  $M_k$  will have exactly  $R_k$  admissible residues, so  $G(qM_k, k) = qR_k$ . The remaining interval of length  $r$  has at most  $R_k$  residues, so  $G(x, k) = G(qM_k, k) + O(R_k) = qR_k + O(R_k)$  but  $q = \lfloor x/M_k \rfloor$ , so

$$G(x, k) = \lfloor x/M_k \rfloor R_k + O(R_k) = (x/\hat{g}(k))(1 + o(1)). \quad \square$$



## 6. Analysis

The running time of our algorithm is linear in the number of residues modulo  $N$ . Since we choose  $N$  based on  $\hat{g}(k)$ , we need to estimate  $\hat{g}(k)$ .

**Theorem 6.1.**  $0.530684 + o(1) \leq \frac{\log \hat{g}(k)}{k/\log k} \leq 1 + o(1).$

Applying the definitions for  $M_k$  and  $R_k$  above, we have

$$\begin{aligned} \hat{g}(k) &= \frac{M_k}{R_k} = \frac{\prod_{p \leq k} p^{\lfloor \log_p k \rfloor + 1}}{\prod_{p \leq k} \prod_{i=0}^{\lfloor \log_p k \rfloor} (p - a_{ip})} = \prod_{p \leq k} \prod_{i=0}^{\lfloor \log_p k \rfloor} \frac{p}{p - a_{ip}} \\ &= \prod_{p \leq \sqrt{k}} \prod_{i=0}^{\lfloor \log_p k \rfloor} \frac{p}{p - a_{ip}} \cdot \prod_{\sqrt{k} < p \leq k} \prod_{i=0}^{\lfloor \log_p k \rfloor} \frac{p}{p - a_{ip}} \\ &= \prod_{p \leq \sqrt{k}} \prod_{i=0}^{\lfloor \log_p k \rfloor} \frac{p}{p - a_{ip}} \cdot \prod_{\sqrt{k} < p \leq k} \frac{p}{p - a_{1p}} \frac{p}{p - a_{0p}}. \end{aligned}$$

Here we observed that  $\lfloor \log_p k \rfloor + 1 = 2$  when  $p > \sqrt{k}$ .

We will show that the product on the factor involving  $a_{0p}$  is exponential in  $k/\log k$ , and is therefore significant; and the other two factors, the product on primes up to  $\sqrt{k}$ , and the factor with  $a_{1p}$ , are both only exponential in  $\sqrt{k}$ .

We bound the first product, on  $p \leq \sqrt{k}$ , with the following lemma.

**Lemma 6.2.** 
$$\prod_{p \leq \sqrt{k}} \prod_{i=0}^{\lfloor \log_p k \rfloor} \frac{p}{p - a_{ip}} \ll e^{3\sqrt{k}(1+o(1))}.$$

*Proof.* We note that  $a_{ip} \leq p - 1$ , giving

$$\prod_{p \leq \sqrt{k}} \prod_{i=0}^{\lfloor \log_p k \rfloor} \frac{p}{p - a_{ip}} \leq \prod_{p \leq \sqrt{k}} p^{\lfloor \log_p k \rfloor + 1} \leq \prod_{p \leq \sqrt{k}} p^{3\lfloor \log_p \sqrt{k} \rfloor}.$$

From [7, Chapter 22] we have the bound  $\sum_{p \leq x} \lfloor \log_p x \rfloor \log p = x(1 + o(1))$ . Exponentiating and substituting  $\sqrt{k}$  for  $x$  gives the desired result.  $\square$

Next, we show that the product involving  $a_{1p}$  is small.

**Lemma 6.3.** 
$$\prod_{\sqrt{k} < p \leq k} \frac{p}{p - a_{1p}} \leq e^{O(\sqrt{k})}.$$

*Proof.* We split the product at  $2\sqrt{k}$ . For the lower portion, we have

$$\prod_{\sqrt{k} < p \leq 2\sqrt{k}} \frac{p}{p - a_{1p}} \leq (2\sqrt{k})^{\pi(2\sqrt{k})} \leq e^{O(\sqrt{k})}.$$

For the upper portion, since  $a_{1p} \leq k/p \leq \sqrt{k}$ , we have

$$\prod_{2\sqrt{k} < p \leq k} \frac{p}{p - a_{1p}} \leq \prod_{2\sqrt{k} < p \leq k} \frac{p}{p - \sqrt{k}} \leq \prod_{2\sqrt{k} < p \leq k} \left(1 + \frac{2\sqrt{k}}{p}\right) \leq \prod_{2\sqrt{k} < p \leq k} \left(1 + \frac{1}{p}\right)^{2\sqrt{k}+1}$$

using the fact that  $(1 + x/p) \leq (1 + 1/p)^x$  if  $x > 1$ ,  $p > 0$ . Mertens's theorem then gives the bound

$$\left( \frac{e^\gamma (\log k)}{e^\gamma (\log(2\sqrt{k}))} (1 + o(1)) \right)^{2\sqrt{k}+1} \leq e^{O(\sqrt{k})}. \quad \square$$

We now have

$$\log \hat{g}(k) = \log \left( \prod_{\sqrt{k} < p \leq k} \frac{p}{p - a_{0p}} \right) + O(\sqrt{k}).$$

The following lemma wraps up the proof of our theorem.

**Lemma 6.4.**  $0.530684 \cdot \frac{k}{\log k} (1 + o(1)) \leq \log \left( \prod_{\sqrt{k} < p \leq k} \frac{p}{p - a_{0p}} \right) \leq \frac{k}{\log k} (1 + o(1)).$

*Proof.* Fix  $a_{1p} = a$ . Then  $k/(a+1) < p \leq k/a$ , and  $a_{0p} = k \bmod p = k - ap$  and  $p - a_{0p} = p - (k - ap) = (a+1)p - k$ . We have

$$\begin{aligned} \log \left( \prod_{\sqrt{k} < p \leq k} \frac{p}{p - a_{0p}} \right) &= \log \left( \prod_{a=1}^{\sqrt{k}} \prod_{k/(a+1) < p \leq k/a} \frac{p}{(a+1)p - k} \right) \\ &= \sum_{a=1}^{\sqrt{k}} \sum_{k/(a+1) < p \leq k/a} (\log p - \log((a+1)p - k)). \end{aligned}$$

The reader should be aware that transforming between simple and double products/sums can introduce error, but this is bounded by at most one term, and we absorb this in our error term.

We split this sum into three pieces to start with:

- (1) The outer sum for  $(\log k)^2 \leq a < \sqrt{k}$ , which we show to be  $o(k/\log k)$ .
- (2) The  $\log p$  term only, for  $a < (\log k)^2$ , which we show to be  $k + o(k/\log k)$ .
- (3) The  $-\log((a+1)p - k)$  term, again for  $a < (\log k)^2$ , which we show to be  $-k + O(k/\log k)$ .

For (1), we have

$$\sum_{a=(\log k)^2}^{\sqrt{k}} \sum_{k/(a+1) < p \leq k/a} (\log p - \log((a+1)p - k)) \leq \sum_{a=(\log k)^2}^{\sqrt{k}} \sum_{k/(a+1) < p \leq k/a} \log p \leq \sum_{\sqrt{k} < p \leq k/(\log k)^2} \log p$$

which is  $O(k/(\log k)^2)$  using  $\sum_{p < x} \log p = x + o(x/\log x)$ . For (2), we have

$$\sum_{a=1}^{(\log k)^2} \sum_{k/(a+1) < p \leq k/a} \log p = \sum_{k/(\log k)^2 < p \leq k} \log p$$

which is  $k + o(k/\log k)$ . For (3), we have

$$- \sum_{a=1}^{(\log k)^2} \sum_{k/(a+1) < p \leq k/a} \log((a+1)p - k). \quad (6-1)$$

Rewriting the inner sum as an integral, using a strong version of the prime number theorem, we get

$$\begin{aligned} - \sum_{k/(a+1) < p \leq k/a} \log((a+1)p - k) &= - \int_{k/(a+1)}^{k/a} \frac{\log((a+1)t - k)}{\log t} dt + o(k/(\log k)^3) \\ &= - \frac{1}{\log(k/(a+\alpha))} \int_{k/(a+1)}^{k/a} \log((a+1)t - k) dt + o(k/(\log k)^3). \end{aligned}$$

Here  $\alpha$  is between 0 and 1, determined implicitly by the mean value theorem. The precise value of  $\alpha$  may depend on both  $k$  and  $a$ . We will use either  $\alpha = 0$  or  $\alpha = 1$ , depending on whether we want an upper or lower bound, respectively.

Using substitution, we can readily show that

$$\int_{k/(a+1)}^{k/a} \log((a+1)t - k) dt = \frac{k(\log(k/a) - 1)}{a(a+1)}.$$

We have for (3), then, a term which equals

$$\sum_{a=1}^{(\log k)^2} \left( - \frac{k(\log(k/a) - 1)}{a(a+1) \log(k/(a+\alpha))} \right) = -k + \frac{k}{\log k} \cdot \sum_{a=1}^{(\log k)^2} \frac{1 - \log\left(1 + \frac{\alpha}{a}\right)}{a(a+1)} \cdot \left( 1 + O\left(\frac{\log \log k}{\log k}\right) \right).$$

The last step requires a bit of algebra, and the observation that  $1/(u-v) = 1/u + v/(u(u-v))$ .

To obtain the upper bound, set  $\alpha = 0$ , and note that  $\sum 1/(a(a+1))$  converges to 1. To obtain the lower bound, set  $\alpha = 1$ , and note that  $\sum (1 - \log(1 + 1/a))/(a(a+1))$  converges to a constant  $\geq 0.530684$ .  $\square$

### **Algorithm running time.**

**Theorem 6.5.** *If the UDH is true, then with probability  $1 - o(1)$ , our algorithm has a running time bounded by*

$$g(k) \cdot \exp \left[ \frac{-ck \log \log k}{(\log k)^2} (1 + o(1)) \right],$$

where  $c > 2$  is constant.

*Proof.* Without loss of generality, we assume that  $g(k) \leq N < k \cdot g(k)$ , as we can guess a smaller  $N$ , run the algorithm, and if it fails to find  $g(k)$ , include another prime  $p$  with  $k/2 < p < k$  in  $N$ , and repeat. Since  $N$  at least doubles each time we do this, the cost of running the algorithm on all  $N < g(k)$ , and failing, is bounded by a factor of  $\log g(k)$  times the cost of the final run with a value of  $N > g(k)$  that succeeds. We absorb this multiplicative factor of  $\log g(k)$  in the  $o(1)$  error term in the exponent of the running time bound above as  $\log g(k) = \Theta(k/\log k)$  with high probability. In particular, this gives us  $\log N = (1 + o(1)) \log g(k)$  with high probability.

For the purposes of this proof, we choose  $N$  to be a product of some primes between  $k/2$  and  $k$ . This is conservative, as the choice of primes or prime powers for inclusion in  $N$ , using the methods discussed earlier, will result in a faster algorithm in practice. So we have

$$\prod_{p|N} p = N \approx g(k)$$

and thus

$$\sum_{p|N} \log p = \log N \sim \log g(k) \ll k / \log k.$$

Since  $\sum_{k/2 < p \leq k} \log p = (k/2)(1 + o(1))$ , we have more primes in this range than we need for  $N$  by a factor of roughly  $(1/2) \log k$ . Thus, we can choose the best  $k/(\log k)^2$  primes (roughly) below  $k$  of the  $k/\log k$  that are available. As a result, we expect to get a filtering factor of  $1/\log k$  for the primes we choose. Indeed, if we choose all primes  $p$  with  $k/2 < p < k/2 + c_1 k/\log k$ , with  $c_1 > 0$  an appropriate constant we fix later, this is the case.

Let's check that this gives us a good value for  $N$ . We have

$$\begin{aligned} \log N &= \sum_{k/2 < p < k/2 + c_1 k/\log k} \log p \\ &= \frac{c_1 k}{(\log k)^2} \log(k/2)(1 + o(1)) = \frac{c_1 k}{\log k} (1 + o(1)), \end{aligned}$$

which is larger than  $\log g(k)$  with high probability if we choose  $c_1$  near 1. (See also [13, (2.29)].) Ideally, we want  $g(k) \leq N \leq kg(k)$  here.

Now we address the filter rate, and hence the running time. For each prime  $p$ ,  $k + 2c_1 k/\log k > 2p > k$ , which implies  $k - p > p - 2c_1 k/\log k$  so that

$$\begin{aligned} a_{0p} &= k \bmod p = k - p \\ &> p - \frac{2c_1 k}{\log k} > p - \frac{4c_1 p}{\log k} = p \left( 1 - \frac{4c_1}{\log k} \right). \end{aligned}$$

Our running time, then, is proportional to the number of acceptable residues modulo  $N$ , which is

$$\begin{aligned} \prod_{k/2 < p < k/2 + c_1 k/\log k} (p - a_{0p}) &= \prod_p \left( p - p \left( 1 - \frac{4c_1}{\log k} \right) \right) = \prod_p p \cdot \frac{4c_1}{\log k} = N \prod_p \frac{4c_1}{\log k} \\ &\leq kg(k) \left( \frac{4c_1}{\log k} \right)^{c_1 k/(\log k)^2 (1+o(1))} \\ &= g(k) \exp \left[ -c_1 \frac{k \log \log k}{(\log k)^2} (1 + o(1)) \right]. \quad \square \end{aligned}$$

The UDH is stronger than what we need to prove a running time sublinear in  $g(k)$ . The central issue is finding enough primes  $p$  with  $k/2 < p \leq k/2 + \Delta$  such that the product of these primes is roughly  $g(k)$ . If the number of primes in this interval is  $\Delta/\log k$ , then we can set  $\Delta \approx \log g(k)$ . Pushing this through

our argument above, we obtain a running time of the form

$$g(k) \cdot \exp \left[ \frac{-c\Delta}{\log k} \log \left( \frac{k}{4\Delta} \right) (1 + o(1)) \right]$$

where  $c > 0$  is constant (and likely we can take  $c$  near 1). Observe that plugging in  $\log g(k) \approx k/\log k$  gives our theorem, but this form is valid so long as we can find enough primes. In fact, if  $\log g(k) \gg k^\theta$ , with  $7/12 < \theta \leq 1$ , we can use a result due to Heath–Brown [8] on primes in short intervals to guarantee this is true.

If  $g(k)$  is smaller than this, we would choose  $\Delta = (\log g(k)/\log k)E(k)$ , where  $E(k)$  is the error term for the prime number theorem for  $\pi(k)$ , to give us the needed  $\log g(k)/\log k$  primes above  $k/2$ . (If we assumed the Riemann hypothesis, this would let us use a smaller  $E(k)$  term.) Pushing this through, we obtain a weaker, but still sublinear, running time.

We were also able to show that

$$\limsup_{k \rightarrow \infty} \frac{\hat{g}(k+1)}{\hat{g}(k)} = \infty.$$

We omit the proof due to a lack of space, but the interesting case is when  $k+1$  is prime. It is conjectured that the same holds true for  $g(k)$  itself, but that remains an open problem [2].

## 7. Computations

We conclude with a brief discussion of the timing results. Our source code and timing results are available as an [online supplement](#).

**7.1. Timing results.** We implemented our algorithm from [Section 2](#) in C++. We started with a sequential program, which we used to compute  $g(k)$  for all  $k \leq 272$ , thereby verifying all previous computations along the way [2; 14; 11]. None of these smaller  $k$  values took more than a couple of hours on a standard desktop computer.

We then parallelized our algorithm, using MPI, by having each core generate a share of the residues. However, if a particular core found a new, smaller residue that passed all filters, that new upper bound would not be communicated to all the other cores for some time. This resulted in a fair amount of wasted work. On the other hand, too-frequent inter-core communication would also slow down the computation, since finding new upper bounds is a rare event. We found that our computation distributed over 192 cores only performed about 40–50 times faster than the single-core version.

Our parallel code took anywhere from under an hour to over 1300 hours to compute each  $g(k)$  value. The timing results, in hours of wall time, are shown in [Figure 2](#). Here the  $y$ -axis on the left is in hours, and the  $y$ -axis on the right is used for  $g(k)$  values, which are plotted on the same graph for comparison. In total, the cluster was exclusively computing  $g(k)$  values for about 9 months. The cluster is composed of Intel Xeon E5-2630 v2 processors, with 15MB cache, running at 2.3 GHz. Our algorithm uses very little memory, and so RAM is not an issue.

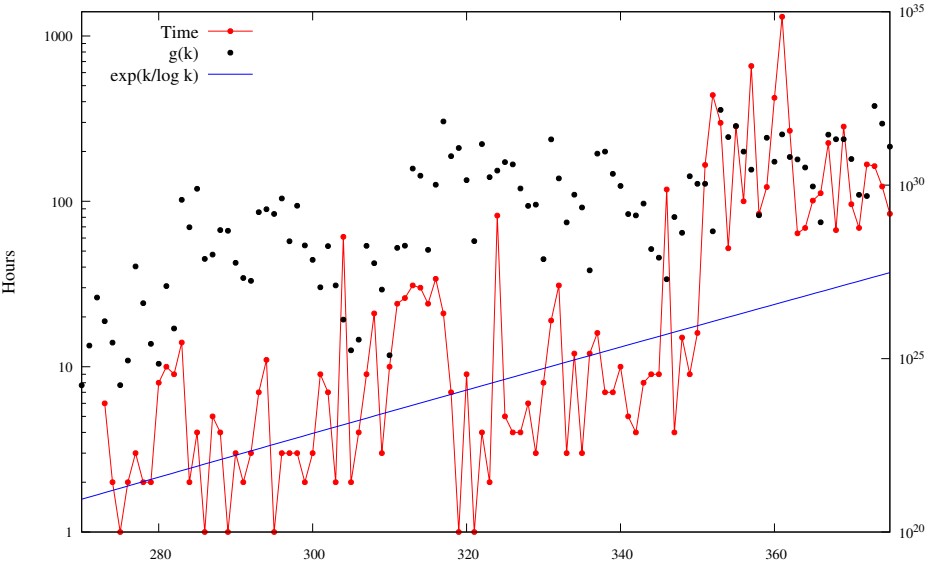


Figure 2. Running time (wall time) in Hours

**7.2. Verification is faster.** It is easy to verify that our claimed  $g(k)$  values all satisfy Kummer’s theorem and are near  $\hat{g}(k)$ . However, we know of no way to independently verify our computations except by repeating the search. Knowing a small admissible candidate gives two significant practical advantages in our algorithm. First, you can work with a modulus  $N$  just larger than the candidate  $g(k)$  value, which is usually smaller than the suggested  $k\hat{g}(k)$  value. Second, you can input the claimed  $g(k)$  value as the starting upper bound for residues. Take the computation of  $g(225)$  as an example. The initial search worked modulo  $N = 1012\ 44299\ 87665\ 22178\ 24000$  and went through at most  $64\ 66521\ 60000$  residues. The candidate for  $g(225)$  was updated three times and the computation took about 26 minutes. A verification computation was done working modulo  $N = 2\ 95172\ 88593\ 77615\ 68000$ , and had at most  $1\ 19750\ 40000$  residues to check, with  $g(225)$  as an input for the initial upper bound. This second computation completed in just 24 seconds. We note that a parallel version of a verification computation can also avoid some of the communication overhead.

**Acknowledgments.** Brianna Sorenson was supported in part by the Butler Summer Institute, by the Honors program, and by the Mathematics Research Camp at Butler University. Jonathan Sorenson and Jonathan Webster were supported in part by a grant from the Holcomb Awards Committee at Butler University.

Special thanks to Rasitha Jayasekare, our friendly neighborhood statistician, for helping us with uniform distribution statistical tests. Also thanks to Michael Filaseta for his help with references.

We thank the three anonymous referees who all contributed very helpful suggestions that improved our paper.

Finally, thanks to Frank Levinson, who generously supports Butler University’s computing research infrastructure.

## References

- [1] Daniel J. Bernstein. Doubly focused enumeration of locally square polynomial values. In *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, volume 41 of *Fields Inst. Commun.*, pages 69–76. Amer. Math. Soc., Providence, RI, 2004.
- [2] E. F. Ecklund, Jr., P. Erdős, and J. L. Selfridge. A new function associated with the prime factors of  $\binom{n}{k}$ . *Math. Comp.*, 28:647–649, 1974.
- [3] P. Erdős, C. B. Lacampagne, and J. L. Selfridge. Estimates of the least prime factor of a binomial coefficient. *Math. Comp.*, 61(203):215–224, 1993.
- [4] Paul Erdős. Some problems in number theory. In A.O.L. Atkin and B.J. Birch, editors, *Computers in Number Theory*, pages 405–414. Academic Press, 1971.
- [5] M. Garey and D. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. Freeman, 1979.
- [6] Andrew Granville and Olivier Ramaré. Explicit bounds on exponential sums and the scarcity of squarefree binomial coefficients. *Mathematika*, 43(1):73–107, 1996.
- [7] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, 5th edition, 1979.
- [8] D.R. Heath-Brown. The number of primes in a short interval. *Journal für die reine und angewandte Mathematik*, 389:22–63, 1988.
- [9] H. Kellerer, U. Pferschy, and D. Pisinger. *Knapsack Problems*. Springer Berlin Heidelberg, 2013.
- [10] S. V. Konyagin. Estimates of the least prime factor of a binomial coefficient. *Mathematika*, 46(1):41–55, 1999.
- [11] Richard F. Lukes, Renate Scheidler, and Hugh C. Williams. Further tabulation of the Erdős-Selfridge function. *Math. Comp.*, 66(220):1709–1717, 1997.
- [12] Kenneth L. Manders and Leonard Adleman. NP-complete decision problems for binary quadratics. *Journal of Computer and System Sciences*, 16(2):168 – 184, 1978.
- [13] J. B. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois Journal of Mathematics*, 6:64–94, 1962.
- [14] R. Scheidler and H. C. Williams. A public-key cryptosystem utilizing cyclotomic fields. Technical Report 15/92, University of Manitoba, Department of Computer Science, November 1992.
- [15] Renate Scheidler and Hugh C. Williams. A method of tabulating the number-theoretic function  $g(k)$ . *Math. Comp.*, 59(199):251–257, 1992.
- [16] Jonathan P. Sorenson. The pseudosquares prime sieve. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of the 7th International Symposium on Algorithmic Number Theory (ANTS-VII)*, pages 193–207, Berlin, Germany, July 2006. Springer. LNCS 4076, ISBN 3-540-36075-1.
- [17] Jonathan P. Sorenson. Sieving for pseudosquares and pseudocubes in parallel using doubly-focused enumeration and wheel datastructures. In Guillaume Hanrot, Francois Morain, and Emmanuel Thomé, editors, *Proceedings of the 9th International Symposium on Algorithmic Number Theory (ANTS-IX)*, pages 331–339, Nancy, France, July 2010. Springer. LNCS 6197, ISBN 978-3-642-14517-9.
- [18] Jonathan P. Sorenson and Jonathan Webster. Strong pseudoprimes to twelve prime bases. *Math. Comp.*, 86(304):985–1003, 2017.
- [19] Jonathan P. Sorenson and Jonathan Webster. Two algorithms to find primes in patterns. *Math. Comp.*, 89(324):1953–1968, 2020.

Received 20 Feb 2020. Revised 7 Sep 2020.

BRIANNA SORENSON: [bsorenso@butler.edu](mailto:bsorenso@butler.edu)

Mathematics, Statistics and Actuarial Science, Butler University, Indianapolis, IN, United States

JONATHAN SORENSON: [jsorenso@butler.edu](mailto:jsorenso@butler.edu)

Computer Science and Software Engineering, Butler University, Indianapolis, IN, United States

JONATHAN WEBSTER: [jewebste@butler.edu](mailto:jewebste@butler.edu)

Mathematics, Statistics and Actuarial Science, Butler University, Indianapolis, IN, United States





# Totally $p$ -adic numbers of degree 3

Emerald Stacy

The height of an algebraic number  $\alpha$  is a measure of how arithmetically complicated  $\alpha$  is. We say  $\alpha$  is totally  $p$ -adic if the minimal polynomial of  $\alpha$  splits completely over the field  $\mathbb{Q}_p$  of  $p$ -adic numbers. We investigate what can be said about the smallest nonzero height of a degree 3 totally  $p$ -adic number.

## 1. Introduction

Recall that an algebraic number  $\alpha$  is *totally  $p$ -adic* (respectively, totally real) if the minimal polynomial of  $\alpha$ ,  $f_\alpha \in \mathbb{Q}[x]$ , splits completely over  $\mathbb{Q}_p$  (respectively,  $\mathbb{R}$ ). We will denote by  $h(\alpha)$  the logarithmic Weil height of  $\alpha$  [BG06].

In 1975, Schinzel used the arithmetic-geometric mean inequality to prove that if  $\alpha$  is a totally real algebraic integer, with  $\alpha \neq 0, \pm 1$ , then

$$h(\alpha) \geq \frac{1}{2} \log \left( \frac{1+\sqrt{5}}{2} \right)$$

with equality if  $\alpha = \frac{1}{2}(1 + \sqrt{5})$  [Sch75]. In 1993, Höhn & Skoruppa used an auxiliary function to provide an alternate proof of Schinzel's bound [HS93]. Bombieri & Zannier [BZ01] proved that an analogue to Schinzel's theorem holds in  $\mathbb{Q}_p$  for each prime  $p$ , although the analogous best possible lower bound is unknown.

Additionally, there have been some results constructing totally  $p$ -adic (or totally real) algebraic numbers of small height. In particular, these results provide an upper bound on the smallest height attained by  $\alpha$  under certain splitting conditions. The degree of a totally  $p$ -adic number is the degree of its minimal polynomial with coefficients in  $\mathbb{Z}$ . Petsche [Pet] proved that for odd primes  $p$ , there exists some totally  $p$ -adic  $\alpha \in \overline{\mathbb{Q}}$  of degree  $d \leq p - 1$ , and

$$0 < h(\alpha) \leq \frac{1}{p-1} \log \left( \frac{p + \sqrt{p^2 + 4}}{2} \right).$$

Recently, Pottmeyer [Pot18] has improved upon Petsche's upper bound, and obtained the existence of totally  $p$ -adic  $\alpha$  such that

$$0 < h(\alpha) \leq \frac{\log p}{p}.$$

In 1980, Smyth created a set of totally real numbers of small height by taking all preimages of 1 under the map  $\phi(x) = x - \frac{1}{x}$ . The heights of the points in this set have a limit point  $\ell \approx 0.27328$  [Smy80]. In [PS19], Petsche and Stacy use an argument inspired by this result of Smyth to provide an upper bound on the smallest limit point of heights of totally  $p$ -adic numbers of degree  $d$ .

In this paper, we fix the degree  $d$  to be 3 and let the prime  $p$  vary. In particular, we define  $\tau_{d,p}$  to be the smallest height attained by a totally  $p$ -adic, nonzero, nonroot of unity, algebraic number of degree  $d$ . For any pair  $d$  and  $p$ , we know  $\tau_{d,p} < \infty$  since we can construct a Newton polygon for an irreducible polynomial of degree  $d$  that splits completely over  $\mathbb{Q}_p$  [Cas86].

In this paper, we develop tools to determine  $\tau_{3,p}$  for all  $p \geq 5$ . In Section 2, we develop and prove an algorithm to determine  $\tau_{3,p}$  for a given prime  $p$ , which we implement in Section 2.5. All code was written for SageMath, version 8.2, and is included within Section 2.5. A table of results can be found in Section 3, and Section 4 describes future areas of interest.

## 2. The algorithm

In Section 2.1, we prove that  $\tau_{3,p} \leq 0.70376$  for all  $p \geq 5$ . To do so, we establish that for every prime  $p$ , there is a cubic polynomial with an abelian Galois group that splits completely over  $\mathbb{Q}_p$ . By the height-length bound [BG06, Proposition 1.6.7], a list of all cubic polynomials with length less than 68 will contain all irreducible, noncyclotomic, cubic polynomials with roots of height less than 0.70376. By the Northcott property there are only finitely many such polynomials, and thus we have a finite list to check for  $\tau_{3,p}$  and our algorithm will terminate.

In Section 2.2, we use the method of Cardano to determine the roots of a cubic polynomial. In Sections 2.3 and 2.4, we establish criteria to determine if those roots are in  $\mathbb{Q}_p$ . The criteria are different depending if  $p \equiv 1 \pmod{3}$  or  $p \equiv 2 \pmod{3}$ , since  $\mathbb{Q}_p$  contains a primitive cube root of unity if and only if  $p \equiv 1 \pmod{3}$ . In Section 2.5, we implement the algorithm, the results of which can be found in Section 3.

**2.1. Establishing termination.** To establish that our algorithm will terminate, we create a finite list of polynomials, and verify that for each prime, there must be a polynomial in our list that will split completely over  $\mathbb{Q}_p$ .

Let  $f_\alpha$  denote the minimal polynomial of  $\alpha$ . Then  $h(\alpha) = \frac{1}{3} \log M(f_\alpha)$ , where  $M(f_\alpha)$  is the Mahler measure of  $f_\alpha$ . Thus, if  $M(f_\alpha) \leq 8.5$ , then  $h(\alpha) \leq 0.71335$ . The function `mahler_measure_cubic` calculates the Mahler measure of the cubic polynomial

$$f(x) = ax^3 + bx^2 + cx + d :$$

```

def mahler_measure_cubic(a,b,c,d):
    M = a
    Poly = a*x^3 + b*x^2 + c*x + d
    Roots = Poly.roots(CC)
    for i in [0..len(Roots)-1]:
        M = M * max(1,abs(Roots[i][0]))
    return M.n(digits=10)

```

For  $f(x) = \sum_{i=0}^d a_i x^i$ , the *length* of  $f$  is  $L(f) = \sum_{i=0}^d |a_i|$ . The length will be useful to us since for any polynomial  $f$ ,

$$L(f) \leq 2^d M(f),$$

where  $d = \deg f$  [BG06, Proposition 1.6.7]. Thus, the following program generates a list of all cubic polynomials with

$$L(f) \leq 2^3(8.5) = 68$$

and removes any polynomial that is either reducible or has Mahler measure greater than 8.5. We use the built-in Sage function `is_irreducible()` to determine if a polynomial is irreducible over  $\mathbb{Q}$ .

In addition to the polynomial and Mahler measure, the list also stores the coefficients of the cubic in its so-called depressed form  $(x^3 + Ax + B)$ , the discriminant of the polynomial, and the height of the roots. For more information on depressing a cubic, please see [Section 2.2](#).

The command `sorted()` will reorganize the array in ascending order of the first value — in this case it will sort by Mahler measure, which is equivalent to sorting by height. The output of this program is 26796 polynomials that are saved as the file `irred_polynomials_L68`. Runtime was 124 minutes.

```

R.<x> = QQ[]
Polynomials=[]
L=68
for a in [1..L]:
    for b in [-L+abs(a)..L-abs(a)]:
        for c in [-L+abs(a)+abs(b)..L-abs(a)-abs(b)]:
            for d in [-L+abs(a)+abs(b)+abs(c)..L-abs(a)-abs(b)-abs(c)]:
                Poly = a*x^3 + b*x^2 + c*x + d
                if Poly.is_irreducible()==True:
                    MM = mahler_measure_cubic(a,b,c,d)
                    A = (3*a*c - b^2) / (3*a^2)
                    B = (27*a^2*d - 9*a*b*c + 2*b^3) / (27*a^3)
                    Delta = B^2 + 4 * A^3 / 27
                    h = 1/3 * log(MM);
                    if MM <= L/8:
                        Polynomials.append([MM,a,b,c,d,A,B,Delta,h])
Polynomials=sorted(Polynomials)

```

Next, we remove from this list all polynomials with nonabelian Galois group. In general, the Galois group of a polynomial  $f(x) \in \mathbb{Z}[x]$  of degree  $d$  is isomorphic to a subgroup of  $A_d$  if and only if the discriminant of  $f$  is a square in  $\mathbb{Q}$  [Con18, Theorem 1.3]. In the case of  $f$  cubic, the Galois group of  $f$  is  $A_3$ , and thus abelian, if and only if the discriminant of  $f$  is a square in  $\mathbb{Q}$ .

Let  $K$  be the number field created by adjoining the roots of  $f$  to  $\mathbb{Q}$  and let  $\Delta$  be the discriminant of  $K$ . By the Kronecker–Weber theorem,  $K$  must be contained within a cyclotomic extension of  $\mathbb{Q}$ . Let  $m$  be the

conductor of  $K$ , meaning the smallest  $m$  such that  $K$  is a subfield of  $\mathbb{Q}(\zeta_m)$ , where  $\zeta_m$  is a primitive  $m$ -th root of unity. To calculate the conductor, we turn to a special case of the Hasse conductor-discriminant formula, as follows.

**Theorem 1** [Has30, Theorem 6]. *Let  $K$  be an abelian extension of  $\mathbb{Q}$ , with  $[K : \mathbb{Q}] = 3$  and discriminant  $\Delta$ . Let  $p_1, p_2, \dots, p_n$  be all the primes (aside from 3) that divide  $\Delta$ . If 3 divides  $\Delta$ , then the conductor of  $K$  is  $9p_1p_2 \cdots p_n$ . If 3 not does divide  $\Delta$ , then the conductor of  $K$  is  $p_1p_2 \cdots p_n$ .*

The following program begins by identifying if each cubic polynomial has an abelian Galois group. If so, then the program calculates the discriminant of  $K$  (the number field obtained by adjoining the roots of  $f$  to  $\mathbb{Q}$ ) by applying the built-in function `absolute_discriminant()`. It then applies [Theorem 1](#) and uses the built-in Sage command `factor()` to determine the conductor of  $K$ . All of this output is stored in the array `AbelianCubics`, which contains the information for 156 polynomials.

```
Polynomials=load('irred_polynomials_L68')
L=len(Polynomials)
AbelianCubics=[]
for i in [0..L-1]:
    Poly = Polynomials[i];
    a = Poly[1];
    b = Poly[2];
    c = Poly[3];
    d = Poly[4];
    D = b^2*c^2 - 4*a*c^3 - 4*b^3*d - 27*a^2*d^2 + 18*a*b*c*d;
    if D.is_square()==True:
        K.<j> = NumberField(a*x^3 + b*x^2 + c*x + d)
        DD = K.absolute_discriminant()
        MM = Poly[0];
        h = Poly[8];
        Factors = DD.factor()
        list_of_factors = list(Factors)
        L = len(list_of_factors)
        Cond = 1
        for i in [0..L-1]:
            Cond = Cond*list_of_factors[i][0]
            if list_of_factors[i][0]==3:
                Cond = Cond*3
        C = Cond
        AbelianCubics.append([h, a*x^3 + b*x^2 + c*x + d ,DD,C]);
```

The following lemma is well known, but for lack of a convenient reference, we provide a proof.

**Lemma 2.** *Let  $\alpha \in \mathbb{Q}(\zeta_n)$  have minimal polynomial  $f_\alpha \in \mathbb{Z}[x]$ , and let*

$$G_\alpha = \{[i] \in (\mathbb{Z}/n\mathbb{Z})^\times \mid \sigma_i(\alpha) = \alpha\},$$

*where  $\sigma_i(\zeta_n) = \zeta_n^i$ . Thus  $G_\alpha$  is the subgroup of  $(\mathbb{Z}/n\mathbb{Z})^\times$  corresponding to  $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\alpha))$  via the isomorphism  $(\mathbb{Z}/n\mathbb{Z})^\times \cong \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ . Let  $p \nmid n$  be a prime. Then  $f_\alpha$  splits completely in  $\mathbb{Q}_p$  if and only if  $[p] \in G_\alpha$ .*

*Proof.* The automorphism  $\sigma_p \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$  satisfies  $\sigma_p(x) \equiv x \pmod{p}$  for all  $x \in \mathbb{Z}[\zeta_n]$  [Bak06, Lemma 4.51]. Since  $\mathbb{Q}(\zeta_n)/\mathbb{Q}$  is an abelian extension,  $\mathbb{Q}(\alpha)/\mathbb{Q}$  is a Galois extension and therefore  $\sigma_p$

restricts to an automorphism  $\sigma_p \in \text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ ; the above congruence implies that  $\sigma_p$  is the Frobenius element of  $\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$  associated to the prime  $p$ .

If  $[p] \in G_\alpha$ , then  $\sigma_p$  is the identity element of  $\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ , which implies that  $p$  splits completely in  $\mathbb{Q}(\alpha)$  [Bak06, Proposition 4.36]; that is  $p\mathcal{O}_{\mathbb{Q}(\alpha)} = \mathfrak{p}_1 \cdots \mathfrak{p}_d$ , where  $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ . It follows that each local degree  $e(\mathfrak{p}_i/p)f(\mathfrak{p}_i/p) = [\mathbb{Q}(\alpha)_{\mathfrak{p}_i} : \mathbb{Q}_p]$  is equal to 1 [Bak06, Theorem 5.25], which means that  $\mathbb{Q}(\alpha)_{\mathfrak{p}_i} = \mathbb{Q}_p$  for  $i = 1, 2, \dots, d$ . In particular,  $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}_p$ , and therefore as  $\mathbb{Q}(\alpha)/\mathbb{Q}$  is Galois, all  $d$  of the Galois conjugates of  $\alpha$  are in  $\mathbb{Q}_p$  as well. Hence  $f_\alpha(x)$  splits completely in  $\mathbb{Q}_p$ . The converse follows from a straightforward reversal of this argument.  $\square$

For each polynomial  $f_\alpha$  in `AbelianCubics`, we want to determine the congruence classes modulo  $m$  of a prime  $p$  for  $f_\alpha$  to split completely in  $\mathbb{Q}_p$ , where  $m$  is the conductor of the splitting field of  $f_\alpha$ . The following code goes through each line in the array `AbelianCubics`, and for each polynomial  $f_\alpha$  in the list, computes the set  $B_\alpha \subseteq (\mathbb{Z}/m\mathbb{Z})^\times$  so that  $f_\alpha$  splits completely in  $\mathbb{Q}_p$  if and only if  $[p] \in B_\alpha$ , where  $[p]$  denotes the residue of  $p \pmod{m}$ .

Note that if  $(\mathbb{Z}/m\mathbb{Z})^\times$  has a unique index 3 subgroup, then this group must be  $G_\alpha$ . In the case that  $(\mathbb{Z}/m\mathbb{Z})^\times$  does not have a unique index 3 subgroup, we check the first 50 primes to determine if there is a root in  $\mathbb{Q}_p$  via Hensel's lemma. When a root of  $f_\alpha$  is determined to be in  $\mathbb{Q}_p$ , we know that for all primes  $q$  with  $q \equiv p \pmod{m}$ ,  $f_\alpha$  must split completely in  $\mathbb{Q}_p$ , by Lemma 2. Further, we know there are  $|(\mathbb{Z}/m\mathbb{Z})^\times|/3$  congruence classes for which  $f_\alpha$  splits completely in  $\mathbb{Q}_p$ . Thus, after testing the first 50 primes, the code checks the cardinality of the set of congruences to ensure all were found. For this particular list of polynomials, 50 is sufficient to identify the index 3 subgroup.

```
AbelianCubics=load('AbelianCubics')
L=len(AbelianCubics);
P = Primes();
for i in [0..L-1]:
    Poly = AbelianCubics[i][1]
    PolyList = Poly.list()
    a = PolyList[3]
    b = PolyList[2]
    c = PolyList[1]
    d = PolyList[0]
    Cond = AbelianCubics[i][3]
    v = [1];
    for j in [0..50]:
        for k in [1..P[j]-1]:
            M = Integer( a*k^3 + b*k^2 + c*k + d )
            M = M%P[j]
            N = Integer( 3*a*k^2 + 2*b*k + c )
            N = N%P[j]
            if M==0 and N>0:
                v.append(P[j]%Cond)
V = sorted(v)
V = set(V)
```

The results of this code are included as an [online supplement](#) to this paper. A sampling of the data is included in Table 1 for reference.

$h(\alpha)$	$f_\alpha$	$\alpha$ is totally $p$ -adic if and only if
0.26986	$x^3 - x^2 - 2x + 1$	$p \equiv 1, 6 \pmod{7}$
0.35252	$x^3 - 3x^2 + 1$	$p \equiv 1, 8 \pmod{9}$
0.60981	$3x^3 - 4x^2 - 5x + 3$	$p \equiv 1, 3, 8, 9, 11, 20, 23, 24, 27, 28, 33, 34, 37, 38, 41, 50, 52, 53, 58, 60 \pmod{61}$
0.69106	$3x^3 - x^2 - 8x + 3$	$p \equiv 1, 3, 7, 8, 9, 10, 17, 21, 22, 24, 27, 30, 43, 46, 49, 51, 52, 56, 63, 64, 65, 66, 70, 72 \pmod{73}$
0.69903	$2x^3 - 9x^2 + 3x + 2$	$p \equiv 1, 2, 4, 8, 16, 31, 32, 47, 55, 59, 61, 62 \pmod{63}$
0.70376	$x^3 - 9x^2 + 6x + 1$	$p \equiv 1, 5, 8, 11, 23, 25, 38, 40, 52, 55, 58, 62 \pmod{63}$

**Table 1.** A sample of the data included in the online supplement.

**Theorem 3.** Let  $p$  be a prime. Then  $\tau_{3,p} \leq 0.70376$ .

*Proof.* For a prime  $p$ , denote by  $\tau_{3,p}^{\text{ab}}$  the smallest nontrivial height of an abelian, cubic, totally  $p$ -adic number. Note that  $\tau_{3,p} \leq \tau_{3,p}^{\text{ab}}$ . Thus, if we show that  $\tau_{3,p}^{\text{ab}} \leq 0.70376$ , we have proven the theorem.

Based on the results from [Table 1](#), we know

$$\tau_{3,3}^{\text{ab}} \leq 0.609817669 \quad \text{and} \quad \tau_{3,7}^{\text{ab}} \leq 0.501878627.$$

All primes  $p \neq 3, 7$ , when reduced modulo 63, are contained in  $(\mathbb{Z}/63\mathbb{Z})^\times$ . Observe that

$$(\mathbb{Z}/63\mathbb{Z})^\times = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20, 22, 23, 25, 26, 29, 31, 32, 34, 37, 38, 40, 41, 43, 44, 46, 47, 50, 52, 53, 55, 58, 59, 61, 62\}.$$

Further, we observe that

$$\tau_{3,p}^{\text{ab}} \leq \begin{cases} 0.269862305 & \text{if } p \equiv 1, 6 \pmod{7}, \\ 0.352525605 & \text{if } p \equiv 1, 8 \pmod{9}. \end{cases}$$

Thus

$$\tau_{3,p}^{\text{ab}} \leq 0.269862305 \text{ for } p \equiv 1, 8, 13, 20, 22, 29, 34, 41, 43, 50, 55, 62 \pmod{63},$$

$$\tau_{3,p}^{\text{ab}} \leq 0.352525605 \text{ for } p \equiv 10, 17, 19, 26, 37, 44, 46, 53 \pmod{63}.$$

It remains to determine an upper bound on  $\tau_{3,p}^{\text{ab}}$  for

$$p \equiv 2, 4, 5, 11, 16, 23, 25, 31, 32, 38, 40, 47, 52, 58, 59, 61 \pmod{63}.$$

Note that each of the above numbers falls into one of the following two sets:

$$p \equiv 1, 2, 4, 8, 16, 31, 32, 47, 55, 59, 61, 62 \pmod{63},$$

$$p \equiv 1, 5, 8, 11, 23, 25, 38, 40, 52, 55, 58, 62 \pmod{63}.$$

Further, we observe that by the last two lines of [Table 1](#), given any prime  $p$ , one of the polynomials in the table must split completely over  $\mathbb{Q}_p$ . □

**2.2. Determining roots of cubic polynomials.** In *Ars Magna*, Cardano describes a method to find the roots of a cubic polynomial  $f$  as elements of  $\mathbb{C}$  [CS68]. This method is analogous to completing the square for a quadratic polynomial. We use Cardano's method to determine if a cubic polynomial in  $K[y]$  splits completely over  $K$ , where  $K$  is an arbitrary field of characteristic not equal to 2 or 3. Beginning with an arbitrary cubic polynomial in  $K[y]$ ,

$$g(y) = ay^3 + by^2 + cy + d,$$

we divide through by the leading coefficient and perform a change of variables  $y = x - b/3$  to eliminate the quadratic term, yielding a monic depressed cubic polynomial with coefficients in  $K$ ,

$$f(x) = x^3 + Ax + B.$$

Note that since the transformations to depress the cubic simply shift the roots by  $b/(3a)$ , so  $g$  splits over  $K$  if and only if  $f$  splits over  $K$ .

**Lemma 4** (Cardano [CS68]). *Let  $L$  be an algebraically closed field of characteristic not equal to 2 or 3, and let  $\zeta$  be a primitive cube root of unity in  $L$ . Let  $f(x) = x^3 + Ax + B \in L[x]$ , and let  $\Delta = B^2 + 4A^3/27$ . If  $A = 0$ , let  $C = -B$ , and if  $A \neq 0$ , let  $C$  be either square root of  $\Delta$  in  $L$ . Let  $u$  be a cube root of  $(-B + C)/2$  and let  $v = -A/(3u)$ . Then the roots of  $f$  are  $u + v$ ,  $\zeta u + \zeta^2 v$ , and  $\zeta^2 u + \zeta v$ .*

To determine when a cubic polynomial  $f(x) \in \mathbb{Q}_p[x]$  splits completely over  $\mathbb{Q}_p$ , the method will depend on whether  $\mathbb{Q}_p$  contains a primitive cube root of unity, which happens exactly when  $p \equiv 1 \pmod{3}$ . Thus, we consider two cases:  $p \equiv 1 \pmod{3}$  and  $p \equiv 2 \pmod{3}$ .

**2.3. Case 1.** Suppose  $p \equiv 1 \pmod{3}$ .

**Theorem 5.** *Let  $K$  be a field of characteristic not equal to 2 or 3, let  $L$  be an algebraic closure of  $K$ , and assume that  $K$  contains a primitive cube root of unity,  $\zeta$ . Let  $f(x) = x^3 + Ax + B \in K[x]$ , and  $\Delta = B^2 + 4A^3/27$ . If  $A = 0$ , let  $C = -B$ , and if  $A \neq 0$ , let  $C$  be either square root of  $\Delta$  in  $L$ . Then  $f$  splits completely over  $K$  if and only if*

- (a)  $\Delta$  is a square in  $K$ , and
- (b)  $(-B + C)/2$  is a cube in  $K$ .

*Proof.* Suppose  $A = 0$ . Then  $\Delta = B^2$  is a square in  $K$ , so (a) is true. Additionally,  $C = -B$  and  $f(x) = x^3 + B$ , which splits completely over  $K$  if and only if  $-B$  is a cube in  $K$ , which happens exactly when (b) holds.

Now suppose  $A \neq 0$ . Let  $u$  be a cube root of  $(-B + C)/2$  and let  $v = -A/(3u)$ . Let  $F$  be a Galois extension of  $K$  containing  $C$  and  $u$ .

Suppose the conditions (a) and (b) are met. By Lemma 4, the roots of  $f$  are  $u + v$ ,  $\zeta u + \zeta^2 v$ , and  $\zeta^2 u + \zeta v$  and thus  $f$  splits completely over  $K$ .

Conversely, suppose that  $f$  splits completely over  $K$ . Let  $\sigma \in \text{Gal}(L/K)$ . Since  $\sigma$  fixes  $u + v$  and  $\zeta u + \zeta^2 v$ ,

$$u + v = \sigma(u) + \sigma(v) \quad \text{and} \quad \zeta u + \zeta^2 v = \zeta \sigma(u) + \zeta^2 \sigma(v). \quad (1)$$

Note that  $\begin{pmatrix} 1 & 1 \\ \zeta & \zeta^2 \end{pmatrix}$  has a nonzero determinant and thus

$$\begin{pmatrix} 1 & 1 \\ \zeta & \zeta^2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \sigma(u) + \sigma(v) \\ \zeta \sigma(u) + \zeta^2 \sigma(v) \end{pmatrix} \quad (2)$$

has a unique solution. By (1),  $x = u$ ,  $y = v$  is a solution to (2) and  $x = \sigma(u)$ ,  $y = \sigma(v)$  is a solution to (2) as well. Therefore  $u = \sigma(u)$ . By the Galois correspondence,  $u \in K$ , and thus (b) holds. Thus  $u^3 = (-B + C)/2 \in K$ . Since  $C = 2u^3 + B$ ,  $C \in K$  and therefore

$$\Delta = B^2 + 4A^3/27 = C^2$$

is a square in  $K$ , and (a) is true. □

**Lemma 6.** *Let  $p$  be a prime,  $p \neq 3$ , and let  $a \in \mathbb{Z}_p$  with  $|a|_p = 1$ . Then  $a$  is a cube in  $\mathbb{Q}_p$  if and only if  $a \pmod{p}$  is a cube in  $\mathbb{Z}_p/p\mathbb{Z}_p$ .*

*Proof.* Suppose that  $a$  is a cube in  $\mathbb{Z}_p$ . Then  $a$  is a cube in  $\mathbb{Z}_p/p\mathbb{Z}_p$  by the nature of quotient rings.

Conversely, suppose  $a_0$  is a cube in  $\mathbb{Z}/p\mathbb{Z}$  where  $a_0 \equiv a \pmod{p}$ , and let  $b_0 \in \mathbb{Z}/p\mathbb{Z}$  satisfy  $b_0^3 \equiv a_0 \pmod{p}$ . Let  $f(x) = x^3 - a$ . Note that  $p$  does not divide 3 or  $b_0$ . By the strong triangle inequality,

$$|f(b_0)|_p = |b_0^3 - a|_p \leq \max\{|b_0^3 - a_0|_p, |a_0 - a|_p\} \leq \frac{1}{p}.$$

Further,

$$|f'(b_0)|_p = |3b_0^2|_p = 1.$$

By Hensel's lemma,  $a$  is a cube in  $\mathbb{Q}_p$ . □

**Theorem 7.** *Let  $p$  be a prime, with  $p \equiv 1 \pmod{3}$ . Then the following algorithm yields  $\tau_{3,p}$ .*

- (1) *Create a list, in ascending order of Mahler measure, of all irreducible, noncyclotomic cubic polynomials in  $\mathbb{Z}[x]$  with Mahler measure bounded above by 8.5. Let  $f(x)$  be the first polynomial on the list.*
- (2) *Convert  $f(x)$  into depressed form  $g(x) = x^3 + Ax + B$  and let  $\Delta = B^2 + 4A^3/27$ .*
- (3) *If  $\Delta$  is not a square in  $\mathbb{Q}_p$ , return to step (2) with the next polynomial on the list.*
- (4) *If  $A = 0$ , let  $C = -B$ , and otherwise let  $C$  be a square root of  $\Delta$  in  $\mathbb{Q}_p$ . If  $(-B + C)/2$  is not a cube in  $\mathbb{Q}_p$ , return to step (2) with the next polynomial on the list. Otherwise, terminate, giving  $\tau_{3,p} = \frac{1}{3} \log M(f)$ .*

*Proof.* Since  $\tau_{3,p} \leq \tau_{3,p}^{\text{ab}}$ , by Theorem 3 we know that  $\tau_{3,p} \leq 0.70376$ . By [BG06, Proposition 1.6.7], a list of all polynomials with length less than 68 will contain all irreducible, noncyclotomic, cubic polynomials



with Mahler measure bounded above by 8.5. Any degree 3 algebraic number of height less than or equal to 0.70376 will be a root of a polynomial in the list. Thus, this algorithm will always terminate successfully.

Let  $f$  be the polynomial being considered. By [Theorem 5](#), steps (3) and (4) will detect exactly when  $f$  splits completely over  $\mathbb{Q}_p$ .  $\square$

**2.4. Case 2.** Suppose  $p \equiv 2 \pmod{3}$ .

**Theorem 8.** *Let  $K$  be a field of characteristic not equal to 2 or 3,  $K'$  be an algebraic closure of  $K$ ,  $\zeta$  be a primitive cube root of unity in  $K'$ , and assume that  $\zeta \notin K$ . Let  $f(x) = x^3 + Ax + B \in K[x]$  with  $B \neq 0$  and let  $\Delta = B^2 + 4A^3/27$ . If  $A = 0$ , let  $C = -B$ , and if  $A \neq 0$ , let  $C$  be either square root of  $\Delta$  in  $K'$ . Then  $f$  splits completely over  $K$  if and only if*

- (a)  $\Delta$  is a square in  $K(\zeta)$  and not a square in  $K$ , and
- (b)  $(-B + C)/2$  is a cube in  $K(\zeta)$  and not a cube in  $K$ .

*Proof.* Let  $u$  be a cube root of  $(-B + C)/2$  and let  $v = -A/(3u)$ . By [Lemma 4](#), the roots of  $f$  are  $u + v$ ,  $\zeta u + \zeta^2 v$ , and  $\zeta^2 u + \zeta v$ .

We first suppose  $f$  splits completely in  $K$ . Let  $L$  be a Galois extension of  $K$  that contains  $u$  and  $\zeta$ . Let  $\sigma \in \text{Gal}(L/K(\zeta))$ . We want to show that  $\sigma$  must fix  $u$ . Since we are assuming that  $f$  splits completely over  $K$ ,  $\sigma$  must fix  $u + v$ ,  $\zeta u + \zeta^2 v$ , and  $\zeta^2 u + \zeta v$ ,

$$u + v = \sigma(u) + \sigma(v), \quad (3)$$

$$\zeta^2 u + \zeta v = \zeta^2 \sigma(u) + \zeta \sigma(v). \quad (4)$$

By multiplying (3) by  $\zeta$  and subtracting (4), we obtain

$$(\zeta - \zeta^2)u = (\zeta - \zeta^2)\sigma(u), \quad (5)$$

so  $\sigma(u) = u$  because  $\zeta \neq \zeta^2$ . Thus, since all elements in  $\text{Gal}(L/K(\zeta))$  fix  $u$ ,  $u$  must be in  $K(\zeta)$ .

It remains to show  $u \notin K$ . Let  $\tau \in \text{Gal}(L/K)$  be such that  $\tau$  interchanges  $\zeta$  and  $\zeta^2$ . We now show that  $\tau$  does not fix  $u$ . Since the roots of  $f$  must all be fixed by  $\tau$ ,

$$\zeta u + \zeta^2 v = \zeta^2 \tau(u) + \zeta \tau(v), \quad (6)$$

$$\zeta^2 u + \zeta v = \zeta \tau(u) + \zeta^2 \tau(v). \quad (7)$$

By multiplying (7) by  $\zeta$ , and subtracting (6), we obtain

$$(1 - \zeta)u = (1 - \zeta)\tau(v) \quad (8)$$

and note that  $\tau(v) = u$ , so  $\tau$  does not fix  $u$ . Thus  $u \notin K$  and (b) holds.

Further,  $u \in K(\zeta)$ , so  $u^3 = (-B + C)/2 \in K(\zeta)$ , and thus  $\Delta$  is a square in  $K(\zeta)$  since  $C \in K(\zeta)$ . Since  $K(u)$  is contained within  $K(\zeta)$ , a quadratic extension of  $K$ , and  $u \notin K$ , it follows that  $[K(u) : K] = 2$ . For sake of contradiction, suppose  $\Delta$  is a square in  $K$ . Then  $u^3 \in K$ , so  $[K(u) : K] = 3$  which is not true. Thus  $\Delta$  is not a square in  $K$ , and (a) holds.

Conversely, suppose that (a) and (b) are true. Note that if  $A = 0$ , then  $\Delta$  is a square in  $K$ , contradicting (a). Thus,  $A \neq 0$ . Let  $\sigma$  denote the nontrivial element of  $\text{Gal}(K(\zeta)/K)$ . Since  $\zeta$  and  $\zeta^2$  share a degree 2 minimal polynomial,  $\sigma$  must permute  $\zeta$  and  $\zeta^2$ .

By (a) and (b),  $u, u^3 \notin K$  and  $u, u^3 \in K(\zeta)$ . Since  $u^3$  and  $v^3$  are the roots of  $r(z) = z^2 + Bz - A^3/27$ , we have  $\sigma(u)^3 = \sigma(u^3) = v^3$ . Therefore, either  $\sigma(u) = v$ ,  $\sigma(u) = \zeta v$ , or  $\sigma(u) = \zeta^2 v$ .

We will now show that  $\sigma(u) = v$  by eliminating the other two options by way of contradiction. We rely on the fact that elements of the Galois group send roots of  $f$  to roots of  $f$ , and that  $\sigma^2(u) = u$ . If  $\sigma(u) = \zeta v$ , then  $u = \zeta^2 \sigma(v)$ , and  $\sigma(u + v) = \sigma(u) + \sigma(v) = \zeta v + \zeta u$ . Since  $\zeta v + \zeta u$  is not a root of  $f$ ,  $\sigma(u) \neq \zeta v$ . If  $\sigma(u) = \zeta^2 v$ , then  $u = \zeta \sigma(v)$ , and  $\sigma(u + v) = \zeta^2 u + \zeta^2 v$ . Since  $\zeta^2 u + \zeta^2 v$  is not a root of  $f$ ,  $\sigma(u) \neq \zeta^2 v$ .

Therefore,  $\sigma(u) = v$  and  $\sigma(v) = u$ . Thus

$$\begin{aligned}\sigma(u + v) &= \sigma(u) + \sigma(v) = v + u, \\ \sigma(\zeta u + \zeta^2 v) &= \sigma(\zeta u) + \sigma(\zeta^2 v) = \zeta^2 v + \zeta u, \\ \sigma(\zeta^2 u + \zeta v) &= \sigma(\zeta^2 u) + \sigma(\zeta v) = \zeta v + \zeta^2 v.\end{aligned}$$

Since  $\sigma$  fixes the roots of  $f$ ,  $f$  splits completely in  $K$ . □

Let  $p \equiv 2 \pmod{3}$ . The third cyclotomic polynomial,  $\Phi_3(x) = x^2 + x + 1$ , has discriminant  $-3$  and is the minimal polynomial for  $\zeta$ . Since  $-3$  is not a square in  $\mathbb{Q}_p$ ,  $\Phi_3(x)$  is irreducible over  $\mathbb{Q}_p$ , and thus  $\mathbb{Q}_p$  does not contain a primitive cube root of unity. There are exactly three quadratic extensions of  $\mathbb{Q}_p$ :  $\mathbb{Q}_p(\sqrt{p})$ ,  $\mathbb{Q}_p(\sqrt{-3})$ , and  $\mathbb{Q}_p(\sqrt{-3p})$ . Let  $K = \mathbb{Q}_p(\sqrt{-3}) = \mathbb{Q}_p(\zeta)$ , the unique unramified quadratic extension of  $\mathbb{Q}_p$ . The  $p$ -adic absolute value on  $\mathbb{Q}_p$  extends uniquely to  $\mathbb{Q}_p(\sqrt{-3})$  by

$$|a + b\sqrt{-3}|_p = |N_{K/\mathbb{Q}_p}(a + b\sqrt{-3})|_p^{1/2} = |a^2 + 3b^2|_p^{1/2}.$$

The following three lemmas summarize some basic facts about this field.

**Lemma 9.** *Let  $p \equiv 2 \pmod{3}$ , and  $K = \mathbb{Q}_p(\sqrt{-3})$ . For  $x \in K^\times$ ,  $|x|_p \in p^{\mathbb{Z}}$ .*

*Proof.* Let  $x = a + b\sqrt{-3}$ , with  $a, b \in \mathbb{Q}_p$  and  $x \neq 0$ . Suppose  $|a|_p \neq |b|_p$ . Then

$$|x|_p = |a^2 + 3b^2|_p^{1/2} = \max\{|a|_p, |b|_p\} \in p^{\mathbb{Z}}.$$

Suppose instead that  $|a|_p = |b|_p = p^\ell$ . Set  $a_0 = p^\ell a$  and  $b_0 = p^\ell b$ . Note that since  $|a_0|_p = |b_0|_p = 1$ , we have  $|a_0|_p, |b_0|_p \in p^{\mathbb{Z}}$ . Thus,

$$|a_0^2 + 3b_0^2|_p \leq \max\{1, |3|_p\} \leq 1.$$

Suppose, for the sake of contradiction, that  $|a_0^2 + 3b_0^2|_p < 1$ . Then we have that  $a_0^2 + 3b_0^2 \equiv 0 \pmod{p}$ , which is a contradiction since  $-3$  is not a quadratic residue modulo  $p$ . Thus

$$|x|_p = |a^2 + 3b^2|_p^{1/2} = |p^{-2\ell}(a_0^2 + 3b_0^2)|_p^{1/2} = p^\ell |a_0^2 + 3b_0^2|_p^{1/2} = p^\ell \in p^{\mathbb{Z}}. \quad \square$$

**Lemma 10.** *Let  $p$  be a prime with  $p \equiv 2 \pmod{3}$ ,  $K = \mathbb{Q}_p(\sqrt{-3})$ , and  $C \in K$ . Let  $k \in \mathbb{N}$ ,  $p \nmid k$ . Then  $f(x) = x^k - C$  has a root in  $K$  if and only if*

- (a)  $|C|_p = p^{k\ell}$  for some  $\ell \in \mathbb{Z}$ , and
- (b)  $p^{k\ell}C \pmod{p}$  is a  $k$ -th power in  $\mathbb{Z}_p[\sqrt{-3}]/(p)$ .

*Proof.* First we assume the existence of  $r \in K$  so that  $f(r) = 0$ , and verify that (a) and (b) hold. By Lemma 9,  $|r|_p = p^\ell$  for some  $\ell \in \mathbb{Z}$ . Since

$$|C|_p = |r^k|_p = p^{k\ell},$$

(a) is true. Further,

$$p^{k\ell}C = p^{k\ell}r^k = (p^\ell r)^k$$

and thus  $p^{k\ell}C$  is the  $k$ -th power of  $p^\ell r \pmod{p}$  in  $\mathbb{Z}[\sqrt{-3}]$ , and therefore also holds after reduction modulo  $(p)$ .

Conversely, we suppose  $C \in \mathbb{Q}_p(\sqrt{-3})$  satisfies conditions (a) and (b), and show that  $C$  is a  $k$ -th power in  $K$ . Replacing  $C$  with  $p^{k\ell}C$ , without loss of generality we may assume  $|C|_p = 1$ . By condition (b), there exists  $a + b\sqrt{-3} \in \mathbb{Z}_p[\sqrt{-3}]/(p)$ , where  $a, b \in \{0, 1, 2, \dots, p-1\}$  and  $C \equiv (a + b\sqrt{-3})^k \pmod{p}$ . Then

$$\begin{aligned} |f(a + b\sqrt{-3})|_p &= |(a + b\sqrt{-3})^k - C|_p \leq \frac{1}{p}, \\ |f'(a + b\sqrt{-3})|_p &= |k(a + b\sqrt{-3})^{k-1}|_p = 1. \end{aligned}$$

Thus, by Hensel's lemma  $f$  has a root in  $K$ . □

**Lemma 11.** *Let  $p$  be a prime with  $p \equiv 2 \pmod{3}$ , and  $K = \mathbb{Q}_p(\sqrt{-3})$ . Let  $x \in \mathbb{Q}_p$  be nonzero and the square of an element in  $K$ . Then exactly one of the following two cases is true:*

- (a)  $x = a^2$  for some  $a \in \mathbb{Q}_p$ .
- (b)  $x = -3b^2$  for some  $b \in \mathbb{Q}_p$ .

*Proof.* Suppose  $x = (a + b\sqrt{-3})^2$  for  $a, b \in \mathbb{Q}_p$ . Then

$$x = a^2 - 3b^2 + 2ab\sqrt{-3}.$$

Since  $\sqrt{-3} \notin \mathbb{Q}_p$ , we have  $ab = 0$ . If  $a = 0$ , then  $x = -3b^2$  and (b) holds. If  $b = 0$ , then  $x = a^2$  and (a) holds. □

The previous lemma gives us the machinery to detect and solve for a square root in  $K$ , since  $x$  is a square in  $K$  and not in  $\mathbb{Q}_p$  if and only if  $x/(-3) = b^2$  for some  $b \in \mathbb{Q}_p$ .

**Theorem 12.** *Let  $p$  be an odd prime, with  $p \equiv 2 \pmod{3}$ . Then the following algorithm yields  $\tau_{3,p}$ .*

- (1) *Create a list, in ascending order of Mahler measure, of all irreducible, noncyclotomic cubic polynomials in  $\mathbb{Z}[x]$  with Mahler measure less than 8.5. Let  $f(x)$  be the first polynomial on the list.*
- (2) *Convert  $f(x)$  into depressed form  $g(x) = x^3 + Ax + B$  and let  $\Delta = B^2 + 4A^3/27$ .*

- (3) If  $\Delta$  is a square in  $\mathbb{Q}_p$  or is not a square in  $\mathbb{Q}_p(\sqrt{-3})$ , return to step (2) with the next polynomial on the list.
- (4) If  $A = 0$ , let  $C = -B$ , and otherwise let  $C$  be a square root of  $\Delta$  in  $\mathbb{Q}_p(\sqrt{-3})$ . If  $(-B + C)/2$  is not a cube in  $\mathbb{Q}_p(\sqrt{-3})$ , return to step (2) with the next polynomial on the list.
- (5) If  $(-B + C)/2$  is a cube in  $\mathbb{Q}_p$ , return to step (2) with the next polynomial on the list. Otherwise, terminate, giving  $\tau_{3,p} = \frac{1}{3} \log M(f)$ .

*Proof.* Since  $\tau_{3,p} \leq \tau_{3,p}^{\text{ab}}$ , by [Theorem 3](#) we know that  $\tau_{3,p} \leq 0.70376$ . By [\[BG06, Proposition 1.6.7\]](#), a list of all polynomials with length less than 68 will contain all irreducible, noncyclotomic, cubic polynomials with Mahler measure bounded above by 8.5. Any degree 3 algebraic number of height less than or equal to 0.70376 will be a root of a polynomial in the list. Thus, this algorithm will always terminate successfully.

Let  $f$  be the polynomial being considered. By [Theorem 8](#), steps (3), (4), and (5) will detect exactly when  $f$  splits completely over  $\mathbb{Q}_p$ .  $\square$

**2.5. Implementation.** The function `is_cube_in_k` checks to see whether  $A + B\sqrt{-3}$  is a cube in  $K = \mathbb{Q}_p(\sqrt{-3})$  by applying [Lemma 10](#).

```
def is_cube_in_k(A,B,p):
    A = K(A);
    B = K(B);
    AA = A.list();
    BB = B.list();
    A0 = AA[0];
    B0 = BB[0];
    if A.abs()<1:
        A0 = 0
    if B.abs()<1:
        B0 = 0
    for c in [0..p-1]:
        for d in [0..p-1]:
            if (c*c*c - 9*c*d*d)%p==A0:
                if (3*c*c*d - 3*d*d*d)%p==B0:
                    return True
    return False
```

The function `is_cube_in_Qp` checks to see if  $A$  is a cube in  $\mathbb{Q}_p$  by applying [Lemma 6](#).

```
def is_cube_in_Qp(A,p):
    val = A.ordp();
    if 3.divides(val)==True:
        L = A.expansion();
        a = L[0];
        if IsCubeInFp(a,p)==True:
            return True;
    return False
```

The function `tau_dp_1mod3` determines  $\tau_{3,p}$  for the prime  $p$  where  $p \equiv 1 \pmod{3}$ , by implementing the algorithm described in [Theorem 7](#). Recall the array `Polynomials` contains the contents of the file `irred_polynomials_L68`, which has  $L$  entries. These were calculated in [Section 2.1](#).

```

def tau_dp_1mod3(p):
    i = 0;
    while i < L-1:
        A = Polynomials[i][5];
        B = Polynomials[i][6];
        D = Polynomials[i][7];
        A = K(A);
        B = K(B);
        D = K(D);
        if QQ(D).is_padic_square(p)==True:
            if A==0:
                C = -B;
            if A!=0:
                C = D.square_root();
            Check = (C - B) / 2;
            if is_cube_in_Qp(Check,p)==True:
                return Polynomials[i]
        i = i + 1;
    return False

```

The function `tau_dp_2mod3` determines  $\tau_{3,p}$  for the prime  $p$  where  $p \equiv 2 \pmod{3}$ , by implementing the algorithm described in [Theorem 12](#).

```

def tau_dp_2mod3(p):
    i = 0;
    while i < L-1:
        D = Polynomials[i][7];
        if D.is_padic_square(p)==False:
            b = D / (-3);
            if b.is_padic_square(p)==True:
                a = - Polynomials[i][6] / 2;
                b = K(b);
                b = sqrt(b) / 2;
                if is_cube_in_K(a,b,p)==True:
                    return Polynomials[i]
        i=i+1;
    return False

```

The following code determines  $\tau_{3,p}$  for all primes  $p$  greater than 5, up to and including the  $N$ -th prime.

```

Polynomials=load('irred_polynomials_L68')
L=len(Polynomials)
P=Primes(); # P is now a list of all primes
N=25
rows = [['P', '$\tau_{3,p}$', 'Polynomial']]
for i in [2..N]:
    p = P.unrank(i);
    K = Qp(p, prec = 6, type = 'capped-rel', print_mode = 'series');
    if p%3==1:
        tdp = tau_dp_1mod3(p)
        Poly = tdp[1]*x^3 + tdp[2]*x^2 + tdp[3]*x + tdp[4];
        h = tdp[8].n(digits=5);
        rows.append([p,h,Poly])
    if p%3==2:
        tdp = tau_dp_2mod3(p)
        Poly = tdp[1]*x^3 + tdp[2]*x^2 + tdp[3]*x + tdp[4];
        h = tdp[8].n(digits=5);
        rows.append([p,h,Poly])

```

### 3. Results

Table 2 contains some values for  $\tau_{3,p}$ .

$p$	$\tau_{3,p}$	$f_\alpha$	$p$	$\tau_{3,p}$	$f_\alpha$	$p$	$\tau_{3,p}$	$f_\alpha$
5	0.36620	$x^3 - 2x^2 - x - 3$	127	0.23105	$x^3 - x^2 - 2$	277	0.23105	$x^3 - x^2 - 2$
7	0.30387	$2x^3 - 2x^2 + x - 2$	131	0.12741	$x^3 - x^2 - 1$	281	0.26986	$x^3 - 2x^2 - x + 1$
11	0.36620	$x^3 - x^2 - 2x - 3$	137	0.30697	$x^3 - x^2 - 3x - 2$	283	0.12741	$x^3 - x^2 - 1$
13	0.26986	$x^3 - 2x^2 - x + 1$	139	0.23105	$x^3 - x^2 - x + 2$	293	0.12741	$x^3 - x^2 - 1$
17	0.23105	$x^3 - x^2 - x + 2$	149	0.12741	$x^3 - x^2 - 1$	307	0.093733	$x^3 - x^2 + 1$
19	0.23105	$x^3 - x^2 - 2$	151	0.28206	$2x^3 - x^2 + 2$	311	0.20313	$x^3 - x^2 - x - 1$
23	0.23105	$x^3 - x^2 + x - 2$	157	0.23105	$x^3 - 2x - 2$	313	0.23105	$x^3 - 2x - 2$
29	0.26986	$x^3 - 2x^2 - x + 1$	163	0.20313	$x^3 - x^2 - x - 1$	317	0.093733	$x^3 - x^2 + 1$
31	0.23105	$x^3 - x - 2$	167	0.093733	$x^3 - x^2 + 1$	331	0.28206	$2x^3 - x^2 + 2$
37	0.27319	$x^3 - x^2 - 2x - 2$	173	0.093733	$x^3 - x^2 + 1$	337	0.26986	$x^3 - 2x^2 - x + 1$
41	0.23105	$x^3 - x^2 + x - 2$	179	0.27319	$x^3 - x^2 - 2x - 2$	347	0.093733	$x^3 - x^2 + 1$
43	0.23105	$x^3 - 2$	181	0.26986	$x^3 - 2x^2 - x + 1$	349	0.12741	$x^3 - x^2 - 1$
47	0.12741	$x^3 - x^2 - 1$	191	0.23105	$x^3 - x^2 - 2$	353	0.23105	$x^3 - x^2 - 2$
53	0.20313	$x^3 - x^2 - x - 1$	193	0.23105	$x^3 - x^2 + x - 2$	359	0.23105	$x^3 - x - 2$
59	0.093733	$x^3 - x^2 + 1$	197	0.23105	$x^3 - x^2 - x + 2$	367	0.23105	$x^3 - x^2 - 2$
61	0.28206	$2x^3 - x^2 + 2$	199	0.20313	$x^3 - x^2 - x - 1$	373	0.23105	$x^3 - x^2 - x + 2$
67	0.12741	$x^3 - x^2 - 1$	211	0.093733	$x^3 - x^2 + 1$	379	0.12741	$x^3 - x^2 - 1$
71	0.23105	$x^3 - x^2 - x + 2$	223	0.093733	$x^3 - x^2 + 1$	383	0.23105	$x^3 - x^2 - x + 2$
73	0.29111	$2x^3 - x^2 - 2$	227	0.12741	$x^3 - x^2 - 1$	389	0.23105	$x^3 - x^2 - x + 2$
79	0.28612	$x^3 - 2x^2 - 2$	229	0.23105	$x^3 - x^2 + x - 2$	397	0.20313	$x^3 - x^2 - x - 1$
83	0.23105	$x^3 - 2x - 2$	233	0.27319	$x^3 - x^2 - 2x - 2$	401	0.20313	$x^3 - x^2 - x - 1$
89	0.27535	$2x^3 - 2x^2 - x + 2$	239	0.26986	$x^3 - 2x^2 - x + 1$	409	0.30387	$2x^3 - 2x^2 + x - 2$
97	0.26986	$x^3 - 2x^2 - x + 1$	241	0.30697	$x^3 - x^2 - 3x - 2$	419	0.20313	$x^3 - x^2 - x - 1$
101	0.093733	$x^3 - x^2 + 1$	251	0.23105	$x^3 - x - 2$	421	0.20313	$x^3 - x^2 - x - 1$
103	0.20313	$x^3 - x^2 - x - 1$	257	0.20313	$x^3 - x^2 - x - 1$	431	0.12741	$x^3 - x^2 - 1$
107	0.23105	$x^3 - x - 2$	263	0.27319	$x^3 - x^2 - 2x - 2$	433	0.23105	$x^3 - 2$
109	0.23105	$x^3 - 2$	269	0.20313	$x^3 - x^2 - x - 1$	439	0.23105	$x^3 - x^2 - x + 2$
113	0.23105	$x^3 - x - 2$	271	0.093733	$x^3 - x^2 + 1$	443	0.23105	$x^3 - x^2 - 2$

Table 2. Some values for  $\tau_{3,p}$ .

### 4. Conclusion and future work

In this paper we relied on the fact that we can determine that a finite list of polynomials is guaranteed to contain one that splits over  $\mathbb{Q}_p$  for any prime  $p$ . We restricted our search to cubic numbers that exist in abelian extensions of  $\mathbb{Q}$  to prove this. Moving forward, we will determine that we can guarantee that for any degree  $d$ , there is some  $N_d \in \mathbb{Z}$  such that  $\tau_{d,p}^{\text{ab}}$  depends only on  $p \pmod{N_d}$ . For example,  $N_2 = 5$  and  $N_3 = 228979643050431$ .

When we look at the small nonzero values attained by the height function on cubic numbers, we see that the smallest value is 0.093733. It would be interesting to classify all primes such that  $\tau_{3,p} = 0.093733$ .

## References

- [Bak06] Matt Baker. [Algebraic number theory course notes](#) (fall 2006) Math 8803, Georgia Tech. Available at [people.math.gatech.edu/~mbaker/pdf/ANTBook.pdf](http://people.math.gatech.edu/~mbaker/pdf/ANTBook.pdf), 2006. Accessed: 2017-12-31.
- [BG06] Enrico Bombieri and Walter Gubler. *Heights in Diophantine Geometry*. Number 4 in New Mathematical Monographs. Cambridge University Press, 2006.
- [BZ01] Enrico Bombieri and Umberto Zannier. A note on heights in certain infinite extensions of  $\mathbb{Q}$ . *Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti Lincei. Matematica e Applicazioni*, 12(1):5–14, 2001.
- [Cas86] John William Scott Cassels. *Local fields*, volume 3. Cambridge University Press, 1986.
- [Con18] Keith Conrad. [Galois groups of cubics and quartics \(not in characteristic 2\)](#). Available at <http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/cubicquartic.pdf>, 2018. Accessed: 2018-06-14.
- [CS68] Girolamo Cardano and C Spon. *Ars magna* (1545). *Opera Omnia*, 4:221–302, 1968.
- [Has30] Helmut Hasse. Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage. *Math. Z.*, 31(1):565–582, 1930.
- [HS93] Gerald Höhn and Nils Peter Skoruppa. Un résultat de Schinzel. *J. Théor. Nombres Bordeaux*, 5(1):185, 1993.
- [Pet] Clayton Petsche. The height of algebraic units in local fields.
- [Pot18] Lukas Pottmeyer. Small totally  $p$ -adic algebraic numbers. 2018 [arXiv:1802.05923](#)
- [PS19] Clayton Petsche and Emerald Stacy. A dynamical construction of small totally  $p$ -adic algebraic numbers. *J. of Number Theory*, 202:27–36, 2019.
- [Sch75] Andrzej Schinzel. Addendum to the paper “On the product of the conjugates outside the unit circle of an algebraic number”. *Acta Arithmetica*, 26:329–331, 1975.
- [Smy80] Chris Smyth. On the measure of totally real algebraic integers. *J. of the Australian Math. Soc.*, 30(2):137–149, 1980.

Received 23 Feb 2020. Revised 1 Aug 2020.

EMERALD STACY: [estacy2@washcoll.edu](mailto:estacy2@washcoll.edu)

Mathematics and Computer Science, Washington College, Chestertown, MD, United States





# Counting points on superelliptic curves in average polynomial time

Andrew V. Sutherland

*In memory of Peter L. Montgomery.*

We describe the practical implementation of an average polynomial-time algorithm for counting points on superelliptic curves defined over  $\mathbb{Q}$  that is substantially faster than previous approaches. Our algorithm takes as input a superelliptic curve  $y^m = f(x)$  with  $m \geq 2$  and  $f \in \mathbb{Z}[x]$  any squarefree polynomial of degree  $d \geq 3$ , along with a positive integer  $N$ . It can compute  $\#X(\mathbb{F}_p)$  for all  $p \leq N$  not dividing  $\text{mlc}(f)\text{disc}(f)$  in time  $O(md^3 N \log^3 N \log \log N)$ . It achieves this by computing the trace of the Cartier–Manin matrix of reductions of  $X$ . We can also compute the Cartier–Manin matrix itself, which determines the  $p$ -rank of the Jacobian of  $X$  and the numerator of its zeta function modulo  $p$ .

## 1. Introduction

Let  $X/k$  be a smooth projective curve of genus  $g > 0$  whose function field is defined by an equation of the form

$$y^m = f(x)$$

with  $m > 1$  prime to the characteristic  $p$  of  $k$  and  $f \in k[x]$  a squarefree polynomial of degree  $d \geq 3$ . We shall call such a curve  $X$  a superelliptic curve. We note that not all authors require  $f$  to be squarefree or  $p \nmid m$ , while others require  $d$  and  $m$  to be coprime; our definition follows the convention in [21; 27] and is equivalent to the class of cyclic covers of  $\mathbb{P}^1$  considered in [2; 13]. One can compute the genus of  $X$  as

$$g = \frac{(d-2)(m-1) + m - \gcd(m, d)}{2} \tag{1}$$

via the Riemann–Hurwitz formula. Well-known examples of superelliptic curves include elliptic curves, hyperelliptic curves, Picard curves, and Fermat curves.

---

The author was supported by Simons Foundation grant 550033.

MSC2010: primary 11G20; secondary 11M38, 11Y16, 14G10.

Keywords: superelliptic curve, Cartier–Manin matrix, Hasse–Witt matrix, average polynomial-time.

We are primarily interested in  $k = \mathbb{Q}$  where  $X$  has an associated  $L$ -function  $L(X, s) = \sum a_n n^{-s}$  that we would like to “compute”. For us this means computing the integers  $a_n$  for all  $n$  up to a bound  $N$  that is large enough for us to approximate special values of  $L(X, s)$  to high precision, and to compute upper bounds on its analytic rank that we can reasonably expect to be sharp. This requires  $N$  to be on the order of the square root of the conductor of the Jacobian of  $X$ , and in practice we typically take  $N$  to be about 30 times this value.

The fact that  $L(X, s)$  is defined by an Euler product implies that it suffices to compute  $a_n$  for prime powers  $n \leq N$ . Nearly all of the prime powers  $n \leq N$  are in fact primes  $p$ , so this task is overwhelmingly dominated by the time to compute  $a_p$  for primes  $p \leq N$ . Indeed, even if we spend  $O(p^e \log^2 p)$  time computing each  $a_{p^e} \leq N$  with  $e > 1$  (which for primes of good reduction can be achieved by naïve point-counting), we will have spent only  $O(N \log N)$  time, which is roughly the time it takes just to write down all the  $a_n$  for  $n \leq N$ . For primes of good reduction for  $X$ , including all  $p \nmid m \operatorname{lc}(f) \operatorname{disc}(f)$ ,<sup>1</sup> we may compute  $a_p$  as

$$a_p = p + 1 - \#X(\mathbb{F}_p);$$

in other words, by counting points on the reduction of  $X$  modulo  $p$ . See [6] for a discussion of how primes of bad reduction may be treated. Alternatively, if one is willing to assume that the Hasse–Weil conjecture for  $L(X, s)$  holds, one can use the knowledge of  $a_n$  at powers of good primes to determine the  $a_n$  at powers of bad primes (and in particular, the primes  $p|m$  not treated by [6]) by using the functional equation to rule out all but one possibility; see [3, §5] for a discussion of this approach when  $g = 2$ .

Another motivation for computing  $a_p$  for good primes  $p \leq N$  is to compute the sequence of normalized Frobenius traces  $a_p/\sqrt{p}$  that appear in generalizations of the Sato–Tate conjecture. The moments of this distribution encode certain arithmetic invariants of  $X$ , including, for example, the rank of the endomorphism ring of its Jacobian [9, Proposition 1], as well as information about its Sato–Tate group [11; 22]. Indeed, the initial motivation for this work (and its first application) was to compute Sato–Tate distributions for the genus 3 superelliptic curves with  $(m, d) \in \{(3, 4), (4, 3), (4, 4)\}$  that arise as smooth plane quartics in the database described in [25] and played a role in the recent classification of Sato–Tate groups of abelian threefolds [12]. The sequence of normalized Frobenius traces can also be used to numerically investigate the error term in the Sato–Tate conjecture, and in particular, predictions regarding its leading constant [7]. The ability to efficiently compute many integer values of  $a_p$  also supports investigations of generalizations of the Lang–Trotter conjecture, as well as a recent question of Serre regarding the density of “record” primes, those with  $-a_p > 2g\sqrt{p} - 1$  (personal communication, 2019).

The algorithm we present here does more than just compute  $a_p$ . Following the approach of [15; 16; 17], which treated the case of hyperelliptic curves, for each good prime  $p$  we compute a  $g \times g$  matrix  $A_p$  giving the action of the Cartier–Manin operator on a basis for the space of regular differentials of the reduction of  $X$  modulo  $p$ ; see Section 2 for details. The matrix  $A_p$  is the transpose of the Hasse–Witt

<sup>1</sup>For  $m|d$  some good primes may divide  $\operatorname{lc}(f)$ , but to simplify the presentation we exclude them here.

matrix. Like the Hasse–Witt matrix, it satisfies

$$\det(I - T A_p) \equiv L_p(T) \pmod{p},$$

where  $L_p(T)$  is the integer polynomial that appears in both the Euler product  $L(X, s) = \prod_p L_p(p^{-s})^{-1}$  and the numerator of the zeta function of the reduction of  $X$  modulo  $p$ :

$$Z_p(T) := \exp\left(\sum_{n \geq 1} \#X(\mathbb{F}_{p^n}) \frac{T^n}{n}\right) = \frac{L_p(T)}{(1-T)(1-pT)}.$$

In particular, we have  $a_p \equiv \text{tr } A_p \pmod{p}$ , and for  $p > 16g^2$  this uniquely determines  $a_p \in \mathbb{Z}$ , since  $|a_p| \leq 2g\sqrt{p}$ , by the Weil bounds. The matrix  $A_p$  is also of independent interest, since it can be used to compute the  $p$ -rank of the reduction of  $X$  modulo  $p$ , something that cannot be deduced solely from  $L_p(T)$ .

Our main result is the following theorem, in which  $\|f\| = \log \max_i |f_i|$  denotes the logarithmic height of a nonzero integer polynomial  $f(x) = \sum_i f_i x^i$ .

**Theorem 1.** *Given a superelliptic curve  $X : y^m = f(x)$  with  $f \in \mathbb{Z}[x]$  of degree  $d$  and  $N \in \mathbb{Z}_{>0}$ , the algorithm `COMPUTECARTIERMANINMATRICES` outputs the Cartier–Manin matrices  $A_p$  of the reductions of  $X$  modulo all primes  $p \leq N$  not dividing  $m \text{lc}(f) \text{disc}(f)$ . If we assume  $m, d, \|f\|$  are bounded by  $O(\log N)$  the algorithm runs in  $O(m^2 d^3 N \log^3 N)$  time using  $O(md^2 N)$  space; it can alternatively compute Frobenius traces  $a_p \in \mathbb{Z}$  for  $p \leq N$  in time  $O(md^3 N \log^3 N)$ .*

**Remark 2.** The assumption  $m, d, \|f\| = O(\log N)$  ensures that the complexity of multiplying the integer matrices used in the algorithm is dominated by the cost of computing FFT transforms of the matrix entries, which eliminates any dependence on the exponent  $\omega$  of matrix multiplication; one can replace  $d^3$  with  $d^{\omega+1}$  and then remove this assumption. We note that our complexity bound relies on the recently improved  $M(n) = n \log n$  bound on integer multiplication [18]. While the algorithm that achieves this bound is not practical, many FFT-based implementations effectively achieve this growth rate within the feasible range of computation, which for our purposes, is certainly limited to integers that fit in random access memory; see [26, Algorithm 8.25], for example.

We also obtain an algorithm that can be used to compute  $A_p$  for a single superelliptic curve  $X/\mathbb{F}_p$ . The asymptotic complexity is comparable to that achieved in [2] which describes the algorithm that is now implemented in version 9 of Sage. We include this result because it contains several components that are used by the average polynomial-time algorithm we present. We should emphasize that the algorithm in [2] can compute  $L_p(T) \pmod{p^n}$  for any  $n \geq 1$ , and taking  $n$  sufficiently large yields  $L_p \in \mathbb{Z}[T]$ , whereas we focus solely on the case  $n = 1$  (we gain a small but not particularly significant performance advantage in this case).

**Theorem 3.** *Given a superelliptic curve  $X : y^m = f(x)$  with  $f \in \mathbb{F}_p[x]$  of degree  $d$ , the algorithm `COMPUTECARTIERMANINMATRIX` is able to compute the Cartier–Manin matrix of  $X$  using  $O(p^{1/2} md^2 \log p)$*

space in  $O(p^{1/2}m(d^{\omega+1} + d^3 \log p) \log p(\log \log p))$  time, and also using  $O((md + d^2) \log p)$  space in  $O((p + d)md^2 \log p \log \log p)$  time.

In the article [2] noted above the authors consider a particular curve

$$X : y^7 = x^3 + 4x^2 + 3x - 1$$

for which they estimate that it would take approximately six months (on a single core) for their algorithm to compute the  $L$ -polynomials  $L_p(T)$  for all primes  $p \leq 2^{24}$  of good reduction. This is an improvement over an estimated three years for an earlier algorithm due to Minzloff [20] that is implemented in Magma. Computing  $L_p(T) \bmod p$  is an easier problem that would likely take about a week or so using the algorithm in [2], based on timings taken using a representative sample of  $p \leq 2^{24}$ . The algorithm we present here can accomplish this task in half an hour, and less than ten minutes if we only compute Frobenius traces.

See Tables 1 and 2 in Section 7 for detailed performance comparisons for various shapes of superelliptic curves.

## 2. The Cartier operator

For background on differentials of algebraic function fields we refer the reader to [8, §2] and [23, §4]. Let  $K$  be a function field of one variable over a perfect field  $k$  of characteristic  $p > 0$  that we assume is the full field of constants of  $K$ . Let  $\Omega_K$  denote its module of differentials, which we identify with its module of Weil differentials via [23, Definition 4.17] and [23, Remark 4.3.7]. Let  $x \in K$  be a separating element, so that  $K/k(x)$  is a finite separable extension, and let  $K^p$  denote the subfield of  $p$ -th powers. Then  $(1, x, \dots, x^{p-1})$  is a basis for  $K$  as a  $K^p$ -vector space, and every  $z \in K$  has a unique representation of the form

$$z = z_0^p + z_1^p x + \dots + z_{p-1}^p x^{p-1},$$

with  $z_0, \dots, z_{p-1} \in K^p$ , and every rational differential form  $\omega = z dx$  can be uniquely written in the form

$$\omega = (z_0^p + z_1^p x + \dots + z_{p-1}^p x^{p-1}) dx.$$

The (modified) *Cartier operator*  $\mathcal{C} : \Omega_K \rightarrow \Omega_K$  is then defined by

$$\mathcal{C}(\omega) = z_{p-1} dx.$$

The Cartier operator is uniquely characterized by the following properties:

- (1)  $\mathcal{C}(\omega_1 + \omega_2) = \mathcal{C}(\omega_1) + \mathcal{C}(\omega_2)$  for all  $\omega_1, \omega_2 \in \Omega_K$ .
- (2)  $\mathcal{C}(z^p \omega) = z \mathcal{C}(\omega)$  for all  $z \in K$  and  $\omega \in \Omega_K$ .
- (3)  $\mathcal{C}(dz) = 0$  for all  $z \in K$ .
- (4)  $\mathcal{C}(dz/z) = dz/z$  for all  $z \in K^\times$ .

In particular, it does not depend on our choice of a separating element  $x$ . Moreover, it maps regular differentials to regular differentials and thus restricts to an operator on the space

$$\Omega_K(0) = \{\omega \in \Omega_K : \omega = 0 \text{ or } \operatorname{div}(\omega) \geq 0\},$$

which we recall is a  $k$ -vector space whose dimension  $g$  is equal to (and often used as the definition of) the genus of  $K$ ; see [23, Example 4.12-17] for these and other standard facts about the Cartier operator.

**Definition 4.** Let  $\omega = (\omega_1, \dots, \omega_g)$  be a basis for  $\Omega_K(0)$  and define  $a_{ij} \in k$  via

$$\mathcal{C}(\omega_j) = \sum_{i=1}^g a_{ij} \omega_i.$$

The Cartier–Manin matrix of  $K$  (with respect to  $\omega$ ) is the matrix  $A = [a_{ij}] \in k^{g \times g}$ .

If  $X/k$  is a smooth projective curve with function field  $k(X) = K$ , we also call  $A$  the Cartier–Manin matrix of  $X$ . This matrix is closely related to the Hasse–Witt matrix  $B$  of  $X$ , which is defined as the matrix of the  $p$ -power Frobenius operator acting on  $H^1(X, \mathcal{O}_X)$  with respect to some basis. As carefully explained in [1], the matrices  $A$  and  $B$  can be related via Serre duality, and for a suitable choice of basis one finds that  $B = [a_{ij}^p]^\top$ . In the case of interest to us  $k = \mathbb{F}_p$  is a prime field and the Cartier–Manin and Hasse–Witt matrices are simply transposes of each other, and hence have the same rank and characteristic polynomials, but we shall follow the warning/request of [1] and call  $A$  the Cartier–Manin matrix, although one can find examples in the literature where  $A$  is called the Hasse–Witt matrix (see [1] for a list).

We shall apply the method of Stöhr–Voloch [24] to compute the Cartier–Manin matrix of a smooth projective curve  $X$  with function field  $K = k(X)$ . Let us write  $K$  as  $k(x)[y]/(F)$ , where  $x \in X$  is a separating element and  $y$  is an integral generator for the finite separable extension  $K/k(x)$  with minimal polynomial  $F \in k[x][y]$ . We now define the differential operator

$$\nabla = \frac{\partial^{2p-2}}{\partial x^{p-1} \partial y^{p-1}}$$

which maps  $x^{(i+1)p-1} y^{(j+1)p-1}$  to  $x^{ip} y^{jp}$  and annihilates monomials not of this form; it thus defines a semilinear map  $\nabla : K \rightarrow K^p$ . Writing  $F_y$  for  $\frac{\partial}{\partial y} F \in k[x, y]$ , for any  $h \in K$  we have the identity

$$\mathcal{C}\left(h \frac{dx}{F_y}\right) = (\nabla(F^{p-1}h))^{1/p} \frac{dx}{F_y}, \quad (2)$$

given by [24, Theorem 1.1]. If we choose a basis for  $\Omega_X(0)$  using regular differentials of the form  $h dx/F_y$ , we can compute the action of the Cartier operator on this basis via (2). To construct such a basis we shall use differentials of the form

$$\omega_{k\ell} = x^{k-1} y^{\ell-1} \frac{dx}{F_y}, \quad (k, \ell \geq 1, \quad k + \ell \leq \deg(F) - 1). \quad (3)$$

Writing  $F(x, y)^{p-1} = \sum_{i,j} F_{ij}^{p-1} x^i y^j$  (defining  $F_{i,j}^{p-1} \in k$  for all  $i, j \in \mathbb{Z}$ ), for  $k, \ell \geq 1$  one finds that

$$\nabla \left( \sum_{i,j \geq 0} F_{ij}^{p-1} x^{i+k-1} y^{j+\ell-1} \right) = \sum_{i,j \geq 1} F_{ip-k, jp-\ell}^{p-1} x^{(i-1)p} y^{(j-1)p}. \quad (4)$$

Now  $F_{ip-k, jp-\ell}^{p-1}$  is nonzero only if we have  $(i+j)p - (k+\ell) \leq (p-1) \deg(F)$ , and  $k+\ell \leq \deg(F) - 1$ , so we can restrict the sum on the RHS to  $i+j \leq \deg(F) - 1$ . From (2) and (4) we obtain

$$\mathcal{C}(\omega_{k\ell}) = \sum_{i,j \geq 1} (F_{ip-k, jp-\ell}^{p-1})^{1/p} \omega_{ij}. \quad (5)$$

When  $X$  is a smooth plane curve the complete set of  $\omega_{ij}$  defined in (3) is a basis for  $\Omega_K(0)$  and we can read off the entries of the Cartier–Manin matrix for  $X$  directly from (5). In general not all of the  $\omega_{ij}$  necessarily lie in  $\Omega_K(0)$ , some of them might not be regular, but the subset that do (those corresponding to adjoint polynomials) form a basis for  $\Omega_K(0)$ ; see [14; 24]. In the case of superelliptic curves this subset is given explicitly by Lemma 6.

**Definition 5.** For  $a, b \in \mathbb{Z}$  with  $b > 0$ , let  $a \bmod b = a - b[a/b]$  denote the unique integer in the interval  $[0, b-1] \cap (a + b\mathbb{Z})$ .

**Lemma 6.** Let  $k$  be a perfect field of positive characteristic  $p$ , let  $X/k$  be a superelliptic curve defined by  $F(x, y) = y^m - f(x) = 0$ , let  $d = \deg f$ , and for  $i, j \geq 1$  let  $\omega_{ij} = x^{i-1} y^{j-1} dx / F_y \in \Omega_K$ , where  $K = k(x)[y]/(F)$  is the function field of  $X$ . Then the set

$$\omega = \{\omega_{ij} : mi + dj < md\}$$

is a  $k$ -basis for  $\Omega_K(0)$ , with  $1 \leq i < d - \lfloor d/m \rfloor$  and  $1 \leq j < m - \lfloor m/d \rfloor$ . Moreover, if we define

$$d_j = d - \lfloor dj/m \rfloor - 1 \quad \text{and} \quad m_i = m - \lfloor mi/d \rfloor - 1, \quad (6)$$

then the  $\omega_{ij} \in \omega$  are precisely those for which  $1 \leq i \leq d_j$  and  $1 \leq j \leq m_i$ .

*Proof.* Note that  $\omega_{ij} = \frac{1}{m} x^{i-1} y^{j-m} dx$ , with  $p \nmid m$ . It follows from [21, Proposition 3.8] (which treats  $X/\mathbb{C}$  but whose proof also works for  $X/k$  and can be independently derived using the methods of [14]) that the set

$$\{x^{i-1} y^{-k} dx : 1 \leq i < d, 1 \leq k \leq m-1, dk - mi \geq \gcd(m, d)\}$$

is a basis for  $\Omega_K(0)$ . Taking  $k = m - j$  and rearranging yields the basis

$$\omega = \{\omega_{ij} : mi + dj \leq md - \gcd(m, d)\} = \{\omega_{ij} : mi + dj < md\},$$

and the bounds on  $i$  and  $j$  immediately follow. □

For  $X/k$  defined by  $F(x, y) = f(x) - y^m = 0$ , if we let  $f_a^n$  denote the coefficient of  $x^a$  in  $f(x)^n$  then

$$F_{ab}^{p-1} = \begin{cases} f_a^{p-1-b/m} & \text{if } m \mid b \text{ and } b \leq m(p-1), \\ 0 & \text{otherwise,} \end{cases}$$

(here we have used  $\binom{p-1}{e}(-1)^e \equiv 1 \pmod{p}$ ), thus for all  $1 \leq i, k < d$  and  $1 \leq j, \ell < m$  we have

$$F_{ip-k, jp-\ell}^{p-1} = \begin{cases} f_{ip-k}^{p-1-(jp-\ell)/m} & \text{if } m \mid (jp-\ell), \\ 0 & \text{otherwise.} \end{cases}$$

Now  $1 \leq j, \ell < m$  and  $p \nmid m$ , so whenever

$$F_{ip-k, jp-\ell}^{p-1} \neq 0,$$

we must have  $\ell = jp \bmod m > 0$  and

$$n_j = p-1 - (jp-\ell)/m = \frac{(m-j)p - (m-\ell)}{m} = p-1 - \lfloor jp/m \rfloor. \quad (7)$$

Let us order the basis for  $\Omega_K(0)$  given by Lemma 6 as  $\omega = (\omega_{11}, \omega_{21}, \dots, \omega_{12}, \dots)$  with the  $\omega_{ij}$  ordered first by  $j$  and then by  $i$ . The Cartier–Manin matrix of  $X$  can then be described in block form with blocks indexed by  $j$  and  $\ell$  containing entries indexed by  $i$  and  $k$ :

$$\begin{aligned} A_p &= [B^{j\ell}]_{j\ell} & 1 \leq j, \ell \leq \mu = m_1 = m - \lfloor m/d \rfloor - 1, \\ B^{j\ell} &= [(b_{ik}^{j\ell})^{1/p}]_{ik} & 1 \leq i \leq d_j \text{ and } 1 \leq k \leq d_\ell, \\ b_{ik}^{j\ell} &= \begin{cases} f_{ip-k}^{n_j} & \text{if } (jp-\ell)/m \in \mathbb{Z}_{\geq 0}, \\ 0 & \text{otherwise.} \end{cases} \end{aligned} \quad (8)$$

The diagonal blocks  $B^{j,j}$  are square but the others typically will not be square, since the bound on  $i$  depends on  $j$  while the bound on  $k$  depends on  $\ell$ . We also note that there is at most one nonzero  $B^{j\ell}$  in each row  $j$ , and in each column  $\ell$  of  $[B^{j\ell}]_{j\ell}$ , since any nonzero  $B^{j\ell}$  must have  $\ell \equiv jp \bmod m$  (there will be no nonzero  $B^{j\ell}$  for  $j$  if no  $\ell \leq \mu$  satisfies  $\ell \equiv jp \bmod m$ ; this happens, for example, when  $j = 1$  and  $d = m = 5$  with  $p \equiv 4 \bmod 5$ ).

**Example 7.** For  $m = 5$  and  $d = 3$  we have  $g = 4$ , and the  $4 \times 4$  matrix  $A_p$  consists of  $3 \times 3 = 9$  blocks: one  $2 \times 2$ , two  $2 \times 1$ , two  $1 \times 2$ , and four  $1 \times 1$ . For  $k = \mathbb{F}_p$ , the matrices  $A_p$  for  $p \equiv 1, 2, 3, 4 \bmod 5$  are

$$\begin{aligned} & \begin{pmatrix} f_{p-1}^{(4p-4)/5} & f_{p-2}^{(4p-4)/5} & 0 & 0 \\ f_{2p-1}^{(4p-4)/5} & f_{2p-2}^{(4p-4)/5} & 0 & 0 \\ 0 & 0 & f_{p-1}^{(3p-3)/5} & 0 \\ 0 & 0 & 0 & f_{p-1}^{(2p-2)/5} \end{pmatrix}, & \begin{pmatrix} 0 & 0 & f_{p-1}^{(4p-3)/5} & 0 \\ 0 & 0 & f_{2p-1}^{(4p-3)/5} & 0 \\ 0 & 0 & 0 & 0 \\ f_{p-1}^{(2p-4)/5} & f_{p-2}^{(2p-4)/5} & 0 & 0 \end{pmatrix}, \\ & \begin{pmatrix} 0 & 0 & 0 & f_{p-1}^{(4p-2)/5} \\ 0 & 0 & 0 & f_{2p-1}^{(4p-2)/5} \\ f_{p-1}^{(3p-4)/5} & f_{p-2}^{(3p-4)/5} & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, & \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & f_{p-1}^{(3p-2)/5} \\ 0 & 0 & f_{p-1}^{(2p-3)/5} & 0 \end{pmatrix}. \end{aligned}$$

For  $m = 3$  and  $d = 5$  we also have  $g = 4$  but now the  $4 \times 4$  matrix  $A_p$  consists of  $2 \times 2 = 4$  blocks:

one  $3 \times 3$ , one  $3 \times 1$ , one  $1 \times 3$ , and one  $1 \times 1$ . For  $k = \mathbb{F}_p$  the matrices  $A_p$  for  $p \equiv 1, 2 \pmod{3}$  are

$$\begin{pmatrix} f_{p-1}^{(2p-2)/3} & f_{p-2}^{(2p-2)/3} & f_{p-3}^{(2p-2)/3} & 0 \\ f_{2p-1}^{(2p-2)/3} & f_{2p-2}^{(2p-2)/3} & f_{2p-3}^{(2p-2)/3} & 0 \\ f_{3p-1}^{(2p-2)/3} & f_{3p-2}^{(2p-2)/3} & f_{3p-3}^{(2p-2)/3} & 0 \\ 0 & 0 & 0 & f_{p-1}^{(p-1)/3} \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 & f_{p-1}^{(2p-1)/3} \\ 0 & 0 & 0 & f_{2p-1}^{(2p-1)/3} \\ 0 & 0 & 0 & f_{3p-1}^{(2p-1)/3} \\ f_{p-1}^{(p-2)/3} & f_{p-2}^{(p-2)/3} & f_{p-3}^{(p-2)/3} & 0 \end{pmatrix}.$$

In both cases  $\text{tr } A_p = 0$  for  $p \not\equiv 1 \pmod{m}$ , but this is not true in general (consider  $m = 4$  and  $d = 3$ , for example).

The block form of the Cartier–Manin matrix  $A_p$  given by (8) implies the following theorem, which plays a key role in our algorithm for computing  $A_p$  and may also be of independent interest.

**Theorem 8.** *Let  $X : y^m = f(x)$  be a superelliptic curve over a perfect field of characteristic  $p > 0$  with  $d = \deg(f)$ . Let  $\omega$  be the basis of  $\Omega_{k(X)}(0)$  given by Lemma 6, and for  $1 \leq j \leq m_1 = m - \lfloor m/d \rfloor - 1$ , let  $\omega_j = \{\omega_{ij'} \in \omega : j' = j\}$ . For  $1 \leq j \leq m_1$  the Cartier operator maps the subspace spanned by  $\omega_j$  to the subspace spanned by  $\omega_\ell$ , with  $\ell \equiv jp \pmod{m}$ , and this action is given by the matrix  $B^{j\ell}$  defined in (8). In particular, when  $p \equiv 1 \pmod{m}$  the Cartier operator fixes each of the subspaces spanned by  $\omega_j$ .*

*Proof.* This is an immediate consequence of (8). □

**Remark 9.** In [5, Lemma 5.1] Bouw gives formulas for the coefficients of the Hasse–Witt matrix of a general cyclic cover  $Y : y^m = f(x)$  of  $\mathbb{P}^1$  in terms of the (possibly repeated) roots of the polynomial  $f \in k[x]$ , where  $k$  is an algebraically close field of characteristic  $p$ . When  $f$  is squarefree, Bouw’s formulas agree with (8), after taking into account the transposition needed to get the Cartier–Manin matrix and a possible change of basis (I’m grateful to Wanlin Li and John Voight for bringing this to my attention). One can compute analogs of the formulas in (8) to handle  $f$  that are not squarefree that take into account the multiplicities of its root, but we do not consider this case here. Note that the genus of  $Y$  and therefore the dimensions of  $A_p$  will be less than that given by (1) when  $f$  is not squarefree, so while the formulas may be more involved, the problem is computationally easier.

### 3. Linear recurrences

The results of the previous section imply that to compute the Cartier–Manin matrix  $A_p$  of a superelliptic curve  $X : y^m = f(x)$  over  $\mathbb{F}_p$  it suffices to compute certain coefficients of certain powers of  $f(x)$ . In this section we derive linear recurrences that allow us to do this efficiently, both when  $f \in \mathbb{F}_p[x]$  and when  $f \in \mathbb{Z}[x]$  and we wish to compute certain coefficients of certain powers of the reduction of  $f$  modulo many primes  $p$ . In this section we generalize [17, §2], which treated the case  $m = 2$ , in which case  $A_p = B$  consists of a single block  $B^{11}$  (so  $j = \ell = 1$ ), the powers  $f^n$  that appear in the matrix entries are always the same ( $n = (p-1)/2$ ), and every prime  $p \nmid m$  is congruent to 1 modulo  $m$ . Here we allow all of these parameters to vary.



Let  $f \in \mathbb{Z}[x]$  be a squarefree polynomial of degree  $d \geq 3$ , which we shall write as  $f(x) = x^c h(x)$  with  $c = 0, 1$  and  $h(0) \neq 0$  (note that  $x^2 \nmid f$ ).<sup>2</sup> Let  $h(x) = \sum_{i=0}^r h_i x^i$ , and for  $n \geq 1$  let  $h_i^n$  denote the coefficient of  $x^i$  in  $h(x)^n$ . As shown in [17, §2], the identities  $h^{n+1} = h \cdot h^n$  and  $(h^{n+1})' = (n+1)h^n$  yield the linear relation

$$\sum_{i=0}^r ((n+1)i - k) h_i h_{k-i}^n = 0, \quad (9)$$

which is valid for all  $k \in \mathbb{Z}$  and  $n \in \mathbb{Z}_{\geq 0}$ . Observing that  $n_j = ((m-j)p - (m-\ell))/m$  is the exponent on  $f$  in every entry of the nonzero block  $B^{j\ell}$  defined in (8), let us set  $n = n_j$  and rewrite (9) as

$$0 = \sum_{i=0}^r ((m-j)p + \ell)i - mk h_i h_{k-i}^{n_j} \equiv \sum_{i=0}^r (\ell i - mk) h_i h_{k-i}^{n_j} \pmod{p}, \quad (10)$$

which is valid for all  $k \in \mathbb{Z}$ . We now define

$$v_k^{n_j} := [h_{k-r+1}^{n_j}, \dots, h_k^{n_j}] \in \mathbb{Z}^r,$$

and put  $s = p - 1 - cn_j$ . The entries of  $v_s^n \pmod{p}$  suffice to compute the first row of block  $B^{j\ell}$  in  $A_p$ ; note that  $n$  (and potentially  $s$ ) depend on  $j$  and will vary from block to block. We have  $v_0^{n_j} = [0, \dots, 0, h_0^{n_j}] = h_0^{n_j} v_0^0$ , where  $v_0^0 = [0, \dots, 0, 1]$ . Noting that  $s < p$  and  $p \nmid m$  and  $p \nmid h_0$  (since  $f$  is squarefree), solving for  $h_k^n$  in (10) yields

$$v_s^{n_j} \equiv \frac{v_0^{n_j}}{(mh_0)^s s!} \prod_{i=0}^{s-1} M_i^\ell \equiv m^{cn_j} h_0^{(c+1)n_j} (-1)^{cn_j+1} (cn_j)! v_0^0 \prod_{i=0}^{s-1} M_i^\ell \pmod{p}, \quad (11)$$

where

$$M_{i-1}^\ell := \begin{bmatrix} 0 & \cdots & 0 & (\ell r - mi)h_r \\ mih_0 & \cdots & 0 & (\ell(r-1) - mi)h_{r-1} \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & mih_0 & (\ell - mi)h_1 \end{bmatrix} \quad (12)$$

is an integer matrix that depends on the integers  $i, \ell, m$  and the polynomial  $h$  of degree  $r$ , but is independent of  $p$ . This independence is the key to obtaining an average polynomial-time algorithm.

**Remark 10.** Alternatively, if we define  $w_k^n = [h_{k+r-1}^{n_j}, h_{k+r-2}^{n_j}, \dots, h_k^{n_j}]$  and  $t = d_j p - d_\ell - cn_j$ , the entries of  $w_t^n$  suffice to compute the last row of block  $B^{j\ell}$  in  $A_p$ . Equivalently, if we put  $\tilde{h}(x) = x^r h(1/x)$  (in other words, reverse the coefficients of  $h$ ) and define  $\tilde{v}_k^n$  in terms of  $\tilde{h}^n$  as above, it suffices to compute  $\tilde{v}_s^n$  where

$$\tilde{s} = rn_j - t = dn_j - d_j p + d_\ell = p - 1 - \lfloor (d_j \bmod m)p/m \rfloor. \quad (13)$$

When  $m \nmid d_j$  we will have  $\tilde{s} < s$  if  $c = 0$  (and possibly even if  $c = 1$ ), in which case we can compute the last row more efficiently than the first.

<sup>2</sup>The reader may wish to assume  $c = 0$  and  $f = h$  on a first reading.

We have shown how to compute the first (or last) row of each of the blocks  $B^{j\ell}$  that appear in the Cartier–Manin matrix of the superelliptic curve  $X$  (either for  $X/\mathbb{F}_p$  or for the reductions of  $X/\mathbb{Q}$  modulo varying primes  $p$ ) by computing reductions of products of integer matrices modulo primes. To compute the remaining rows in the same fashion would require working modulo powers of primes, which is something we wish to avoid. In the next section we show how to efficiently reduce the computation of the remaining rows to the computation of the first row using translated curves, which allows us to always work modulo primes.

#### 4. Translation tricks

Let  $X : y^m = f(x)$  be a superelliptic curve over  $\mathbb{F}_p$  of genus  $g$ , with  $d = \deg(f)$ . Let  $A_p$  be the Cartier–Manin matrix  $A_p$ , and for  $a \in \mathbb{F}_p$ , let  $A_p(a)$  be the Cartier–Manin matrix of the translated curve  $X_a : y^m = f(x + a)$ , whose blocks we denote  $B^{j\ell}(a)$  with entries  $b_{ik}^{j\ell}(a)$ . We omit the exponent  $1/p$  that appears in (8) because we are now working over  $\mathbb{F}_p$ . The curve  $X_a$  is isomorphic to  $X$ , which forces  $A_p$  and  $A_p(a)$  to be conjugate, but these matrices are typically not equal. Our objective in this section is to show that we can compute  $B^{j\ell}$  by solving a linear system that involves the entries that appear in just the first rows of  $B^{j\ell}(a)$ , where  $a$  ranges over  $d_j = d - \lfloor dj/m \rfloor - 1$  distinct values of  $a \in \mathbb{F}_p$ . Note that  $B^{j\ell}$  has  $d_j$  rows and  $d_\ell$  columns, and we recall from (8) that the  $g \times g$  matrix  $A_p$  is made up of  $\mu^2$  blocks  $B^{j\ell}$ , where  $\mu = m_1 = m - \lfloor m/d \rfloor - 1$ , and we have  $d_1 + \cdots + d_\mu = g$ . We shall assume  $p \geq d$ , so that  $d_j < d$  distinct values of  $a$  exist in  $\mathbb{F}_p$ ; for  $p < d$  we can easily compute  $A_p$  directly from (8).

The results in this section generalize [17, §5], which treated the case  $m = 2$ , where  $\mu = 1$  and  $A = B^{11}$ . In our current setting  $A_p$  consists of  $\mu \times \mu$  rectangular blocks  $B^{j\ell}$  that need not be square.

For  $a \in \mathbb{F}_p$  and  $1 \leq j \leq \mu$  we define the upper triangular  $d_j \times d_j$  matrix

$$T^j(a) = [t_{ik}^j(a)]_{ik}, \quad t_{ik}^j(a) = \binom{k-1}{i-1} a^{k-i}, \quad 1 \leq i, k \leq d_j.$$

We also define  $T(a)$  to be the  $g \times g$  block diagonal matrix with the matrices  $T^j(a)$  on the diagonal, for  $1 \leq j \leq \mu$ . We note that

$$T^j(a)^{-1} = T^j(-a)$$

and  $T(a)^{-1} = T(-a)$ , as the reader may verify (or see the proof below).

**Lemma 11.** *For  $a \in \mathbb{F}_p$  we have  $B^{j\ell}(a)T^\ell(a) = T^j(a)B^{j\ell}$  for all  $1 \leq j, \ell \leq \mu$ , and  $A_p(a) = T(a)A_pT(-a)$ .*

*Proof.* From the block structure of  $A_p$  given by (8) it is clear that the first statement implies the second. Let  $\omega(a) = \{\omega_{ij}(a)\}$  be the basis given by Lemma 6 for  $X_a$  and define  $\omega_j(a) = \{\omega_{ij'}(a) \in \omega : j' = j\}$ . By Theorem 8, the Cartier operator of  $X$  maps the subspace spanned by  $\omega_j$  to the subspace spanned by  $\omega_\ell$  via the matrix  $B^{j\ell}$ , and the Cartier operator of  $X_a$  maps the subspace spanned by  $\omega_j(a)$  to the subspace spanned by  $\omega_\ell(a)$  via the matrix  $B^{j\ell}(a)$ . We just need to check that the matrices  $T^\ell(a)$  and  $T^j(a)$  correspond to the change of basis that occurs when we replace  $x$  with  $x + a$ . Noting that  $d(x + a) = dx$

and  $F(x+a)_y = F(x)_y$ , we have

$$\begin{aligned}\omega_{kj}(a) &= (x+a)^{k-1}y^{j-1}dx/F_y = \sum_{i=1}^k \binom{k-1}{i-1} a^{k-i}x^{i-1}y^{j-1}dx/F_y \\ &= \sum_{i=1}^k t_{ik}^j(a)\omega_{ij} = \sum_{i=1}^{d_j} t_{ik}^j(a)\omega_{ij},\end{aligned}$$

and it follows that  $\omega_j(a) = T^j(a)\omega_j$  (here we are viewing  $\omega_j$  and  $\omega_j(a)$  as column vectors). This holds for any  $j$ , including  $\ell$ , and the lemma follows.  $\square$

Let us now consider the computation of the  $d_j \times d_\ell$  block  $B^{j\ell}$ . Computing the  $k$ -th entry in the first row of both sides of the identity  $B^{j\ell}(a)T^\ell(a) = T^j(a)B^{j\ell}$  given by Lemma 11 yields

$$\sum_{s=1}^{d_\ell} b_{1s}^{j\ell}(a)t_{sk}^\ell(a) = \sum_{t=1}^{d_j} t_{1t}^j(a)b_{tk}^{j\ell},$$

which defines a linear equation with  $d_j$  unknowns  $b_{tk}^{j\ell}$  in terms of the  $b_{1s}^{j\ell}(a)$  and matrices  $T^j(a)$  and  $T^\ell(a)$  we assume are known. Taking  $d_j$  distinct values of  $a$ , say  $(a_1, \dots, a_{d_j})$ , yields a linear system with  $d_j$  equations and  $d_j$  unknowns that we can solve because the  $d_j \times d_j$  matrix  $[t_{1t}^j(a_i)]_{it} = [a_i^{t-1}]_{it}$  is an invertible Vandermonde matrix  $V(a_1, \dots, a_{d_j})$ . If we now define the  $d_j \times d_\ell$  matrix

$$B_1^{j\ell}(a_1, \dots, a_{d_j}) = [b_{1s}^{j\ell}(a_i)]_{is} \quad (14)$$

and let  $W_1^{j\ell}$  be the  $d_j \times d_\ell$  matrix whose  $i$ -th row is the  $i$ -th row of  $B_1^{j\ell}$  times  $T^\ell(a_i)$ , we can compute  $B^{j\ell}$  as

$$B^{j\ell} = V(a_1, \dots, a_{d_j})^{-1}W_1^{j\ell}. \quad (15)$$

**Remark 12.** If we use Remark 10 to compute the last row of  $B^{j\ell}$  we can compute the first row of  $B^{j\ell}(a_i)$  for  $a_1, \dots, a_{d_j-1}$  and use (15) to deduce the last row of  $W_1^{j\ell}$  from the last row of  $B^{j\ell}$ . One might suppose that we could instead compute the last rows of the  $B^{j\ell}(a_i)$  instead of their first rows, but this is not enough to deduce  $B^{j\ell}$ .

**Lemma 13.** Let  $X : y^m = f(x)$  be a superelliptic curve over  $\mathbb{F}_p$  with  $d = \deg(f)$ , and let  $a_1, \dots, a_{d_1}$  be distinct elements of  $\mathbb{F}_p$ , where  $d_1 = d - \lfloor d/m \rfloor - 1$ . Given the matrices  $B_1^{j\ell}(a_1, \dots, a_{d_j})$  for  $1 \leq j \leq \mu = m_1 = m - \lfloor m/d \rfloor - 1$  with  $\ell \equiv jp \pmod{m}$ , we can compute the Cartier–Manin matrix  $A_p$  of  $X$  using  $O(md^3)$  ring operations in  $\mathbb{F}_p$  and space for  $O(md + d^2)$  elements of  $\mathbb{F}_p$ .

*Proof.* We can compute  $V(a_1, \dots, a_{d_j})^{-1}$  using  $O(d_j^2)$  ring operations in  $\mathbb{F}_p$  [10], and we can compute  $T^\ell(a_i)$  in  $O(d_j^2)$  ring operations (using  $\binom{k}{i} = \binom{k-1}{i-1} + \binom{k-1}{i}$ ). The computation of  $W^{j\ell}$  requires  $O(d_j d_\ell^2)$   $\mathbb{F}_p$ -operations, and the matrix product in (14) uses  $O(d_j^2 d_\ell)$  ring operations, so it takes  $O(d_j^2 d_\ell + d_\ell d_j^2) = O(d^3)$  ring operations to compute each  $B^{j\ell}$ . There are at most  $\mu < m$  nonzero  $B^{j\ell}$  to compute, so the total cost of computing  $A_p$  given the matrices  $B_1^{j\ell}(a_1, \dots, a_{d_j})$  is  $O(md^3)$  ring operations in  $\mathbb{F}_p$  while storing  $O(md + d^2)$  elements of  $\mathbb{F}_p$ .  $\square$

**Remark 14.** In terms of the genus  $g \sim md/2$ , the bound  $O(md^3)$  is equivalent to  $O(gd^2)$ , which is always bounded by  $O(g^3)$  but can be as small as  $O(g)$  if  $d = O(1)$  (this assumes we use a sparse representation of  $A_p$ ).

**Remark 15.** In addition to playing a key role in our strategy for computing  $A_p$ , using translated curves can improve performance, as noted in the case of hyperelliptic curves in [17, §6.1]. In particular, if  $f(x)$  has a rational root  $a$  then the translated curve  $X_a : y^m = f(x+a) = xh(x)$  will have  $r = d - 1$  and  $c = d - r = 1$ , reducing both the dimension  $r$  and number  $t = p - 1 - cn$  of matrices  $M_k^\ell$  that appear in the product in (11). It thus makes sense to choose our distinct translation points  $a$  to be roots of  $f(x)$  whenever possible. Additionally, if  $d$  is divisible by  $m$  and  $f(x)$  has a rational root  $a$ , we can replace  $X$  with  $X' : y^m = x^d f(1/x + a) = g(x)$ , where  $g(x)$  has degree  $d - 1$ , and this also applies to all translated curves  $X'_a$ . This applies both locally (over  $\mathbb{F}_p$ ) and globally (over  $\mathbb{Q}$ ).

## 5. Accumulating remainder trees and forests

In this section we briefly recall some background on accumulating remainder trees and related complexity bounds. Given a sequence of  $r \times r$  matrices  $M_0, \dots, M_{N-1}$  and a sequence of coprime integers  $m_1, \dots, m_N$  we wish to compute the sequence of reduced partial products

$$A_k = M_0 \cdots M_{k-1} \bmod m_k$$

for  $1 \leq k \leq N$ . For  $0 \leq k \leq N/2$  let  $B_k = M_{2k} M_{2k+1}$  and  $b_k = m_{2k} m_{2k+1}$ , where  $M_N = M_{N+1} = I$  and  $m_0 = m_{N+1} = 1$ . Then  $A_1 = M_0 \bmod m_1$ , and if we recursively compute  $C_k = B_0 \cdots B_{k-1} \bmod b_k = M_0 \cdots M_{2k-1} \bmod m_{2k} m_{2k+1}$  for  $1 \leq k \leq N/2$ , we can then compute

$$A_{2k} = C_k \bmod m_{2k} \quad \text{and} \quad A_{2k+1} = C_k M_{2k} \bmod m_{2k+1},$$

omitting  $C_{2k+1}$  when  $k = N/2$ . This is the REMAINDERTREE algorithm given in [16]. In our setting we actually want to compute products of the form  $V \prod_k M_k$  that involve a row vector  $V$ , and for this problem the REMAINDERFOREST algorithm in [16] achieves an improved time (and especially) space complexity by splitting the remainder tree into  $2^\kappa$ -subtrees, for a suitable choice of  $\kappa$ . We record the following result from [17], in which  $\|x\|$  denotes the logarithm of the largest absolute value appearing in nonzero integer matrix or integer vector  $x$ , including the case where  $x$  is a single nonzero integer.

**Theorem 16** [17]. *Given  $V \in \mathbb{Z}^r$ ,  $M_1, \dots, M_N \in \mathbb{Z}^{r \times r}$ , and  $m_1, \dots, m_N \in \mathbb{Z}$ , let  $n = \lceil \log_2 N \rceil$ , let  $B$  be an upper bound on  $\|\prod_{j=1}^N m_j\|$  such that  $B/2^\kappa$  is an upper bound on  $\|\prod_{j=st}^{st+t-1} m_j\|$  for  $1 \leq s \leq N/t$ , where  $t := 2^{n-\kappa}$ . Let  $B'$  be an upper bound on  $\|V\|$ , and let  $H$  be an upper bound on  $\|m_k\|, \|A_k\|$  for  $1 \leq k \leq N$ , such that  $\log r \leq H$ , and assume that  $r = O(\log N)$ . The REMAINDERFOREST algorithm computes the vectors  $V_k = V M_1 \cdots M_k \bmod m_k \in (\mathbb{Z}/m_k \mathbb{Z})^r$  for  $1 \leq k \leq N$  in*

$$O(r^2 M(B + NH)(n - \kappa) + 2^\kappa r^2 M(B) + r M(B'))$$

*time using space bounded by*

$$O(2^{-\kappa} r^2 (B + NH)(n - \kappa) + r(B + B')).$$

This theorem implies the following corollary, which is all we shall use.

**Corollary 17.** *Fix an absolute constant  $c > 0$ . Let  $N$  be a positive integer, let  $m_1, \dots, m_N$  be a sequence of positive coprime integers with  $\log m_k \leq c \log N$ , let  $M_0, \dots, M_{N-1} \in \mathbb{Z}^{r \times r}$  be integer matrices with  $r, \|M_k\| \leq c \log N$ , and let  $v_0 \in \mathbb{Z}^r$  be a row vector with  $\|v_0\| = cN \log N$ . We can compute the vectors*

$$v_k = v_0 \prod_{i=0}^{k-1} M_i \bmod m_k$$

for  $1 \leq k \leq N$  in  $O(r^2 N \log^3 N)$  time using  $O(r^2 N)$  space.

*Proof.* Applying Theorem 16 with  $\kappa = 2 \log \log N$ ,  $B = cN \log N$ ,  $B' = c \log N$ , and  $H = c \log N$ , yields an  $O(r^2 M(N \log N) \log N)$  time bound using  $O(r^2 N)$  space. Now apply  $M(N) = O(N \log N)$  from [18].  $\square$

## 6. Algorithms

We now give our algorithms for computing the Cartier–Manin matrix  $A_p$  of a superelliptic curve  $X/\mathbb{F}_p$  and for the reductions of a superelliptic curve  $X/\mathbb{Q}$  modulo good primes  $p \leq N$ . In the descriptions below, expressions of the form “ $a \bmod m$ ” denote the least nonnegative remainder in Euclidean division of  $a$  by  $m$ . As above we assume  $X$  is defined by  $y^m = f(x)$  with  $f(x)$  squarefree of degree  $d \geq 3$ . We define  $\mu = m - \lfloor m/d \rfloor - 1$ , and for  $1 \leq j \leq \mu$  we put  $d_j = d - \lfloor dj/m \rfloor - 1$ , with  $d_1 \geq d_2 \geq \dots \geq d_\mu$  as in (6). Recall that the genus of  $X$  is  $g = ((d-2)(m-1) + m - \gcd(m, d))/2$ , as in (1).

**Algorithm** (COMPUTECARTIERMANINMATRIX). Given  $m \geq 2$  and squarefree  $f \in \mathbb{F}_p[x]$  of degree  $3 \leq d \leq p$  with  $p \nmid m$ , compute the Cartier–Manin matrix  $A_p \in \mathbb{F}_p^{g \times g}$  of  $X : y^m = f(x)$  as follows:

- (1) Fix distinct  $a_1, \dots, a_{d_1} \in \mathbb{F}_p$  that include as many roots of  $f(x)$  as possible.
- (2) For  $j$  from 1 to  $\mu$  such that  $\ell = jp \bmod m \leq \mu$ :
  - (a) For  $i$  from 1 to  $d_j$ :
    - (i) Let  $f(x + a_i) = x^c h(x) \in \mathbb{F}_p[x]$  with  $c \in \{0, 1\}$  and put  $r = \deg(h)$ .
    - (ii) Set  $n = ((m-j)p - (m-\ell))/m \in \mathbb{Z}$  and  $s = p-1-cn$ .
    - (iii) Compute  $w_s = v_0^0 \prod_{i=0}^{s-1} M_i^\ell \in \mathbb{F}_p^r$ , with  $M_i^\ell \in \mathbb{F}_p^{r \times r}$  as in (12), and  $u_s = s! \in \mathbb{F}_p$ .
    - (iv) Compute  $\alpha = v_s^n = m^{-s} h_0^{n-s} u_s^{-1} w_s \in \mathbb{F}_p^r$  via (11).
    - (v) Let  $b_1^{j\ell}(a_i) = [\alpha_r, \alpha_{r-1}, \dots, \alpha_{r-d_\ell+1}] \in \mathbb{F}_p^{d_\ell}$ .
  - (b) Let  $B_1^{j\ell} \in \mathbb{F}_p^{d_j \times d_\ell}$  be the matrix with  $i$ -th row  $b_1^{j\ell}(a_i)$  as in (14) and use  $B_1^{j\ell}$  to compute  $B^{j\ell} \in \mathbb{F}_p^{d_j \times d_\ell}$  via (15).
- (3) Output  $A_p = [B^{j\ell}]_{j\ell} \in \mathbb{F}_p^{g \times g}$  defined as in (8), with  $B^{j\ell} = 0$  for  $\ell \not\equiv jp \bmod m$ .

There are two ways to compute  $w_s$  in step (iii). One is to compute  $s$  vector-matrix products  $w_{i+1} = w_i M_i^\ell$  starting with  $w_0 = [0, \dots, 0, 1] \in \mathbb{F}_p^r$ , which can be accomplished using  $O(pr)$  ring operations

in  $\mathbb{F}_p$  using  $O(r \log p)$  space (note that  $M_i^\ell$  has only  $2r - 1$  nonzero entries). Alternatively one can use the Bostan–Gaudry–Schost algorithm [4], which uses an optimized interpolation/evaluation approach to compute products of matrices over polynomial rings evaluated along an arithmetic progression; in our setting we view the  $M_i^\ell$  as matrices of linear polynomials in  $i$  evaluated along the arithmetic progression  $i = 0, 1, 2, \dots, s - 1$ . This involves  $O(p^{1/2}(r^\omega + r^2 \log p))$  ring operations in  $\mathbb{F}_p$  using  $O(r^2 p^{1/2})$  space, via [4, Theorem 8] and [19], and we can similarly compute  $u_s = s!$  (but note that  $u_s = -1$  in the typical case where  $c = 0$ ).

We now prove Theorem 3, which we restate here for convenience.

**Theorem 3.** *Given a superelliptic curve  $X : y^m = f(x)$  with  $f \in \mathbb{F}_p[x]$  of degree  $d$ , the algorithm COMPUTECARTIERMANINMATRIX is able to compute the Cartier–Manin matrix of  $X$  using  $O(p^{1/2}md^2 \log p)$  space in  $O(p^{1/2}m(d^{\omega+1} + d^3 \log p) \log p (\log \log p))$  time, and also using  $O((md + d^2) \log p)$  space in  $O((p + d)md^2 \log p \log \log p)$  time.*

*Proof.* The theorem follows from Lemma 13, provided that we can compute the matrices  $B_1^{j\ell}(a_1, \dots, a_{d_j})$  within the stated complexity bounds. This computation is dominated by the cost of step (iii), which is executed  $O(md)$  times. The cost of a ring operation in  $\mathbb{F}_p$  can be bounded by  $O(M(\log p))$  via [26, Theorem 9.9], which is  $O(\log p \log \log p)$ , by [18]. The Bostan–Gaudry–Schost approach yields a bit-complexity of

$$O(p^{1/2}(d^\omega + d^2 \log p) \log p \log \log p)$$

time and  $O(d^2 p^{1/2} \log p)$  space per iteration, and the vector-matrix multiplication approach yields a bit-complexity of  $O(pd \log p \log \log p)$  and  $O(d \log p)$  space per iteration; the theorem follows.  $\square$

We now present our main result, an average polynomial-time algorithm to compute the Cartier–Manin matrices of the reductions of a superelliptic curve  $X/\mathbb{Q}$  at all good primes  $p \leq N$ .

**Algorithm** (COMPUTECARTIERMANINMATRICES). Given  $m \geq 2$  and squarefree  $f \in \mathbb{Z}[x]$  of degree  $d \geq 3$ , compute the Cartier–Manin matrices  $A_p$  of the reductions of  $X : y^m = f(x)$  modulo primes  $p \leq N$  with  $p \nmid m \operatorname{lc}(f) \operatorname{disc}(f)$  as follows:

- (1) For primes  $p \leq N$  with  $p \nmid m \operatorname{lc}(f) \operatorname{disc}(f)$  initialize  $A_p \in \mathbb{F}_p^{g \times g}$  to the zero matrix.
- (2) Fix distinct  $a_1, \dots, a_{d_1} \in \mathbb{Z}$  that include as many roots of  $f$  as possible.
- (3) For each pair of integers  $j, \ell \in [1, \mu]$ :
  - (a) Compute the set  $P = \{p_1, p_2, \dots\}$  of primes  $p \leq N$  with  $jp \equiv \ell \pmod{m}$  such that  $p \nmid m \operatorname{lc}(f) \operatorname{disc}(f)$  and  $a_1, \dots, a_{d_1}$  are distinct modulo  $p$ .
  - (b) If the set  $P$  is empty proceed to the next pair  $j, \ell$ .
  - (c) For  $i$  from 1 to  $d_j$ :
    - (i) Let  $f(x + a_i) = x^c h(x) \in \mathbb{Z}[x]$  with  $c \in \{0, 1\}$  and put  $r = \deg(h)$ .

- (ii) Let  $N' = N$  if  $c = 0$  and  $N' = \lfloor (jN - \ell)/m \rfloor$  otherwise.
- (iii) Define coprime moduli  $m_1, \dots, m_{N'}$  as follows:
  - If  $c = 0$  then  $m_k = k + 1$  for  $k + 1 \in P$ .
  - If  $c = 1$  then  $m_k = (mk + \ell)/j$  for  $(mk + \ell)/j \in P$ .
  - For any  $m_k$  not defined above, let  $m_k = 1$ .
- For  $p \in P$  let  $k(p)$  denote the index  $k$  of the  $m_k$  for which  $m_k = p$ .
- (iv) Compute  $w_k = v_0^0 \prod_{i=0}^{k-1} M_i^\ell \bmod m_k$  and  $u_k = k! \bmod m_k$  for  $1 \leq k \leq N'$  as in [Corollary 17](#).
- (v) For  $p \in P$  use  $w_{k(p)}, u_{k(p)}$  to compute  $b_1^{j\ell}(a_i) \in \mathbb{F}_p^{d_\ell}$  as in `COMPUTECARTIERMANINMATRIX`.
- (d) For  $p \in P$ , let  $B_1^{j\ell} \in \mathbb{F}_p^{d_j \times d_\ell}$  have rows  $b_1^{j\ell}(a_i) \in \mathbb{F}_p^{d_\ell}$  as in [\(14\)](#), use  $B_1^{j\ell}$  to compute  $B^{j\ell} \in \mathbb{F}_p^{d_j \times d_\ell}$  via [\(15\)](#), and set the  $j, \ell$  block of  $A_p$  to  $B^{j\ell}$  as in [\(8\)](#).
- (4) Let  $S$  be the set of primes  $p \leq N$  satisfying  $p \nmid m \operatorname{lc}(f) \operatorname{disc}(f)$  for which the  $a_1, \dots, a_{d_1}$  are not distinct modulo  $p$ . For  $p \in S$  compute  $A_p$  using algorithm `COMPUTECARTIERMANINMATRIX` if  $p \geq d$  and otherwise compute  $A_p$  directly from [\(8\)](#) by extracting coefficients of powers of  $f \in \mathbb{F}_p[x]$ .
- (5) Output  $A_p \in \mathbb{F}_p^{g \times g}$  for all primes  $p \leq N$  such that  $p \nmid m \operatorname{lc}(f) \operatorname{disc}(f)$ .

**Remark 18.** To compute Frobenius traces  $a_p \in \mathbb{Z}$ , we modify step (3) to loop over integers  $j = \ell \in [1, \mu]$  and output just the traces of the  $A_p$  in step (5). This gives the traces of Frobenius  $a_p \bmod p$ . For  $p > 16g^2$  these determine  $a_p \in \mathbb{Z}$ , by the Weil bounds, and for  $p \leq 16g^2$  we can compute

$$a_p = p + 1 - \#X(\mathbb{F}_p)$$

by enumerating values of  $f(x)$  and looking them up in a precomputed table of  $m$ -th powers.

**Remark 19.** The loop in step (c) is executed (up to)  $\mu g$  times. Each of these computations is completely independent of the others, which makes it easy to efficiently distribute the work across  $\mu g$  threads. In principal one can also parallelize the integer matrix multiplications performed by the `REMAINDERFORREST` algorithm in step (iv), but in practice it is extremely difficult to do this efficiently.

We now prove [Theorem 1](#), which we restate for convenience.

**Theorem 1.** *Given a superelliptic curve  $X : y^m = f(x)$  with  $f \in \mathbb{Z}[x]$  of degree  $d$  and  $N \in \mathbb{Z}_{>0}$ , the algorithm `COMPUTECARTIERMANINMATRICES` outputs the Cartier–Manin matrices  $A_p$  of the reductions of  $X$  modulo all primes  $p \leq N$  not dividing  $m \operatorname{lc}(f) \operatorname{disc}(f)$ . If we assume  $m, d, \|f\|$  are bounded by  $O(\log N)$  the algorithm runs in  $O(m^2 d^3 N \log^3 N)$  time using  $O(md^2 N)$  space; it can alternatively compute Frobenius traces  $a_p \in \mathbb{Z}$  for  $p \leq N$  in time  $O(md^3 N \log^3 N)$ .*

*Proof.* The total time to compute all the sets  $P$  using a sieve is bounded by  $O(N \log N)$  time using  $O(N)$  space, and this also bounds the total time and space for steps (i), (ii), (iii), under our assumption that  $m, d, \|f\| = O(\log N)$ . [Corollary 17](#) yields an  $O(d^2 N \log^3 N)$  bound on each of the  $O(m^2 d)$  iterations of step (iv). This yields the claimed time bound of  $O(m^2 d^3 N \log^3 N)$  for step (c), which we claim



dominates. [Lemma 13](#) implies that the total cost of step (d) is bounded by  $O(\pi(N)m^2d^3 \log N)$ , which is negligible, as is the cost of the rest of the algorithm. Note that the cardinality of the set  $S$  in step (4) is at worst quadratic in  $d$  and  $\log(N)$  under our assumption  $\|f\| = O(\log N)$ , so we can easily afford the calls to `COMPUTECARTIERMANINMATRIX` and use a brute force approach to compute  $A_p$  for primes  $p < d$  of good reduction.

The space bound follows from the bound in [Corollary 17](#), which covers step (iv) (it is easy to see that all of the other steps fit within the claimed bound).

To compute Frobenius traces  $a_p \in \mathbb{Z}$  we apply [Remark 18](#) and note that restricting to  $j = \ell$  in step (3) reduces the number of iterations of the main loop by a factor of  $m$ . The cost of computing  $\#X(\mathbb{F}_p)$  by looking up values of  $f(x)$  in a table of  $m$ -th powers is  $O(pd)$  ring operations in  $\mathbb{F}_p$ . The total time to compute  $a_p = p + 1 - \#X(\mathbb{F}_p)$  for good  $p \leq 16g^2$  is then

$$O(dg^2\pi(g^2) \log g \log \log g) = O(d(\log N)^4 \log \log N),$$

which is negligible. □

## 7. Supplementary material

Tables 1 and 2 compare the performance of the average polynomial-time algorithm `COMPUTECARTIERMANINMATRICES` with the  $\tilde{O}(p^{1/2})$  algorithm for computing zeta functions of cyclic covers implemented in Sage version 9.0. The Sage implementation provides the function `CYCLICCOVER` which takes an integer  $m$  and a squarefree polynomial  $f \in \mathbb{F}_p[x]$  and returns an object that represents a superelliptic curve  $y^m = f(x)$  over  $\mathbb{F}_p$ . Invoking the `FROBENIUS_MATRIX` method of this object with the  $p$ -adic precision set to 1 yields a matrix that encodes essentially the same information as the Cartier–Manin matrix  $A_p$ ; in particular it determines the  $p$ -rank of  $X$  and its zeta function modulo  $p$ .

Each table lists the genus  $g$  and invariants  $m$  and  $d$  of a superelliptic curve  $X: y^m = f(x)$  defined over  $\mathbb{Q}$  with  $f \in \mathbb{Z}[x]$  of degree  $d$ . There is a row for every pair  $m \geq 2$  and  $d \geq 3$  for which  $m^2d^3 \leq 6^5$ , which includes all superelliptic curves of genus  $g \leq 5$  as well as plane quintics and sextics, and other curves of genus up to 15. The times listed are average times in milliseconds for primes  $p \leq N$  for increasing values of  $N$ . For each  $N$  three times are listed: one to compute Frobenius matrices using Sage, one to compute Cartier–Manin matrices using the algorithm `COMPUTECARTIERMANINMATRICES`, and one to compute Frobenius traces via [Remark 18](#). For the Sage timings we only computed Frobenius matrices for every  $n$ -th good prime  $p \leq N$  with  $n$  chosen so that the computation would complete in less than a day (many of the computations would have taken months otherwise).

In [Table 1](#) we show timings with  $f \in \mathbb{Z}[x]$  having coefficients  $f_{d+1-n} = p_n$  for  $1 \leq n \leq d$ , where  $p_n$  is the  $n$ -th prime. These polynomials are all irreducible, so our algorithm was unable to choose any  $a_i$  to be roots of  $f$ ; this is the generic situation, and the worst case for our algorithm. In [Table 2](#) we show timings with  $f \in \mathbb{Z}[x]$  a product of linear factors, which represents the best case for our algorithm.



$g$	$m$	$d$	$N = 2^{20}$			$N = 2^{24}$			$N = 2^{28}$		
			sage	matrix	trace	sage	matrix	trace	sage	matrix	trace
1	2	3	27	0.05	0.05	67	0.13	0.13	230	0.30	0.30
1	2	4	41	0.17	0.16	120	0.42	0.42	454	0.95	0.93
1	3	3	46	0.08	0.08	141	0.20	0.20	499	0.48	0.49
2	2	5	55	0.38	0.38	163	0.92	0.92	580	2.02	2.01
2	2	6	83	0.73	0.74	280	1.77	1.77	1070	3.89	3.92
3	2	7	112	1.30	1.29	307	3.19	3.12	1217	6.47	6.71
3	2	8	169	2.15	2.07	528	5.02	4.94	2106	10.20	10.57
3	3	4	61	0.53	0.26	178	1.38	0.70	702	3.14	1.63
3	4	3	58	0.14	0.15	165	0.37	0.37	601	0.89	0.89
3	4	4	101	0.44	0.44	343	1.14	1.14	1283	2.55	2.63
4	2	9	194	3.22	3.24	576	7.65	7.70	2214	16.12	15.90
4	2	10	319	4.78	4.65	974	11.10	10.98	3693	22.13	22.79
4	3	5	93	1.29	0.65	287	3.37	1.67	1105	7.64	3.68
4	3	6	152	2.59	1.28	535	6.34	3.20	2121	14.04	7.07
4	5	3	68	0.40	0.13	200	1.19	0.40	778	2.96	0.99
4	6	3	112	0.24	0.24	313	0.64	0.64	1184	1.53	1.53
5	2	11	361	7.04	7.06	1024	16.57	16.30	3695	33.61	33.32
5	2	12	555	9.56	9.54	1537	21.84	22.23	5820	45.98	45.65
6	3	7	200	4.61	2.32	632	11.53	5.52	2360	24.18	12.18
6	4	5	130	1.71	1.08	424	4.37	2.73	1658	9.86	5.88
6	5	4	113	1.29	0.42	344	3.76	1.25	1358	9.08	3.03
6	5	5	201	3.06	1.02	671	8.98	2.92	2749	19.39	6.64
6	7	3	94	0.68	0.17	290	2.24	0.56	1146	5.57	1.39
7	3	8	294	8.17	4.05	835	19.07	9.38	3279	40.32	20.49
7	3	9	437	12.77	6.32	1462	28.54	14.50	5567	61.82	29.67
7	4	6	232	3.42	2.12	806	8.58	5.21	3160	18.99	11.54
7	6	4	153	1.08	0.77	524	2.79	2.00	2112	6.46	4.55
7	8	3	111	0.60	0.29	366	1.72	0.83	1333	4.32	2.00
7	9	3	140	0.82	0.26	479	2.64	0.82	1870	6.77	2.03
9	4	7	302	6.49	3.94	941	15.10	9.42	3566	32.97	20.43
9	7	4	156	2.77	0.56	510	9.14	1.78	2012	20.90	4.21
9	8	4	231	1.85	0.92	720	5.43	2.57	2941	12.58	6.12
9	10	3	137	0.76	0.34	429	2.29	1.01	1694	5.82	2.50
10	5	6	265	8.08	2.02	840	22.89	5.62	3256	51.62	12.42
10	6	5	206	2.51	1.83	701	6.28	4.61	2700	14.07	9.88
10	6	6	379	5.05	3.49	1278	11.95	8.59	5202	26.43	18.72
10	11	3	158	1.77	0.25	501	6.11	0.88	1878	15.32	2.12
10	12	3	187	0.80	0.49	636	2.35	1.39	2558	5.87	3.45
12	7	5	246	6.75	1.33	840	20.80	4.13	3228	48.09	9.23
12	9	4	199	2.88	0.87	657	8.87	2.64	2655	21.75	6.24
12	13	3	175	2.43	0.29	616	8.24	1.03	2244	20.02	2.49
13	10	4	264	2.90	1.09	1008	8.62	3.17	3762	20.08	7.47
13	14	3	193	1.58	0.43	619	5.01	1.36	2430	12.79	3.40
13	15	3	235	1.69	0.46	811	5.54	1.45	3238	13.99	3.72
15	11	4	252	6.29	0.79	839	22.76	2.84	3334	52.85	6.59
15	16	3	223	1.79	0.53	733	5.66	1.63	2805	14.16	4.13

**Table 1.** Comparison with  $\tilde{O}(p^{1/2})$  Sage 9.0 implementation [2] for superelliptic curves  $y^m = f(x)$  where  $f \in \mathbb{Z}[x]$  is irreducible of degree  $d$ . Times are millisecond averages per prime  $p \leq N$  for a single thread running on a 2.8GHz Cascade Lake Intel CPU. The sage column lists the average time to execute `CyclicCover(m,f.change_ring(GF(p)).frobenius_matrix(1)` in Sage 9.0, the matrix column lists the average time to compute the Cartier–Manin matrix modulo  $p$  using algorithm `COMPUTECARTIERMANINMATRICES`, and the trace column is the average time to compute the trace of Frobenius via [Remark 18](#).

$g$	$m$	$d$	$N = 2^{20}$			$N = 2^{24}$			$N = 2^{28}$		
			sage	matrix	trace	sage	matrix	trace	sage	matrix	trace
1	2	3	28	0.01	0.01	73	0.04	0.04	230	0.09	0.08
1	2	4	43	0.04	0.05	119	0.12	0.12	456	0.28	0.27
1	3	3	45	0.01	0.01	131	0.02	0.02	500	0.05	0.05
2	2	5	53	0.11	0.12	151	0.31	0.30	583	0.72	0.72
2	2	6	84	0.26	0.28	267	0.66	0.64	1071	1.40	1.40
3	2	7	116	0.55	0.54	311	1.22	1.20	1219	2.58	2.59
3	2	8	164	0.94	0.92	532	2.06	2.04	2094	4.19	4.23
3	3	4	62	0.14	0.07	184	0.41	0.20	701	0.96	0.47
3	4	3	55	0.03	0.03	157	0.08	0.08	605	0.20	0.20
3	4	4	103	0.08	0.09	334	0.23	0.23	1286	0.55	0.54
4	2	9	199	1.50	1.47	586	3.48	3.41	2232	7.10	7.12
4	2	10	295	2.30	2.29	942	5.37	5.24	3816	10.53	10.37
4	3	5	92	0.38	0.19	283	1.06	0.51	1111	2.40	1.21
4	3	6	153	0.79	0.41	529	1.85	0.91	2098	3.96	1.99
4	5	3	68	0.05	0.02	202	0.16	0.05	780	0.39	0.13
4	6	3	95	0.03	0.03	301	0.09	0.09	1186	0.22	0.21
5	2	11	354	3.45	3.46	977	7.85	7.87	3682	15.94	15.85
5	2	12	530	5.11	5.12	1543	11.30	11.17	5857	22.61	22.62
6	3	7	192	1.47	0.72	605	3.57	1.78	2361	7.67	3.79
6	4	5	136	0.32	0.25	416	0.94	0.61	1660	2.17	1.43
6	5	4	108	0.30	0.10	348	1.00	0.32	1369	2.43	0.81
6	5	5	196	0.52	0.15	710	1.48	0.48	2755	3.49	1.16
6	7	3	96	0.06	0.02	296	0.23	0.06	1146	0.63	0.15
7	3	8	276	3.05	1.54	836	7.04	3.49	3234	15.09	7.64
7	3	9	427	4.09	2.16	1409	9.28	4.74	5551	21.20	10.35
7	4	6	227	0.98	0.65	774	2.30	1.48	3143	5.26	3.33
7	6	4	155	0.23	0.17	525	0.66	0.44	2108	1.53	1.04
7	8	3	111	0.06	0.04	343	0.20	0.12	1333	0.51	0.30
7	9	3	141	0.08	0.03	476	0.28	0.09	1876	0.76	0.23
9	4	7	289	1.85	1.23	917	4.56	2.88	3555	10.28	6.23
9	7	4	156	0.61	0.10	509	1.78	0.35	2007	4.47	0.88
9	8	4	211	0.33	0.18	752	1.05	0.50	2946	2.64	1.23
9	10	3	139	0.08	0.04	430	0.26	0.12	1694	0.66	0.31
10	5	6	253	2.08	0.52	825	5.96	1.49	3265	13.97	3.37
10	6	5	213	0.68	0.42	676	1.61	1.06	2693	3.83	2.43
10	6	6	365	1.23	0.86	1276	2.94	2.00	5195	6.46	4.34
10	11	3	154	0.14	0.02	477	0.52	0.08	1878	1.48	0.21
10	12	3	189	0.08	0.07	640	0.26	0.17	2552	0.63	0.42
12	7	5	242	1.22	0.24	879	3.99	0.77	3227	9.89	1.93
12	9	4	204	0.60	0.17	672	1.66	0.52	2663	4.30	1.26
12	13	3	175	0.19	0.02	569	0.71	0.09	2245	2.06	0.25
13	10	4	267	0.64	0.22	942	1.69	0.65	3779	4.32	1.56
13	14	3	191	0.14	0.05	617	0.47	0.15	2429	1.23	0.37
13	15	3	240	0.14	0.04	806	0.50	0.14	3246	1.35	0.36
15	11	4	251	1.15	0.14	836	3.92	0.49	3314	9.89	1.26
15	16	3	218	0.15	0.06	728	0.52	0.19	2797	1.37	0.48

**Table 2.** Timings for superelliptic curves  $X : y^m = f(x)$  when  $f \in \mathbb{Z}[x]$  splits into  $d$  distinct linear factors. Times are millisecond averages per prime  $p \leq N$  for a single thread running on a 2.8GHz Cascade Lake Intel CPU. The sage column lists the average time to execute `CyclicCover(m,f.change_ring(GF(p)).frobenius_matrix(1)` in Sage 9.0, the matrix column lists the average time to compute the Cartier–Manin matrix modulo  $p$  using algorithm `COMPUTECARTIERMANINMATRICES`, and the trace column is the average time to compute the trace of Frobenius via [Remark 18](#).

## References

- [1] Jeffrey D. Achter and Everett W. Howe, *Hasse–Witt and Cartier–Manin matrices: a warning and a request*, Arithmetic geometry: computation and applications, Contemp. Math., no. 722, Amer. Math. Soc., Providence, RI, 2019, pp. 1–18. [MR 3896846](#)
- [2] Vishal Arul, Alex J. Best, Edgar Costa, Richard Magner, and Nicholas Triantafillou, *Computing zeta functions of cyclic covers in large characteristic*, Proceedings of the Thirteenth Algorithmic Number Theory Symposium (Berkeley, CA), Open Book Ser., no. 2, Math. Sci. Publ., 2019, pp. 37–53. [MR 3952003](#)
- [3] Andrew R. Booker, Jeroen Sijsling, Andrew V. Sutherland, John Voight, and Dan Yasaki, *A database of genus-2 curves over the rational numbers*, LMS J. Comput. Math., **19A** (2016), 235–254. [MR 3540958](#)
- [4] Alin Bostan, Pierrick Gaudry, and Éric Schost, *Linear recurrences with polynomial coefficients and application to integer factorization and Cartier–Manin operator*, SIAM J. Comput. **36** (2007), no. 6, 1777–1806. [MR 2299425](#)
- [5] Irene I. Bouw, *The  $p$ -rank of ramified covers of curves*, Compositio Math. **126** (2001), no. 3, 295–322. [MR 1834740](#)
- [6] Irene I. Bouw and Stefan Wewers, *Computing  $L$ -functions and semistable reduction of superelliptic curves*, Glasg. Math. J. **59** (2017), no. 1, 77–108. [MR 3576328](#)
- [7] Alina Bucur, Francesc Fité, and Kiran S. Kedlaya, *Effective Sato–Tate conjecture for abelian varieties and applications*, preprint, 2020. [arXiv 2002.08807](#)
- [8] Claude Chevalley, *Introduction to the Theory of Algebraic Functions of One Variable*, Mathematical Surveys, no. 6, American Mathematical Society, New York, 1951. [MR 0042164](#)
- [9] Edgar Costa, Francesc Fité, and Andrew V. Sutherland, *Arithmetic invariants from Sato–Tate moments*, C. R. Math. Acad. Sci. Paris **357** (2019), no. 11–12, 823–826. [MR 4038255](#)
- [10] A. Eisenberg and G. Fedele, *On the inversion of the Vandermonde matrix*, Appl. Math. Comput. **174** (2006), no. 2, 1384–1397. [MR 2220623](#)
- [11] Francesc Fité, Kiran S. Kedlaya, Víctor Rotger, and Andrew V. Sutherland, *Sato–Tate distributions and Galois endomorphism modules in genus 2*, Compos. Math. **148** (2012), no. 5, 1390–1442. [MR 2982436](#)
- [12] Francesc Fité, Kiran S. Kedlaya, and Andrew V. Sutherland, *Sato–Tate groups of abelian threefolds: a preview of the classification*, preprint, 2019. [arXiv 1911.02071](#)
- [13] Cécile Gonçalves, *A point counting algorithm for cyclic covers of the projective line*, Algorithmic arithmetic, geometry, and coding theory, Contemp. Math., no. 637, Amer. Math. Soc., Providence, RI, 2015, pp. 145–172. [MR 3364447](#)
- [14] Daniel Gorenstein, *An arithmetic theory of adjoint plane curves*, Trans. Amer. Math. Soc. **72** (1952), 414–436. [MR 49591](#)
- [15] David Harvey, Maike Massierer, and Andrew V. Sutherland, *Computing  $L$ -series of geometrically hyperelliptic curves of genus three*, LMS J. Comput. Math., **19A** (2016), 220–234. [MR 3540957](#)
- [16] David Harvey and Andrew V. Sutherland, *Computing Hasse–Witt matrices of hyperelliptic curves in average polynomial time*, LMS J. Comput. Math., **17A** (2014), 257–273. [MR 3240808](#)
- [17] David Harvey and Andrew V. Sutherland, *Computing Hasse–Witt matrices of hyperelliptic curves in average polynomial time, II*, Frobenius distributions: Lang–Trotter and Sato–Tate conjectures, Contemp. Math., no. 663, Amer. Math. Soc., Providence, RI, 2016, pp. 127–147. [MR 3502941](#)
- [18] David Harvey and Joris van der Hoeven, *Integer multiplication in time  $O(n \log n)$* , preprint, 2019.
- [19] David Harvey and Joris van der Hoeven, *Polynomial multiplication over finite fields in time  $O(n \log n)$* , preprint, 2019.
- [20] Moritz Minzloff, *Computing zeta functions of superelliptic curves in larger characteristic*, Math. Comput. Sci. **3** (2010), no. 2, 209–224. [MR 2608297](#)
- [21] Pascal Molin and Christian Neurohr, *Computing period matrices and the Abel–Jacobi map of superelliptic curves*, Math. Comp. **88** (2019), no. 316, 847–888. [MR 3882287](#)
- [22] Jean-Pierre Serre, *Lectures on  $N_X(p)$* , Research Notes in Mathematics, no. 11, CRC Press, 2012. [MR 2920749](#)
- [23] Henning Stichtenoth, *Algebraic function fields and codes*, 2nd ed., Graduate Texts in Mathematics, no. 254, Springer, 2009. [MR 2464941](#)

- [24] Karl-Otto Stöhr and José Felipe Voloch, *A formula for the Cartier operator on plane algebraic curves*, J. Reine Angew. Math. **377** (1987), 49–64. [MR 887399](#)
- [25] Andrew V. Sutherland, *A database of nonhyperelliptic genus-3 curves over  $\mathbb{Q}$* , Proceedings of the Thirteenth Algorithmic Number Theory Symposium (Berkeley, CA) (Renate Scheidler and Jonathan Sorenson, eds.), Open Book Ser., no. 2, Math. Sci. Publ., 2019, pp. 443–459. [MR 3952027](#)
- [26] Joachim von zur Gathen and Jürgen Gerhard, *Modern computer algebra*, 3rd ed., Cambridge University Press, 2013. [MR 3087522](#)
- [27] Yuri G. Zarhin, *Endomorphism algebras of abelian varieties with special reference to superelliptic Jacobians*, Geometry, algebra, number theory, and their information technology applications, Springer Proc. Math. Stat., no. 251, Springer, 2018, pp. 477–528. [MR 3880401](#)

Received 28 Feb 2020. Revised 28 Feb 2020.

ANDREW V. SUTHERLAND: [drew@math.mit.edu](mailto:drew@math.mit.edu)

*Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA, United States*



## Fourteenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational and algorithmic number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the fourteenth ANTS meeting, which took place 29 June to 4 July 2020 via video conference, the plans for holding it at the University of Auckland, New Zealand, having been disrupted by the COVID-19 pandemic. The volume contains revised and edited versions of 24 refereed papers and one invited paper presented at the conference.

## TABLE OF CONTENTS

Commitment schemes and diophantine equations — José Felipe Voloch	1
Supersingular curves with small noninteger endomorphisms — Jonathan Love and Dan Boneh	7
Cubic post-critically finite polynomials defined over $\mathbb{Q}$ — Jacqueline Anderson, Michelle Manes and Bella Tobin	23
Faster computation of isogenies of large prime degree — Daniel J. Bernstein, Luca De Feo, Antonin Leroux and Benjamin Smith	39
On the security of the multivariate ring learning with errors problem — Carl Bootland, Wouter Castryck and Frederik Vercauteren	57
Two-cover descent on plane quartics with rational bitangents — Nils Bruin and Daniel Lewis	73
Abelian surfaces with fixed 3-torsion — Frank Calegari, Shiva Chidambaram and David P. Roberts	91
Lifting low-gonal curves for use in Tuitman's algorithm — Wouter Castryck and Floris Vermeulen	109
Simultaneous diagonalization of incomplete matrices and applications — Jean-Sébastien Coron, Luca Notarnicola and Gabor Wiese	127
Hypergeometric $L$ -functions in average polynomial time — Edgar Costa, Kiran S. Kedlaya and David Roe	143
Genus 3 hyperelliptic curves with CM via Shimura reciprocity — Bogdan Adrian Dina and Sorina Ionica	161
A canonical form for positive definite matrices — Mathieu Dutour Sikirić, Anna Haensch, John Voight and Wessel P.J. van Woerden	179
Computing Igusa's local zeta function of univariates in deterministic polynomial-time — Ashish Dwivedi and Nitin Saxena	197
Computing endomorphism rings of supersingular elliptic curves and connections to path-finding in isogeny graphs — Kirsten Eisenträger, Sean Hallgren, Chris Leonardi, Travis Morrison and Jennifer Park	215
New rank records for elliptic curves having rational torsion — Noam D. Elkies and Zev Klagsbrun	233
The nearest-colattice algorithm: Time-approximation tradeoff for approx-CVP — Thomas Espitau and Paul Kirchner	251
Cryptanalysis of the generalised Legendre pseudorandom function — Novak Kaluđerović, Thorsten Kleinjung and Dušan Kostić	267
Counting Richelot isogenies between superspecial abelian surfaces — Toshiyuki Katsura and Katsuyuki Takashima	283
Algorithms to enumerate superspecial Howe curves of genus 4 — Momonari Kudo, Shushi Harashita and Everett W. Howe	301
Divisor class group arithmetic on $C_{3,4}$ curves — Evan MacNeil, Michael J. Jacobson Jr. and Renate Scheidler	317
Reductions between short vector problems and simultaneous approximation — Daniel E. Martin	335
Computation of paramodular forms — Gustavo Rama and Gonzalo Tornaría	353
An algorithm and estimates for the Erdős–Selfridge function — Brianna Sorenson, Jonathan Sorenson and Jonathan Webster	371
Totally $p$ -adic numbers of degree 3 — Emerald Stacy	387
Counting points on superelliptic curves in average polynomial time — Andrew V. Sutherland	403