Algebra & Number Theory

Volume 5
2011
No. 4

Explicit CM theory for level 2-structures on abelian surfaces

Reinier Bröker, David Gruenewald and Kristin Lauter

mathematical sciences publishers

ALGEBRA AND NUMBER THEORY 5:4(2011)

msp

Explicit CM theory for level 2-structures on abelian surfaces

Reinier Bröker, David Gruenewald and Kristin Lauter

For a complex abelian surface A with endomorphism ring isomorphic to the maximal order in a quartic CM field K, the Igusa invariants $j_1(A)$, $j_2(A)$, $j_3(A)$ generate an unramified abelian extension of the reflex field of K. In this paper we give an explicit geometric description of the Galois action of the class group of this reflex field on $j_1(A)$, $j_2(A)$, $j_3(A)$. Our description can be expressed by maps between various Siegel modular varieties, and we can explicitly compute the action for ideals of small norm. We use the Galois action to modify the CRT method for computing Igusa class polynomials, and our run time analysis shows that this yields a significant improvement. Furthermore, we find cycles in isogeny graphs for abelian surfaces, thereby implying that the 'isogeny volcano' algorithm to compute endomorphism rings of ordinary elliptic curves over finite fields does not have a straightforward generalization to computing endomorphism rings of abelian surfaces over finite fields.

1. Introduction

Class field theory describes the abelian extensions of a given number field K. For $K = \mathbb{Q}$, the Kronecker–Weber theorem tells us that every abelian extension of K is contained in a *cyclotomic extension*. In 1900, Hilbert asked for a similar 'explicit description' for higher degree number fields. This is known as Hilbert's twelvth problem, and it is still largely unsolved.

Besides $K = \mathbb{Q}$, the answer is only completely known for imaginary quadratic fields. In this case, the solution is provided by *complex multiplication* theory; see for example [Silverman 1994, Chapter 2]. The techniques used can be generalized to *CM fields*, that is, imaginary quadratic extensions of totally real fields. However, for general CM fields we do not always get an explicit description of the *maximal* abelian extension. From a computational perspective, the case of general CM fields is far less developed than the imaginary quadratic case.

Gruenewald thanks Microsoft Research, where this research was undertaken, for its hospitality.
MSC2000: 11G15.
Keywords: abelian surface, isogeny, level structure.

In this article, we solely focus on degree 4 primitive CM fields K. For such fields, invariants of principally polarized abelian surfaces (p.p.a.s.) with endomorphism ring isomorphic to the maximal order $\mathbb{O}_K$ of K generate a subfield of the Hilbert class field of the *reflex field* of K (a degree 4 subfield of the normal closure of K). To explicitly compute the resulting extension, we compute an *Igusa class polynomial*

$$P_K = \prod_{\{A \text{ p.p.a.s} \mid \mathrm{End}(A)=\mathbb{O}_K\}/\cong} (X - j_1(A)) \in \mathbb{Q}[X].$$

Here, j_1 is one of the *three* Igusa invariants of A. A contrast with the case of imaginary quadratic fields — where we compute the *Hilbert class polynomial* — is that the polynomial P_K has rational coefficients that are not integers in general, and it need not be irreducible over $\mathbb{Q}$.

There are three methods to explicitly compute the polynomial P_K: complex analytic evaluation of the invariants [Spallek 1994; van Wamelen 1999; Weng 2003], the CRT method using finite field arithmetic [Eisenträger and Lauter 2009] and the computation of a canonical lift [Gaudry et al. 2006; Carls et al. 2008] using p-adic arithmetic for $p = 2, 3$. However, none of these three approaches exploit the Galois action of the maximal abelian extension of the reflex field on the set of principally polarized abelian surfaces with endomorphism ring $\mathbb{O}_K$. The goal of this article is to make this Galois action explicit and give a method to compute it.

Our algorithm to compute the Galois action significantly speeds up the CRT-approach described in [Eisenträger and Lauter 2009] to compute Igusa class polynomials and it can be used to improve the 3-adic approach [Carls et al. 2008] as well. The improvement in computing Igusa class polynomials parallels the improvements given in [Belding et al. 2008] for computing Hilbert class polynomials. Our run time analysis is similar to the analysis in [Belding et al. 2008]. Contrary to the genus 1 algorithm however, the genus 2 algorithm is not quasilinear in the size of the output. We suggest further refinements that might yield a quasilinear algorithm as area of further study in Section 6.

Besides speeding up the computation of Igusa class polynomials, our algorithm gives a method of computing *isogenous* abelian surfaces over finite fields. Computing an isogeny is a basic computational problem in arithmetic geometry, and we expect that our algorithm can be used in a variety of contexts, ranging from point counting on Jacobians of curves to cryptographic protocols.

Our computations naturally lead us to study the (l, l)-isogeny graph of abelian surfaces over finite fields. For ordinary elliptic curves, the l-isogeny graph looks like a volcano and this observation forms the heart of the algorithm [Kohel 1996] to compute the endomorphism ring of an ordinary elliptic curve over a finite field. We show that for abelian surfaces, the (l, l)-isogeny graph does *not* have a volcano

shape. This shows that a straightforward generalization of the elliptic curve algorithm to abelian surfaces does not work.

The structure of this paper is as follows. In Section 2 we recall the basic facts of complex multiplication theory and background on CM abelian surfaces and their invariants. In Section 3 we describe the Galois action on the set of isomorphism classes of abelian surfaces with CM by $\mathbb{O}_K$ in a geometric way. Our algorithm to compute this action is intrinsically linked to Siegel modular functions of higher level. Section 4 gives the definitions and properties of the four Siegel modular functions that we use. The algorithm to compute the Galois action is detailed in Section 5 and we apply it in Section 6 to improving the method to compute an Igusa class polynomial modulo a prime p. We give a detailed run time analysis of our algorithm in Section 6 as well. We illustrate our approach with various detailed examples in Section 7. A final Section 8 contains the obstruction to the volcano picture for abelian surfaces.

2. CM abelian surfaces

2.1. ***CM theory.*** In this section we recall the basic facts of CM theory for higher dimensional abelian varieties. Most of the material presented in this section is an adaptation to our needs of the definitions and proofs of Shimura's [1998] and Lang's [1983] textbooks.

We fix an embedding of $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. By a real number field, we mean a field that is fixed by complex conjugation. With this convention, a *CM field* K is a totally imaginary quadratic extension of a totally real number field. Let K^+ denote the real quadratic subfield of K, and let n be the degree of K^+ over $\mathbb{Q}$. The $2n$ embeddings $K \hookrightarrow \overline{\mathbb{Q}}$ naturally come in pairs. Indeed, we can choose n embeddings $\Phi = \{\varphi_1, \ldots, \varphi_n\}$ such that we have $\mathrm{Hom}(K, \overline{\mathbb{Q}}) = \Phi \cup \overline{\Phi}$. We call such a set Φ a *CM type* for K, and we interpret a CM type in the natural way as a map $K \hookrightarrow \mathbb{C}^n$.

If Φ *cannot* be obtained as a lift of a CM type of a CM subfield of K, then we call Φ *primitive*. For instance, in the simplest case $K^+ = \mathbb{Q}$, CM fields K are imaginary quadratic and every choice for $K \hookrightarrow \overline{\mathbb{Q}}$ determines a primitive CM type. If K has degree, four then every choice of a CM type is primitive when K does not contain an imaginary quadratic field. It is not hard to show [Shimura 1998, Section 8.4] that this occurs exactly for $\mathrm{Gal}(L/\mathbb{Q}) = D_4, C_4$, where L denotes the normal closure of K. We say that the field K is primitive in this case.

In this article, we will only consider primitive quartic CM fields K. For the remainder of this section, we fix such a field K. We say that a principally polarized abelian surface $A/\mathbb{C}$ has *CM* by the maximal order $\mathbb{O}_K$ if there exists an isomorphism $\mathbb{O}_K \xrightarrow{\sim} \mathrm{End}(A)$. The CM type distinguishes these surfaces. More precisely, a surface A that has CM by $\mathbb{O}_K$ has *type* $\Phi = \{\varphi_1, \varphi_2\}$ if the complex

representation $R_{\mathbb{C}}$ of the endomorphism algebra $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ satisfies

$$R_{\mathbb{C}} \cong \varphi_1 \oplus \varphi_2.$$

One shows [Lang 1983, Theorem 1.3.6] that a principally polarized abelian surface that has CM by $\mathbb{O}_K$ of type Φ is *simple*, that is, is not isogenous to the product of elliptic curves.

Let Φ be a CM type for K. For an $\mathbb{O}_K$-ideal I, the quotient $A_I = \mathbb{C}^2/\Phi(I)$ is an abelian surface of type Φ by [Lang 1983, Theorem 4.1]. This surface need not admit a principal polarization. The dual variety of A_I is given by $\hat{A}_I = \mathbb{C}^2/\Phi(\bar{I}^{-1}\mathfrak{D}_K^{-1})$, where

$$\mathfrak{D}_K^{-1} = \{x \in K \mid \mathrm{Tr}_{K/\mathbb{Q}}(x\mathbb{O}_K) \subseteq \mathbb{Z}\}$$

is the inverse different and $\bar{I}$ denotes the complex conjugate of I. If $\pi \in K$ satisfies $\Phi(\pi) \in (i\mathbb{R}_{>0})^2$ and $\pi\mathfrak{D}_K = (I\bar{I})^{-1}$, then the map $A_I \to \hat{A}_I$ given by

$$(z_1, z_2) \mapsto (\varphi_1(\pi)z_1, \varphi_2(\pi)z_2)$$

is an isomorphism [Shimura 1998, pages 102–104] and A_I is principally polarizable. All principally polarized abelian surfaces with CM by $\mathbb{O}_K$ of type Φ arise via this construction.

Let L be the normal closure of K. We extend Φ to a CM type Φ' of L, and we define the *reflex field*

$$K_\Phi = \mathbb{Q}\big(\big\{\textstyle\sum_{\phi\in\Phi'} \phi(x) \mid x \in K\big\}\big).$$

The CM type on K induces a CM type $f_\Phi = \{\sigma^{-1}|_{K_\Phi} : \sigma \in \Phi'\}$ of the reflex field K_Φ. The field K_Φ is a subfield of L of degree 4. In particular, it equals K in the case K is Galois. If $L/\mathbb{Q}$ is dihedral, then K_Φ and K are not isomorphic. However, the two different CM types yield isomorphic reflex fields in this case. Furthermore, we have

$$(K_\Phi)_{f_\Phi} = K$$

and the induced CM type on $(K_\Phi)_{f_\Phi}$ equals Φ.

An automorphism σ of K induces an isomorphism $(A, \Phi) \xrightarrow{\sim} (A^\sigma, \Phi^\sigma)$ of CM abelian surfaces, where $\Phi^\sigma = \{\varphi_1\sigma, \varphi_2\sigma\}$. Thus two CM types that are complex conjugates of each other produce the same sets of isomorphism classes of abelian surfaces. In the Galois case there is only one CM type up to isomorphism and in the dihedral case there are two distinct CM types.

2.2. ***Igusa invariants.*** Any principally polarized abelian surface over $\mathbb{C}$ is of the form $A_\tau = \mathbb{C}^2/(\mathbb{Z}^2 + \mathbb{Z}^2\tau)$, where τ is an element of the *Siegel upper half plane*

$$\mathbb{H}_2 = \{\tau \in \mathrm{Mat}_2(\mathbb{C}) \mid \tau \text{ symmetric}, \Im(\tau) \text{ positive definite}\}.$$

The moduli space $\mathcal{A}_2$ of principally polarized abelian surfaces is 3-dimensional. We are mostly interested in the subspace $\mathcal{M}_2 \subset \mathcal{A}_2$ of Jacobians of curves. The structure of $\mathcal{M}_2$ is well known; we recall it for convenience. Let

$$Y^2 = a_6X^6 + \cdots + a_0 = f(X)$$

be a genus 2 curve and write $\alpha_1, \ldots, \alpha_6$ for the roots of f. For simplifying notation, let (ij) denote the quantity $(\alpha_{k_i} - \alpha_{k_j})$ for a given ordering of the roots. The *Igusa–Clebsch invariants* I_2, I_4, I_6, I_{10} (denoted by A, B, C, D in [Igusa 1960, Section 3]) are defined by

$$\begin{aligned}
I_2 &= a_6^2 \sum_{15} (12)^2(34)^2(56)^2,\\
I_4 &= a_6^4 \sum_{10} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2,\\
I_6 &= a_6^6 \sum_{60} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2(14)^2(25)^2(36)^2,\\
I_{10} &= a_6^{10} \sum_{i<j} (ij) = a_6^{10} \operatorname{disc}(f),
\end{aligned}$$

where we sum over all root orderings $\{\alpha_{k_i}\}$ that give distinct summands; the subscript indicates the number of terms we sum over.

Theorem 2.1. *The moduli space $\mathcal{M}_2$ is isomorphic to*

$$\{[I_2 : I_4 : I_6 : I_{10}] \in \mathbb{P}^3_w(\mathbb{C}) \mid I_{10} \neq 0\},$$

where $\mathbb{P}^3_w$ denotes weighted projective space with weights 2, 4, 6 *and* 10.

Proof. See [Igusa 1960]. □

We note that the condition $I_{10} \neq 0$ ensures that the polynomial f defining the genus 2 curve is separable.

Instead of working with a subset of weighted projective space, many people work with an affine subspace of $\mathcal{M}_2$. This nonweighted subspace is given by

$$(j_1, j_2, j_3) = \left(\frac{I_2^5}{I_{10}}, \frac{I_4 I_2^3}{I_{10}}, \frac{I_6 I_2^2}{I_{10}}\right).$$

The functions j_i are commonly called the *Igusa functions*. We remark that there are various definitions of these functions and there are different opinions for which choice is the best. Our functions are the same as those in [van Wamelen 1999], for example. They have the property that for τ, τ' corresponding to Jacobians of curves, the equality $j_i(\tau) = j_i(\tau') \neq 0$ for $i = 1, 2, 3$ implies that C and C' are isomorphic. A detailed description on computing $j_i(\tau)$ for a point $\tau \in \mathbb{H}_2$ can be found in [Dupont 2006; Weng 2003].

A weak version of the main theorem of complex multiplication theory is that, for a primitive quartic CM field K, the Igusa invariants of an abelian variety with CM by $\mathbb{O}_K$ generate an unramified abelian extension of a reflex field of K. More precisely, we have the following result.

Theorem 2.2 [Spallek 1994, Theorem 5.8]. *Let (K, Φ) be a primitive quartic CM type. Let I be an $\mathbb{O}_K$-ideal with the property that there exists a principal polarization on $A_I = \mathbb{C}^2/\Phi(I)$. Then the field $K_\Phi(j_1(A_I), j_2(A_I), j_3(A_I))$ is a subfield of the Hilbert class field of K_Φ. The polynomial*

$$P_K = \prod_A (X - j_1(A)),$$

with A ranging over the isomorphism classes of principally polarized abelian surfaces with endomorphism ring $\mathbb{O}_K$, has rational coefficients. The same is true for the polynomials Q_K and R_K for the j_2 and j_3-invariants.

We will see in Corollary 3.3 that, for any primitive CM type Φ, there always exists an $\mathbb{O}_K$-ideal I such that A_I is principally polarizable.

3. CM action

Throughout this section, we let K be a fixed primitive quartic CM field. We also fix a CM type $\Phi : K \hookrightarrow \mathbb{C}^2$ and let $A/\mathbb{C}$ be a principally polarized abelian surface that has complex multiplication by $\mathbb{O}_K$ of CM type Φ.

3.1. ***Galois action of the class group.*** We define a group $\mathfrak{C}(K)$ as

$$\{(\mathfrak{a}, \alpha) \mid \mathfrak{a} \text{ a fractional } \mathbb{O}_K\text{-ideal with } \mathfrak{a}\bar{\mathfrak{a}} = (\alpha) \text{ and } \alpha \in K^+ \text{ totally positive}\}/\sim,$$

where two pairs $(\mathfrak{a}, \alpha)$ and $(\mathfrak{b}, \beta)$ are equivalent if and only if there exists a unit $u \in K^*$ with $\mathfrak{b} = u\mathfrak{a}$ and $\beta = u\bar{u}\alpha$. The multiplication is defined componentwise, and $(\mathbb{O}_K, 1)$ is the neutral element of $\mathfrak{C}(K)$.

The group $\mathfrak{C}(K)$ naturally acts on the finite set $S(K, \Phi)$ of isomorphism classes of principally polarized abelian surfaces that have CM by $\mathbb{O}_K$ of a given type Φ. Indeed, any such surface is given by an ideal I determining the variety and a 'Φ-positive' element $\pi \in K$ giving the principal polarization. We now put

$$(\mathfrak{a}, \alpha) \cdot (I, \pi) = (\mathfrak{a}I, \alpha\pi) \quad \text{for } (\mathfrak{a}, \alpha) \in \mathfrak{C}(K).$$

By [Shimura 1998, Section 14.6], the action of $\mathfrak{C}(K)$ on $S(K, \Phi)$ is transitive and free. In particular, we have $|\mathfrak{C}(K)| = |S(K, \Phi)|$.

The structure of the group $\mathfrak{C}(K)$ is best described by the following theorem. Denote by $\mathrm{Cl}^+(\mathbb{O}_{K^+})$ the narrow class group of $\mathbb{O}_{K^+}$ and write $(\mathbb{O}_{K^+}^*)^+$ for the group of totally positive units of $\mathbb{O}_{K^+}$.

Theorem 3.1. *Let K be a primitive quartic CM field. Then the sequence*

$$1 \to (\mathcal{O}_{K^+}^*)^+/N_{K/K^+}(\mathcal{O}_K^*) \xrightarrow{u\mapsto(\mathcal{O}_K,u)} \mathfrak{C}(K) \xrightarrow{(\mathfrak{a},\alpha)\mapsto\mathfrak{a}} \mathrm{Cl}(\mathcal{O}_K) \xrightarrow{N_{K/K^+}} \mathrm{Cl}^+(\mathcal{O}_{K^+}) \to 1$$

is exact.

Proof. The exactness at $(\mathcal{O}_{K^+}^*)^+/N_{K/K^+}(\mathcal{O}_K^*)$ is [Shimura 1998, Section 14.5]. It remains to show that the sequence is exact at $\mathrm{Cl}^+(\mathcal{O}_{K^+})$. To prove this, we first prove[1] that there is a *finite* prime that is ramified in K/K^+.

Suppose that K/K^+ is unramified at all finite primes. By genus theory, we then have $K = K^+(\sqrt{n})$ with $n \in \mathbb{Z}$. However, K then has $\mathbb{Q}(\sqrt{n})$ as quadratic subfield and K is a biquadratic field. This contradicts our assumption that K is primitive.

Because there is a finite prime of K^+ that ramifies in K, the extensions K/K^+ and $H^+(K^+)/K^+$ are linearly disjoint. Here, H^+ denotes the narrow Hilbert class field. By Galois theory, we then have

$$\mathrm{Gal}(H(K)/K) \twoheadrightarrow \mathrm{Gal}(KH^+(K^+)/K) \xrightarrow{\sim} \mathrm{Gal}(H^+(K^+)/K^+). \qquad \square$$

Remark 3.2. The surjectivity of the last arrow was also proved in [Kohel 2008, Lemma 2.1] under the assumption that there exists a finite prime that ramifies in K/K^+. Our proof shows in fact that such a prime always exists.

Corollary 3.3. *Let K be a primitive quartic CM field. The set $S(K)$ of isomorphism classes of principally polarized abelian surfaces with CM by $\mathcal{O}_K$ has cardinality*

$$|S(K)| = \begin{cases} |\mathfrak{C}(K)| & \text{if } \mathrm{Gal}(K/\mathbb{Q}) \cong C_4, \\ 2|\mathfrak{C}(K)| & \text{if } \mathrm{Gal}(K/\mathbb{Q}) \cong D_4. \end{cases}$$

Proof. By Theorem 3.1, the cardinality $|S(K, \Phi)| = |\mathfrak{C}(K)|$ is independent of the choice of a CM type Φ. If we let n denote the number of CM types up to conjugacy, then the theorem follows immediately from the equality

$$|S(K)| = n|S(K, \Phi)|. \qquad \square$$

The Galois group $\mathrm{Gal}(K_\Phi(j_1(A))/K_\Phi)$ acts in the following way on the set $S(K, \Phi)$. With f_Φ the CM type on K_Φ induced by Φ, we define $N_\Phi : K_\Phi \to K$ by

$$N_\Phi(x) = \prod_{\varphi\in f_\Phi} \varphi(x).$$

For an $\mathcal{O}_{K_\Phi}$-ideal I, the $\mathcal{O}_K$-ideal $N_\Phi(I)$ is called the *typenorm* of I. We get a natural map $m : \mathrm{Cl}(\mathcal{O}_{K_\Phi}) \to \mathfrak{C}(K)$ defined by

$$m(\mathfrak{p}) = (N_\Phi(\mathfrak{p}), N_{K_\Phi/\mathbb{Q}}(\mathfrak{p})) \quad \text{for degree 1 prime representatives } \mathfrak{p}.$$

[1] We thank Everett Howe for suggesting this argument.

The Galois group of $K_\Phi(j_1(A))/K_\Phi$ is a quotient of $\mathrm{Gal}(H(K_\Phi)/K_\Phi) \cong \mathrm{Cl}(\mathbb{O}_{K_\Phi})$, and by [Shimura 1998, Section 15.2], the induced map

$$m : \mathrm{Gal}(K_\Phi(j_1(A))/K_\Phi) \to \mathfrak{C}(K)$$

is *injective*. This describes the Galois action. Indeed, the group $\mathfrak{C}(K)$ acts on the set of all principally polarized abelian surfaces that have CM by $\mathbb{O}_K$, and m maps the Galois group injectively into $\mathfrak{C}(K)$. In Example 7.2 we will see that the natural map $\mathrm{Cl}(\mathbb{O}_{K_\Phi}) \to \mathfrak{C}(K)$ need not be injective.

The typenorm can be defined in a slightly different way as well. If $K/\mathbb{Q}$ is Galois with $\mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma\rangle$, then for $\Phi = \{1, \sigma\}$ we have $N_\Phi(\mathfrak{p}) = \mathfrak{p}^{1+\sigma^3}$. If K is not Galois, then we have $N_\Phi(\mathfrak{p}) = N_{L/K}(\mathfrak{p}\mathbb{O}_L)$. We will use this description both for actual computations and in the proof of Lemma 6.5.

In the remainder of Section 3.1, we provide the theoretical framework that will allow us to explicitly compute the CM action. Let I be a $\mathbb{O}_{K_\Phi}$-ideal of norm l. We assume for simplicity that l is prime. We have $m(I) = (N_\Phi(I), l) = (J, l) \in \mathfrak{C}(K)$, where J is an $\mathbb{O}_K$-ideal of norm l^2.

Lemma 3.4. *Let I be an $\mathbb{O}_{K_\Phi}$-ideal of prime norm l with typenorm $N_\Phi(I) = J \subset \mathbb{O}_K$. Then J divides $(l) \subset \mathbb{O}_K$.*

Proof. This follows from the relation $N_\Phi(I)\overline{N_\Phi(I)} = N_{K_\Phi/\mathbb{Q}}(I) = l$. □

For an $\mathbb{O}_K$-ideal M, we define the M-torsion of the abelian surface A by

$$A[M] = \{P \in A(\mathbb{C}) \mid \text{for all } \alpha \in M : \alpha(P) = 0\}.$$

We assume here that we have *fixed* an isomorphism $\mathrm{End}(A) \xrightarrow{\sim} \mathbb{O}_K$, meaning that M is an $\mathrm{End}(A)$-ideal as well. If M is generated by an integer n, then $A[M]$ equals the n-torsion $A[n]$.

Lemma 3.4 implies that $A[J]$ is a 2-dimensional subspace of the l-torsion $A[l]$ of A. The polarization of A induces a symplectic form on $A[l]$, and $A[l]$ is a *symplectic* vector space of dimension 4 over the finite field $\mathbb{F}_l$. By CM theory we know that the quotient $A/A[J]$ is again a *principally polarized* abelian surface. By [Mumford 1970, Section 23], this implies that $A[J]$ is an *isotropic* 2-dimensional subspace of $A[l]$, that is, the symplectic form vanishes on $A[J]$. We recall that an isogeny $A \to B$ between principally polarized abelian surfaces whose kernel is a 2-dimensional isotropic subspace of $A[l]$ is called an (l, l)-*isogeny*, and $A \to A/A[J]$ is an example of an (l, l)-isogeny.

The moduli space of all pairs (A, G), with A a principally polarized abelian surface over $\mathbb{C}$ and G a 2-dimensional isotropic subspace of $A[l]$, can be described by an ideal $V(l) \subset \mathbb{Q}[X_1, Y_1, Z_1, X_2, Y_2, Z_2]$. More precisely, the variety corresponding to $V(l)$ equals the Siegel modular variety $Y_0^{(2)}(l)$ studied, for example,

in [Bröker and Lauter 2009]. As a complex Riemann surface, we have

$$Y_0^{(2)}(l) = \Gamma_0^{(2)}(l) \setminus \mathbb{H}_2,$$

with

$$\Gamma_0^{(2)}(l) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{Sp}_4(\mathbb{Z}) \mid c \equiv 0_2 \bmod l \right\}.$$

If we specialize $V(l)$ at a point $(X_1, Y_1, Z_1) = (j_1(A), j_2(A), j_3(A))$, the resulting ideal $V'(l)$ is 0-dimensional. The corresponding variety is a union of points corresponding to the '(l, l)-isogenous abelian surfaces'. Since there are $[\mathrm{Sp}_4(\mathbb{Z}) : \Gamma_0^{(2)}(l)] = (l^4 - 1)/(l - 1)$ isotropic subspaces of dimension 2 in $A[l]$ by [Bröker and Lauter 2009, Lemma 6.1], there are exactly $(l^4 - 1)/(l - 1)$ solutions to the system of equations given by V'. By construction, the triple

$$(j_1(A/J), j_2(A/J), j_3(A/J))$$

is one of the solutions. There are $l^3 + l^2 + l$ other solutions, and we will see in Section 6 that for CM computations it is relatively easy to determine which of the solutions come from the typenorm of an $\mathbb{O}_{K_\Phi}$-ideal.

Unfortunately, the ideal $V(l)$ can only be computed for very small l. Indeed, the only case that has been done is $l = 2$ [Dupont 2006, Section 10.4.2] and it takes roughly 50 megabytes to store the 3 generators of V. By [Bröker and Lauter 2009], knowing the ideal $V(l)$ for some prime l implies that we have an equation for the *Humbert surface* of discriminant l^2. Since computing Humbert surfaces is a traditionally hard problem, we do not expect that much progress can be made in computing $V(l)$ for primes $l > 2$.

3.2. ***Richelot isogeny.*** Although one could use the ideal $V(2)$ from [Dupont 2006, Section 10.4.2] to compute $(2, 2)$-isogenies, there is a more efficient way. This alternative, known as the *Richelot isogeny*, is classical and we recall it here for convenience. Let K be a field of characteristic different from 2, and let C/K be a nonsingular genus 2 curve. We can choose an equation $Y^2 = f(X)$ for C, with $f \in K[X]$ a monic polynomial of degree 6. Any factorization $f = ABC$ into three monic degree 2 polynomials defines a genus 2 curve C' given by

$$\Delta Y^2 = [A, B][A, C][B, C],$$

where Δ is the determinant of A, B, C with respect to the basis $1, X, X^2$, and $[A, B] = A'B - AB'$ with A' the derivative of A. This new curve is nonsingular precisely when Δ is nonzero.

One proves [Bost and Mestre 1988] that C and C' are $(2, 2)$-isogenous. It is not hard to see that there are exactly $15 = (2^4 - 1)/(2 - 1)$ different curves C' that can be obtained this way. It follows that this construction gives all $(2, 2)$-isogenous Jacobians $\mathrm{Jac}(C')$.

4. Smaller functions

The Igusa functions introduced in Section 2 are 'too large' to be practical in our computation of the CM action: currently we cannot compute an ideal describing the variety $Y_0^2(l)$ for primes $l > 2$. In this section we introduce smaller functions $f_1, \ldots, f_4$ that are more convenient from a computational perspective. For $N > 1$, we define the *congruence subgroup* of level N as the kernel of the reduction map $\mathrm{Sp}_4(\mathbb{Z}) \to \mathrm{Sp}_4(\mathbb{Z}/N\mathbb{Z})$, denoted by $\Gamma(N)$.

For $x, y \in \{0, 1\}^2$, define the functions $\theta_{x,y} : \mathbb{H}_2 \to \mathbb{C}$ by

$$\theta_{x,y}(\tau) = \sum_{n \in \mathbb{Z}^2} \exp \pi i \big((n + \tfrac{1}{2}x)^T \tau (n + \tfrac{1}{2}x) + (n + \tfrac{1}{2}x)^T y \big). \tag{4-1}$$

The functions $\theta_{x,y}$ are known as the *theta constants* and arise naturally from the construction of theta functions [Igusa 1964]. The equality $\theta_{x,y}(\tau) = (-1)^{x^T y}\theta_{x,y}(\tau)$ shows that only 10 of the 16 theta constants are nonzero.

The fourth powers of the functions $\theta_{x,y}$ are Siegel modular forms of weight 2 for the congruence subgroup $\Gamma(2) \subset \mathrm{Sp}_4(\mathbb{Z})$. The Satake compactification $X(2)$ of the quotient $\Gamma(2) \setminus \mathbb{H}_2$ has a natural structure of a projective variety, and the fourth powers $\theta_{x,y}^4$ define an embedding of $X(2)$ into projective space.

Theorem 4.1 [van der Geer 1982, Theorem 5.2]. *Let $M_2(\Gamma(2))$ denote the $\mathbb{C}$-vector space of all Siegel modular forms of weight 2 for the congruence subgroup $\Gamma(2)$. Then the space $M_2(\Gamma(2))$ is 5-dimensional and is spanned by the ten modular forms $\theta_{x,y}^4$. Furthermore, the map $X(2) \to \mathbb{P}^4 \subset \mathbb{P}^9$ defined by the functions $\theta_{x,y}^4$ is an embedding. The image is the quartic threefold in $\mathbb{P}^4$ defined by*

$$u_2^2 - 4u_4 = 0 \quad \textit{with} \quad u_k = \sum_{x,y} \theta_{x,y}^{4k}.$$

The Igusa functions j_1, j_2, j_3 can be readily expressed in terms of $\theta_{x,y}^4$; see for example [Igusa 1967, page 848]. Thus we have an inclusion

$$\mathbb{C}(j_1, j_2, j_3) \subseteq \mathbb{C}(\theta_{x,y}^4/\theta_{x',y'}^4)$$

where we include *all* quotients of theta fourth powers. The functions $\theta_{x,y}^4/\theta_{x',y'}^4$ are rational Siegel modular *functions* of level 2. Whereas $(j_1(\tau), j_2(\tau), j_3(\tau))$ depends only on the $\mathrm{Sp}_4(\mathbb{Z})$-equivalence class of $\tau \in \mathbb{H}_2$, a value $(\theta_{x,y}^4(\tau)/\theta_{x',y'}^4(\tau))_{x,x',y,y'}$ depends on the $\Gamma(2)$-equivalence class of τ. Since the affine points of $\Gamma(2) \setminus \mathbb{H}_2 \subset X(2)$ correspond to isomorphism classes of pairs $(A, \{P_1, P_2, P_3, P_4\})$ consisting of a principally polarized 2-dimensional abelian variety A together with a basis $\{P_1, P_2, P_3, P_4\}$ of the 2-torsion, the functions $\theta_{x,y}^4/\theta_{x',y'}^4$ not only depend on the abelian variety in question but also on an ordering of its 2-torsion. For every isomorphism class $\mathrm{Sp}_4(\mathbb{Z})\tau$ of abelian varieties, there are $[\mathrm{Sp}_4(\mathbb{Z}) : \Gamma(2)] = 720$

values for the tuple $(\theta^4_{x,y}(\tau)/\theta^4_{x',y'}(\tau))_{x,x',y,y'}$. The functions $\theta^4_{x,y}/\theta^4_{x',y'}$ are smaller than the Igusa functions in the sense that their Fourier coefficients are smaller. A natural idea is to get even smaller functions by considering the quotients $\theta_{x,y}/\theta_{x',y'}$ themselves instead of their fourth powers.

We define the four functions $f_1, f_2, f_3, f_4 : \mathbb{H}_2 \to \mathbb{C}$ by

$$f_1 = \theta_{(0,0),(0,0)} \quad f_2 = \theta_{(0,0),(1,1)} \quad f_3 = \theta_{(0,0),(1,0)} \qquad f_4 = \theta_{(0,0),(0,1)},$$

with $\theta_{(x,y),(x',y')} = \theta_{x,y}/\theta_{x',y'}$. We stress that the particular choice of the 'theta constants' is rather arbitrary; our only requirement is that we define 4 different functions. The three quotients $f_1/f_4, f_2/f_4, f_3/f_4$ are rational Siegel modular functions.

Theorem 4.2. *If $\tau, \tau' \in \mathbb{H}_2$ satisfy $(f_1(\tau), \ldots, f_4(\tau)) = (f_1(\tau'), \ldots, f_4(\tau'))$, then we have $(j_1(\tau), j_2(\tau), j_3(\tau)) = (j_1(\tau'), j_2(\tau'), j_3(\tau'))$. Furthermore, the quotients $f_1/f_4, f_2/f_4, f_3/f_4$ are invariant under the subgroup $\Gamma(8)$.*

Proof. The vector space $M_2(\Gamma(2))$ is spanned by $\{f_1^4, \ldots f_4^4, g^4\}$, where $g = \theta_{(0,1),(0,0)}$. The relation in Theorem 4.1, together with the five linear relations between the $\theta^4_{x,y}$ from Riemann's theta formula [Igusa 1964, page 232], yield that g^4 satisfies a degree 4 polynomial P over $L = \mathbb{C}(f_1, f_2, f_3, f_4)$. The polynomial P factors over L as a product of the 2 irreducible quadratic polynomials

$$P_-, P_+ = T^2 - (f_1^4 - f_2^4 + f_3^4 - f_4^4)T + (f_1^2 f_3^2 \pm f_2^2 f_4^2)^2.$$

By looking at the Fourier expansions of $f_1, \ldots, f_4$ and g, we see that g^4 is a root of P_-. Hence, the extension $L(g^4)/L$ is quadratic and generated by a root of P_-.

For each of the 2 choices of a root of P_-, the other 5 fourth powers of theta functions will be uniquely determined. Indeed, the fourth powers are functions on the space $M_2(\Gamma(2))$ and this space is 5-dimensional by Theorem 4.1. This means that we get a priori *two* Igusa triples (j_1, j_2, j_3) for every tuple (f_1, f_2, f_3, f_4). However, a close inspection of the formulas expressing the Igusa functions in terms of theta fourth powers yields that these Igusa triples coincide. Hence, the triple (j_1, j_2, j_3) does not depend on the choice of a root of P_-. This proves the first statement in the theorem.

The second statement follows immediately from a result of Igusa, who proves in [Igusa 1964, page 242] that the field M generated by *all* theta quotients is invariant under a group that contains $\Gamma(8)$. Since the field $\mathbb{C}(f_1/f_4, f_2/f_4, f_3/f_4)$ is a subfield of M, Theorem 4.2 follows. □

Since the functions $f_1/f_4, f_2/f_4, f_3/f_4$ are invariant under $\Gamma(8)$, the moduli interpretation is that they depend on an abelian variety together with a level 8-structure. Let $\mathrm{Stab}(f)$ be the stabilizer of $f_1/f_4, f_2/f_4, f_3/f_4$ inside the symplectic

group $\mathrm{Sp}_4(\mathbb{Z})$. We have inclusions

$$\Gamma(8) \subset \mathrm{Stab}(f) \subset \mathrm{Sp}_4(\mathbb{Z})$$

and the quotient $Y(f) = \mathrm{Stab}(f) \setminus \mathbb{H}_2$ has a natural structure of a quasiprojective variety by the Baily–Borel theorem [1966]. However, this variety is not smooth.

We let

$$\mathbb{H}_2^* = \{\tau \in \mathbb{H}_2 \mid \tau \text{ is not } \mathrm{Sp}_4(\mathbb{Z})\text{-equivalent to a diagonal matrix}\}$$

be the subset of $\mathbb{H}_2$ of those τ that do not correspond to a product of elliptic curves with the product polarization. The argument in [Runge 1993, Section 5] shows that $G = \Gamma(8)/\mathrm{Stab}(f)$ acts freely on $Y(8)$. By [Mumford 1970, Chapter 2, Section 7], the quotient

$$Y(f)^* = \mathrm{Stab}(f) \setminus \mathbb{H}_2^*$$

is a *smooth* variety.

Lemma 4.3. *The map $Y(f)^* \to Y(1)$ induced by the inclusion $\mathrm{Stab}(f) \to \mathrm{Sp}_4(\mathbb{Z})$ has degree $23040 = 32 \cdot 720$.*

Proof. The map factors as $Y(f)^* \to Y(2) \to Y(1)$; thus it suffices to determine the degrees of each part. The degree of the map $Y(f)^* \to Y(2)$ can be seen from the proof of Theorem 4.2: given a projective tuple $(f_4^4, f_2^4, f_3^4, f_4, g^4)$ representing a point Q of $Y(2)$, over a splitting field there are $4^3 = 64$ projective tuples (f_1, f_2, f_3, f_4) and exactly half of these satisfy $P_- = 0$ and hence are valid preimages of Q. Thus $Y(f)^* \to Y(2)$ has degree 32. The degree of $Y(2) \to Y(1)$ equals $[\mathrm{Sp}_4(\mathbb{Z}) : \Gamma(2)] = 720$. This completes the proof. □

From a tuple $(f_1(\tau), \ldots, f_4(\tau))$, the proof of Theorem 4.2 shows how to compute an Igusa triple $(j_1(\tau), j_2(\tau), j_3(\tau))$. For convenience, we make this explicit in the next subsection.

4.1. ***Transformation formulas.*** As in the proof of Theorem 4.2, let $g = \theta_{(0,1),(0,0)}$. Now g^4 is a root of the quadratic polynomial P_-. From values (f_1, f_2, f_3, f_4), we can pick any root of P_- as a value for g^4. The functions $\{f_1^4, \ldots f_4^4, g^4\}$ form a basis of $M_2(\Gamma(2))$. Define new functions x_i by

$$\begin{aligned}
x_1 &= -f_1^4 + 2f_2^4 - f_3^4 + 2f_4^4 + 3g^4,\\
x_2 &= -f_1^4 + 2f_2^4 - f_3^4 - f_4^4,\\
x_3 &= -f_1^4 - f_2^4 - f_3^4 + 2f_4^4,\\
x_4 &= 2f_1^4 - f_2^4 - f_3^4 - f_4^4,\\
x_5 &= -f_1^4 - f_2^4 + 2f_3^4 - f_4^4,\\
x_6 &= 2f_1^4 - f_2^4 + 2f_3^4 - f_4^4 - 3g^4.
\end{aligned}$$

The x_i are called level 2 *Satake coordinate functions*. In terms of these functions we obtain a model for $X[2]$ embedded in $\mathbb{P}^5$ given by

$$s_1 = 0 \quad \text{and} \quad s_2^2 - 4s_4 = 0,$$

where $s_k = \sum_{i=1}^{6} x_i^k$ are the k-th power sums.

The action of $\mathrm{Sp}_4(\mathbb{Z})/\Gamma(2)$ on $x_i(\tau)$ is equivalent to that of $\mathrm{Sym}(\{x_1, \ldots, x_6\})$ permuting the coordinates. Thus we can write level 1 modular functions as symmetric functions of the x_i, and the *Igusa–Clebsch invariants* from Section 2.2 are given by

$$\begin{aligned} I_2 &= \frac{5(48s_6 - 3s_2^3 - 8s_3^2)}{3(12s_5 - 5s_2s_3)}, \\ I_4 &= 3^{-1}s_2^2, \\ I_6 &= 3^{-2}(3I_2I_4 - 2s_3), \\ I_{10} &= 2^{-2}3^{-6}5^{-1}(12s_5 - 5s_2s_3), \end{aligned}$$

from which we can compute absolute Igusa invariants (j_1, j_2, j_3).

Conversely, if $(j_i(\tau))$ corresponds to the Jacobian of a curve, then we can compute a value for $(f_1(\tau), \ldots, f_4(\tau))$ as follows. First we compute the Igusa–Clebsch invariants, then we apply the transformation

$$\begin{aligned} s_2 &= 3I_4, \\ s_3 &= 3/2(I_2I_4 - 3I_6), \\ s_5 &= 5/12s_2s_3 + 3^5 \cdot 5I_{10}, \\ s_6 &= 27/16I_4^3 + 1/6s_3^2 + 3^6/2^2I_2I_{10}, \end{aligned}$$

after which we can compute the level 2 Satake coordinate functions as the roots $x_1, \ldots, x_6$ of the *Satake sextic polynomial*

$$X^6 - \tfrac{1}{2}s_2X^4 - \tfrac{1}{3}s_3X^3 + \tfrac{1}{16}s_2^2X^2 + (\tfrac{1}{6}s_2s_3 - \tfrac{1}{5}s_5)X + (\tfrac{1}{96}s_2^3 + \tfrac{1}{18}s_3^2 - \tfrac{1}{6}s_6)$$

with coefficients in $\mathbb{Q}(s_2, s_3, s_5, s_6)$. One choice for f_1^4, f_2^4, f_3^4, f_4^4 is given by

$$\begin{aligned} f_1^4 &= (-x_2 - x_3 - x_5)/3, \\ f_2^4 &= (-x_3 - x_4 - x_5)/3, \\ f_3^4 &= (-x_2 - x_3 - x_4)/3, \\ f_4^4 &= (-x_2 - x_4 - x_5)/3. \end{aligned}$$

Finally, we extract fourth roots to find values for $(f_1(\tau), \ldots, f_4(\tau))$ satisfying $P_- = 0$. It is easy to find a solution to $P_- = 0$: if $(f_1, \ldots, f_4)$ is not a solution, then $(\sqrt{-1}f_1, \ldots, f_4)$ is a solution.

The coefficients of the Satake sextic polynomial are in $\mathbb{Z}[\frac{1}{2}, \frac{1}{3}, I_2, I_4, I_6, I_{10}]$. In particular, this means that our transformation formulas are also valid over finite fields of characteristic greater than 3.

5. The CM action and level structure

We let $\mathrm{Stab}(f)$ be the stabilizer of the three quotients f_1/f_4, f_2/f_4, f_3/f_4 defined in Section 4. By Theorem 4.2, we have $\Gamma(8) \subseteq \mathrm{Stab}(f)$. For a prime $l > 2$, we now define

$$Y(f; l)^* = (\mathrm{Stab}(f) \cap \Gamma_0^{(2)}(l)) \setminus \mathbb{H}_2^*$$

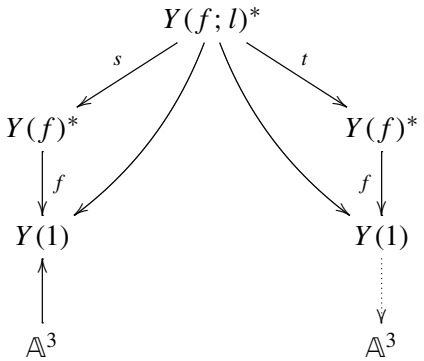
which we view as an equality of Riemann surfaces. By the Baily–Borel theorem, the space $Y(f; l)^*$ has a natural structure of a variety. Since we restricted to $\mathbb{H}_2^*$, the variety is affine. Just like in the case $l = 1$ from Section 4, $Y(f; l)^*$ is smooth.

The moduli interpretation of $Y(f; l)^*$ is the following. Points are isomorphism classes of triples (A, G, L), where A is a principally polarized complex abelian surface, G is a 2-dimensional isotropic subspace of $A[l]$, and L is a level 8-structure. The notion of isomorphism is that (A, G, L) and (A', G', L') are isomorphic if and only if there is an isomorphism $\varphi : A \to A'$ of principally polarized abelian surfaces that satisfies $\varphi(G) = G'$ and $\varphi(L) = L'$.

Lemma 5.1. *The map $Y(f; l)^* \to Y(f)^*$ that is induced by the inclusion map $(\mathrm{Stab}(f) \cap \Gamma_0^{(2)}(l)) \to \mathrm{Stab}(f)$ has degree $(l^4 - 1)/(l - 1)$ for primes $l > 2$.*

Proof. This is clear: the choice of a level 8-structure L is independent of the choice of a subspace of the l-torsion for $l > 2$. □

Besides the map $Y(f; l)^* \to Y(f)^*$ from the lemma, we also have a map $Y(f; l)^* \to Y(f)^*$ given by $(A, G, L) \mapsto (A/G, L')$. Indeed, the isogeny $\varphi : A \to A/G$ induces an isomorphism $A[8] \to (A/G)[8]$ and we have $L' = \varphi(L)$. As was explained in Section 3.2, this map also has degree $(l^4 - 1)/(l - 1)$. Putting all the varieties together, the picture is as follows.



The map s sends $(A, G, L) \in Y(f; l)^*$ to $(A, L) \in Y(f)^*$ and t is the map induced by the isogeny $A \to A/G$. This diagram allows us to find all the abelian surfaces that are (l, l)-isogenous to a given surface A, where we assume that A is the Jacobian of a genus 2 curve. Indeed, we first map the Igusa invariants $(j_1(A), j_2(A), j_3(A))$ to a point in $Y(1)$, say given by the Igusa–Clebsch invariants. We then *choose* (A, L) on $Y(f)^*$ lying over this point. Although there are 23040 choices for L, it does not matter which one we choose. Above (A, L), there are $(l^4-1)/(l-1)$ points in $Y(f; l)^*$ and via the map $t : Y(f; l)^* \to Y(f)^*$ we map all of these down to $Y(f)^*$. Forgetting the level 8-structure now yields $(l^4-1)/(l-1)$ points in $Y(1)$. If A is simple, that is, not isogenous to a product of elliptic curves, then we can transform these into absolute Igusa invariants.

Assuming we can compute an ideal

$$V(f; l) \subset \mathbb{Q}[W_1, X_1, Y_1, Z_1, W_2, X_2, Y_2, Z_2]$$

defining the quasiprojective variety $Y(f; l)^*$, we derive the following algorithm to compute all (l, l)-isogenous abelian surfaces.

Algorithm 5.2. Input: A Jacobian $A/\mathbb{C}$ of a genus 2 curve given by its Igusa invariants, and the ideal $V(f; l)$ defining $Y(f; l)^*$.

Output: The Igusa invariants of all principally polarized abelian surfaces that are (l, l)-isogenous to A.

(1) Compute Igusa–Clebsch invariants $(I_2, I_4, I_6, I_{10}) \in \mathbb{C}^4$ corresponding to A.

(2) Choose an element $(f_1, f_2, f_3, f_4) \in Y(f)^*$ that maps to (I_2, I_4, I_6, I_{10}) using the method described in Section 4.1.

(3) Specialize the ideal $V(f; l)$ in $(W_1, X_1, Y_1, Z_1) = (f_1, f_2, f_3, f_4)$ and solve the remaining system of equations.

(4) For each solution found in the previous step, compute the corresponding point in $Y(1)$ using the method given in Section 4.1.

5.1. ***Computing $V(f; l)$.*** In this subsection, we use an algorithm of Gruenewald [2008] to compute the ideal $V(f; l)$ needed in Algorithm 5.2. Our approach only terminates in a reasonable amount of time in the simplest case $l = 3$.

The expression for the theta constants in (4-1) can be written in terms of the individual matrix entries, and with some minor modifications we can represent it as a power series with integer coefficients. Writing $\tau = \left(\begin{smallmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{smallmatrix}\right) \in \mathbb{H}_2$, we have

$$\theta_{(a,b),(c,d)}(\tau) = (-1)^{\frac{ac+bd}{2}} \sum_{(x_1,x_2)\in\mathbb{Z}^2} (-1)^{x_1c+x_2d} p^{(2x_1+a)^2} q^{(2x_1+a+2x_2+b)^2} r^{(2x_2+b)^2}$$
$$\in \mathbb{Z}[[p, q, r]],$$

where $p = e^{2\pi i(\tau_1-\tau_2)/8}$, $q = e^{2\pi i\tau_2/8}$ and $r = e^{2\pi i(\tau_3-\tau_2)/8}$. We see that it is easy to compute Fourier expansions for the Siegel modular forms f_i.

One of the surfaces (l, l)-isogenous to $\mathbb{C}^2/(\mathbb{Z}^2 + \mathbb{Z}^2 \cdot \tau)$ is $\mathbb{C}^2/(\mathbb{Z}^2 + \mathbb{Z}^2 \cdot l\tau)$, and we want to find a relation between the f_i and the functions $f_i(l\tau)$. The expansion for $f_i(l\tau)$ can be constructed easily from the Fourier expansion of $f_i(\tau)$ by replacing p, q, r with p^l, q^l, r^l.

Starting with $n = 2$, we compute all homogeneous monomials of degree n in $f_i(\tau)$, $f_i(l\tau)$ represented as truncated power series and then use exact linear algebra to find linear dependencies between them. In this manner we obtain a basis for the degree n homogeneous component of the relation ideal. We then check experimentally whether our list of relations generate $V(f; l)$ or not by computing the degree of the projection maps. If one of the projection maps has degree larger than $l^3 + l^2 + l + 1$, then more relations are required, in which case we increment n by 1 and repeat the procedure. We stop once we have found sufficiently many relations to generate $V(f; l)$.

Using this method we computed the ideal $V(f; 3)$. The $(3, 3)$-isogeny relations in $V(f; 3)$ are given by 85 homogeneous polynomials of degree six. The whole ideal takes 35 kilobytes to store in a text file; see the online supplement. The individual relations are fairly small, having at most 40 terms. Furthermore, the coefficients are 7-smooth and bounded by 200 in absolute value, which makes them amenable for computations.

However, we have not rigorously proven that the ideal $V(f; 3)$ is correct. To do this we would need to show that our 85 polynomials define relations between Siegel modular forms rather than just truncated Fourier expansions. From the work of Poor and Yuen [2000] there is a computable bound for which a truncated Fourier expansion uniquely determines the underlying Siegel modular form. Thus with high enough precision our relations are able to be proven. A Gröbner basis computation in Magma [Bosma et al. 1997] informs us that the projection maps have the expected degree 40; hence we have obtained enough relations. Under the assumption that these relations hold, the ideal $V(f; 3)$ is correct.

Our $(3, 3)$-isogeny relations hold for all Jacobians of curves. We remark that if we restrict ourselves to CM-abelian surfaces defined over unramified extensions of $\mathbb{Z}_3$, then there are smaller $(3, 3)$-isogeny relations; see [Carls et al. 2008]. These smaller relations cannot be used however to improve the 'CRT-algorithm' as in Section 6.3.

6. The CM action over finite fields

6.1. ***Reduction theory.*** The theory we developed in Sections 3 through 5 uses the *complex analytic* definition of abelian surfaces and the Riemann surfaces $Y_0^{(2)}(l)$

and $Y(f;l)^*$. We now explain why we can use the results in *positive characteristic* as well. Firstly, if we take a prime p that splits completely in K, then by [Goren 1997, Theorems 1 and 2] the reduction modulo p of an abelian surface $A/H(K_\Phi)$ with endomorphism ring $\mathbb{O}_K$ is *ordinary*. The reduced surface again has endomorphism ring $\mathbb{O}_K$.

Furthermore, one can naturally associate an algebraic stack $\mathfrak{A}_{\Gamma_0(p)}$ to $Y_0^{(2)}(l)$ and prove that the structural morphism $\mathfrak{A}_{\Gamma_0(p)} \to \mathrm{Spec}(\mathbb{Z})$ is smooth outside l; see [Chai and Norman 1990, Corollary 6.1.1]. In more down-to-earth computational terminology, this means the moduli interpretation of the ideal $V \subset \mathbb{Q}[X_1, \ldots, Z_2]$ remains valid when we reduce the elements of V modulo a prime $p \neq l$.

The reduction of $Y(f;l)^*$ is slightly more complicated. The map $Y(8l) \to Y(f;l)^*$ is finite étale by [Katz and Mazur 1985, Theorem A.7.1.1], where we now view the affine varieties $Y(f;l)^*$ and $Y(8l)$ as schemes. It is well known that $Y(N)$ is smooth over $\mathrm{Spec}(\mathbb{Z}[1/N])$ for $N \geq 3$, so in particular, the scheme $Y(f;l)^*$ is smooth over $\mathrm{Spec}(\mathbb{Z}[1/(2l)])$. Again, this means that the moduli interpretation for the ideal $V(f;l) \subset \mathbb{Q}[W_1, \ldots, Z_2]$ remains valid when we reduce the elements of $V(f;l)$ modulo a prime $p \nmid 2l$.

We saw at the end of Section 4 that our transformation formulas are valid modulo p for primes $p > 3$. Putting this all together, we obtain the following result:

Lemma 6.1. *Let l be prime, and let $p \nmid 6l$ be a prime that splits completely in a primitive CM field K. On input of the Igusa invariants of a principally polarized abelian surface $A/\overline{\mathbb{F}}_p$ with $\mathrm{End}(A) = \mathbb{O}_K$ and the ideal $V(f;l) \subset \overline{\mathbb{F}}_p[W_1, \ldots, Z_2]$, Algorithm 5.2 computes the Igusa invariants of all (l,l)-isogenous abelian surfaces.*

6.2. ***Finding (l,l)-isogenous abelian surfaces.*** Now fix a primitive quartic CM field K, and let $p \nmid 6l$ be a prime that splits completely in the subfield

$$K_\Phi(j_1(A), j_2(A), j_3(A))$$

of the Hilbert class field of K_Φ. By the choice of p, the Igusa invariants of an abelian surface $A/\overline{\mathbb{F}}_p$ with $\mathrm{End}(A) = \mathbb{O}_K$ are defined over the prime field $\mathbb{F}_p$. Moreover, p splits in K_Φ and as it splits in its normal closure L it will split completely in K; hence Lemma 6.1 applies.

Algorithm 5.2 applied to the point $(j_1(A), j_2(A), j_3(A))$ and the ideal $V(f;l)$ yields $(l^4-1)/(l-1)$ triples of Igusa invariants. All these triples are Igusa invariants of principally polarized abelian surfaces with endomorphism *algebra* K; some are defined over the prime field $\mathbb{F}_p$ and some are not. However, since p splits completely in the field of moduli $K_\Phi(j_1(A), j_2(A), j_3(A))$, the Igusa invariants of the surfaces that have endomorphism ring $\mathbb{O}_K$ *are defined over the field* $\mathbb{F}_p$.

Algorithm 6.2. Input: The Igusa invariants of a simple principally polarized abelian surface $A/\mathbb{F}_p$ with $\mathrm{End}(A) = \mathbb{O}_K$, and the ideal $V(f; l) \subset \mathbb{F}_p[W_1, \ldots, Z_2]$. Here, l is a prime such that there exists a prime ideal in K_Φ of norm l. Furthermore, we assume that $p \nmid 6l$.

Output: The Igusa invariants of all principally polarized abelian surfaces $A'/\mathbb{F}_p$ with $\mathrm{End}(A') = \mathbb{O}_K$ that are (l, l)-isogenous to A.

(1) Apply Algorithm 5.2 to A and $V(f; l)$. Let S be the set of all Igusa invariants that are defined over $\mathbb{F}_p$.

(2) For each $(j_1(A'), j_2(A'), j_3(A')) \in S$, construct a genus 2 curve C having these invariants using Mestre's algorithm; see [Mestre 1991; Cardona and Quer 2005].

(3) Apply the Freeman–Lauter algorithm [2008] to test whether $\mathrm{Jac}(C)$ has endomorphism ring $\mathbb{O}_K$. Return the Igusa invariants of all the curves that pass this test.

We can predict beforehand *how many* triples will be returned by Algorithm 6.2. We compute the prime factorization

$$(l) = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_k^{e_k}$$

of (l) in K_Φ. Say that we have $n \leq 4$ prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ of norm l in this factorization, disregarding multiplicity. For each of these ideals $\mathfrak{p}_i$ we compute the typenorm map $m(\mathfrak{p}_i) \in \mathfrak{C}(K)$. The size of

$$\{m(\mathfrak{p}_1), \ldots, m(\mathfrak{p}_n)\} \subset \mathfrak{C}(K).$$

equals the number of triples computed by Algorithm 6.2.

Remark 6.3. Step 1 of the algorithm requires working in an extension of $\mathbb{F}_p$. The degree of this extension depends on the splitting behavior of 2 in $\mathbb{O}_K$. An upper bound is given by $4[\mathbb{F}_p(A[2]) : \mathbb{F}_p] \leq 24$, where $\mathbb{F}_p(A[2])$ denotes the field obtained by adjoining the coordinates of all 2-torsion points of A.

6.3. ***Igusa class polynomials.*** The CRT algorithm [Eisenträger and Lauter 2009] for computing the Igusa class polynomials $P_K, Q_K, R_K \in \mathbb{Q}[X]$ of a primitive quartic CM field K also computes the reductions of these 3 polynomials modulo primes p which split completely in the Hilbert class field of K_Φ. The method suggested in [Eisenträger and Lauter 2009] loops over all p^3 possible Igusa invariants and runs an endomorphism ring test for each triple $(j_1(A'), j_2(A'), j_3(A'))$, to see if A' has endomorphism ring $\mathbb{O}_K$.

We propose two main modifications to this algorithm. Firstly, we only demand that the primes p split completely in the subfield $K_\Phi(j_1(A), j_2(A), j_3(A))$ of the Hilbert class field of K_Φ that we obtain by adjoining the Igusa invariants of an

abelian surface A that has CM by $\mathbb{O}_K$. To find such primes, we simply loop over $p = 5, 7, 11 \ldots$, and for the primes $(p) = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3\mathfrak{P}_4 \subset \mathbb{O}_{K_\Phi}$ that split completely in K_Φ we test if

$$m(\mathfrak{P}_1) = (\mu) \subset \mathbb{O}_K \quad \text{and} \quad N(\mathfrak{P}_1) = \mu\bar{\mu},$$

with $\bar{\mu}$ the complex conjugate of μ. By [Shimura 1998, Section 15.3, Theorem 1], a prime p satisfying these conditions splits completely in $K_\Phi(j_1(A), j_2(A), j_3(A))$. It includes the primes that split completely in the Hilbert class field of K_Φ.

Our second modification is a big improvement in computing the Igusa class polynomial modulo p. Instead of looping over all $O(p^3)$ curves, we exploit the Galois action in a similar vein as in [Belding et al. 2008]. Below we give the complete algorithm to compute P_K, R_K, Q_K modulo a prime p meeting our conditions.

Step 1. Compute the class group

$$\mathrm{Cl}(\mathbb{O}_{K_\Phi}) = \langle \mathfrak{p}_1, \ldots, \mathfrak{p}_k \rangle \tag{6-1}$$

of the reflex field, where we take degree 1 prime ideals $\mathfrak{p}_i$. For each of the ideals $\mathfrak{p}_i$ of *odd* norm $N_{K_\Phi/\mathbb{Q}}(\mathfrak{p}_i) = l_i$, compute the ideal $V(f; l_i)$ describing the Siegel modular variety $Y(f; l_i)^*$.

Step 2. Find an abelian surface $A/\mathbb{F}_p$ that has endomorphism ring isomorphic to $\mathbb{O}_K$, as follows. We factor $(p) \subseteq \mathbb{O}_K$ into primes $\mathfrak{P}_1, \overline{\mathfrak{P}}_1, \mathfrak{P}_2, \overline{\mathfrak{P}}_2$ and compute a generator π for the principal ideal $\mathfrak{P}_1\mathfrak{P}_2$. We compute the minimal polynomial f_π of π over $\mathbb{Q}$. We try *random* curves $C/\mathbb{F}_p$ until we find a curve with

$$\#C(\mathbb{F}_p) \in \{p + 1 \pm \mathrm{Tr}_{K/\mathbb{Q}}(\pi)\} \quad \text{and} \quad \#\,\mathrm{Jac}(C) \in \{f_\pi(1), f_\pi(-1)\}. \tag{6-2}$$

By construction, such a curve C has endomorphism algebra K. We test whether $\mathrm{Jac}(C)$ has endomorphism ring $\mathbb{O}_K$ using the algorithm of Freeman and Lauter [2008]. If it does, continue with Step 3, otherwise try more random curves C until we find one for which its Jacobian has endomorphism ring $\mathbb{O}_K$.

Step 3. Let $A/\mathbb{F}_p$ be the surface found in Step 2. The group $G = m(\mathrm{Cl}(\mathbb{O}_{K_\Phi}))$ acts in a natural way on A and we compute the set

$$G \cdot (j_1(A), j_2(A), j_3(A)) \subseteq S(K)$$

as follows. For $x = m(I)$ we write $I = \prod_i \mathfrak{p}_i^{a_i}$. The action of $\mathfrak{p}_1$ is computed using Algorithm 6.2 in case the norm of $\mathfrak{p}_1$ is odd and by applying a Richelot isogeny (see Section 3.2) if $\mathfrak{p}_1$ has norm 2. By successively applying the action of $\mathfrak{p}_1$, we compute the action of $\mathfrak{p}_1^{a_1}$. We then continue with the action of $\mathfrak{p}_2$, and so on. This allows us to compute the action of x on the surface A, and doing this for all x we compute the set $G \cdot (j_1(A), j_2(A), j_3(A))$. This part of the algorithm is analogous the one in [Belding et al. 2008].

Step 4. In contrast to genus 1 and the algorithm in [Belding et al. 2008], it is unlikely that *all* surfaces with endomorphism ring $\mathcal{O}_K$ are found. This is partly because we only find surfaces having the *same* CM type as the initial surface A, so in the dihedral case we are missing surfaces with the second CM type. Even in the cyclic case where there are $|\mathfrak{C}(K)|$ isomorphism classes, it is possible that the map

$$m : \mathrm{Cl}(\mathcal{O}_{K_\Phi}) \to \mathfrak{C}(K)$$

is not surjective, meaning that we do not find all surfaces of a given CM type. The solution is simple: compute the cardinality of $S(K)$ using Corollary 3.3, and if the number of surfaces found is less than $|S(K)|$, go back to Step 2.

Step 5. Once we have found all surfaces with endomorphism ring $\mathcal{O}_K$, expand

$$P_K \bmod p = \prod_{\{A \text{ p.p.a.s.} | \operatorname{End}(A)=\mathcal{O}_K\}/\cong} (X - j_1(A)) \in \mathbb{F}_p[X]$$

and likewise for Q_K and R_K. The main difference with the method of [Eisenträger and Lauter 2009] is that we do *not* find all roots of P_K by a random search: we exploit the Galois action.

6.4. ***Run time analysis.*** We proceed with the run time analysis of the algorithm to compute the Igusa class polynomials using the 'modified CRT-approach' from Section 6.3. The input of the algorithm is a degree four CM field K. The discriminant D of K can be written as $D_1 D_0^2$, with D_0 the discriminant of the real quadratic subfield K^+ of K. We will give the run time in terms of D_1 and D_0.

First we analyze the size of the primes p used in the algorithm. The primes we use split completely in a subfield $S = K_\Phi(j_i(A))$ of the Hilbert class field of the reflex field K_Φ of K. If GRH holds, then there exists [Lagarias and Odlyzko 1977] an effectively computable constant $c > 0$, independent of K, such that the smallest such prime p satisfies

$$p \le c \cdot (\log|\mathrm{disc}(S/\mathbb{Q})|)^2,$$

where $\mathrm{disc}(S/\mathbb{Q})$ denotes the discriminant of the extension $S/\mathbb{Q}$. Since S is a totally unramified extension of K_Φ, we have

$$\mathrm{disc}(S/\mathbb{Q})^{1/[S:\mathbb{Q}]} = \mathrm{disc}(K_\Phi/\mathbb{Q})^{1/[K_\Phi:\mathbb{Q}]}$$

and we derive $\mathrm{disc}(S/\mathbb{Q}) = \mathrm{disc}(K_\Phi/\mathbb{Q})^{[S:K_\Phi]}$. Theorem 3.1 yields the bound $[S : K_\Phi] \le 4h^-(K)$, where $h^-(K) = |\mathrm{Cl}(\mathcal{O}_K)|/|\mathrm{Cl}(\mathcal{O}_{K^+})|$ denotes the *relative* class number of K. Using the bound (see [Louboutin 2003])

$$h^-(K) = \widetilde{O}(\sqrt{D_1 D_0}), \tag{6-3}$$

we derive that the smallest prime p is of size $\widetilde{O}(D_1 D_0)$. Here, the $\widetilde{O}$-notation indicates that factors that are of logarithmic order in the main term have been disregarded.

The Igusa class polynomials have rational coefficients, and at the moment the best known bound for the logarithmic height of the denominator of a coefficient is $\widetilde{O}(D_1^{3/2} D_0^{5/2})$. This bound is proven in [Streng 2010, Section 2.9] and is based on the denominator bounds in [Goren and Lauter 2010]. A careful analysis [Streng 2010, Section 2.11] yields that each coefficient of P_K, R_K, Q_K has logarithmic height $\widetilde{O}(D_1^{3/2} D_0^{5/2})$ as well. A standard argument as in [Belding et al. 2008, Lemma 5.3] shows that the $\widetilde{O}(D_1^{3/2} D_0^{5/2})$ primes that we need can be taken to be of size $\widetilde{O}(D_1^2 D_0^3)$ if GRH holds true. We find these primes in time $\widetilde{O}(D_1^2 D_0^3)$. We remark that better bounds on the denominators of the coefficients translate into better bounds on the size of the primes we need.

If GRH holds true, then the ideals $\mathfrak{p}_i$ in Step 1 can be chosen to have norm at most $12(\log D_1 D_0^2)^2$ by [Bach 1990]. Since the method from Section 5 for computing the ideal $V(f; N(\mathfrak{p}_i))$ is heuristic, we will rely on the following heuristic for our analysis.

Heuristic 6.4. Given a prime $l > 2$, we can compute generators for the ideal $V(f; l)$ in time polynomial in l.

At the moment, our computation of $V(f; l)$ only terminates in a reasonable amount of time for $l = 3$. However, *in theory* we only spend heuristic time $(\log D_1 D_0^2)^n$ in Step 1 for some $n \geq 2$ that is independent of D_1 and D_0. This is negligible compared to other parts of the algorithm.

We continue with the analysis of computing $P_K \bmod p$. As we think that the bound $p = \widetilde{O}(D_1^2 D_0^3)$ is too pessimistic, we will do the analysis in terms of both p and D_1, D_0. First we analyze the time spent on the random searches to find abelian surfaces with endomorphism ring $\mathbb{O}_K$. Every time we leave Step 2, we compute a factor $F \mid P_K \bmod p$ of the (first) Igusa class polynomial. Let $k \leq 2[\mathfrak{C}(K) : m(\mathrm{Cl}(\mathbb{O}_{K_\Phi}))]$ be the number of factors F we need to compute. The first time we invoke Step 2, we will with probability 1 compute a new factor F_1 of P_K. The second time we call Step 2 we need to ensure that we compute a *different* factor $F_2 \mid P_K$. Hence, we expect that we need to call Step 2 $k/(k-1)$ times to compute F_2. We see that we expect that we have to do Step 2

$$k(1 + 1/2 + \cdots + 1/k) = \widetilde{O}(k)$$

times to compute all factors $F_1, \ldots, F_k$.

Lemma 6.5. *We have* $[\mathfrak{C}(K) : m(\mathrm{Cl}(\mathbb{O}_{K_\Phi}))] \leq 2 \cdot 2^{6\omega(D)}$ *for any primitive quartic CM field* K, *where* $\omega(D)$ *denotes the number of prime divisors of* D.

Proof. We will bound the index of the image of the map $\tilde{m} : \mathrm{Cl}(\mathbb{O}_{K_\Phi}) \to \mathrm{Cl}(\mathbb{O}_K)$ inducing m. By Theorem 3.1, this index differs by at most a factor

$$|(\mathbb{O}_{K^+}^*)^+ / N_{K/K^+}(\mathbb{O}_K^*)| \leq 2$$

from $[\mathfrak{C}(K) : m(\mathrm{Cl}(\mathbb{O}_{K_\Phi}))]$.

If $K/\mathbb{Q}$ is dihedral with normal closure L, then the image of the norm map $N_{L/K} : \mathrm{Cl}(\mathbb{O}_L) \to \mathrm{Cl}(\mathbb{O}_K)$ has index at most 2 by class field theory. In the cyclic case, it is not hard to check that $\Im(\tilde{m})$ contains the squares. It suffices to bound the 2-torsion $\mathrm{Cl}(\mathbb{O}_K)$ in this case. The 2-rank of $\mathrm{Cl}(\mathbb{O}_K)$ is determined by *genus theory*. Using a combination of group cohomology and Nakayama's lemma, one can show [Rosen 2011] that the 2-rank is at most $6t$, with t the number of primes that ramify in the cyclic CM extension $K/\mathbb{Q}$. The lemma follows. □

We remark that outside a zero-density subset of very smooth integers, we have $\omega(n) < 2 \log\log n$ and we can then absorb the factor $\widetilde{O}(2^{6\omega(D)}) = 2^{6\omega(D)}\widetilde{O}(\log(D))$ into the $\widetilde{O}$-notation.

The probability that one of the random searches performed in this step will yield an abelian surface $\mathrm{Jac}(C)$ with endomorphism ring $\mathbb{O}_K$ is bounded from below by

$$h^-(K)/p^3 = \tilde{\Omega}(\sqrt{D_1 D_0}/p^3)$$

where we have used the effective lower bound $h^-(K) = \tilde{\Omega}(\sqrt{D_1 D_0})$ proved in [Louboutin 2003]. We therefore expect that we have to compute the number of points on C and on $\mathrm{Jac}(C)$ for

$$\widetilde{O}(p^3/\sqrt{D_1 D_0})$$

curves $C/\mathbb{F}_p$. Since point counting on genus 2 curves is polynomial time by [Pila 1990], this takes time $\widetilde{O}(p^3/\sqrt{D_1 D_0})$.

For all the curves $C/\mathbb{F}_p$ that satisfy equation (6-2), we have to check whether we have $\mathrm{End}(\mathrm{Jac}(C)) \cong \mathbb{O}_K$ or not. The probability that $\mathrm{End}(\mathrm{Jac}(C))$ is isomorphic to $\mathbb{O}_K$ is bounded from below by

$$\frac{h^-(K)}{\sum_{\mathbb{O}} h(\mathbb{O})}, \tag{6-4}$$

where the sum ranges over all orders $\mathbb{O} \subseteq \mathbb{O}_K$ that contain $\mathbb{Z}[\pi, \bar{\pi}]$. Assuming mild ramification conditions on the prime 2, there are only $O(\log n)$ orders $\mathbb{O} \subseteq \mathbb{O}_K$ of index n; see [Nakagawa 1996, Corollary 1]. We assume the following heuristic.

Heuristic 6.6. For any quartic CM field K, there are $O(\log n)$ orders $\mathbb{O} \subseteq \mathbb{O}_K$ of index n.

Justification of heuristic. As indicated in [Nakagawa 1996], the splitting condition on 2 is purely technical and should not affect the result. □

We can bound the class number $h(\mathbb{O})$ by $2[\mathbb{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]h(\mathbb{O}_K)$ by [Stevenhagen 2008, Theorem 6.7]. It follows that we can bound the probability in (6-4) by

$$\Omega\Big(\frac{1}{[\mathbb{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]^{1+\varepsilon} h(\mathbb{O}_{K^+})}\Big),$$

where we have used the bound n^ε for the number of divisors of n. Using the index bound

$$[\mathbb{O}_K : \mathbb{Z}[\pi, \bar{\pi}]] \leq \frac{16p^2}{D_0\sqrt{D_1}}$$

from [Freeman and Lauter 2008, Proposition 6.1], we expect that we have to do

$$O\Big(\frac{2^{6\omega(D)} p^{2+2\varepsilon}\sqrt{D_0}}{(\sqrt{D_1}D_0)^{1+\varepsilon}}\Big)$$

endomorphism ring computations.

At the moment, the only known algorithm [Freeman and Lauter 2008] to test whether $\mathrm{End}(\mathrm{Jac}(C)) \cong \mathbb{O}_K$ holds has a run time $\widetilde{O}(p^{18})$, and one application of this algorithm dominates the computation of $P_K \in \mathbb{Q}[X]$. To make the run time analysis of our algorithm easier once a better algorithm to compute $\mathrm{End}(\mathrm{Jac}(C))$ has been found, we will use the bound $O(X)$ for the run time to compute $\mathrm{End}(\mathrm{Jac}(C))$. In total, we see that we spend

$$\widetilde{O}(2^{6\omega(D)}(p^3/\sqrt{D_1 D_0} + (p^{2+2\varepsilon}\sqrt{D_0}/(\sqrt{D_1}D_0)^{1+\varepsilon})X))$$

time in all calls of Step 2.

The action of $\mathfrak{p}_i$ on $A/\mathbb{F}_p$ in Step 3 is computed in polynomial time in the norm l_i of $\mathfrak{p}_i$. As l_i is, under GRH, of polynomial size in $\log(D_1 D_0^2)$, we spend time

$$\widetilde{O}(\sqrt{D_1 D_0})$$

for every time we call Step 3. We call Step 3 as often as Step 2, so in total we spend time $\widetilde{O}(2^{6\omega(D)}\sqrt{D_1 D_0})$ in Step 3.

The time spent in Step 4 is negligible, and the time spent in Step 5 is $\widetilde{O}(\sqrt{D_1 D_0})$. Combining all five steps, we see that we compute $P_K \bmod p$ in time

$$\widetilde{O}(2^{6\omega(D)}(p^3/\sqrt{D_1 D_0} + (p^{2+2\varepsilon}\sqrt{D_0}/(\sqrt{D_1}D_0)^{1+\varepsilon})X + \sqrt{D_1 D_0})). \tag{6-5}$$

Theorem 6.7. *If GRH and Heuristic assumptions 6.4, 6.6 hold true, then we can compute the polynomials P_K, Q_K, R_K in probabilistic time*

$$\widetilde{O}(2^{6\omega(D)}(D_1^7 D_0^{11} + X D_1^{5+\varepsilon} D_0^{8+2\varepsilon})).$$

Here, X denotes the run time of an algorithm that, given $A/\mathbb{F}_p$, decides whether $\mathrm{End}(A)$ *is isomorphic to $\mathbb{O}_K$ or not.*

Proof. Substitute $p = \widetilde{O}(D_1^2 D_0^3)$ in equation (6-5) to get the time per prime. The result follows from the fact that we need to compute P_K, R_K, Q_K modulo p for $\widetilde{O}(D_1^{3/2} D_0^{5/2})$ primes. □

We conclude this section with some remarks on the run time of our algorithm. At the moment, the main bottleneck is checking whether $\mathrm{End}(A) \cong \mathbb{O}_K$ holds or not. In Section 8 we show that a straightforward generalization of Kohel's algorithm [2008] is impossible and that a new approach is needed.

From a practical point of view, we are limited by the fact that we can only compute the ideal $V(f; 3)$ in a reasonable amount of time. By only using the primes lying over 2 and 3, we only use a subgroup of the group $\mathfrak{C}(K)$ giving the Galois action.

Even when these two problems are solved, there is a bottleneck not present in the genus 1 algorithm from [Belding et al. 2008]. The random searches take time $\widetilde{O}(p^3/\sqrt{D_1 D_0})$; even for the smallest prime p this is of size $\widetilde{O}(D_1^{5/2} D_0^{5/2})$.

Doing only the random searches for this prime already takes more time than it takes to write down the output $P_K, Q_K, R_K \in \mathbb{Q}[X]$. Hence, our algorithm is at the moment *not* quasilinear in the size of the output.

As noted in [Gruenewald 2010, Section 6], we can speed up this step of the algorithm by first computing a model for the Humbert surface describing all principally polarized abelian surfaces that have real multiplication by the quadratic subfield K^+ of K. We then perform our random search on this two-dimensional subspace of the three-dimensional moduli space. The time for the random searches would, for the smallest prime p, drop to

$$\widetilde{O}(D_1^{3/2} D_0^{3/2}).$$

Although this is less than the size of the output, our algorithm is not quasilinear once all primes p are taken into account.

To get a quasilinear algorithm, we think one should do the random searches on a one-dimensional subspace of the moduli space. This approach is an object of further study.

7. Examples and applications

In this section we illustrate our algorithm by computing the Igusa class polynomials modulo primes p for various CM fields. We point out the differences with the analogous genus 1 computations.

Example 7.1. In the first example we let $K = \mathbb{Q}[X]/(X^4 + 185X^2 + 8325)$ be a *cyclic* CM field of degree 4. All CM types are equivalent in this case, and the reflex field of K is K itself. The discriminant of K equals $5^2 \cdot 37^3$, and the real quadratic subfield of K is $K^+ = \mathbb{Q}(\sqrt{37})$. An easy computation shows that the narrow

class group of K^+ is trivial. In particular, all ideal classes of K are principally polarizable, and we have

$$\mathfrak{C}(K) \cong \mathrm{Cl}(\mathbb{O}_K).$$

We compute $\mathrm{Cl}(\mathbb{O}_K) = \mathbb{Z}/10\mathbb{Z} = \langle \mathfrak{p}_3 \rangle$, where $\mathfrak{p}_3$ is a prime lying over 3. The prime ideal $\mathfrak{p}_3$ has norm 3, and its typenorm $N_\Phi(\mathfrak{p}_3)$ generates a subgroup of order 5 in $\mathrm{Cl}(\mathbb{O}_K)$.

The smallest prime that splits in the Hilbert class field of K is $p = 271$. We illustrate our algorithm by computing the Igusa class polynomials for K modulo this prime. First we do a 'random search' to find a principally polarized abelian surface over $\mathbb{F}_p$ with endomorphism ring $\mathbb{O}_K$ in the following way. We factor $(p) \subset \mathbb{O}_K$ into primes $\mathfrak{P}_1, \overline{\mathfrak{P}}_1, \mathfrak{P}_2, \overline{\mathfrak{P}}_2$ and compute a generator π of the principal $\mathbb{O}_K$-ideal $\mathfrak{P}_1\mathfrak{P}_2$. The element π has minimal polynomial

$$f = X^4 + 9X^3 + 331X^2 + 2439X + 73441 \in \mathbb{Z}[X].$$

If the Jacobian $\mathrm{Jac}(C)$ of a hyperelliptic curve C has endomorphism ring $\mathbb{O}_K$, then the Frobenius morphism of $\mathrm{Jac}(C)$ is a root of either $f(X)$ or $f(-X)$. With the factorization

$$f = (X - \tau_1)(X - \tau_2)(X - \tau_3)(X - \tau_4) \in K[X],$$

a *necessary* condition for $\mathrm{Jac}(C)$ to have endomorphism ring $\mathbb{O}_K$ is

$$\#C(\mathbb{F}_p) \in \{p + 1 \pm (\tau_1 + \tau_2 + \tau_3 + \tau_4)\} = \{261, 283\}$$

and

$$\#\,\mathrm{Jac}(C)(\mathbb{F}_p) \in \{f(1),\ f(-1)\} = \{71325, 76221\}.$$

We try random values $(j_1, j_2, j_3) \in \mathbb{F}_p^3$ and write down a hyperelliptic curve C with those Igusa invariants using Mestre's algorithm [Mestre 1991; Cardona and Quer 2005]. If C satisfies the 2 conditions above, then we check whether $\mathrm{Jac}(C)$ has endomorphism ring $\mathbb{O}_K$ using the algorithm in [Freeman and Lauter 2008]. If it passes this test, we are done. Otherwise, we select a new random value (j_1, j_2, j_3).

We find that $w_0 = (133, 141, 89)$ is a set of invariants for a surface $A/\mathbb{F}_p$ with endomorphism ring $\mathbb{O}_K$. We apply Algorithm 6.2 to w_0. The Igusa–Clebsch invariants corresponding to w_0 are $[133, 54, 82, 56]$. With the notation from Section 4, we have $s_2 = 162$, $s_3 = 106$, $s_5 = 128$, $s_6 = 30$. The Satake sextic polynomial

$$\mathcal{S} = X^6 + 190X^4 + 55X^3 + 82X^2 + 18X + 63 \in \mathbb{F}_p[X]$$

factors over $\mathbb{F}_{p^5}$ and we write $\mathbb{F}_{p^5} = \mathbb{F}_p(\alpha)$, where α satisfies $\alpha^5 + 2\alpha + 265 = 0$. We express the 6 roots of $\mathcal{S}$ in terms of α and pick

$$\begin{aligned} f_1^4 &= 147\alpha^4 + 147\alpha^3 + 259\alpha^2 + 34\alpha + 110, \\ f_2^4 &= 176\alpha^4 + 211\alpha^3 + 14\alpha^2 + 134\alpha + 190, \\ f_3^4 &= 163\alpha^4 + 93\alpha^3 + 134\alpha^2 + 196\alpha + 115, \\ f_4^4 &= 226\alpha^4 + 261\alpha^3 + 99\alpha^2 + 9\alpha + 27 \end{aligned}$$

as values for the fourth powers of our Siegel modular functions. The fourth roots of $(f_1^4, f_2^4, f_3^4, f_4^4)$ are all defined over $\mathbb{F}_{p^{10}}$, but the proof of Theorem 4.2 shows that not every choice corresponds to the Igusa invariants of A. We pick fourth roots (r_1, r_2, r_3, r_4) such that the polynomial P_- from Section 4 vanishes when evaluated at $(T, f_1, f_2, f_3, f_4) = (\theta^4_{(0,1),(0,0)}, r_1, r_2, r_3, r_4)$. Here, $\theta^4_{(0,1),(0,0)}$ is computed from the Igusa–Clebsch invariants. For an arbitrary choice of fourth roots for r_1, r_2, r_3, there are two solutions $\pm r_4$ to $P_- = 0$. Indeed, if we take $\mathbb{F}_{p^{10}} = \mathbb{F}_p(\beta)$ with $\beta^{10}+\beta^6+133\beta^5+10\beta^4+256\beta^3+74\beta^2+126\beta+6=0$, then the tuple (r_1, r_2, r_3, r_4) given by

$$\begin{aligned} r_1 &= 179\beta^9 + 69\beta^8 + 203\beta^7 + 150\beta^6 + 29\beta^5 + 258\beta^4 + 183\beta^3 + 240\beta^2 + 255\beta + 226, \\ r_2 &= 142\beta^9 + 105\beta^8 + 227\beta^7 + 244\beta^6 + 72\beta^5 + 155\beta^4 + 2\beta^3 + 129\beta^2 + 137\beta + 23, \\ r_3 &= 63\beta^9 + 112\beta^8 + 132\beta^7 + 244\beta^6 + 94\beta^5 + 40\beta^4 + 191\beta^3 + 263\beta^2 + 85\beta + 70, \\ r_4 &= 190\beta^9 + 41\beta^8 + 62\beta^7 + 170\beta^6 + 151\beta^5 + 240\beta^4 + 270\beta^3 + 56\beta^2 + 16\beta + 257 \end{aligned}$$

is a set of invariants for A together with some level 8-structure.

Next we specialize our ideal $V(f; 3)$ at $(W_1, X_1, Y_1, Z_1) = (r_1, r_2, r_3, r_4)$ and we solve the remaining system of 85 equations in 4 unknowns. Let (r_1', r_2', r_3', r_4') be the solution where

$$r_1' = 184\beta^9 + 48\beta^8 + 99\beta^7 + 83\beta^6 + 20\beta^5 + 232\beta^4 + 16\beta^3 + 223\beta^2 + 85\beta + 108.$$

The quadruple (r_1', r_2', r_3', r_4') are invariants of an abelian surface A' together with level 8-structure that is $(3, 3)$-isogenous to A. To map this quadruple to the Igusa invariants of A', we compute a root of the quadratic polynomial

$$P_-(T, r_1', r_2', r_3', r_4').$$

This root is a value for $\theta^4_{(0,1),(0,0)}$. Since we now know *all* theta fourth powers, we can apply the formulas relating theta functions and Igusa functions in Section 4.1 to find the Igusa triple (238, 10, 158).

In total, we find 16 Igusa triples defined over $\mathbb{F}_p$. All these triples are Igusa invariants of surfaces that have endomorphism *algebra* K. To check which ones have

endomorphism *ring* $\mathbb{O}_K$, we apply the algorithm of Freeman and Lauter [2008]. We find that only the four triples

$$(253, 138, 96),\ (257, 248, 58),\ (238, 10, 158),\ (140, 159, 219)$$

are invariants of surfaces with endomorphism ring $\mathbb{O}_K$. The fact that we find 4 new sets of invariants should come as no surprise. Indeed, there are 4 ideals of norm 3 lying over 3 in $\mathbb{O}_K$ and each ideal gives us an isogenous surface.

Since the typenorm map $m : \mathrm{Cl}(\mathbb{O}_K) \to \mathfrak{C}(K)$ is not surjective, we are forced to do a *second* random search to find a 'new' abelian surface with endomorphism ring $\mathbb{O}_K$. We apply our isogeny algorithm to $w_1 = (74, 125, 180)$ as before, and we again find 4 new sets of invariants:

$$(174, 240, 246), (193, 85, 15), (268, 256, 143), (75, 263, 182).$$

In the end we expand the Igusa polynomials

$$\begin{aligned} P_K &= X^{10} + 92X^9 + 72X^8 + 217X^7 + 98X^6 \\ &\qquad + 195X^5 + 233X^4 + 140X^3 + 45X^2 + 123X + 171, \\ Q_K &= X^{10} + 232X^9 + 195X^8 + 45X^7 + 7X^6 \\ &\qquad + 195X^5 + 173X^4 + 16X^3 + 33X^2 + 247X + 237, \\ R_K &= X^{10} + 240X^9 + 57X^8 + 213X^7 + 145X^6 \\ &\qquad + 130X^5 + 243X^4 + 249X^3 + 181X^2 + 134X + 81 \end{aligned}$$

modulo $p = 271$.

Example 7.2. In the previous example, all the prime ideals of K lying over 3 gave rise to an isogenous abelian surface. This phenomenon does not always occur. Indeed, let K be a primitive quartic CM field and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the prime ideals of norm 3. If we have a principally polarized abelian surface $A/\mathbb{F}_p$ with endomorphism ring $\mathbb{O}_K$, then the number of $(3, 3)$-isogenous abelian surfaces with the same endomorphism ring equals the cardinality of

$$\{m(\mathfrak{p}_1), \ldots, m(\mathfrak{p}_n)\}.$$

There are examples where this set has *less* than n elements.

Take the cyclic field $K = \mathbb{Q}[X]/(X^4 + 219X^2 + 10512)$. The class group of K is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The prime 3 ramifies in K, and we have $(3) = \mathfrak{p}_1^2\mathfrak{p}_2^2$. The primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ in fact generate $\mathrm{Cl}(\mathbb{O}_K)$. It is easy to see that for this field we have

$$m(\mathfrak{p}_1) = m(\mathfrak{p}_2) \in \mathfrak{C}(K),$$

so we only find *one* isogenous surface.

Example 7.3. Our algorithm is not restricted to cyclic CM fields. In this example we let $K = \mathbb{Q}[X]/(X^4 + 22X^2 + 73)$ be a CM field with Galois group D_4. There are 2 equivalence classes of CM types. We fix a CM type $\Phi : K \to \mathbb{C}^2$ and let K_Φ be the reflex field for Φ. We have $K_\Phi = \mathbb{Q}[X]/(X^4 + 11X^2 + 12)$, and K and K_Φ have the same Galois closure L.

Since the real quadratic subfield $K^+ = \mathbb{Q}(\sqrt{3})$ has narrow class group $\mathbb{Z}/2\mathbb{Z}$, the group $\mathfrak{C}(K)$ fits in an exact sequence

$$1 \to \mathbb{Z}/2\mathbb{Z} \to \mathfrak{C}(K) \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 1$$

and a close inspection yields $\mathfrak{C}(K) \cong \mathbb{Z}/4\mathbb{Z}$. The prime 3 factors as $(3) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^2$ in the reflex field, and we have $\mathrm{Cl}(\mathcal{O}_{K_\Phi}) = \mathbb{Z}/4\mathbb{Z} = \langle [\mathfrak{p}_1] \rangle$. The element $m(\mathfrak{p}_1) \in \mathfrak{C}(K)$ has order 4, and under the map

$$\mathfrak{C}(K) \xrightarrow{f} \mathrm{Cl}(\mathcal{O}_K) = \mathbb{Z}/4\mathbb{Z},$$

the element $f(m(\mathfrak{p}_1))$ has order 2. We see that even though the ideal $N_{L/K}(\mathfrak{p}_1\mathcal{O}_L)$ has order 2 in the class group, the typenorm of $\mathfrak{p}_1$ has order 4.

Of the 4 ideal classes of K, only 2 ideal classes are principally polarizable for Φ. The other 2 ideal classes are principally polarizable for 'the other' CM type. Furthermore, the two principally polarizable ideal classes each have *two* principal polarizations.

The prime $p = 1609$ splits completely in the Hilbert class field of K_Φ. As in Example 7.1, we do a random search to find that a surface $A/\mathbb{F}_p$ with Igusa invariants $w_0 = (1563, 789, 704) \in \mathbb{F}_p^3$ has endomorphism ring $\mathcal{O}_K$. We apply Algorithm 6.2 to this point. As output, we get w_0 again and two new points

$$w_1 = (1396, 1200, 1520) \quad \text{and} \quad w_2 = (1350, 1316, 1483).$$

The fact that we find w_0 again should come as no surprise since $m(\mathfrak{p}_3) \in \mathfrak{C}(K)$ is the trivial element. The points w_1 and w_2 correspond to $\mathfrak{p}_1$ and $\mathfrak{p}_2$.

As expected we compute that the cycle

$$w_0 = (1563, 789, 704) \xrightarrow{\mathfrak{p}_1} (1396, 1200, 1520) \xrightarrow{\mathfrak{p}_1} (1276, 1484, 7) \xrightarrow{\mathfrak{p}_1} (1350, 1316, 1483) \xrightarrow{\mathfrak{p}_1} w_0$$

has length 4. To find the full Igusa class polynomials modulo p, we do a second random search. The remaining 4 points are (782, 1220, 257), (1101, 490, 1321), (577, 35, 471), (1154, 723, 1456).

8. Obstruction to isogeny volcanoes

For an ordinary elliptic curve $E/\mathbb{F}_p$ over a finite field, Kohel [1996] introduced an algorithm to compute the endomorphism ring $\mathrm{End}(E)$, which has recently been

improved in [Bisson and Sutherland 2011]. One first computes the endomorphism *algebra* K by computing the trace of the Frobenius morphism π of E. If the index $[\mathbb{O}_K : \mathbb{Z}[\pi]]$ is only divisible by small primes l, then Kohel's algorithm uses the l-isogeny graph to determine the endomorphism ring. The algorithm depends on the fact that the graph of l-isogenies looks like a volcano, and one can quotient by subgroups of order l to move down the volcano until one hits the bottom. We refer to [Fouquet and Morain 2002; Kohel 1996] for the details of this algorithm. This approach succeeds because of the following fact.

Lemma 8.1. *Let E, $E'/\mathbb{F}_p$ be two ordinary elliptic curves whose endomorphism rings are isomorphic to the same order $\mathbb{O}$ in an imaginary quadratic field K. Let $l \neq p$ be a prime such that the index $[\mathbb{O}_K : \mathbb{O}]$ is divisible by l. Then there are no isogenies of degree l between E and E'.*

Proof. This result is well known. Since the proof helps us understand what goes wrong in dimension 2, we give the short proof. Suppose that there does exist an isogeny $\varphi : E \to E'$ of degree l. By the Deuring lifting theorem [Lang 1987, Theorem 13.14], we can lift φ to an isogeny $\widetilde{\varphi} : \widetilde{E} \to \widetilde{E}'$ defined over the ring class field for $\mathbb{O}$. By CM theory, we can write $\widetilde{E}' = \mathbb{C}/I$ with I an *invertible* $\mathbb{O}$-ideal of norm l. But since l divides the index $[\mathbb{O}_K : \mathbb{O}]$, there are no invertible ideals of norm l. □

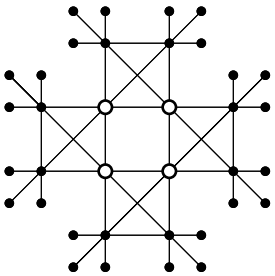
Unlike the elliptic curve case, there are a greater number of possibilities for the endomorphism ring of an (l, l)-isogenous abelian surface $A/\mathbb{F}_p$. Necessarily, the order must contain $\mathbb{Z}[\pi, \bar{\pi}]$, where π corresponds to the Frobenius endomorphism of A. Let $\varphi : A \to A'$ be an (l, l)-isogeny of principally polarized abelian surfaces where $\mathbb{O} = \mathrm{End}(A)$ contains $\mathbb{O}' = \mathrm{End}(A')$. Since φ splits multiplication by l, it follows that $\mathbb{Z} + l\mathbb{O} \subseteq \mathbb{O}' \subseteq \mathbb{O}$ and hence $\mathbb{O}'$ has index dividing l^3 in $\mathbb{O}$. In addition, since the $\mathbb{Z}$-rank is greater than two, it is possible to have several nonisomorphic suborders of $\mathbb{O}$ having the same index.

A natural question is whether the 'volcano approach' for elliptic curves can be generalized to ordinary principally polarized abelian surfaces $A/\mathbb{F}_p$. The extension of Schoof's algorithm [Pila 1990] enables us to compute the endomorphism algebra $K = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$, and the problem is to compute the subring $\mathrm{End}(A) = \mathbb{O} \subseteq \mathbb{O}_K$. By working with explicit l-torsion points for primes $l \mid [\mathbb{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]$, one can determine this subring [Eisenträger and Lauter 2009; Freeman and Lauter 2008]. This approach requires working over large extension field of $\mathbb{F}_p$ and a natural question is whether we can generalize the volcano algorithm directly by using (l, l)-isogenies between abelian surfaces. However, the statement analogous to Lemma 8.1 — *there are no (l, l)-isogenies between A and A'* if $\mathrm{End}(A)$ and $\mathrm{End}(A')$ have isomorphic endomorphisms rings whose conductor in $\mathbb{O}_K$ divides l —

does *not* hold in general. This is a theoretical obstruction to a straightforward generalization of the algorithm for elliptic curves.

The next example shows that the analogue of Lemma 8.1 for abelian surfaces fails.

Example 8.2. In Example 7.3 we found the point $(782, 1220, 257) \in \mathbb{F}_{1609}^3$. Below we depict the connected component of the $(3, 3)$-isogeny graph. The white dots represent surfaces with endomorphism ring $\mathbb{O}_K$, and the black dots correspond to surfaces whose endomorphism ring is nonmaximal. The lattice of suborders of $\mathbb{O}_K$ of 3-power index that contain $\mathbb{Z}[\pi, \bar{\pi}]$ is completely described by the indices of the suborders in this case. We have $\mathbb{Z}[\pi, \bar{\pi}] \subset \mathbb{O}_{27} \subset \mathbb{O}_9 \subset \mathbb{O}_3 \subset \mathbb{O}_K$, where the subscript denotes the index in $\mathbb{O}_K$.



The leaf nodes all have endomorphism ring $\mathbb{O}_{27}$ and the remaining eight black vertices have endomorphism ring $\mathbb{O}_3$. We observe that there are cycles in this graph other than at the 'surface' of the volcano. ◇

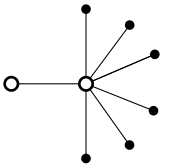
The reason that cycles can occur is the following. Just like in Lemma 8.1, we can lift an isogeny $\varphi : A \to A'$ to characteristic zero. By CM theory, we can now write $\widetilde{A} = \mathbb{C}^2/\Phi(I)$ for some invertible $\mathbb{O}$-ideal I. The isogenous surface $\widetilde{A}'$ equals $\mathbb{C}^2/\Phi(\mathfrak{a}^{-1}I)$ for an invertible $\mathbb{O}$-ideal $\mathfrak{a}$ of norm l^2. The difference from the elliptic curve case is that there *do* exist invertible $\mathbb{O}$-ideals of norm l^2. Hence, the isogeny graph for abelian surfaces need not look like a 'volcano'.

Another ingredient of the endomorphism ring algorithm for elliptic curves can fail. In the elliptic curve case, the following property of the l-isogeny graph is essential. Suppose that $E/\mathbb{F}_p$ has endomorphism ring $\mathbb{O}$ and let $\varphi : E \to E'$ be an isogeny from E to an elliptic curve with endomorphism ring of index l. If φ is defined over $\mathbb{F}_p$, then *all* $l + 1$ isogenies of degree l are defined over $\mathbb{F}_p$.

The analogous statement for dimension 2 is that *all* (l, l)-isogenies are defined over $\mathbb{F}_p$ as soon as there is one (l, l)-isogeny $\varphi : A \to A'$ that is defined over $\mathbb{F}_p$. Here, A' is an abelian surface with endomorphism ring of index dividing l^3. This statement is *not* true, as the following example shows.

Example 8.3. Consider the cyclic quartic CM field $K = \mathbb{Q}[X]/(X^4 + 12X^2 + 18)$, which has class number 2. The Igusa class polynomials have degree 2 and over $\mathbb{F}_{127}$

we find the corresponding moduli points $w_0 = (118, 71, 63)$ and $w_1 = (98, 82, 56)$. The isogeny graph is not regular:



The white dots represent the points having maximal endomorphism ring. There are 7 points isogenous to w_0, which includes w_1. One cannot identify w_1 from the graph structure alone. This demonstrates that the isogeny graph is insufficient to determine the endomorphism rings; the polarized CM lattices are also required. $\diamond$

The shape of this graph can be explained as follows. Let $\pi \in \mathbb{O}_K$ correspond to the Frobenius morphism of a surface A belonging to the vertex w_1. If A' is (l, l)-isogenous to A, then A' is defined over $\mathbb{F}_p$ if and only if its endomorphism ring contains π. Since there are several orders of index dividing l^3 in $\mathbb{O}_K$, it can happen that π is contained in some of them, and not in others. In our example, the black points all have the same endomorphism ring $\mathbb{O}'$ with $\pi \in \mathbb{O}'$. The 33 other isogenous surfaces have an endomorphism ring that contains π^3, but not π.

Acknowledgments

The authors thank Nils Bruin, Everett Howe, David Kohel, and John Voight for helpful discussions and improvements to an early version the paper, the anonymous referee both for various detailed comments and for motivating us to include a run time analysis, and Mike Rosen [2011] for proving a genus theory result that allowed us to prove Lemma 6.5.

References

[Bach 1990] E. Bach, "Explicit bounds for primality testing and related problems", *Math. Comp.* **55**:191 (1990), 355–380. MR 91m:11096 Zbl 0701.11075

[Baily and Borel 1966] W. L. Baily, Jr. and A. Borel, "Compactification of arithmetic quotients of bounded symmetric domains", *Ann. of Math.* (2) **84** (1966), 442–528. MR 35 #6870 Zbl 0154.08602

[Belding et al. 2008] J. Belding, R. Bröker, A. Enge, and K. Lauter, "Computing Hilbert class polynomials", pp. 282–295 in *Algorithmic number theory*, edited by A. J. van der Poorten and A. Stein, Lecture Notes in Comput. Sci. **5011**, Springer, Berlin, 2008. MR 2009j:11200 Zbl 1205.11139

[Bisson and Sutherland 2011] G. Bisson and A. V. Sutherland, "Computing the endomorphism ring of an ordinary elliptic curve over a finite field", *J. Number Theory* **131**:5 (2011), 815–831. MR 2772473 Zbl 05876849

[Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system, I: The user language", *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. MR 1484478 Zbl 0898.68039

[Bost and Mestre 1988] J.-B. Bost and J.-F. Mestre, "Moyenne arithmético-géométrique et périodes des courbes de genre 1 et 2", *Gaz. Math.* **38** (1988), 36–64. MR 89k:14072 Zbl 0682.14031

[Bröker and Lauter 2009] R. Bröker and K. Lauter, "Modular polynomials for genus 2", *LMS J. Comput. Math.* **12** (2009), 326–339. MR 2010k:11096 Zbl 05947706

[Cardona and Quer 2005] G. Cardona and J. Quer, "Field of moduli and field of definition for curves of genus 2", pp. 71–83 in *Computational aspects of algebraic curves*, edited by T. Shaska, Lecture Notes Ser. Comput. **13**, World Sci. Publ., Hackensack, NJ, 2005. MR 2006h:14036 Zbl 1126.14031

[Carls et al. 2008] R. Carls, D. Kohel, and D. Lubicz, "Higher-dimensional 3-adic CM construction", *J. Algebra* **319**:3 (2008), 971–1006. MR 2010e:14042 Zbl 1140.14042

[Chai and Norman 1990] C.-L. Chai and P. Norman, "Bad reduction of the Siegel moduli scheme of genus two with $\Gamma_0(p)$-level structure", *Amer. J. Math.* **112**:6 (1990), 1003–1071. MR 91i:14033 Zbl 0734.14010

[Dupont 2006] R. Dupont, *Moyenne arithmético-géométrique, suites de Borchardt et applications*, thesis, École polytechnique, 2006.

[Eisenträger and Lauter 2009] K. Eisenträger and K. Lauter, "A CRT algorithm for constructing genus 2 curves over finite fields", pp. 161–176 in *Proceedings of Arithmetic, Geometry, and Coding Theory (AGCT-10)*, Séminaires & Congrès **21**, Société de Mathématique Francaise, Paris, 2009.

[Fouquet and Morain 2002] M. Fouquet and F. Morain, "Isogeny volcanoes and the SEA algorithm", pp. 276–291 in *Algorithmic number theory*, edited by C. Fieker and D. R. Kohel, Lecture Notes in Comput. Sci. **2369**, Springer, Berlin, 2002. MR 2005c:11077 Zbl 1058.11041

[Freeman and Lauter 2008] D. Freeman and K. Lauter, "Computing endomorphism rings of Jacobians of genus 2 curves over finite fields", pp. 29–66 in *Algebraic geometry and its applications*, Ser. Number Theory Appl. **5**, World Sci. Publ., Hackensack, NJ, 2008. MR 2010a:14042 Zbl 1151.14314

[Gaudry et al. 2006] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng, "The 2-adic CM method for genus 2 curves with application to cryptography", pp. 114–129 in *Advances in cryptology—ASIACRYPT 2006*, edited by X. Lai and K. Chen, Lecture Notes in Comput. Sci. **4284**, Springer, Berlin, 2006. MR 2009j:94110 Zbl 1172.94576

[van der Geer 1982] G. van der Geer, "On the geometry of a Siegel modular threefold", *Math. Ann.* **260**:3 (1982), 317–350. MR 84a:10028 Zbl 0473.14017

[Goren 1997] E. Z. Goren, "On certain reduction problems concerning abelian surfaces", *Manuscripta Math.* **94**:1 (1997), 33–43. MR 98m:14048 Zbl 0924.14023

[Goren and Lauter 2010] E. Z. Goren and K. Lauter, "Genus 2 curves with complex multiplication", preprint, 2010. arXiv 1003.4759

[Gruenewald 2008] D. Gruenewald, *Explicit Algorithms for Humbert Surfaces*, thesis, University of Sydney, 2008.

[Gruenewald 2010] D. Gruenewald, "Computing Humbert surfaces and applications", pp. 59–69 in *Arithmetic, geometry, cryptography and coding theory 2009* (Marseille, 2009), edited by D. Kohel and R. Rolland, Contemp. Math. **521**, Amer. Math. Soc., Providence, RI, 2010. MR 2744034 Zbl 05831703

[Igusa 1960] J.-i. Igusa, "Arithmetic variety of moduli for genus two", *Ann. of Math.* (2) **72** (1960), 612–649. MR 22 #5637 Zbl 0122.39002

[Igusa 1964] J.-i. Igusa, "On the graded ring of theta-constants", *Amer. J. Math.* **86** (1964), 219–246. MR 29 #2258 Zbl 0146.31703

[Igusa 1967] J.-i. Igusa, "Modular forms and projective invariants", *Amer. J. Math.* **89** (1967), 817–855. MR 37 #5217 Zbl 0159.50401

[Katz and Mazur 1985] N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies **108**, Princeton University Press, 1985. MR 86i:11024 Zbl 0576.14026

[Kohel 1996] D. R. Kohel, *Endomorphism rings of elliptic curves over finite fields*, thesis, University of California, Berkeley, 1996, available at http://tinyurl.com/42lezaq. MR 2695524

[Kohel 2008] D. R. Kohel, "Complex multiplication and canonical lifts", pp. 67–83 in *Algebraic geometry and its applications*, edited by J. Chaumine et al., Ser. Number Theory Appl. **5**, World Sci. Publ., Hackensack, NJ, 2008. MR 2010d:14064 Zbl 1151.14329

[Lagarias and Odlyzko 1977] J. C. Lagarias and A. M. Odlyzko, "Effective versions of the Chebotarev density theorem", pp. 409–464 in *Algebraic number fields: L-functions and Galois properties* (Durham, NC, 1975), edited by A. Fröhlich, Academic Press, London, 1977. MR 56 #5506 Zbl 0362.12011

[Lang 1983] S. Lang, *Complex multiplication*, Grundlehren der Mathematischen Wissenschaften **255**, Springer, New York, 1983. MR 85f:11042 Zbl 0536.14029

[Lang 1987] S. Lang, *Elliptic functions*, 2nd ed., Graduate Texts in Mathematics **112**, Springer, New York, 1987. MR 88c:11028 Zbl 0615.14018

[Louboutin 2003] S. Louboutin, "Explicit lower bounds for residues at $s = 1$ of Dedekind zeta functions and relative class numbers of CM-fields", *Trans. Amer. Math. Soc.* **355**:8 (2003), 3079–3098. MR 2004f:11134 Zbl 1026.11085

[Mestre 1991] J.-F. Mestre, "Construction de courbes de genre 2 à partir de leurs modules", pp. 313–334 in *Effective methods in algebraic geometry* (Castiglioncello, 1990), edited by T. Mora and C. Traverso, Progr. Math. **94**, Birkhäuser, Boston, MA, 1991. MR 92g:14022 Zbl 0752.14027

[Mumford 1970] D. Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics **5**, Tata Institute, Bombay, 1970. MR 44 #219 Zbl 0223.14022

[Nakagawa 1996] J. Nakagawa, *Orders of a quartic field*, Mem. Amer. Math. Soc. **583**, American Mathematical Society, Providence, RI, 1996. MR 96k:11125 Zbl 0865.11069

[Pila 1990] J. Pila, "Frobenius maps of abelian varieties and finding roots of unity in finite fields", *Math. Comp.* **55**:192 (1990), 745–763. MR 91a:11071 Zbl 0724.11070

[Poor and Yuen 2000] C. Poor and D. S. Yuen, "Linear dependence among Siegel modular forms", *Math. Ann.* **318**:2 (2000), 205–234. MR 2001j:11024 Zbl 0972.11035

[Rosen 2011] M. Rosen, "The p-rank of the class group in cyclic p-power extensions", in preparation, 2011.

[Runge 1993] B. Runge, "On Siegel modular forms: I", *J. Reine Angew. Math.* **436** (1993), 57–85. MR 94c:11041 Zbl 0772.11015

[Shimura 1998] G. Shimura, *Abelian varieties with complex multiplication and modular functions*, Princeton Mathematical Series **46**, Princeton University Press, 1998. MR 99e:11076 Zbl 0908.11023

[Silverman 1994] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer, New York, 1994. MR 96b:11074 Zbl 0911.14015

[Spallek 1994] A.-M. Spallek, *Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen*, thesis, Universität Gesamthochschule Essen, 1994.

[Stevenhagen 2008] P. Stevenhagen, "The arithmetic of number rings", pp. 209–266 in *Algorithmic number theory: lattices, number fields, curves and cryptography*, edited by J. P. Buhler and P. Stevenhagen, Math. Sci. Res. Inst. Publ. **44**, Cambridge Univ. Press, 2008. MR 2009k:11213 Zbl 05532104

[Streng 2010] M. Streng, *Complex multiplication of abelian surfaces*, thesis, Universiteit Leiden, 2010.

[van Wamelen 1999] P. van Wamelen, "Examples of genus two CM curves defined over the rationals", *Math. Comp.* **68**:225 (1999), 307–320. MR 99c:11079 Zbl 0906.14025

[Weng 2003] A. Weng, "Constructing hyperelliptic curves of genus 2 suitable for cryptography", *Math. Comp.* **72**:241 (2003), 435–458. MR 2003i:14029 Zbl 1013.11023

Communicated by Hendrik W. Lenstra
Received 2009-10-23 Revised 2011-04-18 Accepted 2011-07-12

reinier@math.brown.edu *Department of Mathematics, Brown University, Box 1917, 151 Thayer Street, Providence, RI 02912, United States*

davidg@maths.usyd.edu.au *Laboratoire de Mathématiques Nicolas Oresme, CNRS UMR 5139, UFR Sciences, Campus 2, Boulevard Maréchal Juin, Université de Caen Basse-Normandie, 14032 Caen cedex, France*

klauter@microsoft.com *Microsoft Research, One Microsoft Way, Redmond, WA 98052, United States*

Algebra & Number Theory

www.jant.org

See inside back cover or www.jant.org for submission instructions.

The subscription price for 2011 is US $150/year for the electronic version, and $210/year (+$35 shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA.

Algebra & Number Theory (ISSN 1937-0652) at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

http://msp.org/

A NON-PROFIT CORPORATION

Typeset in LaTeX

Algebra & Number Theory

Volume 5 No. 4 2011

1937-0652(2011)5:4;1-D