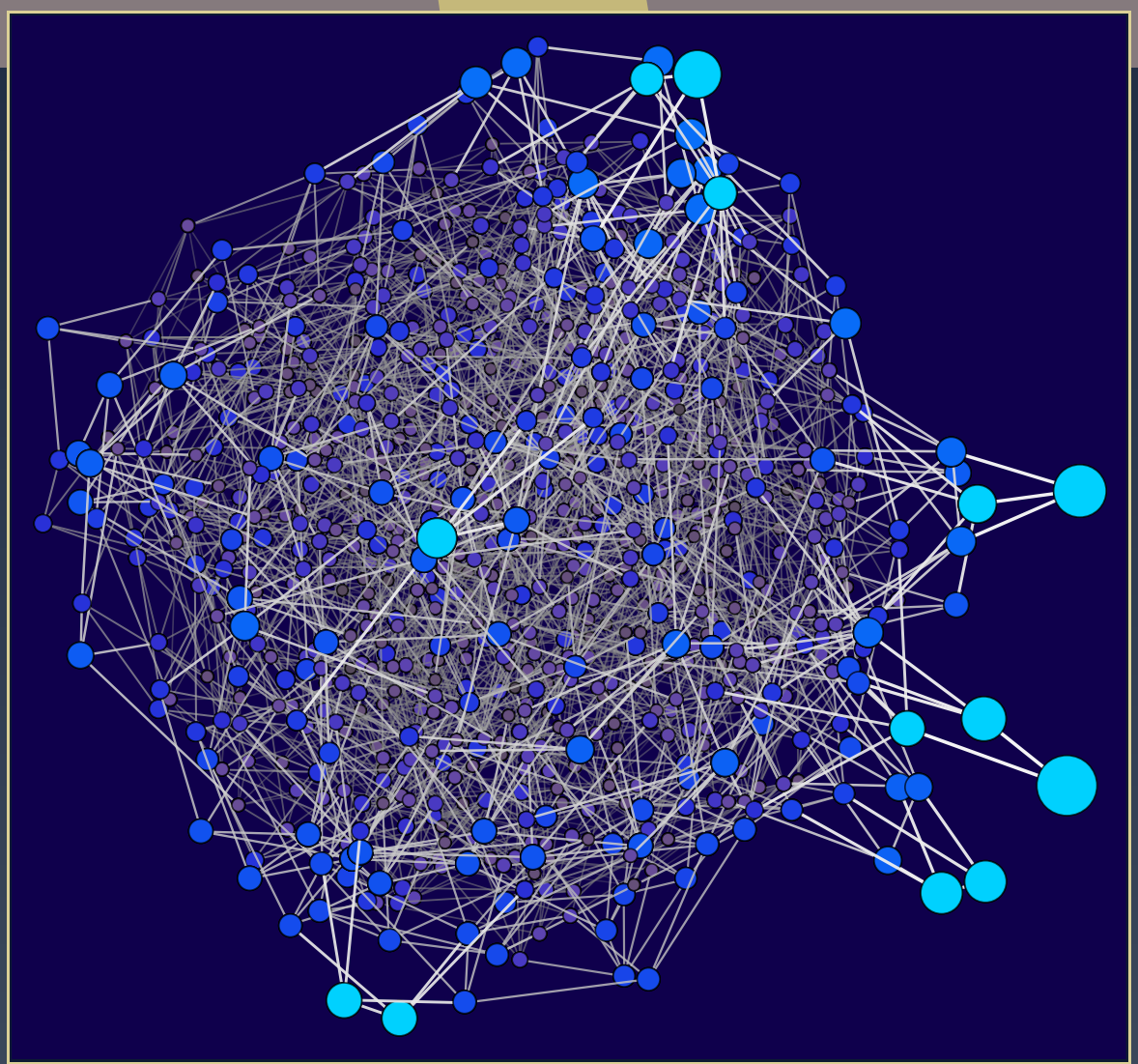
THE OPEN BOOK SERIES 4

ANTS XIV
Proceedings of the Fourteenth Algorithmic Number Theory Symposium

Algorithms to enumerate superspecial Howe curves of genus 4

Momonari Kudo, Shushi Harashita, and Everett W. Howe



msp

THE OPEN BOOK SERIES **4** (2020)
Fourteenth Algorithmic Number Theory Symposium
https://doi.org/10.2140/obs.2020.4.301

Algorithms to enumerate superspecial Howe curves of genus 4

Momonari Kudo, Shushi Harashita, and Everett W. Howe

A *Howe curve* is a curve of genus 4 obtained as the fiber product of two genus-1 double covers of $\boldsymbol{P}^1$. We present a simple algorithm for testing isomorphism of Howe curves, and we propose two main algorithms for finding and enumerating superspecial Howe curves: One involves solving multivariate systems coming from Cartier–Manin matrices, while the other uses Richelot isogenies of curves of genus 2. Comparing the two algorithms by implementation and by complexity analyses, we conclude that the latter enumerates superspecial Howe curves more efficiently. Using these algorithms, we show that there exist superspecial curves of genus 4 in characteristic p for every prime p with $7 < p < 20000$.

1. Introduction

1A. ***Background and motivation.*** Let K be an algebraically closed field of characteristic $p > 0$. A nonsingular curve over K is called *superspecial* (resp. *supersingular*) if its Jacobian variety is isomorphic (resp. isogenous) to a product of supersingular elliptic curves. Superspecial curves are not only theoretically interesting in algebraic geometry and number theory but also have many applications in coding theory, cryptology, and so on, because they tend to have many rational points and their Jacobian varieties have large endomorphism rings. However, it is not always easy to find such curves, and there are only finitely many superspecial curves for a given genus and characteristic. One method of constructing superspecial curves is to consider fiber products of superspecial curves of lower genera. In this paper, we demonstrate that this method can be efficient by considering the simplest example in which the genus is at least 4: the case of Howe curves. A *Howe curve* (so named by Kudo, Harashita and Senda in [23]) is a curve of genus 4 obtained as the fiber product of two genus-1 double covers $E_1 \to \boldsymbol{P}^1$ and $E_2 \to \boldsymbol{P}^1$. In [11], Howe studied these curves in order to quickly construct genus-4 curves with many rational points.

1B. ***Related works.*** The reason that we consider the case of genus $g \geq 4$ is that the enumeration of the isomorphism classes of superspecial curves with $g \leq 3$ has already been done, by Deuring [4] for $g = 1$, by Ibukiyama, Katsura, and Oort [14] for $g = 2$, and by Brock [3] for $g = 3$; see also Ibukiyama [13] and Oort [25] for the existence of such curves for $g = 3$. In contrast to the case $g \leq 3$, the existence or

MSC2020: primary 11G20; secondary 14G15, 14H45.
Keywords: algebraic curves, superspeciality.

nonexistence of a superspecial curve of genus 4 in general characteristic is an open problem, although some results for specific small p are known; see [5, Theorem 1.1] for the nonexistence for $p \leq 3$ and [22, Theorem B] for the nonexistence for $p = 7$. As for enumeration, computational approaches have been proposed recently in [21], [22], and [20] in the case of genus 4. The main strategy common to these papers is to parametrize a family of curves (canonical curves in the first two papers, hyperelliptic curves in the third), and then to find the superspecial curves X in these families by computing the zeros of a multivariate system derived from the condition that the Cartier–Manin matrix of X is zero. With computer algebra techniques such as Gröbner bases, the authors of these papers enumerated superspecial canonical curves for $p \leq 11$ in [21] and [22] and superspecial hyperelliptic curves for $p \leq 23$ in [20]. However, results for larger p have not been obtained yet due to the cost of solving multivariate systems, and no complexity analysis is given in [21], [22], or [20].

Now we turn our attention to Howe curves. Recently, it was proven in [23] that there exists a supersingular Howe curve in every positive characteristic. In particular, the authors of [23] reduce the existence of such a curve to the existence of a zero of a certain multivariate system, as follows: They study a family of Howe curves realized as $E_1 : z^2 = f_1(x)$ and $E_2 : w^2 = f_2(x)$ for cubic polynomials f_1 and f_2 parametrized by elements $(\lambda : \mu : \nu)$ of $\boldsymbol{P}^2$. Let C be the genus-2 curve $y^2 = f_1 f_2$. The supersingularity of H is equivalent to that of E_1, E_2 and C, because there exists an isogeny of 2-power degree from the Jacobian $J(H)$ to $E_1 \times E_2 \times J(C)$ [11, Theorem 2.1]. Thus, once supersingular isomorphism classes of E_1 and E_2 are given, finding supersingular curves H is reduced to finding values of the parameter $(\lambda : \mu : \nu)$ that satisfy a multivariate system derived from the supersingularity of C. The authors of [23] deduced the existence of such a zero $(\lambda : \mu : \nu)$ from various algebraic properties of the defining polynomials of the system.

The above reduction is applicable also for the superspecial case, but the method used in [23] to prove the existence of solutions does not carry over well. For this reason, the superspecial case is still open, and we are left to ask: For which primes $p > 7$ are there superspecial Howe curves in characteristic p?

1C. ***Our contribution.*** We study the existence of superspecial Howe curves by creating efficient algorithms to produce and enumerate them. The following theorems summarize some of what we have found.

Theorem 1.1. *For every prime p with $7 < p < 20000$ or with $p \equiv 5 \bmod 6$, there exists a superspecial Howe curve in characteristic p.*

Theorem 1.2. *For every prime p with $7 < p \leq 199$, the number of isomorphism classes of superspecial Howe curves in characteristic p is given in Table 1.*

The upper bounds on p in these two theorems can easily be increased. For example, on a 2.8 GHz quad-core Intel Core i7 with 16GB RAM, computing the 8351 superspecial Howe curves in characteristic 199 using method (B) below took 124 seconds in Magma. Finding examples of superspecial Howe curves for every p between 7 and 20000 took 680 minutes on the same machine.

p	$n(p)$	ratio	p	$n(p)$	ratio	p	$n(p)$	ratio
11	4	3.462	67	260	0.996	137	2430	1.089
13	3	1.573	71	742	2.388	139	2447	1.050
17	10	2.345	73	316	0.936	149	3082	1.073
19	4	0.672	79	595	1.390	151	3553	1.189
23	33	3.125	83	655	1.320	157	3427	1.020
29	45	2.126	89	863	1.410	163	3518	0.936
31	59	2.281	97	802	1.012	167	6268	1.550
37	41	0.932	101	1207	1.350	173	4780	1.064
41	105	1.755	103	1151	1.213	179	5771	1.159
43	79	1.145	107	1237	1.163	181	5419	1.053
47	235	2.608	109	1193	1.061	191	9610	1.589
53	167	1.292	113	1323	1.056	193	6298	1.009
59	259	1.453	127	2013	1.132	197	6839	1.030
61	243	1.233	131	2606	1.335	199	8351	1.221

Table 1. For each prime p from 11 to 199, we give the number $n(p)$ of superspecial Howe curves over $\overline{\mathbb{F}}_p$ and the ratio of $n(p)$ to the heuristic prediction $p^3/1152$ (see Section 5).

In this paper we discuss two strategies, (A) and (B) below, to find superspecial Howe curves. We also show how isomorphisms between Howe curves can be easily detected from the data that defines them, in (C).

(A) (E_1, E_2)-*first, using Cartier–Manin matrices.* In this strategy, we use the same realization of Howe curves as in [23], that is, the fiber product of

$$E_1 : z^2 y = x^3 + A_1\mu^2 x y^2 + B_1\mu^3 y^3 \quad \text{and} \quad E_2 : w^2 y = (x-\lambda)^3 + A_2\mu^2(x-\lambda)y^2 + B_2\mu^3 y^3$$

over $\boldsymbol{P}^1 = \operatorname{Proj} K[x, y]$. We enumerate pairs (E_1, E_2) of supersingular elliptic curves so that C is superspecial. We first discuss the field of definition of superspecial Howe curves (see Proposition 4.1), which enables us to reduce the size of our search space drastically. Specifically, the coordinates A_1, B_1, A_2, B_2, λ, μ, ν belong to $\mathbb{F}_{p^2}$, whereas in the supersingular case [23] these coordinates can generate larger subfields of $\overline{\mathbb{F}}_p$. For the test of superspeciality, we use the criterion that the Cartier–Manin matrix of C must be zero [14, Lemma 1.1(i)]. This reduces the enumeration problem to solving a system of algebraic equations. See Section 4 for the details of this strategy, including a complexity analysis.

(B) *C-first, using Richelot isogenies.* The second strategy first enumerates superspecial curves $C : y^2 = f(x)$ of genus 2 with $f(x)$ of degree 6 and then enumerates decompositions $f(x) = f_1(x) f_2(x)$ with $f_i(x)$ of degree 3 so that there is a b that makes both curves $E_i : y^2 = (x-b) f_i(x)$ supersingular. The moduli space of curves of genus 2 is of dimension 3. As this dimension is bigger than the space of $(\lambda : \mu : \nu) \in \boldsymbol{P}^2$ considered in (A), this strategy, a priori, looks inefficient. But, surprisingly, we conclude that strategy (B) enumerates superspecial Howe curves much more efficiently than does (A). The advantage of (B) comes from making use of Richelot isogenies. Specifically, we construct some superspecial curves of genus 2 by gluing supersingular elliptic curves together along their 2-torsion [12, §3], and then

produce more such curves by applying Richelot isogenies to the curves already produced. This procedure terminates because there are only finitely many superspecial curves of genus 2, and a recent result of Jordan and Zaytman [16, Corollary 18] shows that we obtain all isomorphism classes of superspecial curves of genus 2 in this way.[1]

(C) ***A new isomorphism test for Howe curves.*** Strategy (A) above produces many not-necessarily-distinct Howe curves, so to prevent overcounting we are left with the task of producing a unique representative for each isomorphism class. As every Howe curve is canonical (see Lemma 2.1), one may check whether two Howe curves are isomorphic by using the isomorphism test for canonical curves given in [22, §6.1], whose implementation is found in [21, §4.3]. This turns out to be very costly, because it uses many Gröbner basis computations. Our Corollary 3.3 gives a much simpler isomorphism test, based on the observation that a Howe curve is completely determined (up to isomorphism) by the degree-2 map to a genus-2 curve it is provided with by virtue of its definition as a fiber product. This isomorphism test is added on as a separate step in strategy (A), but is baked into the algorithm we use for strategy (B).

2. Howe curves and their superspeciality

In this section, we recall the definition of Howe curves, show that they are canonical, and give a computational criterion for their superspeciality.

Let K be an algebraically closed field of characteristic $p \neq 2$. A *Howe curve* over K is a curve which is isomorphic to the desingularization of the fiber product $E_1 \times_{\boldsymbol{P}^1} E_2$ of two genus-1 double covers $E_i \to \boldsymbol{P}^1$ ramified over S_i, where each S_i consists of four points and where $|S_1 \cap S_2| = 1$.

Given a Howe curve, there is an automorphism of $\boldsymbol{P}^1$ that takes the common ramification point of the two genus-1 double covers to infinity. Then the curves E_i can be written $w^2 = f_1$ and $z^2 = f_2$ for separable monic cubic polynomials $f_i \in K[x]$ that are coprime to one another, where x generates the function field of $\boldsymbol{P}^1$.

Lemma 2.1. *Every Howe curve is a canonical curve of genus* 4.

Proof. Let H be a Howe curve, normalized as above so that it is given as the fiber product of $w^2 = f_1$ and $z^2 = f_2$ for coprime separable monic cubic polynomials f_1 and f_2. For each i, let $f_i^{(\mathrm{h})} = y^3 f_i(x/y) \in K[x, y]$ be the homogenous cubic obtained from f_i and let H' be the curve defined in $\boldsymbol{P}^3 = \operatorname{Proj} K[x, y, z, w]$ by

$$z^2 - w^2 = q(x, y), \qquad z^2 y = f_1^{(\mathrm{h})}(x, y),$$

where $q(x, y)$ is the quadratic form

$$q(x, y) = (f_1^{(\mathrm{h})}(x, y) - f_2^{(\mathrm{h})}(x, y))/y.$$

Note that H' and $E_1 \times_{\boldsymbol{P}^1} E_2$ are isomorphic if the locus $y = 0$ is excluded. It is straightforward to see that H' is nonsingular, since f_1 and f_2 are separable and are coprime. Hence H and H' are isomorphic to one another (see [26, Proposition II.2.1]).

[1] As this paper was in press, Jordan and Zaytman updated their preprint to indicate that an equivalent result was proven earlier by Ekedahl and Oort.

It is well known that any nonsingular curve defined by a quadratic form and a cubic form in $\boldsymbol{P}^3$ is a canonical curve of genus 4 [7, Example IV.5.2.2]. □

To study the superspeciality of Howe curves, we first look at the decomposition of their Jacobians. Let f_1 and f_2 be coprime separable monic cubic polynomials, as above. Let $f = f_1 f_2$ and consider the hyperelliptic curve C of genus 2 defined by $u^2 = f$. By [11, Theorem 2.1], there exist two isogenies

$$\varphi : J(H) \to E_1 \times E_2 \times J(C),$$
$$\psi : E_1 \times E_2 \times J(C) \to J(H),$$

such that $\varphi \circ \psi$ and $\psi \circ \varphi$ are both multiplication by 2.

Suppose now that the characteristic p of K is an odd prime. Then $\psi \circ \varphi$ is an automorphism of the p-kernel of $J(H)$ and $\varphi \circ \psi$ is an automorphism of the p-kernel of $E_1 \times E_2 \times J(C)$, so $J(H)[p]$ and $E_1[p] \times E_2[p] \times J(C)[p]$ are isomorphic. Hence H is superspecial if and only if E_1 and E_2 are supersingular and C is superspecial.

Now we recall a criterion for the superspeciality of C. Let γ_i be the coefficient of x^i in $f^{(p-1)/2}$, and set

$$a = \gamma_{p-1}, \quad b = \gamma_{2p-1}, \quad c = \gamma_{p-2} \quad \text{and} \quad d = \gamma_{2p-2}.$$

Let M be the matrix

$$M = \begin{pmatrix} a^p & c^p \\ b^p & d^p \end{pmatrix}. \tag{2-1}$$

Then M is a Cartier–Manin matrix for C, that is, there is a basis for $H^0(C, \Omega^1_C)$ so that left multiplication by M represents the (semilinear) action of the Cartier operator; here Ω^1_C is the sheaf of differential 1-forms on C. (For information about Cartier–Manin matrices, see [1], which addresses issues with earlier literature, including the standard reference [27, §2].)

Lemma 2.2. *Let H be a Howe curve as above. Then H is superspecial if and only if E_1 and E_2 are supersingular and $a = b = c = d = 0$.*

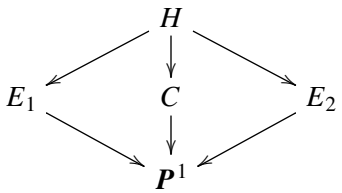
Proof. We already noted that H is superspecial if and only if E_1 and E_2 are supersingular and C is superspecial. But C is superspecial if and only if the Cartier operator acts trivially on $H^0(C, \Omega^1_C)$ [24, Theorem 4.1]. □

3. Detecting isomorphisms of Howe curves

In this section, we give an efficient criterion for determining whether two Howe curves are isomorphic or not. This criterion will be used in both the first and the second approach to enumerating superspecial Howe curves over a finite field.

We continue to work over an algebraically closed field of characteristic $p \neq 2$. Recall from Section 2 that a Howe curve is the desingularization of the fiber product of two genus-1 double covers of $\boldsymbol{P}^1$, where the ramification loci of the two covers overlap in exactly one point. This means that a Howe curve is

precisely a genus-4 curve H that fits into a V_4-diagram of the following form, where C is a curve of genus 2 and E_1 and E_2 are curves of genus 1:



If $E_1 \to \boldsymbol{P}^1$ ramifies at points P, Q_1, Q_2, and Q_3, and if $E_2 \to \boldsymbol{P}^1$ ramifies at P, R_1, R_2, and R_3, then the Weierstrass points of C are the points lying over Q_1, Q_2, Q_3, R_1, R_2, and R_3. On the other hand, the point P splits in the cover $C \to \boldsymbol{P}^1$, and we let P_1 and P_2 be the points of C lying over P.

Thus, to specify a Howe curve, it is enough to provide three pieces of information:

(1) A genus-2 curve C.

(2) An unordered pair of disjoint sets $\{W_1, W_2\}$, each consisting of three Weierstrass points of C.

(3) An unordered pair of distinct points $\{P_1, P_2\}$ on C that are mapped to one another by the hyperelliptic involution.

This data determines the V_4-diagram above, and hence also determines the double cover $\eta : H \to C$, which we call the *structure map* for the given data. Of course, if α is an automorphism of C then $\{\alpha(W_1), \alpha(W_2)\}$ and $\{\alpha(P_1), \alpha(P_2)\}$ will give us a double cover $H \to C$ that is isomorphic to η, namely, $\alpha\eta$.

Lemma 3.1. *The data specifying a Howe curve is recoverable* (*up to automorphisms of* C) *just from the structure map* $\eta : H \to C$.

Proof. The map $C \to \boldsymbol{P}^1$ is unique (up to automorphism of $\boldsymbol{P}^1$), so we recover the entire map $H \to C \to \boldsymbol{P}^1$ from η. This map is a Galois extension with group V_4, so we recover the genus-1 curves in the extension, and hence the division of the Weierstrass points of C. The pair of points $\{P_1, P_2\}$ is simply the set of ramification points of η. □

Theorem 3.2. *Two structure maps* $\eta_1 : H \to C_1$ *and* $\eta_2 : H \to C_2$ *starting from the same Howe curve* H *are isomorphic to one another. That is, there is an isomorphism* $\gamma : C_1 \to C_2$ *and an automorphism* $\delta : H \to H$ *such that the following diagram commutes*:

$$\begin{array}{ccc} H & \xrightarrow{\delta} & H \\ {\scriptstyle \eta_1}\downarrow & & \downarrow{\scriptstyle \eta_2} \\ C_1 & \xrightarrow{\gamma} & C_2 \end{array}$$

Proof. Let U_1 and U_2 be the V_4-subgroups of $\mathrm{Aut}\, H$ specified by η_1 and η_2, and let S be the 2-Sylow subgroup of $\mathrm{Aut}\, H$ that contains U_1. By conjugating U_2 by an automorphism δ (and thereby replacing η_2 with $\eta_2\delta$) we may assume that U_2 is also contained in S. Let α_1 and α_2 be the involutions of H corresponding to the double covers η_1 and η_2, and for each i, let β_i and γ_i be the other nonzero elements of U_i.

If α_1 and α_2 are conjugate to one another in S (or even in $\mathrm{Aut}\, H$), we are done. So assume, to get a contradiction, that α_1 and α_2 lie in different conjugacy classes of S.

We know that the quotient of H by the subgroup $\langle \alpha_i \rangle$ has genus 2, while the quotients of H by $\langle \beta_i \rangle$ and by $\langle \gamma_i \rangle$ have genus 1. The same is true for all of the conjugates of α_i, β_i, and γ_i in S. More generally, if we have two commuting involutions in S that generate a V_4-subgroup, we obtain a diagram

$$\begin{array}{ccccc} & & H & & \\ & \swarrow & \downarrow & \searrow & \\ Y_1 & & Y_2 & & Y_3 \\ & \searrow & \downarrow & \swarrow & \\ & & X & & \end{array} \tag{3-1}$$

We know that none of the curves Y_i can have genus 0 (by Lemma 2.1), so the only possibilities are that either all of the Y_i have genus 2 and X has genus 1, or one of the Y_i has genus 2, the other two have genus 1, and X has genus 0. (This follows from the fact that in any diagram such as (3-1), the genus of H is the sum of the genera of the Y_i minus twice the genus of X; see [17, Theorem B].) Thus, given two commuting involutions in S, if we know the genera of the quotients of H they produce, we can deduce the genus of the quotient of H by their product.

Our strategy, then, will be to enumerate all possible 2-groups S that occur as the 2-Sylow subgroup of the automorphism group of a nonhyperelliptic curve H of genus 4, along with all possible pairs U_1 and U_2 of V_4-subgroups of S that contain elements α_1 and α_2 that are not conjugate in S. We will assume that α_1 and α_2 generate genus-2 curves, while the other involutions in U_1 and U_2 generate genus-1 curves. Given these assumptions, we deduce, for as many involutions as we can, the genera of the curves associated to these involutions.

Suppose δ is an involution in S for which we know that the quotient $Y = H/\langle \delta \rangle$ has genus 2. Let T be the centralizer of δ in S. Then the quotient $T/\langle \delta \rangle$ is contained in the automorphism group of the genus-2 curve Y. Using Igusa's classification of the automorphism groups of genus-2 curves [15, §8], we can show that there are only eight 2-groups that appear as subgroups of the automorphism groups of genus-2 curves. If $T/\langle \delta \rangle$ is not one of these groups, then we have shown that the values of U_1, U_2, α_1, and α_2 cannot correspond to two different realizations of H as a Howe curve.

In order to use this strategy, we need a good bound on the sizes of automorphism groups of nonhyperelliptic curves of genus 4 in characteristic not 2. A result of Henn [10, Satz 1] (see also [6]) shows that in characteristic $p > 2$, the order of the automorphism group of a curve of genus g is strictly less than $8g^3$, except possibly when the curve is of one of the following types:

(1) $x^n + y^m = 1$, where $n = 1 + p^a$ for some $a > 0$ and $m \mid n$.

(2) $y^p - y = x^n$, where $n = 1 + p^a$ for some $a > 0$.

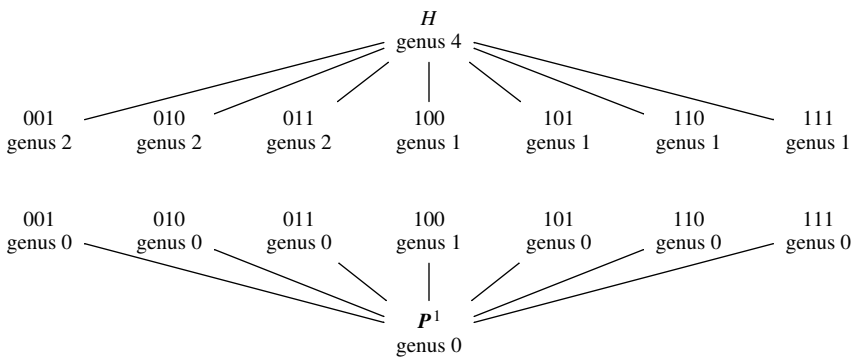
The first type of curve has genus $(n-2)(m-1)/2$, and if this is equal to 4 then either we have $n = 10$ and $m = 2$ (and $p = 3$) or we have $n = 6$ and $m = 3$ (and $p = 5$). In the first case the curve is hyperelliptic; in the second case, as Henn notes, the automorphism group has order 360, which is less than $8g^3$. The

second type of curve has genus $p^a(p-1)/2$, which is never equal to 4, because p is odd. Thus, it will suffice for us to look at every 2-group S of order less than $8 \cdot 4^3 = 512$.

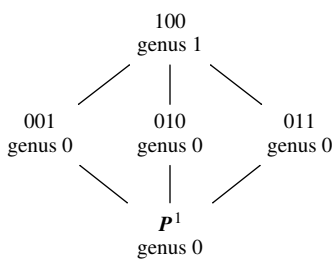
We implemented this computation in Magma; the code is available in the online supplement. We ran our code on all 2-groups of order less than 512, and the only group not eliminated was $S \cong (\boldsymbol{Z}/2\boldsymbol{Z})^3$.

For this S, our computation shows that of the seven involutions in S, three give genus-2 quotients and four give genus-1 quotients, and the three elements that give genus-2 quotients sum to zero. Now consider the seven V_4-subgroups T of S. Each such T gives us a diagram like (3-1) above. For the T that contains the three genus-2 involutions, the genus of H/T is 1, while for the other six V_4-subgroups T, the genus of H/T is 0.

Let us consider the diagram of subextensions between H and its quotient $H/S \cong \boldsymbol{P}^1$. We label the elements of S by vectors in $\mathbb{F}_2^3$, and we label the V_4-subgroups in the same way, with the convention that a V_4-subgroup labeled by v contains the elements with labels g such that the dot product of v and g is 0. Then the diagram of subextensions, with their genera, is as follows:



(For visual clarity, we have left off the heads of the arrows, and omitted the 21 arrows between the middle layers.) But this configuration of genera is not possible; consider for example the following subdiagram:



This diagram violates the genus property we mentioned below diagram (3-1).

This contradiction shows that the involutions α_1 and α_2 corresponding to the structure maps η_1 and η_2 lie in the same conjugacy class of Aut H, so that $\eta_1 = \eta_2\delta$ for an automorphism δ of H. □

Corollary 3.3. *Two triples* $(C, \{W_1, W_2\}, \{P_1, P_2\})$ *and* $(C', \{W_1', W_2'\}, \{P_1', P_2'\})$ *give isomorphic Howe curves if and only if there is an isomorphism* $C \to C'$ *that takes* $\{W_1, W_2\}$ *to* $\{W_1', W_2'\}$ *and* $\{P_1, P_2\}$ *to* $\{P_1', P_2'\}$.

This isomorphism test is very fast; it simply requires determining whether there are any automorphisms of $\boldsymbol{P}^1$ that respect the sets of Weierstrass points and their divisions, and that take the x-coordinate of P_1 and P_2 to that of P_1' and P_2'.

4. First approach: reduction to solving multivariate systems

In this section and the next, we present two approaches to solving the problem of enumerating superspecial Howe curves. As we mentioned in Section 1, the first approach, described in this section, enumerates pairs of supersingular elliptic curves $E_1 : w^2 = f_1$ and $E_2 : z^2 = f_2$ such that $C : y^2 = f_1 f_2$ is superspecial. For this, we shall apply a construction of Howe curves given in [23]. While this construction is different from the original one of [11], it can easily reduce our problem to finding roots of polynomial systems.

4A. ***Reduction to solving multivariate systems over finite fields.*** Let K be an algebraically closed field in characteristic $p > 3$. In [23], the authors parametrize the space of all Howe curves by the projective plane $\boldsymbol{P}^2$. We here briefly recall the parametrization; see [23, §2] for more details. Let $y^2 = x^3 + A_i x + B_i$ $(i = 1, 2)$ be two (nonsingular) elliptic curves, where $A_1, B_1, A_2, B_2 \in K$. Let λ, μ, ν be elements of K such that $\mu \neq 0$ and $\nu \neq 0$, and such that f_1 and f_2 are coprime, where

$$f_1(x) = x^3 + A_1\mu^2 x + B_1\mu^3, \tag{4-1}$$

$$f_2(x) = (x - \lambda)^3 + A_2\nu^2(x - \lambda) + B_2\nu^3. \tag{4-2}$$

A point $(\lambda : \mu : \nu) \in \boldsymbol{P}^2(K)$ satisfying these conditions is said to be *of Howe type* in [23]. Note that the isomorphism classes of E_1 and E_2 are independent of the choice of (λ, μ, ν) provided $\mu \neq 0$ and $\nu \neq 0$. Then the desingularization H of the fiber product $E_1 \times_{\boldsymbol{P}^1} E_2$ is a Howe curve, and vice versa.

This parametrization, together with the criterion of superspeciality in Section 2, enables us to reduce the search for superspecial Howe curves into solving multivariate systems over K; it suffices to compute the solutions $(\lambda : \mu : \nu) \in \boldsymbol{P}^2(K)$ (of Howe type) to $a = b = c = d = 0$, where a, b, c and d are the entries of the Cartier–Manin matrix of the hyperelliptic curve $C : y^2 = f_1 f_2$. Note that a, b, c and d are homogeneous as polynomials in λ, μ and ν, and that $\operatorname{ord}_*(-) = O(p)$ for $* = \lambda, \mu, \nu$ and for $- = a, b, c, d$.

Note that the multivariate systems above are zero-dimensional, since there are only finitely many points $(\lambda : \mu : \nu)$ parametrizing supersingular Howe curves (see [23]), whence the same thing holds for superspecial cases. In fact, we may assume that the coordinates A_1, B_1, A_2, B_2, λ, μ and ν belong to $\mathbb{F}_{p^2}$:

Proposition 4.1. *Any superspecial Howe curve is K-isomorphic to H obtained as above for A_1, B_1, A_2, B_2, μ, ν and λ belonging to $\mathbb{F}_{p^2}$.*

Proof. It suffices to consider the case of $K = \overline{\mathbb{F}}_{p^2}$, since every supersingular elliptic curve can be defined over $\mathbb{F}_{p^2}$ and (λ, μ, ν) is a solution of $a = b = c = d = 0$. Let H' be a superspecial Howe curve over $K = \overline{\mathbb{F}}_{p^2}$. Choose E_1' and E_2' over K so that H' is the normalization of $E_1' \times_{\boldsymbol{P}^1} E_2'$. It is well known that H' descends to a curve H over $\mathbb{F}_{p^2}$ such that the Frobenius map F (the p^2-power map) on $\operatorname{Jac}(H)$

is p or $-p$ and all automorphisms of H are defined over $\mathbb{F}_{p^2}$ (see the proof of [5, Theorem 1.1]). Let E_1 and E_2 be the quotients of H corresponding to E_1' and E_2'. The quotient E_i of H is obtained by an involution $\iota_i \in \mathrm{Aut}(H)$, and therefore is defined over $\mathbb{F}_{p^2}$. The quotient of H by the group generated by ι_1 and ι_2 is isomorphic to $\boldsymbol{P}^1$ over $\mathbb{F}_{p^2}$. Let S_i be the set of the ramified points of $E_i \to \boldsymbol{P}^1$. Since $S_1 \cap S_2$ consists of a single point, this point is invariant under the action of the absolute Galois group of $\mathbb{F}_{p^2}$ and therefore is an $\mathbb{F}_{p^2}$-rational point. An element of $\mathrm{PGL}_2(\mathbb{F}_{p^2})$ sends this point to the infinite point of $\boldsymbol{P}^1$. Since the Frobenius map F on E_i is also $\pm p$, the other elements P of S_i (which are 2-torsion points on E_i) are also $\mathbb{F}_{p^2}$-rational by $F(P) = \pm pP = P$. This implies the desired result. □

4B. ***Concrete algorithm.*** Based on the reduction described in the previous subsection, we present a concrete algorithm:

Algorithm 4.2. Calculating superspecial Howe curves by reduction to solving multivariate systems.

Input: A rational prime $p > 3$.

Output: A list $\mathcal{H}(p)$ of superspecial Howe curves, each of which is represented by a pair (f_1, f_2) of polynomials $f_1, f_2 \in \mathbb{F}_{p^2}[x]$.

(1) Compute the set $\mathcal{S}(p)$ of representatives of the $\overline{\mathbb{F}}_p$-isomorphism classes of supersingular elliptic curves in characteristic p such that each representative is given in Weierstrass form $E_{A,B}$: $y^2 = f_{A,B}(x) = x^3 + Ax + B$ by a pair (A, B) of elements in $\mathbb{F}_{p^2}$.

(2) Set $\mathcal{H}_0(p) \leftarrow \varnothing$. For each pair of E_{A_1,B_1} and E_{A_2,B_2} in $\mathcal{S}(p)$, possibly choosing $(A_1, B_1) = (A_2, B_2)$, conduct Steps (a)–(c) below to compute all $(\lambda, \mu, \nu) \in (\mathbb{F}_{p^2})^3$ of Howe type such that the desingularization H of $E_1 \times_{\boldsymbol{P}^1} E_2$ is superspecial, where $E_1 : w^2 = f_1$ (resp. $E_2 : z^2 = f_2$) is an elliptic curve $\mathbb{F}_{p^2}$-isomorphic to E_{A_1,B_1} (resp. E_{A_2,B_2}).

   (a) Compute the Cartier–Manin matrix M given in (2-1).

   (b) Compute the set $\mathcal{V}(A_1, B_1, A_2, B_2)$ of elements $(\lambda, \mu, \nu) \in (\mathbb{F}_{p^2})^3$ (with $\nu = 1$) such that $M = 0$.

   (c) For each $(\lambda, \mu, \nu) \in \mathcal{V}(A_1, B_1, A_2, B_2)$, if $\mu \neq 0$ and $\nu \neq 0$, set $\mathcal{H}_0(p) \leftarrow \mathcal{H}_0(p) \cup \{(f_1, f_2)\}$, where f_1 and f_2 are as in (4-1) and (4-2).

   Note: By Lemma 4.4 and Proposition 4.6 of [23], for each root (λ, μ, ν) computed in Step (b), the cubics f_1 and f_2 are coprime if $\mu \neq 0$ and $\nu \neq 0$. Moreover, it suffices to compute elements (λ, μ, ν) with $\nu = 1$; see Remark 4.2 of [19] for more details.

(3) Set $\mathcal{H}(p) \leftarrow \varnothing$. For each $(f_1, f_2) \in \mathcal{H}_0(p)$, if the Howe curve H represented by (f_1, f_2) is not isomorphic to any Howe curve of $\mathcal{H}(p)$, set $\mathcal{H}(p) \leftarrow \mathcal{H}(p) \cup \{H\}$.

The complexity of this algorithm is estimated as $\widetilde{O}(p^6)$, as long as $\#\mathcal{H}_0(p) = O(p^3)$; see Section 4C for more details.

Remark 4.3. If one would like to search for a single example of a superspecial Howe curve (or determine the nonexistence of such a curve), it suffices to decide the (non-)existence of a root in Step (b). In this case, it will be estimated in the next subsection that the complexity is $\widetilde{O}(p^5)$.

4C. ***Complexity of the first approach.*** We here briefly discuss the complexity of Algorithm 4.2 together with several variants of computing the roots of a multivariate system in Step (b). For reasons of space, we give only a summary of the estimation of the complexity, and refer to [19, §5.1] for most of the details. In the following, all time complexity bounds refer to arithmetic complexity, which is the number of operations in $\mathbb{F}_{p^2}$. We denote by $\mathsf{M}(n)$ the time to multiply two univariate polynomials over $\mathbb{F}_{p^2}$ of degree n.

For Step (1), one can check that its complexity is dominated by the cost of computing all supersingular j-invariants in characteristic p. This cost is bounded by $O(\log^2(p)\mathsf{M}(p)) = \widetilde{O}(p)$; see [19, §5.1.1] for details.

For Step (2), clearly the complexities of Steps (a) and (b) are larger than that of Step (c). In Step (a), we compute the Cartier–Manin matrix M from $f = f_1 f_2$ *with indeterminates* λ and μ. The cost of computing M is bounded by $\widetilde{O}(p^3)$; see Remark 4.4 below. In Step (b), there are three variants (i)–(iii) to compute all $(\lambda, \mu, \nu) \in (\mathbb{F}_{p^2})^3$ with $\nu = 1$ such that $M = 0$, where M is the Cartier–Manin matrix as in (2-1) with entries a, b, c and d:

(i) Use brute force to enumerate all $(\lambda, \mu) \in (\mathbb{F}_{p^2})^2$ to check whether M is equal to 0 or not.

(ii) Regard one of λ and μ, say λ, as a variable. For each $\mu \in \mathbb{F}_{p^2}$, compute the roots in $\mathbb{F}_{p^2}$ of $G = \gcd(a, b, c, d) \in \mathbb{F}_{p^2}[\lambda]$.

(iii) Regarding both λ and μ as variables, use an approach based on resultants.

It is estimated that the complexity of (i) is $O(p^5)$, and that those of (ii) and (iii) are bounded by the same bound $\widetilde{O}(p^4)$; more precisely, the upper-bound of the complexity of (ii) is less than that of (iii) if we consider logarithmic factors; see [19, §5.1.2].

From this, we adopt the fastest variant (ii) with complexity $\widetilde{O}(p^4)$ in our implementation. The number of (λ, μ, ν) with $\nu = 1$ computed in Step (b) is $\leq p^2 \times \deg(G) = O(p^3)$. Since the number of possible choices of $(E_{A_1,B_1}, E_{A_2,B_2})$ is $\#\mathcal{S}(p) = O(p^2)$, computing (λ, μ, ν) with $\nu = 1$ for all $(E_{A_1,B_1}, E_{A_2,B_2})$ is done in $\#\mathcal{S}(p) \times \widetilde{O}(p^4) = \widetilde{O}(p^6)$ operations in $\mathbb{F}_{p^2}$.

The complexity of Step (3) depends heavily on the number of superspecial Howe curves obtained in Step (2), that is, $\#\mathcal{H}_0(p)$. Since each isomorphism test is done in $O(1)$, the complexity of Step (3) is $O((\#\mathcal{H}_0(p))^2)$. As of this writing, we have not succeeded in finding any sharp bound on $\#\mathcal{H}_0(p)$. We can naively estimate $\#\mathcal{H}_0(p) = O(p^5)$ from the complexity analysis of Step (2), whereas we expect $\#\mathcal{H}_0(p) = O(p^3)$ from the practical behavior [19, §4.2, Table 1]. Thus, the complexity of Step (3) is naively $O(p^{10})$, but in practice $O(p^6)$ which does not exceed the complexity of Steps (1)–(2).

Note that to determine the (non-)existence of a superspecial Howe curve, it is not necessary to compute a root in Step (b), but it suffices to compute the gcd G only. Since each gcd can be computed in time $\widetilde{O}(p)$ by fast gcd algorithms, one can verify that the total complexity of this variant of Algorithm 4.2 is $\widetilde{O}(p^5)$.

Remark 4.4. In Step (a), we compute a Cartier–Manin matrix over $\mathbb{F}_{p^2}[\lambda, \mu]$. Bostan, Gaudry, and Schost showed that in general, computing the Cartier–Manin matrix M of a hyperelliptic curve $y^2 = f(x)$

defined over a field K can be accomplished by multiplying matrices obtained from recurrences for the coefficients of $f(x)^n$; see [2, §8] or [9, §2] for details. The algorithm of Harvey and Sutherland [9], which is an improvement of their earlier algorithm [8] presented at ANTS XI, is also based on this reduction, and it is the fastest algorithm to compute M for the case of $K = \mathbb{F}_p$. From this, we suspect that one of the best ways to compute M in Step (a) would be to extend the Harvey–Sutherland algorithm [9] to the case of $\mathbb{F}_{p^2}(\lambda, \mu)$. However, since we have not yet succeeded in making this extension, we compute M using the reduction mentioned above, or by using formulæ given in [23, §4] for M specific to Howe curves. It is estimated (to appear in a revised version of [19]) that the complexity of the latter method is bounded by $\widetilde{O}(p^3)$, which is less than or equal to that of Step (b).

5. Second approach: use of Richelot isogenies of genus-2 curves

In this section we propose another approach to enumerating superspecial Howe curves. As opposed to the approach in Section 4, this second approach *starts* with a superspecial genus-2 curve C, and then looks to see whether it will fit into a V_4-diagram with supersingular elliptic curves. While this is precisely the structure of Algorithm 5.7 of [11], the problem remains: How can we *quickly* produce a list of *all* of the superspecial genus-2 curves? We begin by addressing this question.

5A. ***Computing superspecial curves of genus 2.*** To produce a list $\mathcal{L}$ of all superspecial genus-2 curves, we use a variant of [11, Algorithm 5.7]. Each superspecial genus-2 curve has a unique model defined over $\mathbb{F}_{p^2}$ that is maximal over $\mathbb{F}_{p^2}$. Given one such curve, all of the curves that are Richelot isogenous to it are also maximal superspecial curves. Thus, given a not-necessarily-complete list of maximal superspecial curves, we can add curves to the list as follows: We go through the list one curve at a time. For each C we compute the curves that are Richelot isogenous to it, and we add each such curve to the list if it is not already on it. To seed our list, we can use the curves that are $(2, 2)$-isogenous to a product of maximal elliptic curves. Then a result of Jordan and Zaytman [16, Corollary 18] shows that this procedure will generate a complete list $\mathcal{L}$ of all superspecial genus-2 curves.

The exact number of curves on the list $\mathcal{L}$ is given by a result of Ibukiyama, Katsura, and Oort [14, Theorem 3.3]. The exact answer depends on the congruence class of p modulo 120, but it follows from their result that for $p > 3$ we have

$$\#\mathcal{L} = \frac{(p-1)(p^2+25p+166)}{2800} + c, \quad \text{where } \frac{-1}{16} \le c \le \frac{209}{180}.$$

5B. ***Testing whether a genus-2 curve fits into a V_4-diagram.*** For each $C \in \mathcal{L}$, given by an equation

$$y^2 = (x-a_1)(x-a_2)(x-a_3)(x-a_4)(x-a_5)(x-a_6),$$

we would like to try to fit C into a Howe curve diagram. For each of the ten ways of splitting the Weierstrass points into two groups of three (for example, into $\{\{a_1, a_2, a_3\}, \{a_4, a_5, a_6\}\}$), we could then

ask for the values of b such that the two genus-1 curves

$$y^2 = (x-b)(x-a_1)(x-a_2)(x-a_3) \tag{5-1}$$

and

$$y^2 = (x-b)(x-a_4)(x-a_5)(x-a_6) \tag{5-2}$$

are both supersingular. (We also consider "$b=\infty$", corresponding to the curves $y^2=(x-a_1)(x-a_2)(x-a_3)$ and $y^2=(x-a_4)(x-a_5)(x-a_6)$.) Since there are about $p/12$ supersingular j-invariants and hence about $p/2$ supersingular λ-invariants, there are about $p/2$ values of b that will make the first curve (5-1) supersingular, and we can compute these values in time $\widetilde{O}(p)$. For each b, we then check whether the second curve (5-2) is supersingular. If we were to model this as choosing a random λ-invariant in $\mathbb{F}_{p^2}$ and asking whether it is supersingular, we would expect success with probability around $1/(2p)$.

It is easy to incorporate isomorphism testing into this algorithm so that it produces each superspecial Howe curve exactly once: All we have to do is keep track of how the automorphism group of C acts on the divisions of its Weierstrass points and on the good values of b.

Thus, in time $\widetilde{O}(p^4)$, we can produce unique representatives for each superspecial Howe curve. Heuristically, the number of superspecial Howe curves we find should be the number of superspecial genus-2 curves ($\approx p^3/2880$), times the number of Weierstrass point divisions (10), times the number of values of b that make the first elliptic curve supersingular ($\approx p/2$), times the probability that the second curve is supersingular ($\approx 1/(2p)$). Heuristically, then, we expect to find about $p^3/1152$ superspecial Howe curves.

5C. *Concrete algorithm.*

Algorithm 5.1. Calculating superspecial Howe curves using Richelot isogenies of genus-2 curves.

Input: A rational prime $p > 3$.

Output: A list $\mathcal{H}(p)$ of superspecial Howe curves, each of which is represented by a pair (f_1, f_2) of polynomials $f_1, f_2 \in \mathbb{F}_{p^2}[x]$, corresponding to the curve $y^2 = f_1, z^2 = f^2$.

(1) Compute the set $\mathrm{MaxEll}(p^2)$ of $\mathbb{F}_{p^2}$-isomorphism classes of $\mathbb{F}_{p^2}$-maximal elliptic curves over $\mathbb{F}_{p^2}$. Since every supersingular curve has a unique maximal twist, this can be done as in Step (1) of Algorithm 4.2.

(2) Set $\mathcal{L} \leftarrow \varnothing$. For each pair (E, E') of elements in $\mathrm{MaxEll}(p^2)$, compute the (at most 6) curves C whose Jacobians are $(2,2)$-isogenous to $E \times E'$ (see [12, §3]). Adjoin each of these to $\mathcal{L}$ if it is not isomorphic to an element of $\mathcal{L}$.

(3) Write $\mathcal{L} = \{C_1, \ldots, C_n\}$. Set $i = 1$.

  (a) For each nonsingular curve C' which is Richelot isogenous to C_i, if C' is not isomorphic to any element of $\mathcal{L}$, set $N \leftarrow |\mathcal{L}|$ and put $C_{N+1} = C'$ and $\mathcal{L} \leftarrow \mathcal{L} \cup \{C_{N+1}\}$.

  (b) If $i < |\mathcal{L}|$, set $i \leftarrow i+1$ and go to (a).

(4) Set $\mathcal{H}(p) \leftarrow \varnothing$.

(5) For each $C \in \mathcal{L}$, check whether C fits into a Howe curve diagram with supersingular double covers $E_i \to \boldsymbol{P}^1$.

   (a) For each splitting of the Weierstrass point of C into two disjoint three-element sets, compute the j-invariants of the genus-1 curves (5-1) and (5-2), as functions of the indeterminate b. Find the values of b that make the first curve supersingular, and for each such value, check to see whether the second curve is supersingular. Record each value of b for which both curves are supersingular.

   (b) Using Corollary 3.3, find unique representatives $y^2 = f_1, z^2 = f_2$ for the curves produced in the previous step, and adjoin (f_1, f_2) to $\mathcal{H}(p)$.

We noted in the previous subsection that Step (5) takes $\widetilde{O}(p^4)$ arithmetic operations over $\mathbb{F}_{p^2}$, and the other steps clearly take fewer operations than this.

6. Implementations and proofs

In this section, we describe our implementations of the algorithms in the previous sections and our proofs of the main results stated in the Introduction. As we have seen, there are two approaches to enumerating superspecial Howe curves: (A) (E_1, E_2)-first and (B) C-first. The arguments in the previous sections show that (B) has an advantage in the complexity analysis. Here we see that (B) is far superior to (A) also when we execute their implementations. Indeed, Theorems 1.1 and 1.2 in the Introduction were obtained by Magma implementations based on (B) that were run on a PC with Ubuntu 16.04 LTS OS at 3.40GHz CPU (Intel Core i7-6700) and 15.6 GB memory. The same result for $p \leq 53$ was obtained by implementing the method (A) over Magma with an execution by the same PC. Although it took 11871 seconds to obtain Theorem 1.2 for $p \leq 53$ by (A), the second strategy (B) finishes the enumeration for $p \leq 199$ in only 924 seconds; see Table 2 for benchmark timing data for small p.

The code for our implementations is available in the online supplement. In case (A), it is very costly to find Cartier–Manin matrices, and in addition to that there are many pairs (E_1, E_2) of supersingular elliptic curves. This fact is consistent with the complexity analysis in Section 4C. On the other hand, the method (B) contains few intensive computations and it enables us to find and enumerate superspecial Howe curves very efficiently.

The preceding remarks prove the computational results in Theorems 1.1 and 1.2, and we are left to prove the statement in Theorem 1.1 concerning primes $p \equiv 5 \bmod 6$. This fact is shown by using the Howe curve defined by $E_1 : z^2y = x^3 + y^3$ and $E_2 : w^2y = x^3 + ay^3$ with $a \in \{-1, 1/4\}$. Indeed, if $p \equiv 5 \bmod 6$, then these two elliptic curves are supersingular and moreover $y^2 = (x^3 + 1)(x^3 + a)$ is superspecial. This can be checked by observing that the curve has two nonhyperelliptic involutions, given by $(x, y) \mapsto (a^{1/3}/x, \pm a^{1/2}y/x^3)$, so that its Jacobian is $(2, 2)$-isogenous to a product of elliptic curves. For $a = -1$ we find that these two curves are both isomorphic to the $j = 0$ curve with CM by -3,

p	(A)	(B)	p	(A)	(B)	p	(A)	(B)
5	0.02	0.08	19	6.14	0.12	41	1118.63	0.71
7	0.01	0.01	23	27.59	0.21	43	1423.26	0.80
11	0.17	0.04	29	114.70	0.31	47	2686.17	1.03
13	0.76	0.05	31	193.82	0.34	53	5678.32	1.46
17	3.92	0.09	37	617.23	0.54			

Table 2. Benchmark timing data for (A) Algorithm 4.2 and (B) Algorithm 5.1. All times shown are in seconds.

and for $a = 1/4$ we find that they are both isomorphic to the $j = -12288000$ curve with CM by -27. In both cases, these elliptic curves are supersingular for primes $p \equiv 5 \bmod 6$.

We remark that this curve for $a = 1/4$ is isomorphic to the curve $X^3 + Y^3 + W^3 = 2YW + Z^2 = 0$ in $\boldsymbol{P}^3$ studied by the Kudo in [18], by the correspondence $x = X$, $y = Y + W$, $z = \sqrt{-3/2}Z$ and $w = \sqrt{-3/4}(Y - W)$.

Acknowledgments

Kudo and Harashita thank Everett Howe for joining as the third author; he told them the second strategy (B), which had not been considered in the earlier version [19]. Howe thanks Professors Kudo and Harashita for inviting him to join them in this work. The authors thank the referees for their careful reading and for helpful suggestions and comments. This work was supported by JSPS Grant-in-Aid for Scientific Research (C) 17K05196, JSPS Grant-in-Aid for Research Activity Start-up 18H05836 and 19K21026, and JSPS Grant-in-Aid for Young Scientists 20K14301.

References

[1] Jeffrey D. Achter and Everett W. Howe, *Hasse–Witt and Cartier–Manin matrices: a warning and a request*, Arithmetic geometry: computation and applications (Y. Aubry, E. W. Howe, and C. Ritzenthaler, eds.), Contemp. Math., vol. 722, Amer. Math. Soc., Providence, RI, 2019, pp. 1–18. MR 3896846

[2] Alin Bostan, Pierrick Gaudry, and Éric Schost, *Linear recurrences with polynomial coefficients and application to integer factorization and Cartier–Manin operator*, SIAM J. Comput. **36** (2007), no. 6, 1777–1806. MR 2299425

[3] Bradley Wayne Brock, *Superspecial curves of genera two and three*, Ph.D. thesis, Princeton University, 1993. MR 2689446

[4] Max Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272.

[5] Torsten Ekedahl, *On supersingular curves and abelian varieties*, Math. Scand. **60** (1987), no. 2, 151–178. MR 914332

[6] Massimo Giulietti and Gábor Korchmáros, *Nakajima's remark on Henn's proof*, Electron. Notes Discrete Math. **40** (2013), 135–138.

[7] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York–Heidelberg, 1977, Graduate Texts in Mathematics, No. 52. MR 0463157

[8] David Harvey and Andrew V. Sutherland, *Computing Hasse–Witt matrices of hyperelliptic curves in average polynomial time*, LMS J. Comput. Math. **17** (2014), suppl. A, 257–273. MR 3240808

[9] David Harvey and Andrew V. Sutherland, *Computing Hasse–Witt matrices of hyperelliptic curves in average polynomial time, II*, Frobenius distributions: Lang–Trotter and Sato–Tate conjectures (D. Kohel and I. Shparlinski, eds.), Contemp. Math., vol. 663, Amer. Math. Soc., Providence, RI, 2016, pp. 127–147. MR 3502941

[10] Hans-Wolfgang Henn, *Funktionenkörper mit grosser Automorphismengruppe*, J. Reine Angew. Math. **302** (1978), 96–115. MR 511696

[11] Everett W. Howe, *Quickly constructing curves of genus 4 with many points*, Frobenius distributions: Lang–Trotter and Sato–Tate conjectures (D. Kohel and I. Shparlinski, eds.), Contemp. Math., vol. 663, Amer. Math. Soc., Providence, RI, 2016, pp. 149–173. MR 3502942

[12] Everett W. Howe, Franck Leprévost, and Bjorn Poonen, *Large torsion subgroups of split Jacobians of curves of genus two or three*, Forum Math. **12** (2000), no. 3, 315–364. MR 1748483

[13] Tomoyoshi Ibukiyama, *On rational points of curves of genus 3 over finite fields*, Tohoku Math. J. (2) **45** (1993), no. 3, 311–329. MR 1231559

[14] Tomoyoshi Ibukiyama, Toshiyuki Katsura, and Frans Oort, *Supersingular curves of genus two and class numbers*, Compositio Math. **57** (1986), no. 2, 127–152. MR 827350

[15] Jun-ichi Igusa, *Arithmetic variety of moduli for genus two*, Ann. of Math. (2) **72** (1960), 612–649. MR 114819

[16] Bruce W. Jordan and Yevgeny Zaytman, *Isogeny graphs of superspecial abelian varieties and generalized Brandt matrices*, preprint, 2020. arXiv:2005.09031

[17] Ernst Kani and Michael Rosen, *Idempotent relations and factors of Jacobians*, Math. Ann. **284** (1989), no. 2, 307–327. MR 1000113

[18] Momonari Kudo, *On the existence of superspecial and maximal nonhyperelliptic curves of genera four and five*, Comm. Algebra **47** (2019), no. 12, 5020–5038. MR 4019321

[19] Momonari Kudo and Shushi Harashita, *Algorithm to enumerate superspecial Howe curves of genus* 4, preprint, 2020. arXiv:2003.04153

[20] Momonari Kudo and Shushi Harashita, *Algorithmic study of superspecial hyperelliptic curves over finite fields*, preprint, 2019. arXiv:1907.00894

[21] Momonari Kudo and Shushi Harashita, *Computational approach to enumerate non-hyperelliptic superspecial curves of genus* 4, Tokyo J. Math **43** (2020), no. 1, 259–278. MR 4121797

[22] Momonari Kudo and Shushi Harashita, *Superspecial curves of genus* 4 *in small characteristic*, Finite Fields Appl. **45** (2017), 131–169. MR 3631358

[23] Momonari Kudo, Shushi Harashita and Hayato Senda, *The existence of supersingular curves of genus* 4 *in arbitrary characteristic*, Res. Number Theory **6** (2020), no. 4, article 44. MR 4170348

[24] Niels O. Nygaard, *Slopes of powers of Frobenius on crystalline cohomology*, Ann. Sci. École Norm. Sup. (4) **14** (1981), no. 4, 369–401 (1982). MR 654203

[25] Frans Oort, *Hyperelliptic supersingular curves*, Arithmetic algebraic geometry (Texel, 1989) (G. van der Geer, F. Oort, and J. Steenbrink, eds.), Progr. Math., vol. 89, Birkhäuser Boston, Boston, MA, 1991, pp. 247–284. MR 1085262

[26] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094

[27] Noriko Yui, *On the Jacobian varieties of hyperelliptic curves over fields of characteristic* $p > 2$, J. Algebra **52** (1978), no. 2, 378–410. MR 491717

Received 25 Feb 2020. Revised 1 Aug 2020.

MOMONARI KUDO: kudo@mist.i.u-tokyo.ac.jp
Department of Mathematical Informatics, Graduate School of Information Science and Technology, The University of Tokyo, Bunkyo-ku, Tokyo, Japan

SHUSHI HARASHITA: harasita@ynu.ac.jp
Graduate School of Environment and Information Sciences, Yokohama National University, Hodogaya-ku, Yokohama, Japan

EVERETT W. HOWE: however@alumni.caltech.edu
San Diego, CA, United States

VOLUME EDITORS

Stephen D. Galbraith
Mathematics Department
University of Auckland
New Zealand
https://orcid.org/0000-0001-7114-8377

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

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

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

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

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

First published 2020.

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org **http://msp.org**

THE OPEN BOOK SERIES 4

Fourteenth Algorithmic Number Theory Symposium

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

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

TABLE OF CONTENTS