Computing Igusa Class Polynomials

Marco Streng

September 19, 2008

Abstract

We give the first runtime bound and proof of correctness of any algorithm that computes the genus two class polynomials of a primitive quartic CM field K. Our algorithm is a complex analytic algorithm and runs in time $\widetilde{O}(\Delta^{7/2})$, where Δ is the discriminant of K.

1 Introduction

The *Hilbert class polynomial* $H_K \in \mathbf{Z}[X]$ of an imaginary quadratic number field K has as roots the j-invariants of complex elliptic curves having complex multiplication (CM) by $\mathcal{O}_K$. These roots generate the Hilbert class field of K and Weber [35] computed H_K for many small K. The CM method uses the reduction of H_K modulo large primes p to construct elliptic curves over $\mathbf{F}_p$ with a prescribed number of points, for example for cryptography. The bit size of H_K grows exponentially with K, like $\widetilde{O}(\Delta_K)$, hence so does the runtime of the algorithms that compute it.

If we go from elliptic curves (genus 1) to genus 2 curves, we get the *Igusa class polynomials* $H_{K,n} \in \mathbf{Q}[X]$ $(n = 1, 2, 3)$ of a *quartic CM field* K. Their roots are the Igusa invariants of all complex genus 2 curves having CM by $\mathcal{O}_K$. As for genus 1, these roots generate class fields and the reduction modulo large primes p yields cryptographic curves of genus 2. Computing these polynomials is considerably more complicated, also because of denominators. Recently, various algorithms have been developed [7, 10, 31, 33], but there were no runtime or precision bounds available.

This paper describes a complete and correct algorithm that computes Igusa class polynomials $H_{K,n}$ of any *primitive quartic CM field* $K = \mathbf{Q}(\sqrt{\Delta_0}, \sqrt{-a + b\sqrt{\Delta_0}})$, where Δ_0 is a real quadratic discriminant and $a, b \in \mathbf{Z}$ are such that $-a+b\sqrt{\Delta_0}$ is totally negative. We may and will assume $0 < a, b < \Delta_K$, as Lemma 3.5 shows that each quartic CM field has such representations. We will disregard the degenerate case of non-primitive quartic CM fields, i.e., those that can be given with $b = 0$. We give the following runtime bound for our algorithm.

Main Theorem. *Algorithm 11.1 computes $H_{K,n}$ $(n = 1, 2, 3)$ for any primitive quartic CM field K in which 2 and 3 do not ramify. It has a runtime of $\widetilde{O}(\Delta^{7/2}\Delta_0^{-3/2})$ and the bit size of the output is $\widetilde{O}(\Delta^2\Delta_0^{-1})$.*

An essential part of the proof is the denominator bound, as provided by Goren and Lauter [16] and Goren [14, 15]. As these results assume ramification bounds on the primes 2 and 3, we have a similar restriction on K. This restriction will disappear as soon as Goren's results are extended to this case.

We do not claim that our runtime is optimal, but an exponential runtime is unavoidable, because the degree of the Igusa class polynomials (as with Hilbert class polynomials) is already bounded from below by a power of the discriminant.

Overview

Section 2 provides a precise definition of the Igusa class polynomials that we will work with, and mentions other definitions occurring in the literature. Our main theorem is valid for all types of Igusa class polynomials.

Section 3 gives the bounds on the denominators of Igusa class polynomials. Section 4 shows how to reconstruct a rational polynomial from its complex roots, and the precision needed for that in terms of an upper bound on the denominator of the polynomial and the absolute values of the zeroes.

Instead of enumerating curves, it is easier to enumerate their Jacobians, which are principally polarized abelian varieties. We provide the necessary theory in Section 5.

Van Wamelen [33] gave a method for enumerating all isomorphism classes of principally polarized abelian varieties with CM by a given order. We give an improvement of his results in Section 6.

Section 7 shows how principally polarized abelian varieties give rise to points in the *Siegel upper half space* $\mathcal{H}_2$. Two such points correspond to isomorphic principally polarized abelian varieties if and only if they are in the same orbit under the action of the *symplectic group* $\mathrm{Sp}_4(\mathbf{Z})$.

In Section 8, we analyse the algorithm that replaces points in $\mathcal{H}_2$ by $\mathrm{Sp}_4(\mathbf{Z})$-equivalent points in a *fundamental domain* $\mathcal{F}_2$.

In Section 9, we use the *Hilbert upper half space* to give bounds on the entries of the matrices computed in Section 8. The theory of that section also allows us to generalize much-cited results from Spallek's thesis [31] and to give a theoretically very interesting alternative to the computation in Section 6.

The absolute Igusa invariants can be computed from the matrices in the Siegel upper half space by means of *theta constants.* Section 10 introduces theta constants and gives a vast simplification of the formulas that express Igusa invariants in terms of theta constants, reducing the formulas from more than a full page to only a few lines. We then give bounds on the absolute values of theta constants and Igusa invariants in terms of the bounds from Section 9. We finish that section by showing how to evaluate the theta constants, and hence the absolute Igusa invariants to a given precision.

Finally, Section 11 puts all the results together into a single algorithm and a proof of the main theorem.

2 Igusa class polynomials

The *Hilbert class polynomial* of an imaginary quadratic number field K is the polynomial of which the roots in $\mathbf{C}$ are the *j-invariants* of the elliptic curves over $\mathbf{C}$ with complex multiplication by the ring of integers $\mathcal{O}_K$ of K. For a genus 2 curve, one needs three invariants, the *absolute Igusa invariants* i_1, i_2, i_3, to fix its isomorphism class.

The following theory can be found in Igusa's paper [18]. Let k be a field of characteristic different from 2. Any curve of genus 2 over k has an affine model of the form $y^2 = f(x)$, where $f \in k[x]$ is a separable polynomial of degree 6. Let $\alpha_1, \ldots, \alpha_6$ be the six distinct roots of f in $\overline{k}$, and let a_6 be the leading coefficient. For a permutation $\sigma \in S_6$, let (ij) denote the difference $(\alpha_{\sigma(i)} - \alpha_{\sigma(j)})$. We can then define the *homogeneous Igusa-Clebsch invariants* as

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

where the sum is taken over all different expressions in the roots of f obtained when σ varies over S_6. The subscript indicates the number of expressions encountered. More precisely, there are 15 ways of partitioning the six roots of f into three subsets of two. Each yields a triple f_1, f_2, f_3 of monic quadratic polynomials, and the summand in I_2 is the product of their discriminants. Similarly, there are 10 ways of partitioning the six roots of f into two subsets of three, and each yields a summand in I_4, which is the product of two cubic discriminants. For each of the 10 ways of partitioning the six roots of f into two subsets of three, there are 6 ways of giving a bijection between those two subsets, and each gives a summand for I_6. Finally, I_{10} is simply the discriminant of f, which is non-zero as f is separable. The above invariants were introduced by Igusa [18], who called them A, B, C, D and based them on invariants of Clebsch [5].

By the symmetry in the definition, each of the homogeneous invariants is actually a polynomial in the coefficients of f, hence an element of k.

We define the *absolute Igusa invariants* by

$$\begin{aligned}
i_1 &= I_2^5 I_{10}^{-1},\\
i_2 &= I_2^3 I_4 I_{10}^{-1},\\
i_3 &= I_2^2 I_6 I_{10}^{-1}.
\end{aligned}$$

The values of the absolute Igusa invariants of a curve C depend only on the $\overline{k}$-isomorphism class of the curve C. Conversely, for any triple

$(i_1^0, i_2^0, i_3^0) \in k^3$, if 3 and i_1^0 are non-zero in k, then there exists a (unique up to isomorphism) curve C of genus 2 over $\overline{k}$ with $i_n(C) = i_n^0$ ($n = 1, 2, 3$) and this curve can be constructed using an algorithm of Mestre [26].

Definition 2.1. Let K be a primitive quartic CM field. The *Igusa class polynomials* of K are the three polynomials

$$H_{K,n} = \prod_C (X - i_n(C)) \quad \in \mathbf{Q}[X] \quad (n \in \{1,2,3\}),$$

where the product ranges over the isomorphism classes of genus 2 curves over $\mathbf{C}$ of which the Jacobian has complex multiplication by $\mathcal{O}_K$.

For a definition of the Jacobian or complex multiplication, see Section 5. We will see in Section 6 that the product in the definition is indeed finite. The polynomial is rational, because any conjugate of a CM curve has CM by the same order.

2.1 Alternative definitions

In the literature, one finds various sets of absolute Igusa invariants. Most notably, Igusa defined homogeneous invariants J_{2n} ($n = 1, \ldots, 5$) in terms of a general hyperelliptic equation and used them to define absolute invariants that have good reduction behaviour at 2. If the base field k has characteristic 0, then Igusa's absolute invariants, and most of the other invariants in the literature, lie in the $\mathbf{Q}$-algebra A of homogeneous elements of degree 0 of $\mathbf{Q}[I_2, I_4, I_6, I_{10}^{-1}]$. Our main theorem remains true if (i_1, i_2, i_3) in the definition of the Igusa class polynomials is replaced by any finite list of elements of A.

Cardona-Quer invariants

To deal with the case $i_1 = 0$, Cardona and Quer [4] introduce an alternative set of absolute Igusa invariants that we will call *Cardona-Quer invariants*. Their invariants have the advantage that they do give a bijection between $\overline{k}^3$ and the set of isomorphism classes of genus 2 curves over $\overline{k}$, but the disadvantage that they are not functions on the moduli space of genus 2 curves (which the elements of the ring A above are). They are given by the same formula as before if $I_2 \neq 0$ and otherwise by

$$(i_1, i_2, i_3) = \begin{cases} (0,\ I_4^5 I_{10}^{-2},\ I_4 I_6 I_{10}^{-1}) & \text{if } I_2 = 0 \text{ and } I_4 \neq 0; \\ (0,\ 0,\ I_6^5 I_{10}^{-3}) & \text{if } I_2 = I_4 = 0. \end{cases} \tag{1}$$

Our main theorem also holds if the absolute Igusa invariants in the definition of the Igusa class polynomials are replaced by the Cardona-Quer invariants.

Interpolation formulas

If we take one root of each of the Igusa class polynomials, then we get a triple of invariants and thus (if $i_1 \neq 0$) an isomorphism class of curve of genus 2. That way, the three Igusa class polynomials describe d^3 triples of invariants, where d is the degree of the polynomials. The d triples corresponding to CM curves are among them, but the Igusa class polynomials give no means of telling which they are.

To solve this problem (and thus greatly reduce the number of curves to be checked during the CM method), Gaudry et al. [11] introduced polynomials

$$\widehat{H}_{K,n} = \sum_{C} j_n(C) \prod_{C' \neq C} (X - j_1(C')) \quad \in \mathbf{Q}[X], \quad (n \in \{2,3\}).$$

If $H_{K,1}$ has no roots of multiplicity greater than 1, then the triples of invariants corresponding to curves with CM by $\mathcal{O}_K$ are exactly the triples (i_1, i_2, i_3) such that

$$H_{K,1}(i_1) = 0, \quad i_n = \frac{\widehat{H}_{K,n}(i_1)}{H'_{K,1}(i_1)} \quad (n \in \{2,3\}).$$

Our main theorem is also valid if we replace $H_{K,2}$ and $H_{K,3}$ by $\widehat{H}_{K,2}$ and $\widehat{H}_{K,3}$.

3 Denominators

Let K be a primitive quartic CM field. In this section, we give bounds on the degree and the denominators of Igusa class polynomials. We will give our bounds in terms of the real quadratic discriminant Δ_0 and the norm $\Delta_1 = N_{K_0/\mathbf{Q}}(\Delta_{K/K_0})$ of the relative discriminant Δ_{K/K_0} of K over its maximal real subfield K_0. Note that $\Delta = \Delta_1 \Delta_0^2$.

By the *denominator* of a polynomial $f \in \mathbf{Q}[X]$, we mean the minimal positive integer c such that $cf \in \mathbf{Z}[X]$. The main result of this section is the following.

Theorem 3.1. *If* 2 *and* 3 *do not ramify in* K*, then the logarithm of the denominator of each of the Igusa class polynomials of* K *is bounded by* $\widetilde{O}(\Delta_1^{3/2}\Delta_0^{5/2})$.

We start by bounding the degree. Let K_0 be the real quadratic subfield of K. Denote the class numbers of K and K_0 by h and h_0 and let $h_1 = h/h_0$. It is well known that the degree of $H_i(X)$ is h_1 if K is cyclic and $2h_1$ if K is non-Galois. For a proof, see Lemma 6.8. The following result bounds this degree.

Lemma 3.2 (Louboutin [25])**.** There exists a contant $d > 0$ such that for all primitive quartic CM fields K, if Δ is sufficiently large, then

$$\Delta_1^{1/2}\Delta_0^{1/2}(\log \Delta)^{-d} \leq h_1 \leq \Delta_1^{1/2}\Delta_0^{1/2}(\log \Delta)^{d}.$$

Proof. Louboutin [25, Theorem 14] gives upper and lower bounds of the form

$$\left(\frac{1}{2} - O(\frac{\log\log\Delta}{\log\Delta})\right)\log(\Delta_1\Delta_0)$$

on $\log h_1$ for all CM fields of a fixed degree that do not contain an imaginary quadratic subfield. This implies that there exists $d > 0$ such that for sufficiently large Δ, we have

$$h_1 \leq (\Delta_1\Delta_0)^{\frac{1}{2}} \exp\left(d\frac{\log\log\Delta}{\log\Delta}\log\Delta\right),$$

which proves the upper bound. The lower bound is analogous. □

The field K can be written as $K = \mathbf{Q}(\sqrt{-a+b\sqrt{d}})$, where a, b and d are positive integers and $d = \Delta_0/4$ if $4|\Delta_0$ and $d = \Delta_0$ otherwise. Primes that may occur in the denominators of the coefficients of class polynomials are bounded in terms of a and d by Goren and Lauter [16] as follows.

Lemma 3.3. The coefficients of each of the polynomials $H_{K,n}(X)$ for $K = \mathbf{Q}(\sqrt{-a+b\sqrt{d}})$ are S-integers, where S is the set of primes smaller than $4da^2$.

Proof. Corollary 5.2.1 of [16] is exactly this result but with d replaced by d^2. We will now show how to adapt the proofs of [16] to remove a factor d. In Corollary 2.1.2, it suffices to have only $N(k_1)N(k_2) < p/4$ in order for k_1 and k_2 to commute. Then, in the proof of Theorem 3.0.4, it suffices to take as hypothesis only $p > d(\mathrm{Tr}(r))^2$. As $d(\mathrm{Tr}(r))^2 \geq d\delta_1\delta_2 \geq N(x)N(by^\vee)$, this implies that x and $by^\vee$ are in the same imaginary quadratic field K_1. As in the original proof, this implies that $ywy^\vee$ is also contained in K_1 and hence $\psi(\sqrt{r}) \in M_2(K_1)$, so $K = \mathbf{Q}(\sqrt{r}) \mapsto M_2(K_1)$. □

Remark 3.4. Lemma 3.3 as phrased above is for class polynomials defined in terms of invariants in $\mathcal{R} = \mathbf{Z}[I_2, I_4, I_6, I_{10}^{-1}]$. If an invariant $j \in m^{-1}\mathcal{R}$ is used with $m \in \mathbf{Z}$, then the result is still valid if the primes dividing m are added to S.

As Lemma 3.3 holds for any representation of K of the form $K = K_0(\sqrt{-a+b\sqrt{d}})$, we may choose a, b such that a is minimal. The following result shows how good a can be.

Lemma 3.5. Let K be a quartic CM field with discriminant Δ and let Δ_0 be the discriminant of the real quadratic subfield K_0.

For all $a, b, d \in \mathbf{Z}$ such that $K = \mathbf{Q}(\sqrt{-a+b\sqrt{d}})$, we have $\Delta_1 \leq a^2$. Conversely, there exist such $a, b, d \in \mathbf{Z}$ with $a^2 \leq 64\Delta_1\Delta_0$.

Proof. The first bound is trivial because Δ_1 divides $a^2 - b^2d \leq a^2$. For the bound in the other direction, we show the existence of a suitable element $-a + b\sqrt{d}$ using a geometry of numbers argument.

We identify $K \otimes_{\mathbf{Q}} \mathbf{R}$ with $\mathbf{C}^2$ via its pair of infinite primes. Then $\mathcal{O}_K$ is a lattice in $\mathbf{C}^2$ of covolume $2^{-2}\sqrt{\Delta}$. Let ω_1, ω_2 be a basis of $\mathcal{O}_{K_0}$ and consider the open parallelogram $\omega_1(-1,1) + \omega_2(-1,1) \subset \mathcal{O}_{K_0} \otimes \mathbf{R} \cong \mathbf{R}^2$. We define the open convex symmetric region

$$V_Y = \{x \in \mathbf{C}^2 : \mathrm{Re}(x) \in \omega_1(-1,1) + \omega_2(-1,1), |\mathrm{Im}(x)| \in (-Y,Y)^2\}.$$

Then $\mathrm{vol}(V_Y) = \sqrt{\Delta_0}4Y^2$ and by Minkowski's convex body theorem, V_Y contains a non-zero element $\alpha \in \mathcal{O}_K$ if $\mathrm{vol}(V_Y) > 4\sqrt{|\Delta|}$. Pick $Y = \sqrt[4]{|\Delta/\Delta_0| + \epsilon}$ and let $r = 2(\alpha - \overline{\alpha})^2$. Then r is of the form $-a + b\sqrt{d}$ with integers a and b. Now for any embedding $\sigma : \mathcal{O}_K \to \mathbf{C}$, we have $|\sigma(r)| = 2(2\mathrm{Im}(\sigma(\alpha)))^2 < 2(2Y)^2 = 8\sqrt{|\Delta/\Delta_0| + \epsilon}$. In particular, for every ϵ, we find an a with $2a \leq 16\sqrt{|\Delta/\Delta_0| + \epsilon}$. As a is in a discrete set, we get $a \leq 8\sqrt{|\Delta/\Delta_0|}$ if we let ϵ tend to 0. □

Recent, not yet published, results by Eyal Goren bound the exponents to which primes may occur in the denominator. Let K^{r} be the *reflex field* (see Shimura [30]) of K, which has the same normal closure as K, and let H^{r} be the Hilbert class field of K^{r}. By the main theorem of complex multiplication [30, Main Theorem 1 in Section 15.3], each of the Igusa class polynomials splits into linear factors over H^{r}. Goren [14, 15] gives explicit positive real constants c_1, c_2 such that the following holds.

Lemma 3.6 ([14, 15])**.** Let K be a primitive quartic CM field. Let $j \in H^{\mathrm{r}}$ be a zero of one of the Igusa class polynomials of K, $\mathfrak{p}$ a prime of H^{r} lying over a rational prime p and $e(\mathfrak{p}/p)$ its ramification index. If $e(\mathfrak{p}/p) < p$, then $-\mathrm{ord}_{\mathfrak{p}}(j) \leq c_1 + c_2\frac{\log(da)}{\log p}$. □

Remark 3.7. As H^{r} is unramified over K^{r}, we have $e(\mathfrak{p}/p) \leq 4$, so the condition $e(\mathfrak{p}/p) < p$ is satisfied automatically for $p \geq 5$, is equivalent to $e \leq 2$ for $p = 3$ and equivalent to $e = 1$ for $p = 2$.

Remark 3.8. In order to have results that hold regardless of the decomposition of 2 and 3, one should generalize Lemma 3.6 to the case $e(\mathfrak{p}/p) \geq p$.

There is also the possibility of reducing the number of "bad" decomposition types by generalizing results of Goren [12]. For example, [10, Theorem 3.5] shows that if p decomposes as $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^2$ in K, then the reduction of a CM abelian surface modulo any prime over p has p-rank 1 and hence is not the product of two supersingular elliptic curves with the product polarization. This shows that in that case, p will not occur in the denominator.

Now let $f \in \mathbf{Q}[x]$ be a monic irreducible factor of a class polynomial. Let p be a prime number such that any prime $\mathfrak{p}$ of K^{r} over p satisfies $e(\mathfrak{p}/p) < p$.

Corollary 3.9. The prime p occurs in denominators of coefficients of f to a power at most $\deg(f) \cdot (c_1 + c_2\frac{\log(da)}{\log p})$.

Proof. Let j be any root of f in H^{r} and let $L = \mathbf{Q}(j)$. Let $p = \prod \mathfrak{p}_i$ be the decomposition of p in L. Write $B = c_1 + c_2\log(da)/\log p$. By Lemma 3.6, we have $v_{\mathfrak{p}_i}(j) \geq -B$ for every i. Therefore, $p^B j$ is $\mathfrak{p}_i$-integral and hence so is $p^{B\deg(f)}f$. □

Proof of Theorem 3.1. By Lemma 3.3 and Corollary 3.9, the denominator of each of the class polynomials is at most

$$\begin{array}{ll} & 2h_1 \sum\limits_{\substack{p \text{ prime} \\ p \leq 4da^2}} (c_1 \log p + c_2 \log(da)) \\ \leq & 2h_1(c_1 + c_2)\#\{p \text{ prime} \leq 4da^2\} \log(4da^2) \\ \sim & 8(c_1 + c_2)h_1 da^2, \end{array}$$

where $\sim$ means that the quotient goes to 1 as da^2 goes to infinity. The quotient goes to 1 by the prime number theorem. If we choose a, b as in Lemma 3.5, it follows that this is $O(h_1 \Delta_1 \Delta_0^2) = \widetilde{O}(\Delta_1^{3/2}\Delta_0^{5/2})$. □

Improvements

The bound $\widetilde{O}(\Delta_1^{3/2}\Delta_0^{5/2})$ of Theorem 3.1 appears to be far from optimal.

The method of proof of Lemma 3.3 suggests that it should be possible to replace the bound a^2d by $\Delta_1\Delta_0$, saving a factor Δ_0 in Theorem 3.1. The bound $\Delta_1\Delta_0$ is also exactly what follows from a conjecture of Bruinier and Yang in the case where Δ_0 and Δ_1 are prime (Conjecture 1.1 and Corollary 1.6 of [38]). That conjecture has recently been proven in an even more restrictive setting by Yang [38, Theorem 1.2].

It is suggested by experiments of Kristin Lauter [21] that each prime dividing the denominator of the Igusa class polynomials divides $\Delta_1 - x^2$ for some $x < \sqrt{\Delta_1}$. If such a thing is true, then, combined with Goren's results, it would give a bound of $\widetilde{O}(h_1\sqrt{\Delta_1}) = \widetilde{O}(\Delta_1\Delta_0^{1/2})$ on the denominator.

4 Recovering a polynomial from its roots

In this section, we show how to compute the Igusa class polynomials from complex approximations of their roots. This will tell us the precision with which we need to know these roots. The rest of the paper will be about approximating these roots.

We will compute an approximation of the class polynomials from approximations of its roots in Section 4.2. Then in Section 4.4, we compute numerators and denominators of the coefficients from their approximations.

Complex polynomials are represented in computers by approximations that are of the form $2^{-p}(a + ib)$, where a and b are polynomials in $\mathbf{Z}[x]$ given by the binary expansions of their coefficients and p is a non-negative integer. Complex numbers are complex polynomials of degree 0.

4.1 Polynomial multiplication

For a complex polynomial g, let $|g|_1$ (resp. $|g|_\infty$) be the sum (resp. maximum) of the absolute values of the coefficients of g. We find $|g_1g_2|_\infty \leq |g_1|_\infty |g_2|_1$ and $|g|_1 \leq (\deg(g) + 1)|g|_\infty$.

The following algorithm computes products of integer polynomials.

Algorithm 4.1. Input: Polynomials $g_1, g_2 \in \mathbf{Z}[X]$, given by the binary expansions of their coefficients.
Output: The product $g_1 g_2 \in \mathbf{Z}[X]$.

1. Let $k = \lceil \log_2 |g_1|_\infty \rceil + \lceil \log_2 |g_2|_\infty \rceil + \lceil \log_2(\deg(g_1) + 1) \rceil$.
2. Evaluate the polynomials in 2^k by writing the binary expansions of their coefficients behind each other with the right number of zeroes between them.
3. Multiply the results using fast integer multiplication.
4. Read off the binary expansions of the coefficients of $g_1 g_2$ from the result.

This algorithm takes time $M((\deg(g_1 g_2) + 1) \log_2 |g_1 g_2|_\infty)$, where $M(n) = O(n \log n \log \log n)$ is the time needed for a multiplication of n-bit integers.

The *error* $\epsilon(g, \widetilde{g})$ of an approximation $\widetilde{g}$ of a polynomial g is $|g - \widetilde{g}|_\infty$. Suppose we have approximations $\widetilde{g}_k = 2^{-p}(a_k + ib_k)$ of g_k for $k = 1, 2$. The following algorithm computes an approximation of their product.

Algorithm 4.2. Input: Approximations $\widehat{g}_1 = 2^{-p}(a_1 + ib_1)$ and $\widehat{g}_2 = 2^{-p}(a_2 + ib_2)$ of complex polynomials g_1, g_2.
Output: An approximation $\widehat{g_1 g_2} = 2^{-p}(a + ib)$ of $g_1 g_2$.

1. Compute $a' = a_1 a_2 - b_1 b_2$ and $b' = a_1 b_2 + b_1 a_2$ using Algorithm 4.1.
2. Truncate a' and b' by removing their p least significant bits to get a and b. In other words, let a and b be such that $2^p a \equiv a' \pmod{2^p}$ and $2^p b \equiv b' \pmod{2^p}$.

Lemma 4.3. Algorithm 4.2 takes time

$$M((\deg(g_1 g_2) + 1)(\log_2 |g_1 g_2|_\infty + 2^p)).$$

The error $\epsilon(g_1 g_2, \widetilde{g}_1 \widetilde{g}_2)$ is at most

$$|g_1|_1 \epsilon(g_2, \widetilde{g}_2) + |g_2|_1 \epsilon(g_1, \widetilde{g}_1) + (\deg(g_1) + 1)\epsilon(g_1, \widetilde{g}_1)\epsilon(g_2, \widetilde{g}_2) + 2^{-p}.$$

Proof. The runtime follows from the fact that we simply apply Algorithm 4.1 four times. The triangle inequality for $|\cdot|_\infty$ gives us the bound on the error. □

4.2 Reconstructing a polynomial from its roots

Let $z_1, \ldots, z_n$ be complex numbers. The purpose of this section is to compute an approximation of $f = \prod_{i=1}^n (X - z_i) \in \mathbf{C}[X]$ from and approximation of $z_1, \ldots, z_n$. Suppose that $|z_i| + 1 \leq s_i$ and $s = \prod s_i$.

Algorithm 4.4. Input: a positive integer u and approximations $\widetilde{z}_1, \ldots, \widetilde{z}_n$ of $z_1, \ldots, z_n$ with error

$$\epsilon(z_i, \widetilde{z}_i) \leq 2^{-u + \sum_{j \neq i} \log_2 s_j + 3 \log_2 n + 3}.$$

Output: an approximation $\widetilde{f}$ of $f = \prod_{i=1}^{n}(X - z_i) \in \mathbf{C}[X]$ with error

$$\epsilon(f, \widetilde{f}) \leq 2^{-u}.$$

1. Build a binary tree of depth $l = \lceil \log_2 n \rceil$ with at the leaves the n linear polynomials $X - \widetilde{z}_i$ and $2^l - n$ times the constant polynomial 1.
2. From the leaves up to the root, at every node t of the tree, put the product of the two nodes below it, computed by Algorithm 4.2 with $p = -u + \sum_{j \neq i} \log_2 s_j + 3 \log_2 n + 3$.
3. Output the root of the tree.

Theorem 4.5. *Algorithm 4.4 is correct and has a runtime of*

$$O(nm \log(nm)^2 \log\log(nm)),$$

where $m = \max\{u, \log n, \log s\}$.

Proof of Theorem 4.5. For every node t of the tree, denote by $d(t)$ the set of leaves i below t with $i \leq n$. At every node t of the tree, there is a polynomial

$$g_t = \prod_{i \in d(t), i \leq n} (X - z_i)$$

of which the polynomial $\widetilde{g}_t$ computed in the algorithm is an approximation. Let b_k (resp. κ_k) be the maximum over all nodes t at distance at most k to the leaves of

$$|g_t|_1 \prod_{i \in d(t)} s_i^{-1} \qquad (\text{resp.} \max\{2^{-p}, \epsilon(g_t, \widetilde{g}_t) \prod_{i \in d(t)} s_i^{-1}\}).$$

Then clearly $b_k \leq 1$ for all k. Moreover, by Lemma 4.3, we have

$$\kappa_{k+1} \leq 2\kappa_k + (2^k + 1)\kappa_k^2 + 2^{-p} \leq 3\kappa_k + (2^k + 1)\kappa_k^2.$$

If $\kappa_0 \leq n^{-3}$, then by induction this implies that $\kappa_k \leq 4^k \kappa_0$ for all k, so $\kappa_l < (2n)^2 \kappa_0$. In particular, the error of each coefficient of the output is at most $(2n)^2 \kappa_0 s$.

This means that $\kappa_0 = 2^{-u-3\log n - 3 - \log_2 s}$ is sufficient. At the k-th level of the tree, there will be 2^{l-k} polynomial multiplications of degree at most 2^k where each coefficient has a bit size of $O(m)$, so each of the $l < 1 + \log_2 n$ levels takes time $O(M(nm))$, which proves the complexity. □

4.3 The polynomials $\widehat{H}_{K,n}$

The polynomials $\widehat{H}_{K,n}$ from Section 2.1 are the sum of h_1 polynomials that are each computed from their roots in quasi-linear time. To evaluate the sum, we make a binary tree as in Algorithm 4.4 with addition instead of multiplication. We thus compute $\widehat{H}_{K,n}$ from the Igusa invariants in time $\widetilde{O}(h_1)$ times the bound from Theorem 4.5. This is still dominated by the time mentioned in the main theorem.

4.4 Recognizing rational coefficients

If the denominator of a polynomial $f \in \mathbf{Q}[X]$ divides d, then df is an integer polynomial that can be recognized from an approximation $\widetilde{f}$ of f by rounding the coefficients, provided that the error $\epsilon(f, \widetilde{f})$ is at most $1/(2d)$. Therefore, we need an absolute precision of $u = 1 + \log_2 d$ bits. In our case, d can be computed in quasi-linear time as a product of primes as follows.

Algorithm 4.6. Input: The discriminant Δ of a primitive quartic CM field K and the relative class number h_1.
Output: D such that $DH_i \in \mathbf{Z}[X]$

1. List all numbers up to 256Δ.
2. Use the sieve of Eratosthenes to eliminate all non-primes.
3. List each found prime the number of times given in the upper bound $h_1(c_1 + c_2 \frac{\log(16\Delta)}{\log p})$ of Corollary 3.9.
4. Output the product of all found primes (with multiplicity), computed using a binary tree as in Algorithm 4.4.

We can then compute DH_i and round its coefficients to nearest integers.

In practice, the denominator will be much smaller, but we don't know what it is. Therefore, in practice, one uses the LLL-algorithm for guessing rational values for the coefficients.

5 Jacobians

Instead of enumerating CM curves, we enumerate their *Jacobians*, which are given by lattices of a special form.

Let C be a smooth projective irreducible algebraic curve over $\mathbf{C}$. We give the definition of the Jacobian as in [1]. Let $H^0(\omega_C)$ be the complex vector space of holomorphic 1-forms on C and denote its dual by $H^0(\omega_C)^*$. The *genus* g of C is the dimension of this vector space. This paper is about the case $g = 2$, but we treat the general case in this section as it is not harder. The homology group $H_1(C, \mathbf{Z})$ is a free abelian group of rank $2g$ and we get a canonical injection $H_1(C, \mathbf{Z}) \to H^0(\omega_C)^*$, given by $\gamma \mapsto (\omega \mapsto \int_\gamma \omega)$, where the integral is taken over any representative cycle of the class $\gamma \in H_1(C, \mathbf{Z})$. The image of $H_1(C, \mathbf{Z})$ in $H^0(\omega_C)$ is a lattice of rank $2g$ in a g-dimensional complex vector space and the quotient $J(C) = H^0(\omega_C)^*/H_1(C, \mathbf{Z})$, which is a complex torus, is called the *Jacobian* of C.

The *endomorphism ring* $\mathrm{End}(\mathbf{C}^g/\Lambda)$ of a complex torus $\mathbf{C}^g/\Lambda$ is the ring of $\mathbf{C}$-linear automorphisms of $\mathbf{C}^g$ that map Λ to into itself. A *CM field* is a totally imaginary quadratic extension of a totally real number field. We say that a complex torus T of (complex) dimension g has *complex multiplication* or *CM* by an order $\mathcal{O}$ in a CM field K if K has degree $2g$ and there exists an embedding $\mathcal{O} \to \mathrm{End}(T)$. We say that a curve has CM if its Jacobian does.

It turns out that $J(C)$ is not just any complex torus, but that it comes with a natural *principal polarization.* A polarization of a complex torus $\mathbf{C}^g/\Lambda$ is an alternating $\mathbf{R}$-bilinear form $E : \mathbf{C}^g \times \mathbf{C}^g \to \mathbf{R}$ such that $E(\Lambda, \Lambda) \subset \mathbf{Z}$ and $E(iu, iv) = E(u, v)$ for all $u, v \in \mathbf{C}^g$ [1, Section 2.1]. The degree of a polarization is $\sqrt{\det M}$, where M is a matrix that expresses E in terms of a $\mathbf{Z}$-basis of Λ. We call a polarization *principal* if its degree is 1. If we denote by $\cdot$ the intersection pairing on $H_1(C, \mathbf{Z})$ extended $\mathbf{R}$-linearly to $H^0(\omega_C)^*$, then $E : (u, v) \mapsto -u \cdot v$ defines a principal polarization on $J(C)$ and by the Jacobian of C, we mean the torus together with this principal polarization.

A torus for which there exists a polarization is called an *abelian variety* and a torus together with a (principal) polarization, such as the Jacobian of a curve, is called a *(principally) polarized abelian variety.*

We have now associated to every curve a principally polarized abelian variety. Next, we show that this in fact gives a bijection between curves of genus 2 up to isomorphism and certain principally polarized abelian surfaces (dimension 2 varieties) up to isomorphism.

An *isomorphism* of (principally) polarized abelian varieties $f : (\mathbf{C}^g/\Lambda, E) \to (\mathbf{C}^g/\Lambda', E')$ is a $\mathbf{C}$-linear isomorphism $f : \mathbf{C}^g \to \mathbf{C}^g$ such that $f(\Lambda) = \Lambda'$ and $f^*E_2 = E_1$, where $f^*E_2(u, v) = E_2(f(u), f(v))$ for $u, v \in \mathbf{C}^g$.

Theorem 5.1 (Torelli)**.** *Two curves over* $\mathbf{C}$ *are isomorphic if and only if their Jacobians are isomorphic (as polarized abelian varieties).*

Proof. This is Theorem 11.1.7 of [1]. □

The product of two polarized abelian varieties (T_1, E_1) and (T_2, E_2) has a natural polarization $(v, w) \mapsto E_1(v_1, w_1) + E_2(v_2, w_2)$ called the *product polarization.*

Theorem 5.2 (Weil)**.** *Any principally polarized abelian surface over* $\mathbf{C}$ *is either a product of elliptic curves with the product polarization or the Jacobian of a smooth projective curve of genus* 2*.*

Proof. This is [36, Satz 2] and [1, Corollary 11.8.2]). □

6 Abelian varieties with CM

In this section, we give an algorithm that computes a representative of every isomorphism class of complex principally polarized abelian varieties with CM by the ring of integers $\mathcal{O}_K$ of a primitive quartic CM field K. We give statements that hold for general CM fields where they are not harder.

6.1 Ideals and polarizations

Let K be any CM field of degree $2g$, i.e., a totally imaginary quadratic extension of a totally real number field K_0 of degree g. A *CM type* Φ of a CM field K is a set of g embeddings $K \to \mathbf{C}$ such that $\Phi \cup \overline{\Phi}$ is the complete set of $2g$ embeddings. By abuse of notation, we interpret

Φ as a map $\Phi : K \to \mathbf{C}^g$ by writing $\Phi = \{\phi_1, \ldots, \phi_g\}$ and setting $\Phi(\alpha) = (\phi_1(\alpha), \ldots, \phi_g(\alpha))$.

Let K be a CM field of degree $2g$ which does not contain a strict CM subfield, and let $\mathcal{D}_{K/\mathbf{Q}}$ be its different. Suppose that Φ is a CM type of K, that $\mathfrak{a}$ is a fractional $\mathcal{O}_K$-ideal, and that $\xi \in K$ is a generator of the $\mathcal{O}_K$-ideal $(\mathfrak{a}\overline{\mathfrak{a}}\mathcal{D}_{K/\mathbf{Q}})^{-1}$ such that $\phi(\xi)$ lies on the positive imaginary axis for every $\phi \in \Phi$. The map $E : \Phi(K) \times \Phi(K) \to \mathbf{Q}$ given by

$$E(\Phi(\alpha), \Phi(\beta)) = \mathrm{Tr}_{K/\mathbf{Q}}(\xi\alpha\overline{\beta}) \quad \text{for } \alpha, \beta \in K$$

can be extended uniquely $\mathbf{R}$-linearly to an $\mathbf{R}$-bilinear form $E : \mathbf{C}^g \times \mathbf{C}^g \to \mathbf{R}$. We denote the pair $(\mathbf{C}^g/\Phi(\mathfrak{a}), E)$ by $A_{\Phi,\mathfrak{a},\xi}$.

Theorem 6.1. *Suppose that K is a CM field of degree $2g$ that does not contain a strict CM subfield.*

1. *For any triple $(\Phi, \mathfrak{a}, \xi)$ as above, we have that $A_{\Phi,\mathfrak{a},\xi}$ is a principally polarized abelian variety with CM by $\mathcal{O}_K$.*
2. *Every principally polarized abelian variety with CM by $\mathcal{O}_K$ is isomorphic to $A_{\Phi,\mathfrak{a},\xi}$ for some triple $(\Phi, \mathfrak{a}, \xi)$ as above.*
3. *For every pair of triples $(\Phi, \mathfrak{a}, \xi)$ and $(\Phi', \mathfrak{a}', \xi')$ as above, the principally polarized abelian varieties $A_{\Phi,\mathfrak{a},\xi}$ and $A_{\Phi',\mathfrak{a}',\xi'}$ are isomorphic if and only if there exist $\sigma \in \mathrm{Aut}(K)$ and $\gamma \in K^*$ such that*
   - *(a)* $\Phi' = \Phi \circ \sigma$,
   - *(b)* $\sigma\mathfrak{a}' = \gamma\mathfrak{a}$ *and*
   - *(c)* $\sigma\xi' = (\gamma\overline{\gamma})^{-1}\xi$.

Proof. Part 1 (resp. 2) is a combination of the parts 1 (resp. 2) of Theorems 1 and 3 of [33] (originally [31, Satz 3.13 and Satz 3.14]).

It remains to prove part 3. For any automorphism σ of K, the principally polarized abelian varieties

$$A_{\Phi,\mathfrak{a},\xi} \quad \text{and} \quad A_{\Phi\circ\sigma,\sigma^{-1}\mathfrak{a},\sigma^{-1}\xi}$$

are equal by definition. Conversely, we claim that if $(\Phi, \mathfrak{a}, \xi)$ and $(\Phi', \mathfrak{a}', \xi')$ are isomorphic, then there exists an authomorphism σ of K such that $\Phi' = \Phi \circ \sigma$.

Proof of the claim: suppose that $A_{\Phi,\mathfrak{a},\xi}$ and $A_{\Phi',\mathfrak{a}',\xi'}$ are isomorphic via an isomorphism $f : \mathbf{C}^g/\Phi(\mathfrak{a}) \to \mathbf{C}^g/\Phi'(\mathfrak{a}')$. Then f induces the isomorphism

$$m : \mathrm{End}(\mathbf{C}^g/\Phi'(\mathfrak{a}')) \to \mathrm{End}(\mathbf{C}^g/\Phi(\mathfrak{a})), \quad \text{given by} \quad l \mapsto f^{-1}lf.$$

We also have the map $\iota_\Phi : K \to \mathrm{End}(\mathbf{C}^g/\Phi(\mathfrak{a})) \otimes \mathbf{Q}$, given by

$$\iota_\Phi(\alpha) = \mathrm{diag}\,\Phi(\alpha)$$

and an analogous map $\iota_{\Phi'} : K \to \mathrm{End}(\mathbf{C}^g/\Phi'(\mathfrak{a}')) \otimes \mathbf{Q}$. Both are isomorphisms by [33, Theorem 1(3)], so we get an automorphism $\sigma = (\mathrm{diag}\,\Phi)^{-1} \circ m \circ \mathrm{diag}\,\Phi'$ of K. The map m is given by an invertible

$(g \times g)$-matrix $(m_{ij})_{ij}$, so $\operatorname{diag}\Phi \circ \sigma = m \operatorname{diag}\Phi'$ implies $\phi_i\sigma = m_{ij}\phi'_j$. As Φ consists of distinct embeddings, we find that m is a permutation matrix and that $\Phi \circ \sigma = \Phi'$, which proves the claim.

It now follows that $A_{\Phi,\mathfrak{a},\xi}$ and $A_{\Phi',\mathfrak{a}',\xi'}$ are isomorphic if and only if (1) there exists an automorphism σ of K such that $\Phi' = \Phi \circ \sigma$ and (2) $A_{\Phi,\mathfrak{a},\xi}$ is isomorphic to $A_{\Phi,\sigma\mathfrak{a}',\sigma\xi'}$. By Theorem 5 of [33] (originally [31, Satz 3.19]), the last condition is equivalent to the existence of $\gamma \in K^*$ such that $\sigma\mathfrak{a}' = \gamma\mathfrak{a}$ and $\sigma\xi' = (\gamma\overline{\gamma})\xi$, which finishes the proof of the theorem. □

Remark 6.2. For a general version of Theorem 6.1, where K may contain a strict CM subfield, one needs the notion of compatibility of a polarization E and an embedding $\iota : \mathcal{O}_K \to \operatorname{End}(\mathbf{C}^g/\Lambda)$. We call E and ι *compatible* if

$$E(\alpha x, y) = E(x, \overline{\alpha} y) \quad \text{for all } x, y \in \mathbf{C}^g \text{ and } \alpha \in \operatorname{End}(\mathbf{C}^g/\Lambda).$$

If K is a general CM field, then parts 1 and 3 of Theorem 6.1 still hold. Moreover, the polarization of part 1 is compatible with $\iota = \operatorname{diag}\Phi : \mathcal{O}_K \to \operatorname{End}(\mathbf{C}^g/\Phi(\mathfrak{a}))$. Part 2 of Theorem 6.1 holds under the additional condition that there exists an embedding ι that is compatible with the polarization.

On a simple abelian variety A, every polarization is compatible with every embedding $\iota : \mathcal{O}_K \to \operatorname{End}(A)$ [20, Theorem 1.4.5(iii)]. Moreover, for any abelian variety A, any embedding $\iota : \mathcal{O}_K \to \operatorname{End}(A)$ induces a $\mathbf{C}$-linear representation of K, because $\operatorname{End}(A) \subset \operatorname{End}(\mathbf{C}^g)$. That representation is equivalent to the representation $\alpha \mapsto \operatorname{diag}\Phi(\alpha)$ for some CM type Φ [20, §1.3]. If Φ is *primitive*, i.e., does not restrict to a CM type of a strict CM subfield, then A is simple [20, Theorem 1.3.4].

We call two CM types Φ and Φ' *equivalent* if there exists an automorphism σ of K such that $\Phi' = \Phi \circ \sigma$. We say that a CM type Φ of K is *induced* from a CM subfield K' if $\{\phi_{|K'} : \phi \in \Phi\}$ is a CM type of K', and that it is *primitive* if it is not induced from any strict CM subfield. Theorem 6.1 gives us the following.

Algorithm 6.3. Input: A CM field K that does not contain a strict CM subfield.
Output: A complete set of representatives for the equivalence classes of abelian varieties with CM by $\mathcal{O}_K$ over $\mathbf{C}$.

1. Let T be a complete set of representatives of the equivalence classes of CM types.
2. Let U be a complete set of representatives of the group
$$\mathcal{O}_{K_0}^*/N_{K/K_0}(\mathcal{O}_K^*)$$
of units of $\mathcal{O}_{K_0}$ modulo norms of units of $\mathcal{O}_K$.
3. Let I be a set of representatives of the ideal class group of K.
4. Take those $\mathfrak{a}$ in I such that $(\mathfrak{a}\overline{\mathfrak{a}}\mathcal{D}_{K/\mathbf{Q}})^{-1}$ is principal and generated by an element $\xi \in K$ such that ξ^2 is totally negative in K_0. For each such $\mathfrak{a}$, choose a ξ.

5. For every pair $(\mathfrak{a}, \xi)$ as in step 4 and every unit $u \in U$, take the CM type Φ consisting of those embeddings of K into $\mathbf{C}$ that map $u\xi$ to the positive imaginary axis.

6. Return the abelian varieties $A_{\Phi,\mathfrak{a},u\xi}$ for those triples $(\Phi, \mathfrak{a}, u\xi)$ of step 5 for which Φ is in T.

Proof. By part 1 of Theorem 6.1, the output consists only of principally polarized abelian varieties with CM by $\mathcal{O}_K$. Conversely, by part 2 of Theorem 6.1, every principally polarized abelian variety A with CM by $\mathcal{O}_K$ is isomorphic to $A_{\Phi,\mathfrak{a},\xi}$ for some triple $(\Phi, \mathfrak{a}, \xi)$. We can change this triple as in part 3 of Theorem 6.1 by a unique $\sigma \in \mathrm{Aut}(K)$ and $\gamma = 1 \in K^*$ to get $\Phi \in T$. This uniquely determines Φ and σ. In the same way, we can use $\sigma = 1$ and $\gamma \in K^*$ to get $\mathfrak{a}$ in the set of step 4. We get that A is isomorphic to $A_{\Phi,\mathfrak{a},u\xi}$ for some $u \in \mathcal{O}_K^*$ and a unique triple $(\Phi, \mathfrak{a}, \xi)$ with $\Phi \in T$, $\mathfrak{a}$ in the set of step 4, and ξ as found in step 4. Only the choice of u is left and by part 3 of Theorem 6.1, the isomorphism class depends exactly on the class of u in $\mathcal{O}_K^*/N_{K/K_0}(\mathcal{O}_K^*)$. □

Remark 6.4. Algorithm 6.3 is basically [33, Algorithm 1] with the difference that we don't have any duplicate abelian varieties.

Let h (resp. h_0) be the class number of K (resp. K_0) and let $h_1 = h/h_0$. We say that an abelian variety A is *of type* Φ for a CM type Φ if A is of the form $A_{\Phi,\mathfrak{a},\xi}$ for some pair $(\mathfrak{a}, \xi)$.

Proposition 6.5. The number of pairs (Φ, A), where Φ is a CM type and A is an isomorphism class of abelian varieties over $\mathbf{C}$ with CM by $\mathcal{O}_K$ of type Φ, is

$$h_1 \cdot \#\mathcal{O}_{K_0}^*/N_{K/K_0}(\mathcal{O}_K^*).$$

Proof. By Theorem 6.1, the set that we need to count is in bijection with the set S of pairs $(\mathfrak{a}, \xi)$, consisting of a fractional $\mathcal{O}_K$-ideal $\mathfrak{a}$ and a generator $\xi \in K^*$ of $(\mathfrak{a}\overline{\mathfrak{a}}\mathcal{D}_{K/\mathbf{Q}})^{-1}$ such that $\xi^2 \in K_0$ is totally negative, up to the action of K^* given by $x(\mathfrak{a}, \xi) = (x\mathfrak{a}, x^{-1}\overline{x}^{-1}\xi)$.

Such a pair $(\mathfrak{a}_0, \xi_0) \in S$ exists by [33, Theorem 4]. We now get a bijection between S and the group C of pairs $(\mathfrak{b}, u)$, consisting of a fractional $\mathcal{O}_K$-ideal $\mathfrak{b}$ and a totally positive generator $u \in K_0^*$ of $\mathfrak{b}\overline{\mathfrak{b}}$, up to the action of K^* given by $x(\mathfrak{b}, u) = (x\mathfrak{b}, x\overline{x}u)$. It is clear that the map $C \to S : (\mathfrak{b}, u) \mapsto (\mathfrak{b}\mathfrak{a}_0, u^{-1}\xi_0)$ is a bijection.

We show that the sequence

$$0 \longrightarrow \mathcal{O}_{K_0}^*/N_{K/K_0}(\mathcal{O}_K^*) \xrightarrow[u\mapsto(\mathcal{O}_K,u)]{} C \xrightarrow[(\mathfrak{b},u)\mapsto\mathfrak{b}]{} \mathrm{Cl}(K) \xrightarrow[N_{K/K_0}]{} \mathrm{Cl}(K_0) \longrightarrow 0$$

is exact, which shows that C has the correct order. Well-definedness of the maps and exactness of the sequence follow directly from the definitions, except for the surjectivity of the norm map, which is [34, Theorem 10.1]. □

6.2 Quartic CM fields

We now give three results that describe the set of equivalence classes of CM types, the group $\mathcal{O}_{K_0}^*/N_{K/K_0}(\mathcal{O}_K^*)$, and the number of isomorphism classes of CM abelian varieties in the case $g = 2$.

Lemma 6.6. Let K be a quartic CM field with the four distinct embeddings $\phi_1, \phi_2, \overline{\phi_1}, \overline{\phi_2}$ and let $\Phi = \{\phi_1, \phi_2\}, \Phi' = \{\phi_1, \overline{\phi_2}\}$.

1. If K is Galois with group $C_2 \times C_2$, then each CM type is non-primitive. In that case, there are two equivalence classes of CM types $\{\Phi, \overline{\Phi}\}$ and $\{\Phi', \overline{\Phi'}\}$, each class induced from a different imaginary quadratic subfield of K.
2. If K is cyclic Galois, then all CM types are equivalent and primitive.
3. If K is non-Galois, then each CM type is primitive and the equivalence classes of CM types are $\{\Phi, \overline{\Phi}\}$ and $\{\Phi', \overline{\Phi'}\}$.

In particular, for a quartic CM field, either all or none of the CM types are primitive and we call the field *primitive* or *non-primitive* accordingly.

By Lemma 6.6, we can take the set T of Algorithm 6.3 to consist of a single CM type if K is cyclic and we can take $T = \{\Phi, \Phi'\}$ if K is non-Galois. The following lemma gives the set U.

Lemma 6.7. If K is a primitive quartic CM field, then

$$\mathcal{O}_{K_0}^*/N_{K/K_0}(\mathcal{O}_K^*) = \mathcal{O}_{K_0}^*/{\mathcal{O}_{K_0}^*}^2 = \{\pm 1, \pm c\},$$

where c is the class of the fundamental unit of $\mathcal{O}_{K_0}$ modulo squares.

Proof. As K has degree 4 and does not contain a primitive third or fourth root of unity, it is either $\mathbf{Q}(\zeta_5)$ or does not contain a root of unity different from ± 1. What we need to prove is true for $\mathbf{Q}(\zeta_5)$, so assume that K is not $\mathbf{Q}(\zeta_5)$.

Let ϵ (resp. ϵ_0) be a generator of $\mathcal{O}_K^*$ (resp. $\mathcal{O}_{K_0}^*$) modulo torsion and assume without loss of generality that ϵ_0 is not totally negative. Then $\epsilon_0 = \pm\epsilon^k$ for some integer k, where without loss of generality, we have $k > 0$. By taking the norm N_{K/K_0}, we find $\epsilon_0^2 = N_{K/K_0}(\epsilon)^k$, so either $k = 1$ and we are done, or $k = 2$ and $\epsilon_0 = N_{K/K_0}(\epsilon)$ is totally positive.

Suppose that $k = 2$. Then $\epsilon_0 = \pm\epsilon^2$ and as $\epsilon \notin K_0$, we find that the sign is negative and $\epsilon = \sqrt{-\epsilon_0}$ generates K over K_0 and hence over $\mathbf{Q}$. As ϵ_0 is totally positive, we get that ϵ_0 and its inverse are conjugate over $\mathbf{Q}$. As the square of $\pm\epsilon^{\pm 1}$ is $-\epsilon_0^{\pm 1}$, it follows that all elements of the set $\{\pm\epsilon^{\pm 1}\}$ are conjugate over $\mathbf{Q}$. The group $C_2 \times C_2$ acts on this set by taking inverses and by multiplication by -1. This action is faithful, because $\epsilon \neq -\epsilon$ and if $\epsilon^{-1} = \pm\epsilon$, then $\epsilon^2 = \pm 1$, contradicting the assumption that ϵ has infinite order. In particular, K is Galois with group $C_2 \times C_2$. □

Lemma 6.8. Let K be a quartic CM field. If K is cyclic, then there are h_1 isomorphism classes of abelian surfaces with CM by $\mathcal{O}_K$. If K is non-Galois, then there are $2h_1$ such isomorphism classes.

Proof. Proposition 6.5 counts each such class exactly two or four times depending on whether K is Galois (by Example 6.6). Lemma 6.7, shows that $\#\mathcal{O}_{K_0}^*/N_{K/K_0}(\mathcal{O}_K^*) = 4$. □

6.3 Implementation details

In practise, Algorithm 6.3 takes up only a very small portion of the time needed for Igusa class polynomial computation. The purpose of this section is to show that indeed Algorithm 6.3 can be run in time $\widetilde{O}(|\Delta|)$ and to show that the size of the output for each isomorphism class is small: only polynomial in $\log\Delta$.

It is well known that class group computations for number fields K of fixed degree can be performed in time $\widetilde{O}(|\Delta|^{\frac{1}{2}})$, where Δ is the discriminant of K (see for example [24, 29]). The representatives of the ideal classes that are given in the output will be integral ideals of norm below the Minkowski bound $(4/\pi)^g(2g)!(2g)^{-2g}|\Delta|^{1/2}$.

The class group computations show that for each $\mathfrak{a}$, we can check in time $\widetilde{O}(|\Delta|^{\frac{1}{2}})$ if $\mathfrak{a}\overline{\mathfrak{a}}\mathcal{D}_{K/\mathbf{Q}}$ is principal and, if so, write down a generator ξ. Then we check if $\zeta\xi$ is totally imaginary for any of the roots of unity ζ in K (note that $\mathbf{Q}(\zeta_5)$ is the only primitive quartic CM field with more than 2 roots of unity). If $g = 2$, then the set T and the group $\mathcal{O}_{K_0}^*/N_{K/K_0}(\mathcal{O}_K^*)$ are already given below Lemma 6.6 and in Lemma 6.7, where ϵ of Lemma 6.7 is a by-product of the class group computations. In particular, if $g = 2$, then it takes time at most $\widetilde{O}(|\Delta|)$ to perform all the steps of Algorithm 6.3.

A priori, the bit size of ξ can be as large as the regulator of K, but we can easily make it much smaller as follows. We identify $K \otimes \mathbf{R}$ with $\mathbf{C}^g$ via the complex absolute values of K and consider the standard Euclidean norm on $\mathbf{C}^g$. Then we find a short vector $b\sqrt{|\xi|^{-1}} \in \sqrt{|\xi|^{-1}}\mathcal{O}_K \subset K \otimes \mathbf{R}$ using the LLL-algorithm [22] and replace $\mathfrak{a}$ by $b\mathfrak{a}$ and ξ by $(b\overline{b})^{-1}\xi$. By Theorem 6.13, this does not change the corresponding isomorphism class of principally polarized abelian variety. This also doesn't change the fact that ξ is in $\mathcal{O}_K$ and $\mathfrak{a}$ is an integral ideal. Finally, we also compute an LLL-reduced basis of $\mathfrak{a} \subset \mathcal{O}_K \otimes \mathbf{R}$. In the special case $g = 2$, we get the following result.

Lemma 6.9. On input a primitive quartic CM field K, the output of Algorithm 6.3 has bit size $\widetilde{O}(\Delta^{1/2})$ for each isomorphism class of complex principally polarized abelian surfaces with CM by $\mathcal{O}_K$.

Proof. We start with $\mathfrak{a}$ of norm below the Minkowski bound, hence $N(\xi^{-1}) = N(\mathfrak{a})^2 N(\mathcal{D}) \leq C\Delta^3$ for some constant C.

The covolume of the lattice $\sqrt{|\xi|^{-1}}\mathcal{O}_K$ is $\pi^g N(\xi^{-1})^{1/2}\Delta^{1/2}$, so we find a vector $b\sqrt{|\xi|^{-1}}$ of length at most $C'N(\xi^{-1})^{1/(4g)}\Delta^{1/(4g)}$ for some constant C'. In particular, $b\overline{b}\xi^{-1}$ has all absolute values below

${C'}^2 N(\xi^{-1})^{1/(2g)}\Delta^{1/(2g)}$. Therefore, $b\bar{b}\xi^{-1}$ has bit size $O(\log\Delta)$ and norm at most ${C'}^{4g}N(\xi^{-1})\Delta$, so b has norm at most ${C'}^{2g}\Delta^{1/2}$.

This implies that $b\mathfrak{a}$ has norm at most $C''\Delta$, so an LLL-reduced basis has bit size $O(\log\Delta)$.

All elements we encountered can be given (up to multiplication by units in $\mathcal{O}_{K_0}^*$) with all absolute values below the square root of the norm times an absolute value of a fundamental root. Therefore, the size of the numbers in the LLL-algorithm is $\widetilde{O}(\mathrm{Reg}_K) = \widetilde{O}(|\Delta|^{1/2})$. □

7 Symplectic bases and the Siegel upper half space

Let $(\mathbf{C}^g/\Lambda, E)$ be a principally polarized abelian variety. The lattice Λ has a basis which is *symplectic* with respect to E, i.e., a basis $e_1,\ldots,e_g,v_1,\ldots,v_g$ with respect to which E is given by the matrix Ω, given in terms of $(g\times g)$-blocks as

$$\Omega = \begin{pmatrix} 0 & 1_g \\ -1_g & 0 \end{pmatrix}.$$

The vectors v_i form a $\mathbf{C}$-basis of $\mathbf{C}^g$ and if we rewrite everything in terms of this basis, then Λ becomes $Z\mathbf{Z}^g + \mathbf{Z}^g$ with

$$Z \in \mathcal{H}_g = \{Z \in \mathrm{Mat}_g(\mathbf{C}) : Z^t = Z \text{ and } \mathrm{Im}\, Z \text{ is positive definite}\}.$$

We define the *symplectic group* $\mathrm{Sp}_{2g}(\mathbf{Z})$ by

$$\mathrm{Sp}_{2g}(\mathbf{Z}) = \{M \in \mathrm{GL}_{2g}(\mathbf{Z}) : M^t\Omega M = \Omega\}.$$

In terms of $(g\times g)$-blocks, the matrix

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

is in $\mathrm{Sp}_{2g}(\mathbf{Z})$ if and only if

1. A^tC and B^tD are symmetric and
2. $A^tD - C^tB = 1$.

The set $\mathrm{Sp}_{2g}(\mathbf{Z})$ is a subgroup of GL_{2g} which acts on $\mathcal{H}_g$ via

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} Z = (AZ+B)(CZ+D)^{-1}.$$

The association of Z to $(\mathbf{C}^g/Z\mathbf{Z}^g + \mathbf{Z}^g, E)$ gives a bijection between $\mathrm{Sp}_g(\mathbf{Z})\setminus\mathcal{H}_g$ and the set of principally polarized abelian varieties over $\mathbf{C}$ up to isomorphism.

7.1 A symplectic basis for $\Phi(\mathfrak{a})$

Now it is time to compute symplectic bases. As the bit size of all data is polynomial in $\log \Delta$ now, we can easily compute a matrix for the form $(\alpha, \beta) \mapsto \mathrm{Tr}(\xi \alpha \overline{\beta})$ with respect to our basis of $\mathfrak{a}$. The coefficients of that matrix are integers of bit size polynomial in $\log \Delta$. The following standard Gram-Schmidt-based algorithm computes a symplectic basis.

Algorithm 7.1. Input: $A \in \mathrm{Mat}_{2n}(\mathbf{Z})$ with determinant 1 and $A^T = -A$.
Output: An invertible matrix M such that

$$M^t A M = \begin{pmatrix} 0 & 1_n \\ -1_n & 0 \end{pmatrix}.$$

1. Let $e_i' \in \mathbf{Z}^n$ be a unit vector linearly independent of e_j and v_j for $j \in \{1, \ldots, i-1\}$.
2. Let
$$e_i = \frac{1}{k}\left(e_i' - \sum_{j=1}^{i-1} (e_j^t A e_i') v_j + \sum_{j=1}^{i-1} (v_j^t A e_i') e_j \right),$$
where k is the largest positive integer such that e_i is in $\mathbf{Z}^{2n}$.
3. Let v_i' be such that $e_i^t A v_i' = 1$.
4. Let
$$v_i = v_i' - \sum_{j=1}^{i-1} (e_j^t A v_i') v_j + \sum_{j=1}^{i-1} (v_j^t A v_i') e_j.$$

Let the first n columns of M be the e_i and the last n the v_i.

The only non-obvious step is step 3. Existence of such a v_i' follows from the fact that A is invertible and e_i cannot be divided by integers greater than 1. The vector v_i' can be computed in polynomial time using LLL or simply a repeated euclidean algorithm. For fixed n, the algorithm is quasi-linear in the (bit) size of the input, while the size of the output is linear in the size of the input.

We now get a symplectic basis of height linear in $\log \Delta$. That means that the corresponding period matrix can also be given with entries of height linear in $\log \Delta$.

8 The fundamental domain of the Siegel upper half space

In the genus 1 case, to compute the j-invariant of a point $z \in \mathcal{H} = \mathcal{H}_1$, one should first move z to the *fundamental domain* for $\mathrm{SL}_2(\mathbf{Z})$, or at least away from $\mathrm{Im}\, z = 0$, to get good convergence.

In genus 2, when computing θ-values at a point $Z \in \mathcal{H}_2$, as we will do in Section 10, we move the point to the fundamental domain for $\mathrm{Sp}_4(\mathbf{Z})$, or something larger.

For $g = 1$, the fundamental domain $\mathcal{F} \subset \mathcal{H}$ is the set of $z = x + iy \in \mathcal{H}$ that satisfy

1. $-\frac{1}{2} < x \leq \frac{1}{2}$ and
2. $|z| \geq 1$.

A third condition $x \geq 0$ if $|z| = 1$ is needed in order to make the point in $\mathcal{F}$ unique for every orbit, but we will omit that condition. To move z into this fundamental domain, we simply iterate the following until z is in $\mathcal{F}$:

1. $z \leftarrow z + \lfloor -x + \frac{1}{2} \rfloor$
2. $z \leftarrow -\frac{1}{z}$ if $|z| < 1$

We also phrase this in terms of the positive definite binary quadratic form f such that $f(z,1) = 0$. Such a form is defined up to scalar multiplication and given by $f(a,b) = (a,b)Y(a,b)^t$ for a positive definite symmetric real matrix

$$Y = \begin{pmatrix} y_1 & y_3 \\ y_3 & y_2 \end{pmatrix}.$$

We give an analysis of the above algorithm in terms of these matrices, which comes in handy in the genus 2 case. The action of $\mathrm{SL}_2(\mathbf{Z})$ on $\mathcal{H}$ corresponds to the action on positive definite symmetric real matrices, given by $U(Y) = U^t Y U$ for $U \in \mathrm{SL}_2(\mathbf{Z})$. We call Y *reduced* if the corresponding $z \in \mathcal{H}$ is in $\mathcal{F}$, i.e., if and only if

$$\begin{array}{l} 0 \leq 2|y_3| \leq y_1 \leq y_2 \quad \text{and} \\ y_3 \geq 0 \quad \text{if } 2|y_3| = y_1. \end{array}$$

Algorithm 8.1. Input: A positive definite symmetric matrix $Y_0 \in \mathrm{Mat}_2(\mathbf{R})$.
Output: $U \in \mathrm{SL}_2(\mathbf{Z})$ and $Y = U^t Y_0 U$ such that Y is reduced.
Start with $Y = Y_0$ and iterate the following until Y is reduced.

1. Let $\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}$ act for $r = \lfloor -y_3/y_1 + \frac{1}{2} \rfloor$.
2. Let $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ act if $y_1 > y_2$.

We can bound the runtime in terms of the *minima* of the matrix Y. We define the *first and second consecutive minima* $m_1(Y)$ and $m_2(Y)$ of a symmetric positive definite matrix Y as follows. Let $m_1(Y) = p^t Y p$ be minimal among all column vectors $p \in \mathbf{Z}^2$ different from 0 and let $m_2(Y) = q^t Y q$ be minimal among all $q \in \mathbf{Z}^2$ linearly independent of p. We call $m_1(Y)$ also simply the *minimum* of Y. If Y is reduced, then we have

$$m_1(Y) = y_1, \quad m_2(Y) = y_2 \quad \text{and} \quad \frac{3}{4} y_1 y_2 \leq \det Y \leq y_1 y_2,$$

so for every positive definite symmetric matrix Y, we have

$$\frac{3}{4} m_1(Y) m_2(Y) \leq \det Y \leq m_1(Y) m_2(Y). \tag{2}$$

As we have

$$Y^{-1} = \frac{1}{\det Y} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} Y \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

it also follows that

$$m_i(Y^{-1}) = \frac{m_i(Y)}{\det Y}, \quad (i \in \{1, 2\}). \tag{3}$$

For any matrix A, let $|A|$ be the maximum of the absolute values of the entries.

Lemma 8.2. Algorithm 8.1 is correct and takes $O(\log(|Y_0|/m_1(Y_0)))$ operations in R. The inequalities $|Y| \leq |Y_0|$ and $|U| \leq 8|Y_0|/(3m_1(Y_0))$ hold for the output and also for the values of Y and U throughout the execution of the algorithm.

Proof. Let $z = x + iy \in \mathcal{H}$ correspond to Y and $z_0 \in \mathcal{H}$ to Y_0. By drawing a picture, one easily sees that if $|x| \leq \frac{1}{2}$ and $y \geq 1/\sqrt{12}$, then z is in

$$\mathcal{F} \cup \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \mathcal{F} \cup \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix} \mathcal{F},$$

hence in $\mathcal{F}$ after at most one more iteration. On the other hand, if $y < 1/\sqrt{12}$, then $|z|^2 = x^2 + y^2 \leq \frac{7}{12}$, hence y grows by a factor of at least $\frac{12}{7}$ during that iteration. In particular, the number of iterations is at most $O(\log \max\{1/y, 1\})$.

Now $m_1(Y)/y_1$ is the square of the length of the shortest vector in $\mathbf{Z} + z\mathbf{Z}$, hence is at most $\min\{y^2, 1\}$, so we get $\max\{1/y, 1\} \leq \sqrt{y_1/m_1(Y)}$, which proves the bound on the number of iterations.

The value of $|Y|$ is decreasing, hence the bound $|Y| \leq |Y_0|$ is trivial.

Next, we prove that the entries of the output U are bounded by $\sqrt{4|Y_0|/(3m_1(Y_0))}$. Let U, Y be the output. Then $Y = C^t C$, where C is upper-triangular with columns $(\sqrt{y_1}, 0)$ and $(y_3/\sqrt{y_1}, \sqrt{y_2 - y_3^2/y_1})$. Reducedness of Y implies that $\sqrt{y_2 - y_3^2/y_1} \geq \sqrt{3y_1/4}$. As we have $Y_0 = (CU^{-1})^t(CU^{-1})$, we find that the entries of CU^{-1} are bounded by $\sqrt{|Y_0|}$, hence the entries of U^{-1} (and hence U) are bounded by $\sqrt{|Y_0|}/\sqrt{3y_1/4}$, where $y_1 = m_1(Y_0)$.

Finally, if (U', Y') is the value during the algorithm and (U, Y) is the output, then $U' = UU''^{-1}$, where U is the output and U'' is what the output would be if the input was Y'. We find $|U'| \leq 2|Y_0|/(3m/4)$. □

For genus 2, the *fundamental domain* $\mathcal{F}_2$ is defined to be the set of $Z = X + iY \in \mathcal{H}_2$ for which

(F1) the real part X is reduced, i.e., $-\frac{1}{2} \leq x_i < \frac{1}{2}$ $(i = 1, 2, 3)$,

(F2) the imaginary part Y is reduced, i.e., $0 \leq 2y_3 \leq y_1 \leq y_2$, and

(F3) $|\det(M^*Z)| \geq 1$ for all $M \in \mathrm{Sp}_4(\mathbf{Z})$, where M^*Z is defined by

$$M^*Z = CZ + DM \quad \text{for} \quad M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}_4(\mathbf{Z}).$$

Reduction of the real part is trivial and obtained by $X \mapsto X + B$, for a unique $B \in \mathrm{Mat}_2(\mathbf{Z})$. Here $X \mapsto X + B$ corresponding to the action of

$$\begin{pmatrix} 1 & B \\ 0 & 1 \end{pmatrix} \in \mathrm{Sp}_4(\mathbf{Z})$$

on Z.

Reduction of the imaginary part is reduction of positive definite symmetric matrices as in Algorithm 8.1, but with the extra condition $y_3 \geq 0$, which can be optained by applying the $\mathrm{GL}_2(\mathbf{Z})$-matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

It follows that U^tYU is reduced for a unique $U \in \mathrm{GL}_2(\mathbf{Z})$, and to reduce the imaginary part of Z, we replace Z by

$$U^tZU = \begin{pmatrix} U^t & 0 \\ 0 & U^{-1} \end{pmatrix} Z$$

for that U.

The third condition has a finite formulation, as Gottschling [17] computed a set $\mathfrak{G} \subset \mathrm{Sp}_4(\mathbf{Z})$ of 19 matrices such that, under conditions (F1) and (F2), condition (F3) is equivalent to the condition

(F3') $|\det(M^*Z)| \geq 1$ for all $M \in \mathfrak{G}$.

For our purposes, it suffices to consider the set $\mathcal{B} \subset \mathcal{H}_2$, given by (F1), (F2), and

(F3") $y_1 \geq \sqrt{3/4}$.

The condition (F3") follows immediately from (F1) and $z_1 \geq 1$, which is equivalent to $|\det(N_0^*Z)| \geq 1$ for the single matrix

$$N_0 = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathfrak{G},$$

so $\mathcal{B}$ contains $\mathcal{F}_2$.

The reduction algorithm that moves $Z \in \mathcal{H}_2$ into $\mathcal{F}_2$ or simply $\mathcal{B}$ reads as follows.

Algorithm 8.3. Input: $Z_0 \in \mathcal{H}_2$.
Output: Z in $\mathcal{F}_2$ (resp. $\mathcal{B}$) and a matrix

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}_4(\mathbf{Z})$$

such that Z equals $MZ_0 = (AZ_0 + B)(CZ_0 + D)^{-1}$.
We start with $Z = Z_0$ and iterate the following until Z is reduced.

1. Reduce the imaginary part.
2. Reduce the real part.

3. Apply N to Z for $N \in \mathfrak{G}$ (resp. $N = N_0$) with $|\det(N^*Z)| < 1$ minimal, if such an N exists.

We will bound the number of iterations by showing that $\det Y$ is increasing and bounded, that we have a bounded number of steps with $|y_1| \geq \frac{1}{2}$, and that every step with $|y_1| < \frac{1}{2}$ leads to a doubling of $\det Y$.

Lemma 8.4. For any point $Z \in \mathcal{H}_2$ and any matrix $M \in \mathrm{Sp}_4(\mathbf{Z})$, we have

$$\det \mathrm{Im}(MZ) = \frac{\det \mathrm{Im}\, Z}{|\det(M^*Z)|^2}.$$

Proof. In [19, Proof of Proposition 1.1] it is computed that

$$\mathrm{Im}(MZ) = {(M^*Z)^t}^{-1}(\mathrm{Im}\, Z)(M^*\overline{Z})^{-1}. \tag{4}$$

Taking determinants on both sides proves the result. □

Steps 1 and 2 do not change $\det Y$ and Lemma 8.4 shows that step 3 increases $\det Y$, so $\det Y$ is increasing througout the algorithm.

The following result allows us to bound $m_2(Y)$ and $\det Y$ during the algorithm. It will also be very important in Section 9, where we bound the entries of the matrix Z that Algorithm 8.3 computes.

Lemma 8.5. For any point $Z = X + iY \in \mathcal{H}_2$ and any matrix $M \in \mathrm{Sp}_4(\mathbf{Z})$, we have

$$m_2(\mathrm{Im}(MZ)) \leq \frac{4}{3}\max\{m_1(Y)^{-1}, m_2(Y)\}.$$

Proof. We imitate part of the proof of [19, Lemma 3.1]. As we can replace M by

$$\begin{pmatrix} U^t & 0 \\ 0 & U^{-1} \end{pmatrix} M$$

for $U \in \mathrm{GL}_2(\mathbf{Z})$, we can assume without loss of generality that the matrix $(\mathrm{Im}(MZ))^{-1}$ is reduced. Let $(c, d) \in \mathbf{Z}^4$ with $c, d \in \mathbf{Z}^2$ be the third row of M. By (4), we have

$$(\mathrm{Im}(MZ))^{-1} = (M^*\overline{Z})Y^{-1}(M^*Z)^t,$$

so $m_1((\mathrm{Im}(MZ))^{-1}) = (cX + d)Y^{-1}(Xc^t + d^t) + cYc^t$. The matrix M is invertible, so if c is zero, then d is non-zero. Therefore, it follows that

$$m_1((\mathrm{Im}(MZ))^{-1}) \geq \min\{m_1 Y, m_1(Y^{-1})\}.$$

By (2) and (3), we get

$$\begin{aligned} m_2(\mathrm{Im}(MZ)) &\leq \frac{4\det \mathrm{Im}(MZ)}{3m_1(\mathrm{Im}(MZ))} = \frac{4}{3m_1((\mathrm{Im}(MZ))^{-1})} \\ &\leq \frac{4}{3}\max\{\frac{1}{m_1(Y)}, \frac{\det Y}{m_1(Y)}\} \\ &\leq \frac{4}{3}\min\{(m_1(Y))^{-1}, m_2(Y)\}, \end{aligned}$$

which proves the result. □

Lemma 8.6. There is a constant upper bound c, independent of the input Z_0, on the number of iterations of Algorithm 8.3 in which Z satisfies $y_1 \geq \frac{1}{2}$ at the beginning of step 3.

Proof. Let $\mathcal{C}$ be the set of points in $\mathcal{H}_2$ that satisfy (F1), (F2) and $y_1 \geq \frac{1}{2}$. At the beginning of step 3, both (F1) and (F2) hold, so we need to bound the number of iterations for which $Z \in \mathcal{C}$ at the beginning of step 3. Suppose that such an iteration exists, and denote the value of Z at the beginning of step 3 of that iteration by Z'. As $\det Y$ increases during the algorithm, each iteration has a different value of Z, so it suffices to bound the number of $Z \in \mathrm{Sp}_4(\mathbf{Z})Z' \cap L$. By [19, Theorem 3.1], the set

$$\mathfrak{C} = \{M \in \mathrm{Sp}_4(\mathbf{Z}) : \mathcal{C} \cap M\mathcal{C} \neq \emptyset\}$$

is finite. As $\mathfrak{C}$ surjects onto $\mathrm{Sp}_4(\mathbf{Z})Z' \cap L$ via $M \mapsto MZ'$, we get the constant upper bound $\#\mathfrak{C}$ on the number of iterations with $Z \in \mathcal{C}$. □

Lemma 8.7. At every iteration of step 4 of Algorithm 8.3 in which $y_1 < \frac{1}{2}$, the value of $\det Y$ increases by a factor of at least 2.

Proof. If $y_1 < \frac{1}{2}$, then for the element $N_0 \in \mathfrak{G}$, we have $|\det N^* Z|^2 = |z_1|^2 = |x_1|^2 + |y_1|^2 \leq \frac{1}{2}$, so by Lemma 8.4, the value of $\det Y$ increases by a factor ≥ 2. □

We can now bound the number of iterations. For any matrix $Z = X + iY \in \mathcal{H}_2$, let $t(Z) = \log \max\{m_1(Y)^{-1}, m_2(Y)\}$.

Proposition 8.8. The number of iterations of Algorithm 8.3 is at most $O(t(Z_0))$ for every input Z_0.

Proof. Let c be a constant of Lemma 8.6, let Z_0 be the input of Algorithm 8.3 and let Z be the value after k iterations. By Lemma 8.7, we have

$$2^{k-c} \det Y_0 \leq \det Y \leq m_2(Y)^2 \leq (\frac{4}{3})^2 \max\{m_1(Y_0)^{-2}, m_2(Y_0)^2\}$$

by Lemma 8.5, so

$$2^{k-c} \leq (\frac{4}{3})^3 \max\{m_1(Y_0)^{-3} m_2(Y_0)^{-1}, m_1(Y_0)^{-1} m_2(Y_0)\}. \qquad \square$$

To avoid a laborious error analysis, we assume that all computations are performed inside some number field $F \subset \mathbf{C}$. Indeed, for an abelian variety A with CM by $\mathcal{O}_K$, we have $Z \in \mathrm{Mat}_2(F)$, where F is the normal closure of K. For a runtime analysis, we need to bound the *height* of the numbers involved. Such height bounds are also used for lower bounds on the off-diagonal part of the output Z, which we will need in Section 10.

The height $h(x)$ of an element $x \in F^*$ is defined as follows. Let S be the set of absolute values that extend either the standard archimedean absolute value of $\mathbf{Q}$ or one of the non-archimedean absolute values

$|x| = p^{-\mathrm{ord}_p(x)}$. For each $v \in S$, let $\deg(v) = [F_v : \mathbf{Q}_v]$ be the degree of the completion F_v of F at v. Then

$$h(x) = \sum_v \deg(v) \max\{\log |x|_v, 1\}.$$

We denote the maximum of the heights of all entries of a matrix $Z \in \mathcal{H}_2$ by $h(Z)$.

During the execution of Algorithm 8.3, instead of computing the new value of Z directly from the old one at every step, we keep track of the matrix $M \in \mathrm{Sp}_4(\mathbf{Z})$ that sends the input Z_0 to the current value of Z. Every time M changes, we compute the new value of Z by computing MZ_0. This makes sure that we are always working with a 'small' representation of Z. More precisely, the height of any entry of $Z = MZ_0$ is bounded by $2h + 2\log|M|$ plus a constant, where $|A|$ for a matrix A is the maximum of the absolute values of the entries.

Lemma 8.9. During the execution of Algorithm 8.3, let M be the matrix that maps the input Z_0 to the current value of Z. The value of $\log|M|$ is bounded by $O(\log|Z_0|)$ during the first iteration and increases by at most $O(t(Z_0))$ in every other iteration, where the O does not depend on Z_0 or the iteration.

Proof. The value of $\log|M|$ increases by at most $O(\log|Z|)$ during steps 1 and 2 and by at most $\log 4$ during step 3, so it suffices to prove that at the beginning of every iteration but the first, we have $\log|Z| = O(t(Z_0))$.

At the beginning of step 3, Lemma 8.5 and the fact that $|x_i| \leq \frac{1}{2}$ show that we have $\log|Z| = O(t(Z_0))$. During step 3, Z gets replaced by

$$\begin{aligned}&(AZ + B)(CZ + D)^{-1}\\ &= \tfrac{1}{\det(CZ+D)}(AZ + B)\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}(CZ + D)\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\end{aligned}$$

where

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

is in a finite set $\mathfrak{G}$. Therefore, after step 3, we have $\log|Z| = O(t(Z_0)) + O(-\log|\det(CZ+D)|)$. Finally, we notice that Lemma 8.5 and Lemma 8.4 together imply the upper bound $O(t(Z_0))$ on $-\log|\det(CZ + D)|$. Therefore, $\log|Z|$ is $O(t(Z_0))$ at the beginning of every but the first iteration. □

Recall that $t(Z_0) = \log\max\{m_1(Y_0)^{-1}, m_2(Y_0)\}$ for $Z_0 = X_0 + iY_0 \in \mathcal{H}_2$.

Theorem 8.10. *Let F be a number field. Algorithm 8.3, on input $Z_0 \in \mathrm{Mat}_2(F) \cap \mathcal{H}_2$, returns an $\mathrm{Sp}_4(\mathbf{Z})$-equivalent matrix $Z \in \mathcal{F}_2$. The runtime is $\widetilde{O}(h\log|Z_0|) + \widetilde{O}(t(Z_0)^4)$, and the output Z satisfies $h(Z) = O(h(Z_0)) + O(t(Z_0)^2)$, where the O and $\widetilde{O}$ depend only on the degree of F.*

Proof. By Proposition 8.8 and Lemma 8.9, $\log|M|$ is bounded by $O(\log|Z_0|)+O(t(Z_0)^2)$, so the height of every entry of Z is bounded by $O(t(Z_0)^2)+O(h(Z_0))$. This implies that basic arithmetic operations take time $\widetilde{O}(t(Z_0)^2)+\widetilde{O}(h(Z_0))$ throughout the algorithm. The first iteration takes $O(\log|Z_0|)+O(t(Z_0))$ such operations (Lemma 8.2) and all other $O(t(Z_0))$ iterations take $O(t(Z_0))$ operations, so there are $O(\log|Z_0|)+O(t(Z_0)^2)$ arithmetic operations, yielding a total time $\widetilde{O}(t(Z_0)^4)+\widetilde{O}(h\log|Z_0|)$ □

Corollary 8.11. Let $Z_0 \in \mathrm{Mat}_2(F)\cap\mathcal{H}_2$ be the input of Algorithm 8.3 and

$$Z=\begin{pmatrix} z_1 & z_3 \\ z_3 & z_2 \end{pmatrix}$$

the output. Then either z_3 is zero or $-\log|z_3|$ is bounded from above by $O(h(Z_0))+O(t(Z_0)^2)$, where the O depends only on the degree of the number field F.

Proof. This follows from the fact that the height of z_3 is $O(h(Z_0))+O(t(Z_0)^2)$. □

Now that we know how to move points to the fundamental domain, the following shows how to see if two points are $\mathrm{Sp}_4(\mathbf{Z})$-equivalent. That way, one could, for example, eliminate duplicate abelian varieties if one chooses to use a non-proven method for the class group computations in Algorithm 6.3.

Lemma 8.12. Let $\mathfrak{G}'$ consist of the 38 matrices

$$\begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & e_1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & e_1 \end{pmatrix},$$
$$\begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & -1 & d & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & e_1 & e_3 \\ 0 & 1 & e_3 & e_2 \end{pmatrix},$$

where d ranges over $0,\pm1,\pm2$ and each e_i over $\{0,\pm1\}$. Then $\mathfrak{G}'$ contains $\mathfrak{G}$. Moreover, for every element Z of $\mathcal{F}_2$, the set $\mathrm{Sp}_4(\mathbf{Z})Z\cap\mathcal{F}_2$ can be computed as follows. For every element M of $\mathfrak{G}'$ such that $|\det(M^*Z)|=1$,

1. set $Z' =\leftarrow MZ$,
2. reduce the imaginary part Y',
3. reduce the real part X',
4. output Z'.

Proof. If both Z and NZ lie in $\mathcal{F}_2$, then we have $|\det N^*Z|=1$, and Z satisfies (F1), (F2), and $|z_1|,|z_2|\geq 1$. The proof of [17, Satz 1] shows that this implies that the bottom half of N consists of the (2×2)-blocks

$U^{-1}C, U^{-1}D$, where U is in $\mathrm{GL}_2(\mathbf{Z})$ and C, D make up the bottom row of an element M of $\mathfrak{G}'$.

Now N and

$$\begin{pmatrix} U^t & 0 \\ 0 & U^{-1} \end{pmatrix} M$$

are symplectic matrices with the same bottom half and this implies that N is equal to

$$\begin{pmatrix} 1 & T \\ 0 & 1 \end{pmatrix} \begin{pmatrix} U^t & 0 \\ 0 & U^{-1} \end{pmatrix} M$$

for some symmetric integer matrix T. In particular, $U^t(\operatorname{Im} MZ)U = \operatorname{Im} NZ$ satisfies (F2), hence U is the matrix found in step 2. □

9 Relative quadratic extensions

In Sections 6 – 8, we gave an algorithm that gives one period matrix Z in the fundamental domain $\mathcal{F}_2$ of the Siegel upper half space $\mathcal{H}_2$ for every isomorphism class of principally polarized abelian surface over $\mathbf{C}$ with CM by $\mathcal{O}_K$. In Section 10, we give bounds on the Igusa invariants in terms of the entries of Z. The purpose of the currect section is to bound the entries of Z. We will study the *Hilbert moduli space* of abelian varieties with real multiplication for this.

The theory of the Hilbert moduli space also allows us to generalize Spallek's method for enumerating period matrices of CM abelian surfaces to the case where K_0 has arbitrary class number (Section 9.2), and to present a new alternative method for enumerating those period matrices (Section 9.3). Sections 9.2 and 9.3 can be read independently of each other and are not needed for the rest of the text.

In order to give upper bounds on the second consecutive minimum $m_2(Y)$ that hold for every CM-by-$\mathcal{O}_K$ period matrix $Z = X + iY$, we first show the existence of a 'good' period matrix Z' in every $\mathrm{Sp}_4(\mathbf{Z})$-orbit, where 'good' means that the first minimum $m_1(Y')$ of the imaginary part Y' of Z' is large, while the second minimum $m_2(Y)$ is small.

The bounds that we give are as follows. For a quartic CM field K, let Δ be the discriminant of K and let Δ_0 be the discriminant of its real quadratic subfield K_0. Then we have $\Delta = \Delta_1\Delta_0^2$, where Δ_1 is the norm of the relative discriminant of K/K_0.

Proposition 9.1. Let K be a primitive quartic CM field. Every isomorphism class of principally polarized abelian varieties with complex multiplication by $\mathcal{O}_K$ has a representative with period matrix $Z' = X' + iY'$, where

$$\frac{1}{\Delta_0} \leq 4 \det Y' \leq \sqrt{\Delta_1} \quad \text{and}$$

$$\frac{1}{2\Delta_0} \leq m_1(Y') \leq m_2(Y') \leq \frac{1}{3}\Delta_1^{1/2}\Delta_0^{1/2}.$$

Corollary 9.2. Let K be a primitive quartic CM field. Every period matrix Z with CM by $\mathcal{O}_K$ satisfies

$$m_2(\operatorname{Im} Z) \leq \frac{4}{3}\max\{2\Delta_0, \frac{1}{3}\Delta_1^{1/2}\Delta_0^{1/2}\}.$$

Proof. Any such period matrix Z^* can be obtained via $\mathrm{Sp}_4(\mathbf{Z})$-transformation from the matrix Z' of Proposition 9.1. Lemma 8.5 bounds $m_2(\operatorname{Im} Z)$ in terms of the minima of Y'. □

9.1 The Hilbert upper half space

We will find Z' as in Proposition 9.1 by writing a fractional $\mathcal{O}_K$-ideal $\mathfrak{a}$ from Section 6 as $z\mathfrak{b} + \mathfrak{b}^{-1}$, where z and $\mathfrak{b}$ are chosen in such a way that $m_1(Y')$ is large. The study of such z and $\mathfrak{b}$ and how they relate to the corresponding abelian variety is most naturally seen as the study of the *Hilbert upper half space* and the action of the group $\mathrm{SL}(\mathfrak{b} \oplus \mathfrak{b}^{-1})$ on it. The *Hilbert upper half space* classifies polarized abelian varieties with *multiplication structure* by a totally real order.

Let F be a number field for which the complex conjugation automorphism does not depend on the choice of embedding of F into $\mathbf{C}$. In other words, let F be either a totally real number field or a CM field. Let $A = (T, E)$ be a polarized abelian variety.

Definition 9.3. A *multiplication structure by $\mathcal{O}_F$ on A* is a ring homomorphism $\iota : \mathcal{O}_F \to \mathrm{End}(A)$ such that $E(\iota(x)u, v) = E(u, \iota(\overline{x})v)$ for all $x \in \mathcal{O}_F$ and all $u, v \in T$. An *isomorphism $f : (A, \iota) \to (A', \iota')$ of polarized abelian varieties over* $\mathbf{C}$ *with multiplication structure by $\mathcal{O}_F$* is a morphism of polarized abelian varieties f such that $\iota'(\alpha) \circ f = f \circ \iota(\alpha)$ for all $\alpha \in \mathrm{End}(A)$.

Lemma 9.4. Let K be a CM field that does not contain a strict CM subfield and let A be a principally polarized abelian variety ith CM by $\mathcal{O}_K$. Then A has a multiplication structure by $\mathcal{O}_K$, which is unique up to automorphism of K.

Let K_0 be the totally real subfield of degree g of K. Then A has a multiplication structure by $\mathcal{O}_{K_0}$ that extends to a multiplication structure by $\mathcal{O}_{K_0}$. It is unique up to automorphisms of K_0 that extend to automorphisms of K.

Proof. Existence of a multiplication structure by $\mathcal{O}_K$ is [20, Theorem 1.4.5(iii) and Theorem 1.3.4] As K is a CM field, all automorphisms of K commute with complex conjugation, hence uniqueness is exactly up to automorphism of K. For the multiplication structure by $\mathcal{O}_{K_0}$, we take the restriction of the multiplication structure by $\mathcal{O}_K$. □

Let K_0 be any totally real number field of degree g and let $\phi_1, \ldots, \phi_g$ be the embeddings of K_0 into $\mathbf{R}$. For simplicity, we assume that the different $\mathcal{D}_{K_0/\mathbf{Q}}$ of K_0 is principal and generated by δ. If $g = 2$, then this is true with $\delta = \sqrt{\Delta_0}$. We identify $K_0 \otimes \mathbf{C}$ with $\mathbf{C}^g$ via the sequence of embeddings $\phi_1, \ldots, \phi_g$. In each copy of $\mathbf{C}$, there is a copy of the classical upper half plane

$$\mathcal{H} = \mathcal{H}_1 = \{z \in \mathbf{C} : \operatorname{Im} z > 0\}.$$

The *Hilbert upper half space* is the g-fold cartesian product $\mathcal{H}^g \subset \mathbf{C}^g = K_0 \otimes \mathbf{C}$ and comes with an action of the group $\mathrm{SL}_2(K_0)$, given by

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} z = \frac{\alpha z + \beta}{\gamma z + \delta},$$

where multiplication and addition take place in the ring $K_0 \otimes \mathbf{C}$. The same formula also defines an action of $\mathrm{SL}_2(K_0)$ on $\mathbf{P}^1(K_0)$.

For any fractional $\mathcal{O}_{K_0}$-ideal $\mathfrak{b}$ and any point $z \in \mathcal{H}^g \subset K_0 \otimes \mathbf{C}$, let Ψ_z be the map

$$\begin{array}{ccc} K_0 \oplus K_0 & \to & K_0 \otimes \mathbf{C} = \mathbf{C}^g \\ (x, y) & \mapsto & zx + y. \end{array}$$

The image $\Lambda_{z,\mathfrak{b}} \subset \mathbf{C}^g$ of $\mathfrak{b} \oplus \mathfrak{b}^{-1}$ under Ψ_z is a lattice. The map $E_z : \Lambda_{z,\mathfrak{b}} \times \Lambda_{z,\mathfrak{b}} \to \mathbf{R}$, given by

$$E_z(\Psi_z(x, y), \Psi_z(x', y')) = \mathrm{Tr}_{K_0/\mathbf{Q}}(\delta^{-1}(yx' - xy'))$$

for $x, y, x', y' \in K_0$, can uniquely be extended $\mathbf{R}$-linearly to an $\mathbf{R}$-bilinear form on $\mathbf{C}^g \times \mathbf{C}^g$. Let ι be the map from $\mathcal{O}_{K_0}$ to $\mathrm{End}_{\mathbf{R}}(\mathbf{C}^g)$ given by

$$(\iota\alpha)\Psi_z(x, y) = \Psi_z(\alpha x, \alpha y).$$

Denote the triple $(\mathbf{C}^g/\Lambda_{z,\mathfrak{b}}, E_z, \iota)$ by $A_{z,\mathfrak{b}}$ and $A_z = A_{z,\mathcal{O}_{K_0}}$.

Theorem 9.5. *For any totally real number field K_0 of degree g, if $\mathcal{D}_{K_0/\mathbf{Q}}$ is principal, then we have a bijection*

$$\begin{array}{ccc} \mathrm{SL}_2(\mathcal{O}_{K_0}) \setminus \mathcal{H}^g & \to & \left\{ \begin{array}{c} \textit{isomorphism classes of abelian} \\ \textit{varieties with multiplication} \\ \textit{structure by } \mathcal{O}_{K_0} \end{array} \right\} \\ z & \mapsto & A_z. \end{array}$$

We will prove (and also need) the following more general version. Let $b_1, \ldots, b_g$ be a $\mathbf{Z}$-basis of $\mathfrak{b}^{-1}$. Consider the $\mathbf{Q}$-linear trace form $(x, y) \mapsto \mathrm{Tr}(xy)$ on $K_0 \times K_0$. Let $b_1^*, \ldots, b_g^*$ be the dual basis of the basis $b_1, \ldots, b_g$. Then by [28, §III.2], $b_1^*, \ldots, b_g^*$ is a $\mathbf{Z}$-basis of $\mathcal{D}_{K_0/\mathbf{Q}}^{-1}\mathfrak{b} = \delta\mathfrak{b}$.

Theorem 9.6. *Let K_0 be a totally real number field of degree g for which the different $\mathcal{D}_{K_0/\mathbf{Q}}$ is principal.*

1. *For any pair $(z, \mathfrak{b})$ as above, we have that $A_{z,\mathfrak{b}}$ is a principally polarized abelian variety with multiplication structure by $\mathcal{O}_{K_0}$. Moreover, the $\mathbf{Z}$-basis*

$$\delta^{-1}b_1^*z, \ldots, \delta^{-1}b_g^*z, b_1, \ldots, b_g$$

of $\Lambda_{z,\mathfrak{b}}$ is symplectic for E_z.

2. *Any principally polarized abelian variety with multiplication structure by $\mathcal{O}_{K_0}$ is isomorphic to $A_{z,\mathcal{O}_{K_0}}$ for some $z \in \mathcal{H}^g$.*
3. *For any two pairs $(z, \mathfrak{b})$, $(z', \mathfrak{b}')$ as above, we have $A_{z,\mathfrak{b}} \cong A_{z',\mathfrak{b}'}$ if and only if there exists an element*

$$M = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \in \mathrm{SL}_2(K_0)$$

such that $z = Az'$, $\alpha \in \mathfrak{b}^{-1}\mathfrak{b}', \beta \in \mathfrak{b}^{-1}\mathfrak{b}'^{-1}, \gamma \in \mathfrak{b}\mathfrak{b}'$ *and* $\delta \in \mathfrak{b}\mathfrak{b}'^{-1}$.

Proof. We give two proofs of which the first is the quickest, but the second is more elementary. Parts 1, 2 and the special case of 3 with $\mathfrak{b} = \mathfrak{b}'$ are a special case of [13, Theorem 2.2.17(2)] (take $\mathfrak{U} = \mathcal{D}_{K_0/\mathbf{Q}}^{-1}\mathfrak{b}$, $\mathfrak{B} = \mathfrak{b}^{-1}$, $\mathfrak{C} = \mathcal{O}_{K_0}$ and identify principal polarizations λ with isomorphisms $m : \mathcal{M}_A^+ \to \mathcal{O}_{K_0}^+ : \lambda \mapsto 1$). It is easy to check that the basis of part 1 is symplectic. The general version of 3 is a straightforward generalization.

As a more elementary proof, part 1 without the word 'principally' is a special case of [1, Proposition 9.2.1] (originally [30, Theorem 24.6(1)]). The basis given in part 1 is symplectic and hence the polarization is principal, which proves part 1.

Proposition 9.2.3 of [1] (originally [30, Theorem 24.6(2)]) only shows that 2 holds with $\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}$ replaced by any $\mathcal{O}_{K_0}$-submodule M of $K_0 \oplus K_0$ that is free of rank $2g$ as a $\mathbf{Z}$-module and with δ^{-1} removed from the definition of E_z. We now give the proof of our version. Let $\eta : \mathfrak{b} \oplus \mathcal{O}_{K_0} \to \Lambda$ be an $\mathcal{O}_{K_0}$-isomorphism for some $\mathcal{O}_{K_0}$-ideal $\mathfrak{b}$. For any $u, v \in K_0^2$, consider the $\mathbf{Q}$-linear character

$$K_0 \to \mathbf{Q} : a \mapsto E(\eta(au), \eta(v)).$$

As the trace form

$$K_0 \times K_0 \to \mathbf{Q} : (x, y) \mapsto \mathrm{Tr}_{K_0/\mathbf{Q}}(xy)$$

is non-degenerate, we find $T(u, v) \in K_0$ such that

$$E(\eta(au), \eta(v)) = \mathrm{Tr}_{K_0/\mathbf{Q}}(aT(u, v)) \quad \text{for all } a \in K_0, u, v \in K_0^2.$$

We get for all $a, x \in K_0, u, v \in K_0^2$ that

$$\mathrm{Tr}_{K_0/\mathbf{Q}}(aT(xu, v)) = E(\eta(axu), \eta(v)) = \mathrm{Tr}_{K_0/\mathbf{Q}}(axT(u, v)),$$

hence $T(xu, v) = xT(u, v)$ and since $E(\eta(xu), \eta(v)) = E(\eta(u), \eta(xv))$, we also get $T(u, xv) = xT(u, v)$. In other words, T is a K_0-bilinear form $K_0^2 \times K_0^2 \to K_0$. Moreover, T is alternating, because E is alternating. In particular, there exists an element $x \in K_0$ such that T is given by

$$T(u, v) = u^t \begin{pmatrix} 0 & x \\ -x & 0 \end{pmatrix} v \quad \text{for all } u, v \in K_0^2.$$

As E is a principal polarization, we find that $x\mathfrak{b}$ is the dual of $\mathcal{O}_{K_0}$ for the trace form, hence is $\mathcal{D}_{K_0/\mathbf{Q}}^{-1}$ by [28, §III.2]. Without loss of generality, we replace $\mathfrak{b}$ by $\mathcal{O}_{K_0} = \delta x\mathfrak{b}$ and η by

$$\eta \circ \begin{pmatrix} \delta^{-1}x^{-1} & 0 \\ 0 & 1 \end{pmatrix},$$

so that

$$T(u,v) = u^t \begin{pmatrix} 0 & \delta^{-1} \\ -\delta^{-1} & 0 \end{pmatrix} v.$$

We now continue the proof of [1, Proposition 9.2.3] after the equation

$$T(\underline{b}, \underline{c}) = {}^t\underline{b} \begin{pmatrix} 0 & 1_m \\ -1_m & 0 \end{pmatrix} \underline{c}$$

and find $\mathcal{M} = \mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}$, which proves 2.

The special case of 3 with $\mathfrak{b} = \mathfrak{b}'$ is a special case of [1, Proposition 9.2.2] (originally [30, Theorem 24.6(3)]) and the general version is a straightforward generalization. □

Remark 9.7. For the general case, where $\mathcal{D}_{K_0/\mathbf{Q}}$ is not necessarily principal, one needs only to replace $\mathfrak{b}^{-1} \oplus \mathfrak{b}$ by $\mathcal{D}_{K_0/\mathbf{Q}}^{-1}\mathfrak{b}^{-1} \oplus \mathfrak{b}$, to remove δ^{-1} from the definition of E_z and from the symplectic basis, and to and change the inclusions of part 3 of Theorem 9.6.

The following lemma gives bounds on the consecutive minima of the imaginary part of the period matrix corresponding to $A_{z,\mathfrak{b}}$. For any element z of $\mathbf{C}^g$ write $P(z) = \prod_{i=1}^g |z_i|$, so $P(x) = |N_{K_0/\mathbf{Q}}(x)|$ for $x \in K_0 \subset K_0 \otimes \mathbf{C} = \mathbf{C}^g$. We also denote the vector of imaginary parts of a vector $z \in \mathbf{C}^g$ by $\operatorname{Im} z \in \mathbf{R}^g$.

Lemma 9.8. *Suppose that $g = 2$, i.e. assume that K_0 is a real quadratic number field. For $z \in \mathcal{H}^2$ and a fractional $\mathcal{O}_{K_0}$-ideal $\mathfrak{b}$, let Y be the imaginary part of the period matrix Z corresponding to $A_{z,\mathfrak{b}}$ (for the symplectic basis of part 1 of Theorem 9.6). Then we have $\det Y = N(\mathfrak{b})^2 P(\operatorname{Im} z)$ and*

$$\frac{P(\operatorname{Im} z) N(\mathfrak{b})^2}{\Delta_0} \leq m_1(Y)^2 \leq m_2(Y)^2 \leq \frac{16}{9} P(\operatorname{Im} z) N(\mathfrak{b})^2 \Delta_0.$$

Proof. Let u, v be a basis of $\mathfrak{b}^{-1}$. Let c be the non-trivial automorphism of K_0. Then $uv^c - vu^c = \pm N(\mathfrak{b})^{-1}\delta$. Without loss of generality, we assume that the sign here is positive Let $u^* = v^c N(\mathfrak{b})\delta^{-1}$ and $v^* = -u^c N(\mathfrak{b})\delta^{-1}$. Then $\operatorname{Tr}(uu^*) = \operatorname{Tr}(vv^*) = 1$ and $\operatorname{Tr}(uv^*) = \operatorname{Tr}(vu^*) = 0$ and (hence) u^*, v^* is a basis of $\mathcal{D}_{K_0/\mathbf{Q}}^{-1}\mathfrak{b}$. The symplectic basis of $\Lambda_{z,\mathfrak{b}}$ with respect to E_z given in part 1 of Theorem 9.6 now reads

$$N(\mathfrak{b}) \begin{pmatrix} z_1 v_2 \\ -z_2 v_1 \end{pmatrix}, \quad N(\mathfrak{b}) \begin{pmatrix} -z_1 u_2 \\ z_1 u_1 \end{pmatrix}, \quad \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}, \quad \begin{pmatrix} v_1 \\ v_2 \end{pmatrix},$$

where $u_i = \phi_i()$ and $v_i = \phi_i(v)$ for $i \in \{1, 2\}$. Let $\Omega \in \operatorname{Mat}_2(\mathbf{C})$ have the first two vectors as columns and $\Omega' \in \operatorname{Mat}_2(\mathbf{R})$ the last two, so $Z = \Omega'^{-1}\Omega$. We have

$$\Omega'^{-1} = \frac{N(\mathfrak{b})}{\delta} \begin{pmatrix} v_2 & -v_1 \\ -u_2 & u_1 \end{pmatrix}$$

and hence

$$Z = \frac{N(\mathfrak{b})^2}{|\delta|} \begin{pmatrix} z_1 v_2^2 + z_2 v_1^2 & -z_1 u_2 v_2 - z_2 u_1 v_1 \\ -z_1 u_2 v_2 - z_2 u_1 v_1 & z_1 u_2^2 + z_2 u_1^2 \end{pmatrix}. \tag{5}$$

The values of the binary quadratic form $Y = \operatorname{Im} Z$ are the values of

$$\frac{N(\mathfrak{b})^2}{|\delta|}(\operatorname{Im} z_1 \phi_1(t)^2 + \operatorname{Im} z_2 \phi_2(t)^2), \quad t = mu + nv \in \mathfrak{b}^{-1}, m, n \in \mathbf{Z}.$$

As $|\phi_1(t)\phi_2(t)| = |N_{K_0/\mathbf{Q}}(t)| \geq N(\mathfrak{b})^{-1}$, we find

$$m_1(Y') \geq 2\sqrt{P(\operatorname{Im} z)}|N_{K_0/\mathbf{Q}}(t)|\frac{N(\mathfrak{b})^2}{\Delta_0^{1/2}} \geq 2\sqrt{P(\operatorname{Im} z)}\frac{N(\mathfrak{b})}{\Delta_0^{1/2}}$$

if $t \neq 0$.

As Ω' is real, we also get $Y = \Omega'^{-1} \operatorname{Im} \Omega$ and hence $\det Y = (\det \Omega')^{-1} \det(\operatorname{Im} \Omega)$. As we have $\det \Omega_2 = N(\mathfrak{b}^{-1})$ and $\det \operatorname{Im} \Omega_1 = P(\operatorname{Im} z)N(\mathfrak{b})$, we get that $\det Y = P(\operatorname{Im} z)N(\mathfrak{b})^2$.

Finally, $m_1(Y)m_2(Y) \leq \frac{4}{3} \det Y$, which gives the upper bound on $m_2(Y)$. □

To see what bounds we can obtain for $P(\operatorname{Im} z)N(\mathfrak{b})^2$, we will analyse $\mathrm{SL}_2(\mathcal{O}_{K_0}) \setminus \mathcal{H}^g$. Our main reference is Van der Geer [32]. For any $\sigma \in \mathbf{P}^1(K_0)$, choose $\alpha, \beta \in K_0$ such that $\sigma = (\alpha : \beta)$ and let

$$\mathfrak{b} = \alpha\mathcal{O}_{K_0} + \beta\mathcal{O}_{K_0}.$$

Choose $\alpha^*, \beta^* \in \mathfrak{b}^{-1}$ such that $\alpha\beta^* - \beta\alpha^* = 1$ and let

$$M_\sigma = \begin{pmatrix} \alpha & \alpha^* \\ \beta & \beta^* \end{pmatrix}.$$

For $\sigma \in \mathbf{P}^1(K_0)$, $z \in \mathcal{H}^g$, define

$$\mu(\sigma, z) = \frac{N(\mathfrak{b})^2 P(\operatorname{Im} z)}{|P(-\beta z + \alpha)|^2}.$$

Note that μ is independent of the choice of α, β and we have $\mu(\infty, z) = P(y)$. We can think of $\mu(\sigma, z)^{-1}$ as the distance from z to σ.

Lemma 9.9. For every point z in $\mathcal{H}^g$, there exists a point $\sigma \in \mathbf{P}^1(K_0)$ such that $\mu(\sigma, z) \geq (2^g\Delta_0)^{-1}$.

Proof. This is what is proven in the proof of Lemma 2.2 of [32], where last line should read $s^{-1} > 2^n D_K$. □

Lemma 9.10. For any $z \in \mathcal{H}^g$, with σ as in Lemma 9.9, the principally polarized abelian variety A_z as in Theorem 9.6 is isomorphic to $A_{w,\mathfrak{b}}$ with $w = M_\sigma^{-1} z$. Furthermore, we have $P(\operatorname{Im} w) \geq (4N(\mathfrak{b})^2\Delta_0)^{-1}$.

Proof. The isomorphism is a special case of 3 of Theorem 9.6. Furthermore, $\mu(\sigma, z) = N(\mathfrak{b})^2 N(y)/|P(-\beta z + \alpha)|^2 = N(\mathfrak{b})^2 P(\operatorname{Im} w)$. □

Let K be a CM field with maximal totally real subfield K_0. As a CM type extends the set of embeddings of K_0 into $\mathbf{R}$, it induces an isomorphism of $K \otimes \mathbf{C}$ with $K_0 \otimes \mathbf{C} = \mathbf{C}^g$ and we will identify those rings through that isomorphism. For any element $x \in K \setminus K_0$, there is a unique CM type Φ_x such that $\operatorname{Im} \phi(x) > 0$ for all $\phi \in \Phi_x$.

Lemma 9.11. If $A_{w,\mathfrak{b}}$ has CM by $\mathcal{O}_K$, then $w = \Phi_x(x)$ for some $x \in K \setminus K_0$. Moreover, $(x-\overline{x})\mathfrak{b}\mathcal{O}_K$ contains $\mathcal{D}_{K/K_0}$ and we have $P(\operatorname{Im} w)^2 \leq \frac{1}{16}\Delta_1 N(\mathfrak{b})^{-4}$.

Proof. Real multiplication is given by

$$K_0 \to \mathrm{Mat}_g(\mathbf{C}) : \alpha \mapsto \mathrm{diag}(\phi_1(\alpha), \ldots, \phi_g(\alpha)).$$

Complex multiplication is an extension of this map to a map $K \to \mathrm{Mat}_g(\mathbf{C})$, hence is given by an extension of each of the ϕ_i, i.e., a CM type Φ. For any $\alpha \in \mathcal{O}_K$, we thus get $\phi_i\alpha = \phi_i(f)w_i + \phi_i(g)$ with $f \in \mathfrak{b}^2, g \in \mathcal{O}_{K_0}$, so we get $w = \Phi(x)$ with $x = (\alpha - g)f^{-1}$ and $\Phi = \Phi_x$. Then $\alpha - \overline{\alpha} = f(x-\overline{x})$, so $\alpha - \overline{\alpha} \in (x-\overline{x})\mathfrak{b}^2$. As the $\alpha - \overline{\alpha}$ generate $\mathcal{D}_{K/K_0}$ as an $\mathcal{O}_K$-ideal, this proves the inclusion of ideals.

Now $P(\operatorname{Im} w)^2 = N_{K/\mathbf{Q}}(\frac{1}{2}(x-\overline{x}))$, $N(\mathfrak{b})^2 = N_{K/\mathbf{Q}}(\mathfrak{b})$ and $\Delta_1 = N_{K_0/\mathbf{Q}}(\Delta_{K/K_0}) = N_{K/\mathbf{Q}}(\mathcal{D}_{K/K_0})$, hence the final statement follows. □

Proof of Proposition 9.1. Given a CM abelian variety, take the isomorphic one from Lemma 9.10. This gives a lower bound on $P(\operatorname{Im} w)N(\mathfrak{b})^2$ and we get an upper bound from Lemma 9.11. Lemma 9.8 gives upper and lower bounds on the minima and the determinant in terms of $P(\operatorname{Im} w)N(\mathfrak{b})^2$. □

9.2 Generalization of Spallek's results

Spallek, in her thesis [31], gave a method for writing down the period matrices of a complete set of reprentatives of the isomorphism classes of abelian surfaces with CM by a given primitive quartic CM field K of which the real quadratic subfield K_0 has class number one. This method has been the method of choice of various authors ([37, 9]). In this section, we simplify the results and generalize them to arbitrary primitive quartic CM fields. This is not needed for the rest of the text.

Assume $g = 2$. Let $\omega \in K_0$ be such that $\mathcal{O}_{K_0} = \mathbf{Z}[\omega]$. We obtain the following results, which are generalizations of results from Spallek's thesis.

Lemma 9.12. Suppose that $z \in K$ is such that $z\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$ is an $\mathcal{O}_K$-ideal. Let ϕ_1, ϕ_2 be the embeddings of K into $\mathbf{C}$ given by $\phi_1\omega > \phi_2\omega$ and $\operatorname{Im}\phi_i(z) > 0$. Then A_z corresponds to the point

$$\frac{1}{\sqrt{\Delta_0}}(\phi_1 + \phi_2)\begin{pmatrix} z\omega^2 & -z\omega \\ -z\omega & z \end{pmatrix}$$

in the Siegel upper half space $\mathcal{H}_2$.

Proof. Choose $u = \omega^\sigma$ and $v = 1$ in (5). □

Theorem 9.13. *Let K be a primitive quartic CM field. A complete set of representatives for the equivalence classes of abelian varieties over $\mathbf{C}$ with CM by $\mathcal{O}_K$ can be given as follows.*

1. *Let $\Phi = \{\phi_1, \phi_2\}$ be a CM type of K.*

2. *Let $\epsilon \in \mathcal{O}_{K_0}$ be such that $\langle -1\rangle \times \langle \epsilon\rangle$ has odd index in $\mathcal{O}_{K_0}^*$.*
3. *Let $\mathcal{K}' \subset K$ be such that $\{z\mathcal{O}_{K_0} + \mathcal{O}_{K_0} : z \in \mathcal{K}'\}$ is a complete set of representatives of the ideal classes of K that contain an ideal of the form $z\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$.*
4. *Let $\mathcal{K} = \pm\mathcal{K}' \cup \pm\epsilon\mathcal{K}'$.*
5. *Remove all z from $\mathcal{K}$ for which* $\operatorname{Im}\phi_1 z < 0$.
6. *If K is cyclic Galois, remove all z from $\mathcal{K}$ for which* $\operatorname{Im}\phi_2 z < 0$.
7. *Return A_z for all $z \in \mathcal{K}$.*

Proof. Algorithm 6.3 gives a complete set of representatives of the isomorphism classes of principally polarized abelian varieties over $\mathbf{C}$ with CM by $\mathcal{O}_K$. We use Lemma 6.7 to compute $\mathcal{O}_{K_0}^*/N_{K/K_0}(\mathcal{O}_K^*)$ (which consists of the classes of ± 1 and $\pm\epsilon$) and Example 6.6 to compute a complete set of representatives for the equivalence classes of CM types ($\{\Phi\}$ if K is cyclic Galois and $\{\Phi, \{\phi_1, \overline{\phi_2}\}\}$ if K is non-Galois).

Part 2 of Theorem 9.6 shows that if a CM lattice Λ has a polarization, then Λ is free as an $\mathcal{O}_{K_0}$-module, hence so is the ideal $\mathfrak{a}$ of Theorem 6.1. In particular, $\mathfrak{a}$ is then equivalent to an ideal of the form $z\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$. Conversely, part 1 of Theorem 9.6 gives, for each ideal $z\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$, a principal polarization E_z. In fact, E_z is equal to the polarization from Theorem 6.1 with $\xi = \delta(\overline{z} - z)^{-1}$. In particular, multiplication of ξ by $u \in \mathcal{O}_{K_0}^*$ corresponds to multiplication of z by u^{-1}, so $\mathcal{K}$ corresponds exactly to the set of triples $(\mathfrak{a}, \xi, u)$ of step 5 of Algorithm 6.3. Steps 5 and 6 are exactly the selection of step 6 of Algorithm 6.3. □

Of course, a similar result holds for arbitrary g with $z\mathcal{O}_{K_0} + \mathcal{O}_{K_0}$ replaced by $z\mathcal{D}_{K_0/\mathbf{Q}}^{-1} + \mathcal{O}_{K_0}$.

9.3 Alternative computation

The group $\Gamma = \mathrm{SL}_2(\mathcal{O}_{K_0})$ acts on $\mathcal{H}^g$ as above. We will now describe the *fundamental domain* for this action as defined in [32, Section I.3]. For $\sigma \in \mathbf{P}^1(K_0)$, let α, β, M_σ, $\mu(z,\sigma)$ and $\mathfrak{b}$ be as in Section 9.1.

Define the *sphere of influence* F_σ of σ to be the set

$$F_\sigma = \{z \in \mathcal{H}^2 : \mu(\sigma, z) \geq \mu(\tau, z) \text{ for all } \tau \in \mathbf{P}^1(K_0)\}.$$

For example,

$$F_\infty = \{z \in \mathcal{H}^2 : |P(-\beta z + \alpha)|^2 \geq N(\mathfrak{b}) \text{ for all } \alpha, \beta \in \mathcal{O}_{K_0}\}.$$

Let T_σ be a translational fundamental parallelogram of $\mathbf{R}^2$ for $\mathfrak{b}^{-2}$ and W_σ a fundamental domain of $\mathbf{R}_+^2$ for the multiplication by $\mathcal{O}_{K_0}^{*2}$. If $g = 2$, then we can let W_σ be the set of elements y such that $\epsilon < |y_1/y_2| \leq \epsilon$, where ϵ is an absolute value > 1 of a fundamental unit. Let $E_\sigma = \{z \in \mathcal{H}^2 : \mathrm{Re}(z) \in T_\sigma, \mathrm{Im}(z) \in W_\sigma\}$ and let

$$B_\sigma = M_\sigma E_\sigma \cap F_\sigma.$$

Let S be a set of representatives of the class group of K_0, each representative given by a pair (α,β) of $\mathcal{O}_{K_0}$-generators and identified with a point $\sigma=\alpha/\beta\in\mathbf{P}^1(K_0)$. Let $B=\cup_{\sigma\in S}B_\sigma$.

If K_0 has class number one, then it suffices to take $S=\{(1,0)\}$, of which the only element corresponds to $\sigma=\infty$.

Lemma 9.14. Every point in $\mathcal{H}^2$ is Γ-equivalent to a point in B.

For a point $z\in B_\sigma$, all equivalent points of B can be determined as follows.

1. List all $\tau\in\mathbf{P}^1(K_0)$ such that $\mu(\sigma,z)=\mu(\tau,z)$.
2. For each such τ, take any $\gamma\in\Gamma$ such that $\gamma\tau\in S$.
3. For each such pair (τ,γ), take the unique $\gamma'\in\Gamma_{\gamma\tau}$ such that $\gamma'\gamma z\in M_\sigma E_{\gamma\tau}$ and output $\gamma'\gamma z$.

Proof. By [32, Section I.2], we have $\mu(\gamma\sigma,\gamma z)=\mu(\sigma,z)$ for all $\sigma\in\mathbf{P}^1(K_0)$, $z\in\mathcal{H}^g$ and $\gamma\in\Gamma$, hence $\gamma F_\sigma=F_{\gamma\sigma}$. Moreover, α/β and α'/β' in $\mathbf{P}^1(K_0)$ are Γ-equivalent if and only if the corresponding ideals $\mathfrak{b}$ and $\mathfrak{b}'$ are in the same ideal class ([32, Proposition 1.1]).

Therefore, every $z\in\mathcal{H}^g$ is equivalent to a point in F_σ for some $\sigma\in S$. By [32, Proof of Proposition 1.1], the stabilizer Γ_σ of σ is

$$M_\sigma^{-1}\{\begin{pmatrix}\epsilon & \mu\\ 0 & \epsilon^{-1}\end{pmatrix}:\epsilon\mathcal{O}_{K_0}^*,\mu\in\mathfrak{b}^{-2}\}M_\sigma,$$

which shows that every point in F_σ is Γ-equivalent to a point in B_σ. This completes the proof of the first statement.

Now suppose that z is in B_σ and $\gamma_0 z$ is in $B_{\sigma'}$ with $\sigma,\sigma'\in S$ and $\gamma_0\in\Gamma$. Then $z\in F_{\gamma_0^{-1}\sigma'}$, so $\tau=\gamma_0^{-1}\sigma'$ is listed in Step 1. Then in Step 2, an element γ is chosen such that $\gamma\tau\in S$. As the equivalence classes of points in $\mathbf{P}^1(K_0)$ correspond bijectively to the ideal classes of K_0 and τ is Γ-equivalent to $\sigma'\in S$, this implies that $\gamma\tau=\sigma'$.

Existence and uniqueness of γ' follows from the fact that $M_\sigma E_{\gamma\tau}$ is a fundamental domain for $\Gamma_{\gamma\tau}$. As both γ' and $\gamma_0\gamma^{-1}$ are in $\Gamma_{\sigma'}$ and send γz to $M_\sigma E_{\gamma\tau}=M_\sigma E_{\sigma'}$, we get $\gamma'=\gamma_0\gamma^{-1}$, hence $\gamma'\gamma z=\gamma_0 z$. This shows that $\gamma_0 z$ is indeed listed in Step 3. □

By Lemma 9.9, every point z in F_σ satisfies $\mu(\sigma,z)>(2^g\Delta_0)^{-1}$.

As we did before, we identify $z\in B_\sigma$ with $w\mathfrak{b}\oplus\mathfrak{b}^{-1}$ where

$$w=M_\sigma^{-1}z\in M_\sigma^{-1}B_\sigma=M_\sigma^{-1}F_\sigma\cap E_\sigma.$$

As before, we have $N(\operatorname{Im}w)\geq(4N(\mathfrak{b})^2\Delta_0)^{-1}$.

If $A_{w,\mathfrak{b}}$ has CM by the ring of integers of $K=K_0(\sqrt{D})$, then $w=\Phi_x(x)$ as in Lemma 9.11. From the fact that $x\mathfrak{b}+\mathfrak{b}^{-1}\subset K$ is an $\mathcal{O}_K$-module, we deduce that $aw^2+2bw+c=0$ and $w=\frac{\sqrt{D}-b}{a}$ for some $a\in\mathfrak{b}^2, b\in\mathcal{O}_{K_0}, c\in A^{-2}$ with $b^2-ac=D$. We have $P(\operatorname{Im}w)^2=P(D)/P(a)^2$, hence $P(a)\leq 4N(\mathfrak{b})^2\Delta_0\sqrt{P(D)}$. At the same time, b/a is in a translational fundamental domain and a in a multiplicative one, so we can enumerate all pairs (a,b) and check if $c=(b^2-D)/a$ is in $\mathfrak{b}^{-2}$. For each, we compute the period matrix corresponding to the symplectic basis of $A_{w,\mathfrak{b}}$ as in the proof of Lemma 9.8.

So assuming that we can compute the unit group and class group of K_0 and a complete set of representatives of the elements of $\mathcal{O}_{K_0}$ of norm below any given bound up to the action of $\mathcal{O}_{K_0}^*$, we get the following algorithm for computing all period matrices for abelian varieties with CM by $\mathcal{O}_K$.

1. Compute a set of representatives S of the class group of K_0.
2. Compute an element D such that $K = K_0(\sqrt{D})$. Compute a $\mathbf{Z}$-basis of $\mathcal{O}_K$ and write each element of that basis in the form $x_i + y_i\sqrt{D}$ with $x_i, y_i \in K_0$.
3. For each $\mathfrak{b} \in S$, compute a complete set of representatives of all $a \in \mathfrak{b}^2/\mathcal{O}_{K_0}^*$ with $\phi_1(a) > 0$ and absolute value of the norm below $N(\mathfrak{b})^2\sqrt{|P(D)|}\Delta_0$.
4. For each $(\mathfrak{b}, a)$, compute all $b \in \mathcal{O}_{K_0}$ that lie in a fundamental domain for translation by $\mathfrak{b}^{-2}a$ and for which a divides $b^2 - D$.
5. For each triple $(\mathfrak{b}, a, b)$ and each basis element $x_i + y_i\sqrt{D}$ of $\mathcal{O}_K$, check if $y_i a \in \mathfrak{b}^2, x_i \pm y_i b \in \mathcal{O}_{K_0}, a^{-1}y_i(D - b^2) \in \mathfrak{b}^{-2}$. Remove the triple from the list if one of these conditions is not satisfied.
6. For each remaining triple, check if it corresponds to a point in $F_{\mathfrak{b}}$. If so, compute the corresponding period matrix and perform the steps of Lemma 9.14 to remove all equivalent triples from the list.

By the same argument as in the proof of Lemma 3.5, there exists a D such that $N(D) = O(\Delta_1\Delta_0)$.

By Lemma 9.11, we can in fact restrict to $a \in (2\mathfrak{b}^2\sqrt{D}\mathcal{D}_{K/K_0}^{-1}) \cap K_0 \subset \mathfrak{b}^2$ in step 3.

Step 5 checks if multiplication by $x_i + y_i\sqrt{D}$ maps $\frac{\sqrt{D}-b}{a}\mathfrak{b} + \mathfrak{b}^{-1}$ to itself, i.e., if there is actual CM by $\mathcal{O}_K$.

We will analyse the algorithm in the case of quartic CM fields in Section 9.5. First, we will need to know how to enumerate elements of bounded norm in a real quadratic order.

9.4 Real quadratic fields

If K_0 is quadratic, then the class group and the fundamental unit can be computed using the theory of cycles of *reduced ideals* as described for example by Lenstra [23]. It is straightforward to derive from that theory the following method for enumerating the elements of norm below B. This method can be performed as a precomputation and the output can also used for step 6.

Actually, the following theory computes the group of totally positive units ${\mathcal{O}_{K_0}}_+^*$ and the strict class group $\mathrm{Cl}^+(K_0)$ consisting of fractional ideals modulo ${\mathcal{O}_{K_0}}^{+*}$, but it is easy to check if an element of $\mathcal{O}_{K_0}^*$ is a square and thus compute the class group and unit group.

We study binary quadratic forms $ax^2+bxy+cy^2$ over $\mathbf{Z}$ of which the discriminant $b^2 - 4ac$ is equal to Δ_0. To each such form, we associate the fractional $\mathcal{O}_{K_0}$-ideal $\mathbf{Z}+\frac{\sqrt{D_0}-b}{2a}\mathbf{Z}$. This gives a bijection between binary quadratic forms of discriminant Δ_0 and fractional $\mathcal{O}_{K_0}$-ideals together with a $\mathbf{Z}$-basis with first basis element 1. This bijection induces in turn a bijection between $\mathrm{Cl}^+(K_0)$ and the set of forms up to $\mathrm{SL}_2(\mathbf{Z})$. We call such a form *reduced* if

$$|\sqrt{\Delta_0}-2|a||<b<\sqrt{\Delta_0}$$

and we call it *almost-reduced* if $b\in J_a$, where

$$J_a=\begin{cases}]-|a|,|a|] & \text{if } |a|>\sqrt{\Delta_0} \\ ]\sqrt{\Delta_0}-2|a|,\sqrt{\Delta_0}[& \text{otherwise.}\end{cases}$$

An ideal $\mathfrak{b}$ corresponds to an almost-reduced form if and only if $\mathfrak{b}\cap\mathbf{Q}=\mathbf{Z}$. We call an ideal *reduced* if it corresponds to a reduced form. Every class in $\mathrm{Cl}^+(K_0)$ contains a reduced ideal and the following linear-time algorithm computes an equivalent reduced form for any input form.

Algorithm 9.15. Input: a binary quadratic form (a,b,c) of discriminant Δ_0.
Output: an $\mathrm{SL}_2(\mathbf{Z})$-equivalent reduced form.

```
1. Set $(a,b,c)\leftarrow(c,-b,a)$.
2. Let $b'\in J_a$ be equivalent to $b$ modulo $2a$ and let $c'=(b^2-\Delta_0)/(4a)$. Set $(a,b,c)\leftarrow(a,b',c')$.
3. If $(a,b,c)$ is not reduced, go to step 1.
```

If we apply this algorithm to a reduced form f, then it stops after a single iteration and returns another reduced form $\rho(f)$. The map ρ is a permutation of the set of reduced forms and two reduced forms are $\mathrm{SL}_2(\mathbf{Z})$-equivalent if and only if they are in the same $\langle\rho\rangle$-orbit.

We can now start by listing all reduced forms and putting them in a lookup table. We repeatedly apply ρ to sort them into $\langle\rho\rangle$-orbits. While doing this, we also compute a set of representatives S (containing $\mathcal{O}_{K_0}$) of the $\langle\rho\rangle$-orbits and for every reduced ideal $\mathfrak{b}$ keep track of the ρ-steps so that we can compute $x\in K_0^*$ with $x^{-1}\mathfrak{b}\in S$. Finally, the unit group is generated by the x that we get if we apply ρ to $\mathcal{O}_{K_0}$ until we get $\mathcal{O}_{K_0}$ again.

A more sophisticated method uses *short representations* of x and computes those not by repeatedly applying ρ but by moving through the cycle of reduced ideals in a smarter way as in [3]. For us, writing out x will be fast enough.

Now that we have the class group and unit group, we enumerate all ideals of norm at most B. The norm of the ideal corresponding to (a,b,c) is $1/a$, so the ideals of norm below B are exactly the $n\mathfrak{b}^{-1}$ with $n\in\mathbf{Z}$ and $\mathfrak{b}$ corresponding to an almost-reduced form (a,b,c) with $an^2\leq B$. Therefore, we enumerate all almost reduced forms with $a\leq B$. If we apply the reduction algorithm to them, then we get an ideal in our lookup table, so we know how to write it as an element of K_0 times an element of S.

All numbers have height at most linear in the regulator R_0 of K_0. Enumerating all reduced forms takes time $\widetilde{O}(\Delta_0)$. There are $\widetilde{O}(h_0R_0)$

of them and the generators x will have height $\widetilde{O}(R_0)$, so walking over the reduced forms with ρ and computing the generators x takes time $\widetilde{O}(h_0 R_0^2) = \widetilde{O}(\Delta)$. Then computing all almost-reduced forms with $a \leq B$ takes time $\widetilde{O}(B^2)$, where $\widetilde{O}$ means up to factors that are polynomial in $\log B$ and $\log \Delta$. Finally, the following lemma shows that it takes time $\widetilde{O}(BR_0)$ to write down generators x for them. In total, the time is thus bounded by $\widetilde{O}(B^2) + \widetilde{O}(\Delta)$.

Lemma 9.16. There are at most $B(1 + \log B)$ ideals of norm at most B.

Proof. Let $d(n)$ be the number of divisors of n. The number of ideals $i(n)$ of norm n is at most $d(n)$. Indeed, this is true for prime powers and if $\gcd(m, n) = 1$, then $d(mn) = d(m)d(n)$, $i(mn) = i(m)i(n)$.

Therefore, the number of ideals of norm at most n is at most $\sum_{k=1}^{n} d(n) = \sum_{k=1}^{n} \sum_{m|k} 1 = \sum_{m=1}^{n} \lfloor n/m \rfloor \leq n \sum_{m=1}^{n} m^{-1} \leq n(1 + \log n)$. □

Heuristically, there are much less. The region in $K_0 \otimes \mathbf{R}$ with norm at most B in a fundamental wedge for $\mathcal{O}_{K_0}^*$ has volume $2BR_0$, so there are about $2BR_0/\Delta = \widetilde{O}(B\Delta^{-1/2}h_0^{-1})$ principal ideals of norm at most B and hence about $\widetilde{O}(B\Delta^{-1/2})$ ideals in total.

9.5 Analysis of the alternative algorithm

Reduced ideals have norm at most $\sqrt{\Delta_0}$, so in step 3, we only need elements a of norm at most $\Delta_0^{5/2}\Delta_1^{1/2}$, which takes time $\widetilde{O}(\Delta_0^5\Delta_1)$ by the previous section. The number of them inside $\mathfrak{b}^2$ is equal to the number of ideals of norm at most $\sqrt{P(D)}\Delta_0$ in the ideal class of $\mathfrak{b}^{-2}$, which is at most $\widetilde{O}(\Delta_1^{1/2}\Delta_0^{3/2})$ by Lemma 9.16. The number of b found in step 4 for each $(\mathfrak{b}, a)$ is then also at most $O(\Delta_1^{1/2}\Delta_0^{3/2})$

At the end of step 5, we then have at most $\widetilde{O}(h_0\Delta_1\Delta_0^3)$ triples $\mathfrak{b}, a, b$ and each takes space $\widetilde{O}(R_0)$, where $\widetilde{O}$ means that we neglect factors that are polynomial in $\log \Delta$.

By Lemma 8.12, it is actually not necessary to do step 6. We can compute all the period matrices, move them to a fundamental domain and then check if they are equivalent. For each of them, the height is $\widetilde{O}(R_0)$ and we have $\log s = \widetilde{O}(1)$, where s is as defined in Section 8. For each of the $\widetilde{O}(h_0\Delta_1\Delta_0^3)$ triples $\mathfrak{b}, a, b$, we need time $\widetilde{O}(R_0^2)$ to compute the corresponding period matrix in $\mathcal{F}_2$, so the total time is $\widetilde{O}(\Delta_1\Delta_0^4)$.

10 Theta constants

To compute the absolute Igusa invariants corresponding to a point $Z \in \mathcal{H}_2$, we use *theta constants.* For $z \in \mathbf{C}$, let $E(z) = e^{\pi i z}$. We call an element $c \in \{0, \frac{1}{2}\}^4$ a *theta characteristic* and write $c = (c_1, c_2, c_3, c_4)$,

$c' = (c_1, c_2)$ and $c'' = (c_3, c_4)$. We define the *theta constant of characteristic* c to be the function $\theta[c] : \mathcal{H}_2 \to \mathbf{C}$ given by

$$\theta[c](Z) = \sum_{n \in \mathbf{Z}^2} E((n + c')Z(n + c')^t + 2(n + c')c''^t)$$

and following Dupont [6], we set

$$\theta_{16c_2+8c_1+4c_4+2c_3} = \theta[c].$$

We call a theta characteristic — and the corresponding theta constant — even or odd depending on whether $4c'c''^t$ is even or odd. The odd theta constants are zero by the anti-symmetry in the definition, and there are exactly 10 even theta constants $\theta_0, \theta_1, \theta_2, \theta_3, \theta_4, \theta_6, \theta_8, \theta_9, \theta_{12}$ and θ_{15}.

Let T be the set of even theta characteristics and define

$$S = \{C \subset T \mid \#C = 6, \sum_{c \in C} c \in \mathbf{Z}^4\}.$$

Then S consists of 15 subsets of T of 6 even theta characteristics, and we define

$$\begin{aligned}
h_4 &= \sum_{c \in E} \theta[c]^8, \\
h_{10} &= \prod_{c \in E} \theta[c]^2, \\
h_{12} &= \sum_{C \in S} \prod_{c \in C} \theta[c]^4, \\
h_{16} &= \sum_{\substack{C \in S \\ d \in E \setminus C}} \theta[d]^8 \prod_{c \in C} \theta[c]^4,
\end{aligned}$$

so each h_k is a sum of t_k monomials of degree $2k$ in the 10 even theta constants, where $t_4 = 10$, $t_{10} = 1$, $t_{12} = 15$ and $t_{16} = 60$.

Lemma 10.1. Let Z be a point in $\mathcal{H}_2$. If $h_{10}(Z)$ is non-zero, then the principally polarized abelian variety corresponding to Z is the Jacobian of a curve $C/\mathbf{C}$ of genus 2 with invariants

$$\begin{aligned}
I_2(C) &= h_{12}(Z)/h_{10}(Z), \\
I_4(C) &= h_4(Z), \\
I_6(C) &= h_{16}(Z)/h_{10}(Z), \\
I_{10}(C) &= h_{10}.
\end{aligned}$$

Proof. Thomae's identities [27] give an equation for such a curve C in terms of the theta constants. If we use these formulas to write out the definition of I_{2k} and use standard identities between the theta constants, then Lemma 10.1 follows. This was done by Spallek [31], who gave a page-filling explicitly written-out definition of the h_k, that contains a few misprinted exponents. The same result with the correct exponents can be found in [37] and [9], and, in a form that fills only half a page, in [6, Section 6.3.3]. □

Corollary 10.2. Each element of the ring $\mathbf{Q}[I_2, I_4, I_6, I_{10}, I_{10}^{-1}]$ can be expressed as a polynomial in the theta constants divided by a power of the product of all even theta constants.

This means that if we give upper and lower bounds on the absolute values of the theta constants, then we get upper bounds on the absolute values of the absolute invariants and we can bound the precision needed for the theta constants in terms of the precision needed for the absolute invariants.

10.1 Bounds on the theta constants

For $Z \in \mathcal{H}_2$, denote the real part by X and the imaginary part by Y. We denote the diagonal entries of Z by z_1, z_2, the off-diagonal entries (which are equal to each other) by z_3, and the real and imaginary parts of z_i by x_i and y_i. Recall that $\mathcal{B} \subset \mathcal{H}_2$ is given by

(F1) X is reduced, i.e., $|x_i| \leq 1/2$ for $i = 1, 2, 3$,

(F2) Y is reduced, i.e., $0 \leq 2y_3 \leq y_1 \leq y_2$, and

(F3") $y_1 \geq \sqrt{3/4}$.

Proposition 10.3. For every $Z \in \mathcal{B}$, we have

$$\begin{aligned}
|\theta_j(Z) - 1| &< 0.405 && j \in \{0, 1, 2, 3\} \\
\left|\frac{\theta_j(Z)}{2E(\frac{1}{4}z_1)} - 1\right| &< 0.348 && j \in \{4, 6\} \\
\left|\frac{\theta_j(Z)}{2E(\frac{1}{4}z_2)} - 1\right| &< 0.348 && j \in \{8, 9\} \quad \text{and} \\
\left|\frac{\theta_j(Z)}{2((-1)^j + E(z_3))E(\frac{z_1+z_2-2z_3}{4})} - 1\right| &< 0.438 && j \in \{12, 15\}.
\end{aligned}$$

Proof. The proof of Proposition 9.2 of Klingen [19] gives infinite series as upper bounds for the left hand sides. A numerical inspection shows that the limits of these series are less than 0.553, 0.623, 0.623 and 0.438. The bounds of Klingen can be improved by estimating more terms of the theta series individually and thus getting a smaller error term. This has been done in Propositions 6.1 through 6.3 of Dupont [6], improving the first three bounds to 0.405, $2|E(z_1/2)| \leq 0.514$ and $2|E(z_2/2)| \leq 0.514$. The proof of [6, Proposition 6.2] shows that for the second and third bound, we can also take 0.348. □

Remark 10.4. Actually, we can replace the condition $y_1 \geq \sqrt{3}/2 \approx 0.866$ in the definition of $\mathcal{B}$ by the weaker condition $y_1 \geq 0.640$. In that case, Dupont's estimates would give different upper bounds in Proposition 10.3 that are still less than 1.

Lemma 10.5. Let z_3 be a non-zero complex number with $\mathrm{Im}(z_3) \geq 0$ and $|\mathrm{Re}(z_3)| \leq \frac{1}{2}$. Then we have $\left|1 - e^{\pi i z_3}\right| \geq \min\{\frac{1}{4}, |z_3|\}$.

Proof. If $|\mathrm{Re}(z_3)| \geq \frac{1}{6}$, then $|1 - e^{\pi i z_3}| \geq \sin(\pi/6) = \frac{1}{2}$. If $\mathrm{Im}(z_3) \geq \frac{1}{10}$, then $|1 - e^{\pi i z_3}| \geq 1 - e^{\pi/10} > \frac{1}{4}$.

If $|\mathrm{Re}(z_3)| < \frac{1}{6}$ and $\mathrm{Im}(z_3) < \frac{1}{10}$, then let $a = \pi i z_3$, so

$$\left|1 - e^{\pi i z_3}\right| = \left|a + \frac{a^2}{2!} + \frac{a^3}{3!} + \cdots\right| \geq |a|\,(1 - |a|\,(e-2)) \geq |z_3| \qquad \square$$

Theorem 10.6. *For every $Z \in B$, we have*

$$\begin{aligned} 0.595 < |\theta_j(Z)| &< 1.405, && (j \in \{0,1,2,3\}) \\ 1.304 M^{-1} < |\theta_j(Z)| &< 1.366, && (j \in \{4,6,8,9\}) \\ 1.050 M^{-2} < |\theta_{12}(Z)| &< 1.553, && \textit{and} \\ 1.124 M^{-2} N^{-1} < |\theta_{15}(Z)| &< 1.553, \end{aligned}$$

where $M = e^{\pi \frac{y_2}{4}}$ and $N = \max\{4, |z_3|^{-1}\}$.

Proof. This follows form the bounds of Proposition 10.3 if we use Lemma 10.5 to estimate $|1 - E(z_3)|$ from below and we use the bounds

$$|(1 + E(z_3))| > 1, \quad \exp(-\pi y_i/4) \geq 0.506 \quad (i \in \{1,2\}) \quad \text{and}$$
$$\exp\left(-\pi \frac{y_1 + y_2 - 2\,|y_3|}{4}\right) > \exp\left(-\pi \frac{y_2}{2}\right) \geq 0.256. \qquad \square$$

10.2 Computing the theta constants

Algorithm 10.7. Input: A positive integer s, an approximation of a matrix $Z \in \mathcal{B}$, and the theta characteristic $c \in \{0, \frac{1}{2}\}^{2g}$.
Output: An approximation of $\theta[c](0, Z)$.

1. For R_1, R_2 determined below, return

$$A = \sum_{\substack{n \in \mathbf{Z}^2 \\ |n_i| \leq R_i}} E\left((n + c')Z(n + c')^t + 2(n + c')c''^t\right)$$

evaluated to a precision t determined below.

Theorem 10.8. *Algorithm 10.7 above evaluates the theta constants in $Z \in B$ with an absolute error of at most 2^{-s}. The algorithm takes time $(\det Y)^{-1}\widetilde{O}(s^2)$ and requires Z to be given with an absolute error of at most 2^{-t}, where $t = O(s)$.*

Proof. We first bound

$$|A - \theta[c](0, Z)| \leq \sum_{\substack{n \in \mathbf{Z}^2 \\ n_1 > R_1 \text{ or } n_2 > R_2}} \exp(-\frac{3}{4}\pi((n_1 + c_1)^2 y_1 + (n_2 + c_2)^2 y_2)).$$

As $0 \leq 2y_3 \leq y_1 \leq y_2$, we have $n_1^2 y_1 + n_1 n_2 y_3 + n_2^2 y_2 \geq \frac{3}{4}(n_1^2 y_1 + n_2^2 y_2)$ for all $n \in \mathbf{R}^2$, so if we let

$$\begin{aligned} f(t, l) &= \sum_{k=l}^{\infty} \exp(-\frac{3}{4}\pi k^2 t) \leq \sum_{k=l^2}^{\infty} \exp(-\frac{3}{4}\pi k t) \\ &< \frac{3}{2}\exp(-\frac{3}{4}\pi l^2 t), \end{aligned}$$

then

$$|A - \theta[c](0, Z)| \quad \leq \quad 4f(y_1, R_1)f(y_2, 0) + 4f(y_1, 0)f(y_2, R_2),$$

and we can solve RHS $\leq 2^{-s+1}$ to get a suitable $R_i = y_i^{-1/2}O(\sqrt{s})$. The number of terms to be evaluated is therefore $(\det Y)^{-1}O(s)$ (with $\det Y \geq 9/16$) and each evaluation takes time $\widetilde{O}(t)$. The error of each term is at most 2^{-t} and there are $O(s)$ terms, so the error in A is $O(s)2^{-t}$, hence a precision of $t = O(s)$ suffices. □

We can now compute absolute Igusa invariants using the expressions for them in terms of theta constants in Lemma 10.1.

10.3 Improvements

It may be possible to improve upon this complexity by variations of Algorithm 10.7, by evaluation of multiple theta constants at once, or by evaluation of a theta constant at multiple points in $\mathcal{H}_2$ at once. We will not go into the details of any of those possibilities, because the time and space needed for that would be much better spent on proving the quasi-linear time conjectural method described by Régis Dupont in his thesis [6]. Dupont gives a method for computing theta constants in genera 1 and 2 using Newton iterations and (a generalization of) the arithmetic-geometric mean (AGM). Proving results for the genus 2 version of Dupont's method is beyond the scope of this paper, partially because there is no error analysis yet, even for the genus 1 method, and partially because the correctness of the genus 2 method depends on a few assumptions that Dupont did not succeed in proving.

11 The algorithm

Algorithm 11.1. Input: A positive quadratic discriminant Δ_0 and positive integers a and b such that $K = \mathbf{Q}(\sqrt{-a + b\sqrt{\Delta_0}})$ is a primitive quartic CM field.
Output: The Igusa class polynomials $H_{K,n}$ for $n = 1, 2, 3$.

1. Compute a $\mathbf{Z}$-basis of $\mathcal{O}_K$ using the algorithm of Buchmann and Lenstra [2] and use this to compute the discriminant Δ of K.
2. Compute a complete set $\{A_1, \ldots, A_{h_1}\}$ of representatives of the h_1 isomorphism classes of principally polarized abelian surfaces with CM by $\mathcal{O}_K$, using Algorithm 6.3.
3. From Δ and h_1, compute a number d such that $dH_{K,n}$ is in $\mathbf{Z}[X]$ for $n = 1, 2, 3$, using Algorithm 4.6.
4. For $j = 1, \ldots, h_1$, do the following.
   (a) Compute a symplectic basis (and hence a period matrix in $\mathcal{H}_2$) of A_j using Algorithm 7.1.
   (b) Replace the period matrix by an $\mathrm{Sp}_4(\mathbf{Z})$-equivalent period matrix $Z_j \in \mathcal{F}_2$, using Algorithm 8.3.

   (c) Use the formulas of Lemma 10.1 and the bounds of Proposition 10.3 to get upper and lower bounds on $|\theta[c](Z_j)|$ for all even theta characteristics c and upper bounds $s_{j,n}$ on $|i_n(Z_j)|+1$ $(n=1,2,3)$.

5. Let $p = \lceil \log_2 d + 3\log_2 h_1 + 4\rceil + \max_{n\in\{1,2,3\}}\lceil\sum_{j=1}^{h_1}\log_2 s_{j,n}\rceil$. This is the precision with which we will approximate the Igusa invariants.

6. For $j=1,\ldots,h_1$, do the following.

   (a) Evaluate the theta constants, using Algorithm 10.7, to a precision r that is sufficient for computing $i_n(A_j)$ $(n=1,2,3)$ with an error of at most 2^{-p}. Such a precision r can be obtained from the formulas of Lemma 10.1 and the bounds computed in step 4c.

   (b) Use the formulas of Lemma 10.1 to evaluate $i_n(A_j)$ for $(n = 1,2,3)$ to precision p.

7. For $n=1,2,3$, do the following.

   (a) Use Algorithm 4.4 to compute an approximation $\widetilde{H}_{K,n}$ of $H_{K,n}$ for $n=1,2,3$ from the approximations of Igusa invariants of step 6b.

   (b) Compute $dH_{K,n}$ by rounding the coefficients of $d\widetilde{H}_{K,n}$ to nearest integers.

   (c) Output $H_{K,n}$.

If Cardona-Quer invariants as in Section 2.1 are used in the definition of Igusa class polynomials, then we should do the following.

1. Perform the above algorithm with not only the standard (non-Cardona-Quer) Igusa invariants i_1, i_2, i_3, but also $i_4 = I_4^5 I_{10}^{-2}$. Call the output P_1, P_2, P_3, P_4.

2. If $P_1(0)\neq 0$, which is ‘usually’ true, then output P_1, P_2, P_3 and stop.

3. Otherwise, perform the above algorithm with the Cardona-Quer invariants. At Step 6b, decide whether $I_2(Z_j)$ is zero by deciding if the root $i_1(Z_j)$ of P_1 is zero. This can be done using the height of P_1, the bounds on $i_1(Z_k)$ with $k\neq j$, and a suitable approximation of $i_1(Z_j)$. In the same way, if $I_2(Z_j)$ is zero, then we need to decide if $I_4(Z_j)$ is zero, which can be done using P_4.

To compute the polynomials $\widehat{H}_{K,n}$ $(n=2,3)$ of Section 2.1, modify step 7a as in Section 4.3.

Proof of the main theorem. By Algorithm 4.6, the polynomials $dH_{K,n}$ have integer coefficients. A precision of $1+\log_2 d$ for the coefficients of $H_{K,n}$ suffices for recognizing these coefficients and hence by Algorithm 4.4, the output is correct, because the error of $i_n(A_j)$ is at most 2^{-p}.

Next, we bound the precisions p and r. We start by bounding absolute values of the theta constants from above and below using Theorem 10.6. For that, we need upper bounds on the imaginary parts of the diagonal entries of each Z_j and lower bounds on the absolute values of the off-diagonal entries. Corollary 9.2 gives the upper bound $\frac{4}{3}\max\{2\Delta_0, \frac{1}{3}\Delta_1^{1/2}\Delta_0^{1/2}\}$ on the imaginary part of each diagonal entry of each Z_j. We claim that the off-diagonal entry z_3 of $Z_j \in \mathcal{H}_2$ is nonzero. Indeed, if $z_3 = 0$, then $Z_j = \mathrm{diag}(z_1, z_2)$ with $z_1, z_2 \in \mathcal{H} = \mathcal{H}_1$ and Z is the product of the elliptic curves corresponding to z_1 and z_2, contradicting the fact that A_j is simple [20, Theorem 1.3.4]. The claim and Corollary 8.11 together now give an upper bound on $\log(1/z_3)$, which is polynomial in $\log\Delta$ by Lemma 6.9. Therefore, Theorem 10.6 tells us that the lower bounds we get on theta constants in step 4c are of the form $c_1\mathrm{exp}(-c_2{\Delta_1}^{1/2}\Delta_0)$ for some pair of positive constants c_1, c_2, while the upper bounds are constant. By Lemma 10.1, we get upper bounds of the form $c_1\mathrm{exp}(c_2{\Delta_1}^{1/2}\Delta_0)$ on $I_{2k}(A_j)$ for some pair of positive constants c_1, c_2 and hence, upper bounds of the same form on $i_n(A_j)$, where c_1, c_2 depend in some explicit way on the choice of absolute Igusa invariants $i_n \in \mathbf{Q}[I_2, I_4, I_6, I_{10}^{-1}]$.

As $\log d = \widetilde{O}(\widetilde{O}(\Delta_1^{3/2}\Delta_0^{5/2})$ by Theorem 3.1 (and h_1 is even smaller by Lemma 3.2), we find $p = \widetilde{O}(\Delta_1^{3/2}\Delta_0^{5/2})$ in step 5. By the bounds on the theta constants and the formulas of Lemma 10.1, we find that bounds of the same form hold for r.

Finally, we can bound the runtime. Under the assumption that $K = \mathbf{Q}(\sqrt{-a + b\sqrt{\Delta_0}})$ is a good representation of K, we can factor $(a^2 - b^2\Delta_0)\Delta_0^2$ and hence find the ring of integers in step 1 in time $O(\Delta)$.

As shown in Section 6.3, step 2 takes time $\widetilde{O}(\Delta^{1/2})$. Step 3 takes time $\widetilde{O}(d) = \widetilde{O}(\Delta_1^{3/2}\Delta_0^{5/2})$.

Step 4a takes time polynomial in $\log\Delta$ by Lemma 6.9 and Theorem 8.10. The same holds for steps 4b and 4c and each summand of step 5. The number of iterations or summands of these steps is $2h_1 = \widetilde{O}(\Delta_1^{1/2}\Delta_0^{1/2})$ by Lemmas 3.2 and 6.8. In particular, steps 4 and 5 take time $\widetilde{O}(\Delta_1^{1/2}\Delta_0^{1/2})$.

By Theorem 10.8, it takes time $\widetilde{O}(r^2)$ to do a single iteration of step 6a. In particular, all iterations of this step together take time $\widetilde{O}(\Delta_1^{7/2}\Delta_0^{11/2})$. Steps 6b and 6b take time only $\widetilde{O}(r)$ and hence all iterations together take time $\widetilde{O}(\Delta_1^2\Delta_0^3)$.

Finally, by Theorem 4.5, step 7a takes time $\widetilde{O}(h_1)$ times $\widetilde{O}(p_n)$, which is $\widetilde{O}(\Delta_1^2\Delta_0^3)$. The same amount of time is needed for the final two steps.

The output consists of at most $2h_1$ coefficients, each of which has a bit size of $\widetilde{O}(\Delta_1^{3/2}\Delta_0^{5/2})$ (dominated by our bounds on d), hence the size of the output is $\widetilde{O}(\Delta_1^2\Delta_0^3)$. This proves the main theorem. □

It also follows that using Dupont's alternative method of evaluating theta constants [6], the heuristic runtime of Algorithm 11.1 is $\widetilde{O}(\Delta_1^2\Delta_0^3) = \widetilde{O}(\Delta^2)$, which can still be improved if better bounds on the denominators are found.

References

[1] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, second edition, 2004.

[2] Johannes Buchmann and Hendrik W. Lenstra, Jr. Approximatting rings of integers in number fields. *Journal de Theorie des Nombres de Bordeaux*, 6:221–260, 1994.

[3] Johannes Buchmann, Christoph Thiel, and Hugh Williams. Short representation of quadratic integers. In *Computational algebra and number theory (Sydney, 1992)*, volume 325 of *Math. Appl.*, pages 159–185. Kluwer Acad. Publ., Dordrecht, 1995.

[4] Gabriel Cardona and Jordi Quer. Field of moduli and field of definition for curves of genus 2. In *Computational aspects of algebraic curves*, volume 13 of *Lecture Notes Ser. Comput.*, pages 71–83. World Sci. Publ., Hackensack, NJ, 2005.

[5] A. Clebsch. Zur Theorie der binären algebraischen Formen. *Math. Ann.*, 3(2):265–267, 1870.

[6] Régis Dupont. *Moyenne arithmético-géométrique, suites de Borchardt et applications.* PhD thesis, École Polytechnique, April 2006.

[7] Kirsten Eisenträger and Kristin E. Lauter. A CRT algorithm for constructing genus 2 curves over finite fields. To appear in "Arithmetic, Geometry and Coding Theory", proceedings of AGCT-10, Marseille 2005, arXiv:math/0405305v2, 2005.

[8] David Freeman and Kristin E. Lauter. Computing endomorphism rings of Jacobians of genus 2 curves over finite fields. In *Algebraic Geometry and its Applications*, pages 29–66. World Scientific, 2008. Proceedings of SAGA 2007, arXiv:math/0701305v2.

[9] Gerhard Frey and Tanja Lange. Complex multiplication. In H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, editors, *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Math. Appl., pages 455–473. Chapman & Hall/CRC, 2006.

[10] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng. The p-adic CM-method for genus 2. arXiv:math/0503148v1, 2002.

[11] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng. The 2-adic CM-method for genus 2 curves with application to cryptography. In *ASIACRYPT 2006*, volume 4284 of *LNCS*, pages 114–129. Springer-Verlag, 2006.

[12] Eyal Z. Goren. On certain reduction problems concerning abelian surfaces. *manuscripta mathematica*, 94(1):33–43, 1997.

[13] Eyal Z. Goren. *Lectures on Hilbert modular varieties and modular forms*, volume 14 of *CRM Monograph Series*. American Mathematical Society, Providence, RI, 2002. With the assistance of Marc-Hubert Nicole.

[14] Eyal Z. Goren. Personal communication, 2007.

[15] Eyal Z. Goren. Class invariants for genus 2 curves, part II. 4-th Spring Conference on Siegel Modular Forms and Abelian Varieties, Lake Hamana, Japan, slides available at http://research.microsoft.com/∼klauter/JapanTalk2007CombinedV2.pdf, 2007.

[16] Eyal Z. Goren and Kristin E. Lauter. Class invariants for quartic cm fields. *Annales de l'Institut Fourier*, 57(2):457–480, 2007.

[17] Erhard Gottschling. Die Randflächen des Fundamentalbereiches der Modulgruppe. *Math. Annalen*, 138:103–124, 1959.

[18] Jun-Ichi Igusa. Arithmetic variety of moduli for genus two. *The Annals of Mathematics*, 72(3):612–649, 1960.

[19] Helmut Klingen. *Introductory lectures on Siegel modular forms*, volume 20 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1990.

[20] Serge Lang. *Complex Multiplication*, volume 255 of *Grundlehren der mathematischen Wissenschaften*. Springer, 1983.

[21] Kristin E. Lauter. Primes in the denominators of igusa class polynomials. arXiv:math/0301240v1, 2003.

[22] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261(4):515–534, 1982.

[23] Hendrik W. Lenstra, Jr. On the calculation of regulators and class numbers of quadratic fields. In *Journées Arithmétiques 1980*, pages 123–150. Cambridge University Press, 1982.

[24] Hendrik W. Lenstra, Jr. Algorithms in algebraic number theory. *Bull. Amer. Math. Soc. (N.S.)*, 26(2):211–244, 1992.

[25] Stéphane 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):3079–3098 (electronic), 2003.

[26] Jean-François Mestre. Constuction de courbes de genre 2 à partir de leurs modules. In *Effective methods in algebraic geometry*, volume 94 of *Progress in Mathematics*, pages 313–334. Birkhäuser Boston, 1991.

[27] David Mumford. *Tata lectures on theta II*, volume 43 of *Progress in Mathematics*. Birkhäuser, 1984.

[28] Jürgen Neukirch. *Algebraische Zahlentheorie*. Springer, 1992.

[29] René Schoof. Computing Arakelov class groups. In Joe Buhler and Peter Stevenhagen, editors, *Surveys in Algorithmic Number Theory*. Cambridge University Press, 2008.

[30] Goro Shimura. *Abelian Varieties with Complex Multiplication and Modular Functions*. Princeton University Press, 1998.

[31] Anne-Monika Spallek. *Kurven vom Geschlecht* 2 *und ihre Anwendung in Public-Key-Kryptosystemen*. PhD thesis, Institut für Experimentelle Mathematik, Universität GH Essen, 1994.

[32] Gerard van der Geer. *Hilbert modular surfaces*, volume 16 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*. Springer-Verlag, Berlin, 1988.

[33] Paul van Wamelen. Examples of genus two CM curves defined over the rationals. *Mathematics of Computation*, 68(225):307–320, 1999.

[34] Lawrence C. Washington. *Introduction to Cyclotomic Fields*. Number 83 in Graduate Texts in Mathematics. Springer-Verlag, 1982.

[35] Heinrich Weber. *Algebraische Zahlen*, volume 3 of *Lehrbuch der Algebra*. Braunschweig, Friedrich Vieweg, 1908.

[36] André Weil. Zum Beweis des Torellischen Satzes. *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa.*, 1957:33–53, 1957.

[37] Annegret Weng. Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Mathematics of Computation*, 72(241):435–458, 2002.

[38] Tonghai Yang. Arithmetic intersection and the Faltings height. http://www.math.wisc.edu/∼thyang/RecentPreprint.html, 2007.