Computing isogenies from modular equations between Jacobians of genus 2 curves

Jean Kieffer, Aurel Page, Damien Robert

Computing isogenies from modular equations between Jacobians of genus 2 curves

Jean Kieffer[1], Aurel Page[1,2], Damien Robert[1,2]

[1] Université de Bordeaux, France [2] Inria Bordeaux Sud-Ouest, France
{jean.kieffer,damien.robert,aurel.page}@math.u-bordeaux.fr

Abstract

Let k be a field of large enough characteristic. We present an algorithm solving the following problem: given two genus 2 curves over k with isogenous Jacobians, compute an isogeny between them explicitly. This isogeny can be either an ℓ-isogeny or, in the real multiplication case, an isogeny with cyclic kernel. The algorithm uses modular equations for these isogeny types.

1 Introduction

There are two versions of the problem of computing isogenies between elliptic curves or abelian varieties. First, given the source abelian variety together with a description of the kernel, one can ask to compute the target variety and explicit formulæ for the isogeny. Second, given two abelian varieties that are guaranteed to be isogenous, one can ask to compute an isogeny between them and its kernel explicitly. Here we are interested in the second question.

In the case of elliptic curves, an algorithm was given by Elkies [17]. Given two ℓ-isogenous elliptic curves, it uses modular polynomials to compute rational fractions defining this isogeny. This algorithm is used to speed up Schoof's point counting algorithm for elliptic curves over finite fields [38]: replacing kernels of *endomorphisms* by kernels of *isogenies* yields smaller subgroups of the elliptic curve, and therefore smaller polynomial computations, while giving the same amount of information on the Frobenius. This gave rise to the well-known SEA point counting algorithm [39].

The situation for point counting in genus 2 is different: the existing complexity estimates and records only use kernels of endomorphisms [19, 20]. One can therefore ask whether the idea of using isogenies generalizes. Modular polynomials have now been computed in genus 2: the smallest ones are known both for ℓ-isogenies [31] and, in the real multiplication case, cyclic β-isogenies [28, 32]. This opened the way for Atkin-style methods in point counting [3], but isogeny computations in genus 2 remain the missing step to generalize Elkies's method.

The object of this paper is precisely to fill this gap. We state our main result only in the case of β-isogenies; see Theorem 4.34 for a variant with ℓ-isogenies. Investigating whether we can use it to lower the point counting complexity in genus 2, as Elkies's algorithm for elliptic curves, is a major goal for future work.

Theorem 1.1. *Let K be a real quadratic field, and let $\beta \in \mathbb{Z}_K$ be a totally positive prime. Let k be a field such that*

$$\operatorname{char} k > 4 \operatorname{Tr}_{K/\mathbb{Q}}(\beta) + 7.$$

Assume that there is an algorithm that can evaluate derivatives of modular equations of level β at a given point over k, using $C_{\mathrm{ev}}(\beta)$ operations in k; also assume that there is an algorithm that can compute square roots in field extensions of k of degree at most 4 using C_{sqrt} operations in k.

Then there is an algorithm which, given two Jacobians of genus 2 curves over k with real multiplication by $\mathbb{Z}_K$ that are β-isogenous and generic, returns an explicit description of this β-isogeny within

$$O\big(C_{\mathrm{ev}}(\beta)\big) + \widetilde{O}\big(\operatorname{Tr}_{K/\mathbb{Q}}(\beta)\big) + O_K(1) + O(C_{\mathrm{sqrt}})$$

operations in k.

We refer to §4 for a precise description of the input and output of the algorithm and the precise meaning of the term "generic". The implied constants in the complexity estimate, $O_K(1)$ excepted, are independent of K. Unfortunately, designing evaluation algorithms for genus 2 modular equations, and hence obtaining estimates on $C_{\mathrm{ev}}(\beta)$, is out of the scope of this paper. Note that if $\ell \in \mathbb{N}$ is a prime that splits in a product of totally positive prime elements of $\mathbb{Z}_K$, then we can find a decomposition $\ell = \beta\overline{\beta}$ with $\operatorname{Tr}(\beta) \in O_K\big(\sqrt{\ell}\big)$. A natural way to obtain an input for the isogeny algorithm is to compute roots of modular equations.

Our algorithm is a direct generalization of previous works in genus 1 [6, 17]. Let us give a brief outline of how to compute a β-isogeny $\varphi\colon \mathcal{J} \to \mathcal{J}'$.

- First, we find suitable hyperelliptic curves $\mathcal{C}$ and $\mathcal{C}'$ of genus 2, given by explicit equations, such that $\operatorname{Jac}(\mathcal{C}) \simeq \mathcal{J}$ and $\operatorname{Jac}(\mathcal{C}') \simeq \mathcal{J}'$. These equations specify bases of differential forms on $\mathcal{J}$ and $\mathcal{J}'$; this allows us to evaluate modular forms in terms of the coefficients of the curves.
- Second, we compute the action of φ on these differential forms. This is where we differentiate modular equations; a crucial step is to compute derivatives of Igusa invariants.
- Third, we solve a differential system locally around a rational point, and recover the expression of φ globally.

The only difference with genus 1, in a sense, is that we have to consider two differential forms instead of just one, and Siegel or Hilbert modular forms instead of classical ones. The third step is more standard, and is similar to the methods of [14, 13].

This paper is organized as follows. In Section 2, we give the necessary background on Siegel and Hilbert modular forms, and the different types of isogenies and modular equations in genus 2. In Section 3, we explain how to compute the expression of a given modular form in terms of the coefficients of the curve, and apply it to derivatives of Igusa invariants. We present the algorithm and prove Theorem 1.1 in Section 4. Finally, in Appendix A, we present a variant in the case $K = \mathbb{Q}(\sqrt{5})$ and compute an example of cyclic isogeny of degree 11.

Acknowledgement. The authors were supported by the ANR grant Ciao.

2 Background on modular forms and isogenies

We present the basic facts about Siegel and Hilbert modular only in the genus 2 case. References for this section are [43] for Siegel modular forms, and [9] for Hilbert modular forms, where the general case is treated.

We write 4×4 matrices in block notation using 2×2 blocks. Write m^t for the transpose of a matrix m, and use m^{-t} as a shorthand for $(m^{-1})^t$. Denote the diagonal 2×2 matrix with entries x, y on the diagonal by $\mathrm{Diag}(x, y)$.

2.1 Siegel modular forms

The Siegel threefold. Denote by $\mathcal{H}_2$ the set of complex symmetric 2×2 matrices with positive definite imaginary part. For every $\tau \in \mathcal{H}_2$, the quotient

$$A(\tau) = \mathbb{C}^2/\Lambda(\tau) \quad \text{where } \Lambda(\tau) = \mathbb{Z}^2 \oplus \tau\mathbb{Z}^2$$

can be naturally endowed with the structure of a principally polarized abelian surface over $\mathbb{C}$, with a basis of differential forms given by

$$\omega(\tau) = (dz_1, dz_2).$$

Recall that the symplectic group $\mathrm{Sp}_4(\mathbb{Z})$ acts on $\mathcal{H}_2$ in the following way:

$$\forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}_4(\mathbb{Z}),\ \forall \tau \in \mathcal{H}_2,\ \gamma\tau = (a\tau + b)(c\tau + d)^{-1}.$$

Proposition 2.1 ([4, 8.1.4])**.** *Let $\tau \in \mathcal{H}_2$, and $\gamma \in \mathrm{Sp}_4(\mathbb{Z})$ with blocks a, b, c, d. Then there is an isomorphism*

$$\eta_{\gamma,\tau} \colon A(\tau) \to A(\gamma\tau), \quad z \mapsto (c\tau + d)^{-t} z.$$

In particular we have $\eta_{\gamma,\tau}^*(\omega(\gamma\tau)) = (c\tau + d)^{-t}\omega(\tau)$.

Theorem 2.2 ([4, 8.1.3])**.** *Let A be a complex principally polarized abelian surface. Then there exists $\tau \in \mathcal{H}_2$ such that A is isomorphic to $A(\tau)$, and τ is uniquely determined up to action of $\mathrm{Sp}_4(\mathbb{Z})$.*

The quotient space $\mathcal{A}_2(\mathbb{C}) = \mathrm{Sp}_4(\mathbb{Z})\backslash\mathcal{H}_2$ is the set of complex points of an algebraic variety $\mathcal{A}_2$ defined over $\mathbb{Z}$. Theorem 2.2 shows that $\mathcal{A}_2(\mathbb{C})$ is a moduli space for principally polarized abelian surfaces over $\mathbb{C}$. More generally, $\mathcal{A}_2$ is a moduli space over $\mathbb{Z}$ for principally polarized abelian varieties, either in the coarse sense or as a stack [43, §10]. Hence, most of the computations that we make in the paper have an algebraic meaning; in order to prove that they are valid over any field, it is enough to do so over $\mathbb{C}$, since $\mathcal{A}_2$ is smooth as a stack over $\mathbb{Z}$. Alternatively, we can use a lifting argument to characteristic zero.

Siegel modular forms. Let $\rho\colon \mathrm{GL}_2(\mathbb{C}) \to \mathrm{GL}(V)$ be a finite-dimensional holomorphic representation of $\mathrm{GL}_2(\mathbb{C})$. We can assume that ρ is irreducible. A *Siegel modular form* of weight ρ is a holomorphic map $f\colon \mathcal{H}_2 \to V$ satisfying the transformation rule

$$\forall \tau \in \mathcal{H}_2,\ \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}_4(\mathbb{Z}), \quad f(\gamma\tau) = \rho(c\tau + d) f(\tau).$$

We say that f is *scalar-valued* if V has dimension 1, and *vector-valued* otherwise. A *modular function* is only required to be meromorphic instead of holomorphic.

Remark 2.3. There is no need to enforce the holomorphy condition at the cusps: Koecher's principle asserts that it is automatically satisfied. Since every irreducible representation of $\mathrm{GL}_1(\mathbb{C})$ is 1-dimensional, only scalar-valued modular forms occur in genus 1; this is no longer the case in genus 2.

From a geometric point of view, Siegel modular forms are sections of certain algebraic line bundles on $\mathcal{A}_2$. These line bundles can be realized as certain powers, depending on the weight ρ, of the *Hodge bundle*; the fibre of the Hodge bundle over the isomorphism class of an abelian surface A can be identified with the dual of the vector space $\Omega^1(A)$ of differential forms on A. As a consequence, if f is a Siegel modular form of weight ρ, and ω is a basis of $\Omega^1(A)$, then the quantity $f(A, \omega)$ has an algebraic meaning. See [43, §10] for more details.

Over $\mathbb{C}$, we can compute $f(A, \omega)$ as follows. Choose $\tau \in \mathcal{H}_2$ and an isomorphism $\eta\colon A \xrightarrow{\sim} A(\tau)$ as in Theorem 2.2, and let $r \in \mathrm{GL}_2(\mathbb{C})$ be the base-change matrix such that

$$\omega = r\, \eta^*\big(\omega(\tau)\big).$$

Then

$$f(A, \omega) = \rho(r^{-t}) f(\tau).$$

It is easy to check that $f(A, \omega)$ does not depend on the choice of τ and η.

2.2 An explicit view on Siegel modular forms in genus 2

Weights. The classification of finite-dimensional holomorphic representations of $\mathrm{GL}_2(\mathbb{C})$ is well known.

Definition 2.4. Let $n \geq 0$ be an integer. We denote by Sym^n the n-th symmetric power of the standard representation of $\mathrm{GL}_2(\mathbb{C})$ on $\mathbb{C}^2$.

Explicitly, Sym^n is a representation on the vector space $\mathbb{C}_n[x]$ of polynomials of degree at most n, with

$$\mathrm{Sym}^n\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) W(x) = (bx+d)^n W\left(\frac{ax+c}{bx+d}\right).$$

Proposition 2.5. *The irreducible finite-dimensional holomorphic representations of* $\mathrm{GL}_2(\mathbb{C})$ *are exactly the representations* $\det^k \mathrm{Sym}^n$*, for* $k \in \mathbb{Z}$ *and* $n \in \mathbb{N}$.

Proof. Since $\mathrm{SL}_2(\mathbb{C})$ is a simply connected Lie group, there is an equivalence between holomorphic finite-dimensional representations of $\mathrm{SL}_2(\mathbb{C})$ and representations of its Lie algebra $\mathfrak{sl}_2(\mathbb{C})$ [7, Ch. III, §6.1, Th. 1]. By [8, Ch. VIII, §1.3, Th. 1], irreducible representations of $\mathfrak{sl}_2(\mathbb{C})$ are classified by their higher weight; on the Lie group side, this shows that the holomorphic finite-dimensional irreducible representations of $\mathrm{SL}_2(\mathbb{C})$ are exactly the Sym^n for $n \in \mathbb{N}$. The case of $\mathrm{GL}_2(\mathbb{C})$ follows easily. □

The weight of a scalar-valued Siegel modular form is $\det^k$ for some $k \in \mathbb{Z}$, and in fact $k \geq 0$. Writing Sym^n as a representation on $\mathbb{C}_n[x]$ allows us to multiply Siegel modular forms; hence, they naturally generate a graded $\mathbb{C}$-algebra.

Fourier expansions. Let f be a Siegel modular form on $\mathcal{H}_2$ of any weight, with underlying vector space V. If $s \in \mathcal{M}_2(\mathbb{Z})$ is symmetric, then

$$\forall \tau \in \mathcal{H}_2,\ f(\tau + s) = f(\tau).$$

Hence, if we write

$$\tau = \begin{pmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{pmatrix} \quad \text{and} \quad q_j = \exp(2\pi i\, \tau_j) \text{ for } 1 \leq j \leq 3,$$

then f has a Fourier expansion of the form

$$f(\tau) = \sum_{n_1,n_2,n_3 \in \mathbb{Z}} c_f(n_1,n_2,n_3)\, q_1^{n_1} q_2^{n_2} q_3^{n_3}.$$

The Fourier coefficients $c_f(n_1,n_2,n_3)$ belong to V, and can be nonzero only when $n_1 \geq 0$, $n_3 \geq 0$, and $n_2^2 \leq 4n_1n_3$. Note that n_2 can still be negative. In genus 1, this would be simply the classical q-expansion $f(\tau) = \sum_{n \geq 0} a_n q^n$.

Remark 2.6. When computing with q-expansions, we consider them as elements of the power series ring $\mathbb{C}(q_2)[[q_1,q_3]]$. Writing the beginning of a q-expansion means computing modulo an ideal of the form $\left(q_1^\nu, q_3^\nu\right)$ for some precision $\nu \geq 0$.

Structure of scalar-valued forms. The full graded $\mathbb{C}$-algebra of Siegel modular forms in genus 2 is not finitely generated [43, §25], but it is if we restrict to scalar-valued modular forms. We only state the result for even weight.

Theorem 2.7 ([23, 24])**.** *The graded $\mathbb{C}$-algebra of scalar-valued even-weight Siegel modular forms in genus 2 is generated by four algebraically independent modular forms ψ_4, ψ_6, χ_{10}, and χ_{12} of respective weights $\det^k$ with $k = 4, 6, 10, 12$ and q-expansions*

$$\begin{aligned}
\psi_4(\tau) &= 1 + 240(q_1 + q_3) \\
&\quad + \big(240q_2^2 + 13440q_2 + 30240 + 13340q_2^{-1} + 240q_2^{-2}\big)q_1q_3 + \cdots \\
\psi_6(\tau) &= 1 - 504(q_1 + q_3) \\
&\quad + \big(-504q_2^2 + 44352q_2 + 166320 + 44352q_2^{-1} - 504q_2^{-2}\big)q_1q_3 + \cdots \\
\chi_{10}(\tau) &= \big(q_2 - 2 + q_2^{-1}\big)q_1q_3 + \cdots \\
\chi_{12}(\tau) &= \big(q_2 + 10 + q_2^{-1}\big)q_1q_3 + \cdots
\end{aligned}$$

The q-expansions in Theorem 2.7 are easily computed from the expressions in terms of theta functions. The equality $\chi_{10}(\tau) = 0$ occurs exactly when $A(\tau)$ is isomorphic to a product of elliptic curves with the product polarization; otherwise, $A(\tau)$ is isomorphic to the Jacobian of a hyperelliptic curve.

Definition 2.8. Following Streng [40, §2.1], we define the *Igusa invariants* to be

$$j_1 = -2^{-8}\frac{\psi_4\psi_6}{\chi_{10}}, \quad j_2 = 3 \cdot 2^{-7}\frac{\psi_4^2\chi_{12}}{\chi_{10}^2}, \quad j_3 = 2^{-18}\frac{\psi_4^5}{\chi_{10}^2}.$$

They are Siegel modular functions of trivial weight.

Proposition 2.9. *The Igusa invariants define a birational map $\mathcal{A}_2(\mathbb{C}) \to \mathbb{C}^3$.*

Proof. By the theorem of Baily and Borel [2, 10.11], scalar-valued Siegel modular forms of sufficiently high even weight realize a projective embedding of $\mathcal{A}_2$. Therefore, by Theorem 2.7, the Igusa invariants generate the function field of $\mathcal{A}_2$. □

Proposition 2.9 shows that generically, giving (j_1, j_2, j_3) in $\mathbb{C}$ uniquely specifies an isomorphism class of principally polarized abelian surfaces over $\mathbb{C}$. This correspondence only holds on an open set: Igusa invariants are not defined on products of elliptic curves, and do not represent a unique isomorphism class when $\psi_4 = 0$. Algebraically, Igusa invariants are defined over $\mathbb{Z}[1/2]$; they realize a birational map from $\mathcal{A}_2$ to $\mathbb{P}^3$ over any field k provided that $\operatorname{char} k \neq 2$.

Examples of vector-valued forms. Derivatives of Igusa invariants play an important role in the isogeny algorithm. The fundamental fact is that they are modular function themselves.

Proposition 2.10. *Let f be a Siegel modular function of trivial weight. Then the derivative*

$$\frac{df}{d\tau} := \frac{\partial f}{\partial \tau_1}x^2 + \frac{\partial f}{\partial \tau_2}x + \frac{\partial f}{\partial \tau_3}$$

is a Siegel modular function of weight Sym^2.

Proof. Differentiate the relation $f(\gamma\tau) = f(\tau)$ with respect to τ. □

Proposition 2.10 has an algebraic interpretation. For every principally polarized abelian surface A, the Kodaira–Spencer map is a canonical isomorphism between the vector space $\mathrm{Sym}^2(\Omega^1(A))$ and the tangent space of $\mathcal{A}_2$ at A [1, 1.4.1]. Therefore, the derivative of an invariant is naturally a meromorphic section of the vector bundle on $\mathcal{A}_2$ defining modular forms of weight Sym^2.

We conclude with another example of a vector-valued modular form that we will use in the sequel.

Example 2.11. Following Ibukiyama [22], let $E_8 \subset \mathbb{R}^8$ denote the lattice of half-integer vectors $v = (v_1, \dots, v_8)$ subject to the conditions

$$\sum_{k=1}^{8} v_k \in 2\mathbb{Z} \quad \text{and} \quad \forall\, 1 \le k, l \le 8,\ v_k - v_l \in \mathbb{Z}.$$

Set $a = (2, 1, i, i, i, i, 0)$ and $b = (1, -1, i, i, 1, -1, -i, i)$, where $i^2 = -1$. Define

$$f_{8,6}(\tau) = \frac{1}{111456000} \sum_{j=0}^{6} \binom{6}{j} \Theta_j(\tau)\, x^j$$

where, using the notation $\langle v, w\rangle = \sum_{k=1}^{8} v_k w_k$,

$$\Theta_j(\tau) = \sum_{v,v' \in E_8} \langle v, a\rangle^j \cdot \langle v', a\rangle^{6-j} \cdot \begin{vmatrix} \langle v, a\rangle & \langle v', a\rangle \\ \langle v, b\rangle & \langle v', b\rangle \end{vmatrix}^4 \cdot \exp\Big(i\pi\big(\langle v, v\rangle\tau_1 + 2\langle v, v'\rangle\tau_2 + \langle v', v'\rangle\tau_3\big)\Big).$$

Then $f_{8,6}$ is a nonzero Siegel modular form of weight $\det^8 \mathrm{Sym}^6$. This definition provides an explicit, but slow, method to compute the first coefficients of the q-expansion; using the expression of $f_{8,6}$ in terms of theta series [12] would be faster. We have

$$\begin{aligned} f_{8,6}(\tau) = {} & \big((4q_2^2 - 16q_2 + 24 - 16q_2^{-1} + 4q_2^{-2})q_1^2 q_3 + \cdots\big)\, x^6 \\ & + \big((12q_2^2 - 24q_2 + 24q_2^{-1} - 12q_2^{-2})q_1^2 q_3 + \cdots\big)\, x^5 \\ & + \big((-q_2 + 2 - q_2^{-1})q_1 q_3 + \cdots\big)\, x^4 \\ & + \big((-2q_2 + 2q_2^{-1})q_1 q_3 + \cdots\big)\, x^3 \\ & + \big((-q_2 + 2 - q_2^{-1})q_1 q_3 + \cdots\big)\, x^2 \\ & + \big((12q_2^2 - 24q_2 + 24q_2^{-1} - 12q_2^{-2})q_1 q_3^2 + \cdots\big)\, x \\ & + \big((4q_2^2 - 16q_2 + 24 - 16q_2^{-1} + 4q_2^{-2})q_1 q_3^2 + \cdots\big)\,. \end{aligned}$$

2.3 Hilbert modular forms

Hilbert surfaces. Let K be a real quadratic number field, with ring of integers $\mathbb{Z}_K$. Choose an embedding of K in $\mathbb{R}$, and write $K = \mathbb{Q}\big(\sqrt{\Delta}\big)$, where Δ is the fundamental discriminant of K. Denote real conjugation in K by a bar. Let $\mathbb{Z}_K^\vee$ be the trace dual of $\mathbb{Z}_K$, in other words $\mathbb{Z}_K^\vee = 1/\sqrt{\Delta}\ \mathbb{Z}_K$. Call Φ the embedding $x \mapsto (x, \overline{x})$ from K to $\mathbb{R}^2$.

Denote by $\mathcal{H}_1$ the complex upper half-plane. For every $t = (t_1, t_2) \in \mathcal{H}_1^2$, the quotient

$$A_K(t) = \mathbb{C}^2/\Lambda_K(t) \quad \text{where } \Lambda_K(t) = \Phi\big(\mathbb{Z}_K^\vee\big) \oplus \mathrm{Diag}(t_1, t_2)\, \Phi\big(\mathbb{Z}_K\big)$$

can be naturally endowed with the structure of a principally polarized abelian surface over $\mathbb{C}$, with a basis of differential forms given by

$$\omega_K(t) = (dz_1, dz_2),$$

and a real multiplication embedding

$$\iota_K(t) \colon \mathbb{Z}_K \hookrightarrow \mathrm{End}^{\mathrm{sym}}\big(A_K(t)\big)$$

given by multiplication via Φ. Here $\mathrm{End}^{\mathrm{sym}}(A)$ denotes the set of endomorphisms of A that are invariant under the Rosati involution. At the level of abelian varieties, the involution σ of $\mathcal{H}_1^2$ given by

$$\forall t_1, t_2 \in \mathcal{H}_1,\ \sigma\big((t_1, t_2)\big) = (t_2, t_1)$$

exchanges the two differential forms in the basis, and exchanges the real multiplication embedding with its conjugate.

Finally, we introduce the modular group. Define

$$\mathrm{SL}_2\big(\mathbb{Z}_K \oplus \mathbb{Z}_K^\vee\big) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(K) \mid a, d \in \mathbb{Z}_K,\ b \in \big(\mathbb{Z}_K^\vee\big)^{-1},\ c \in \mathbb{Z}_K^\vee \right\}.$$

The embedding Φ induces a map

$$\mathrm{SL}_2\big(\mathbb{Z}_K \oplus \mathbb{Z}_K^\vee\big) \hookrightarrow \mathrm{SL}_2(\mathbb{R})^2.$$

Through this embedding, the group $\mathrm{SL}_2\big(\mathbb{Z}_K \oplus \mathbb{Z}_K^\vee\big)$ acts on $\mathcal{H}_1^2$, by the usual action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathcal{H}_1$ on each coordinate.

Theorem 2.12 ([4, §9.2])**.** *Let A be a principally polarized abelian surface over $\mathbb{C}$ endowed with a real multiplication embedding $\iota \colon \mathbb{Z}_K \hookrightarrow \mathrm{End}^{\mathrm{sym}}(A)$. Then there exists $t \in \mathcal{H}_1^2$ such that (A, ι) is isomorphic to $\big(A_K(t), \iota_K(t)\big)$. Moreover, t is uniquely determined up to action of $\mathrm{SL}_2\big(\mathbb{Z}_K \oplus \mathbb{Z}_K^\vee\big)$.*

The quotient $\mathcal{A}_{2,K}(\mathbb{C}) = \mathrm{SL}_2\big(\mathbb{Z}_K \oplus \mathbb{Z}_K^\vee\big)\backslash\mathcal{H}_1^2$ is the set of complex points of an algebraic variety $\mathcal{A}_{2,K}$, called a *Hilbert surface*.

Hilbert modular forms. Let $k_1, k_2 \in \mathbb{Z}$. A *Hilbert modular form* of weight (k_1, k_2) is a holomorphic function $f\colon \mathcal{H}_1^2 \to \mathbb{C}$ satisfying the transformation rule

$$\forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}_K \oplus \mathbb{Z}_K^\vee),\ \forall t \in \mathcal{H}_1^2,\ f(\gamma t) = \big(c\,t_1 + d\big)^{k_1} \big(\overline{c}\,t_2 + \overline{d}\big)^{k_2} f(t).$$

We say that f is *symmetric* if $f \circ \sigma = f$. If f is nonzero and symmetric, then its weight (k_1, k_2) is automatically *parallel*, meaning $k_1 = k_2$. A Hilbert modular *function* is only required to be meromorphic instead of holomorphic.

Remark 2.13. Koecher's principle holds for Hilbert modular forms as well. All irreducible representations of the underlying group $\mathrm{GL}_1(\mathbb{C})^2$ are 1-dimensional, so there is no need to consider vector-valued forms.

The analogue of Proposition 2.10 for Hilbert modular forms is the following.

Proposition 2.14. *Let f be a Hilbert modular function of weight $(0,0)$. Then the derivatives*

$$\frac{\partial f}{\partial t_1} \quad \text{and} \quad \frac{\partial f}{\partial t_2}$$

are Hilbert modular functions of weight $(2,0)$ and $(0,2)$ respectively.

Proof. Differentiate the relation $f(\gamma t) = f(t)$. □

From a geometric point of view, we have two line bundles $\mathcal{L}_1$ and $\mathcal{L}_2$ on $\mathcal{A}_{2,K}$ whose fibres over the isomorphism class of (A, ι) are given by

$$\big\{\omega \in \Omega^1(A) \,|\, \forall \beta \in \mathbb{Z}_K,\ \iota(\beta)^*\omega = \beta\omega \text{ (resp. } \overline{\beta}\omega)\big\}^\vee.$$

Hilbert modular forms of weight (k_1, k_2) are holomorphic sections of the line bundle $\mathcal{L}_1^{k_1} \otimes \mathcal{L}_2^{k_2}$ [42, X.3].

Definition 2.15. Let A be a principally polarized abelian surface over $\mathbb{C}$ endowed with a real multiplication embedding $\iota\colon \mathbb{Z}_K \hookrightarrow \mathrm{End}^{\mathrm{sym}}(A)$, and let ω be a basis of $\Omega^1(A)$. We say that (A, ι, ω) is *Hilbert-normalized* if

$$\forall \alpha \in \mathbb{Z}_K,\ \iota(\alpha)^* = \begin{pmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{pmatrix} \quad \text{in the basis } \omega.$$

This definition makes sense over any field k once we choose a value of $\sqrt{\Delta}$ in k. If (A, ι, ω) is Hilbert-normalized and f is a Hilbert modular form of weight (k_1, k_2), then the quantity $f(A, \iota, \omega)$ has an algebraic meaning.

Over $\mathbb{C}$, we can compute $f(A, \iota, \omega)$ as follows. Choose $t \in \mathcal{H}_1^2$ and an isomorphism $\eta\colon (A, \iota) \xrightarrow{\sim} \big(A_K(t), \iota_K(t)\big)$ as in Theorem 2.12, and let $r \in \mathrm{GL}_2(\mathbb{C})$ be the base-change matrix such that

$$\omega = r\,\eta^*\big(\omega_K(t)\big).$$

Then r is diagonal, $r = \mathrm{Diag}(r_1, r_2)$, and

$$f(A, \iota, \omega) = r_1^{-k_1} r_2^{-k_2} f(t).$$

2.4 The Hilbert embedding

Forgetting the real multiplication structure yields a map $\mathcal{A}_{2,K} \to \mathcal{A}_2$ from the Hilbert surface to the Siegel threefold. In fact, this forgetful map comes from a linear map

$$H\colon \mathcal{H}_1^2 \to \mathcal{H}_2$$

called the *Hilbert embedding*, which we now describe explicitly. Let

$$e_1 = 1 \quad \text{and} \quad e_2 = \begin{cases} \dfrac{1-\sqrt{\Delta}}{2} & \text{if } \Delta = 1 \bmod 4, \\ \sqrt{\Delta} & \text{otherwise.} \end{cases}$$

Then (e_1, e_2) is a $\mathbb{Z}$-basis of $\mathbb{Z}_K$. Set

$$R = \begin{pmatrix} e_1 & e_2 \\ \overline{e_1} & \overline{e_2} \end{pmatrix},$$

and define

$$H\colon \mathcal{H}_1^2 \to \mathcal{H}_2, \qquad t = (t_1, t_2) \mapsto R^t \operatorname{Diag}(t_1, t_2)\, R.$$

Proposition 2.16. *For every $t \in \mathcal{H}_1^2$, multiplication by R^t on $\mathbb{C}^2$ induces an isomorphism $A_K(t) \xrightarrow{\sim} A\big(H(t)\big)$.*

Proof. By definition, $\Phi\big(\mathbb{Z}_K\big) = R\,\mathbb{Z}^2$, and since $\mathbb{Z}_K^\vee$ is the trace dual of $\mathbb{Z}_K$, we have $\Phi\big(\mathbb{Z}_K^\vee\big) = R^{-t}\,\mathbb{Z}^2$. Then a direct computation shows that

$$\forall t \in \mathcal{H}_1^2,\ \Lambda\big(H(t)\big) = R^t\,\Lambda_K(t). \qquad \square$$

In particular, under this isomorphism, the bases of differential forms satisfy

$$\omega\big(H(t)\big) = R^t\,\omega_K(t).$$

The Hilbert embedding is compatible with the actions of the modular groups.

Proposition 2.17 ([27, 3.1])**.** *1. The action of $\mathrm{SL}_2\big(\mathbb{Z}_K \oplus \mathbb{Z}_K^\vee\big)$ on $\mathcal{H}_1^2$ is transformed into the action of $\mathrm{Sp}_4(\mathbb{Z})$ on $\mathcal{H}_2$ by means of the morphism*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} R^t & 0 \\ 0 & R^{-1} \end{pmatrix} \begin{pmatrix} a^* & b^* \\ c^* & d^* \end{pmatrix} \begin{pmatrix} R^{-t} & 0 \\ 0 & R \end{pmatrix}$$

where we write $x^* = \operatorname{Diag}(x, \overline{x})$ for $x \in K$.

2. Define

$$M_\sigma = \begin{pmatrix} 1 & 0 & & \\ \delta & -1 & & (0) \\ & & 1 & \delta \\ & (0) & 0 & -1 \end{pmatrix}$$

where $\delta = 1$ if $\Delta = 1 \bmod 4$, and $\delta = 0$ otherwise. Then we have

$$\forall t \in \mathcal{H}_1^2,\ H\big(\sigma(t)\big) = M_\sigma H(t).$$

Moreover, pulling back a Siegel modular form via the Hilbert embedding gives a Hilbert modular form.

Proposition 2.18. *Let $k \in \mathbb{Z}$, $n \in \mathbb{N}$, and let $f\colon \mathcal{H}_2 \to \mathbb{C}_n[x]$ be a Siegel modular form of weight $\rho = \det^k \mathrm{Sym}^n$. Define the function $g\colon \mathcal{H}_1^2 \to \mathbb{C}$ by*

$$\forall t \in \mathcal{H}_1^2,\ g(t) = \rho(R) f\big(H(t)\big),$$

and define the functions g_i for $0 \le i \le n$ by

$$\forall t \in \mathcal{H}_1^2,\ g(t) = \sum_{i=0}^{n} g_i(t)\, x^i.$$

Then g_i is a Hilbert modular form of weight $(k+i,\, k+n-i)$.

Proof. It is enough to check the transformation rule. Let $t \in \mathcal{H}_1^2$, write $\tau = H(t)$, and let

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2\big(\mathbb{Z}_K \oplus \mathbb{Z}_K^\vee\big).$$

By Proposition 2.17, we have $g(\gamma t) = \rho(R) f(\widetilde{\gamma}\tau)$ where

$$\widetilde{\gamma} = \begin{pmatrix} R^t & 0 \\ 0 & R^{-1} \end{pmatrix} \begin{pmatrix} a^* & b^* \\ c^* & d^* \end{pmatrix} \begin{pmatrix} R^{-t} & 0 \\ 0 & R \end{pmatrix} = \begin{pmatrix} * & * \\ R^{-1}c^*R^{-t} & R^{-1}d^*R \end{pmatrix}.$$

Therefore

$$\begin{aligned} g(\gamma t) &= \rho(R)\rho\big(R^{-1}c^*R^{-t}\tau + R^{-1}d^*R\big) f(\tau) \\ &= \rho\big(c^* \operatorname{Diag}(t_1, t_2)\ + d^*\big)\rho(R) f(\tau) \\ &= \rho\big(\operatorname{Diag}(c\,t_1 + d, \overline{c}\,t_2 + \overline{d})\big) g(t). \end{aligned}$$

On diagonal matrices $\mathrm{Diag}(r_1, r_2)$, the representation $\det^k \mathrm{Sym}^n$ splits: the coefficient before x^i is multiplied by $(r_1 r_2)^k r_1^i r_2^{n-i}$. The result follows. □

Corollary 2.19. *If f is a scalar-valued Siegel modular form of weight $\det^k$, then $H^*f : t \mapsto f\big(H(t)\big)$ is a symmetric Hilbert modular form of weight (k,k).*

Proof. Since $\det(R)^k$ is a nonzero constant, by Proposition 2.18, the function H^*f is a Hilbert modular form of weight (k,k). Moreover $\det(M_\sigma) = 1$, so H^*f is symmetric by Proposition 2.17. □

The image of the Hilbert embedding in $\mathcal{A}_2$ is called a *Humbert surface*. It can be described by an equation in terms of Igusa invariants, which grows quickly with the discriminant Δ, but can be computed in small cases [21].

Proposition 2.20. *Igusa invariants generate the field of symmetric Hilbert modular functions of weight $(0,0)$. They define a birational map from $\mathcal{A}_{2,K}$ to the closed subset of $\mathbb{C}^3$ given by the Humbert equation.*

Proof. The image of the Hilbert embedding in $\mathcal{A}_2$ is not contained in the codimension 1 subset where Igusa invariants are not a local isomorphism to $\mathbb{P}^3$. □

To ease notation, we also write j_k for H^*j_k, for each $1 \le k \le 3$.

2.5 Isogenies between abelian surfaces

Let k be a field, and let A be a principally polarized abelian surface over k. Denote its dual by $A^\vee$ and its principal polarization by $\pi\colon A \xrightarrow{\sim} A^\vee$. Recall that for every line bundle $\mathcal{L}$ on A, there is a morphism $\varphi_{\mathcal{L}}\colon A \to A^\vee$ defined by $\varphi_{\mathcal{L}}(x) = T_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$, where T_x denotes translation by x on A. Finally, let $\mathrm{NS}(A)$ denote the Néron–Severi group of A, consisting of line bundles up to algebraic equivalence.

Theorem 2.21 ([33, Prop. 14.2])**.** *For every $\xi \in \mathrm{End}^{\mathrm{sym}}(A)$, there is a unique symmetric line bundle $\mathcal{L}_A^\xi$ such that $\varphi_{\mathcal{L}_A^\xi} = \pi \circ \xi$. This association induces an isomorphism of groups*

$$\big(\mathrm{End}^{\mathrm{sym}}(A), +\big) \simeq \big(\mathrm{NS}(A), \otimes\big).$$

Under this isomorphism, line bundles giving rise to polarizations correspond to totally positive elements in $\mathrm{End}^{\mathrm{sym}}(A)$.

In this notation, $\mathcal{L}_A^1$ is the line bundle associated with the principal polarization π. We can now define the two types of isogenies that we consider in this article.

Definition 2.22. Let k be a field.

1. Let $\ell \in \mathbb{N}$ be a prime, and let A, A' be principally polarized abelian surfaces over k. An isogeny $\varphi\colon A \to A'$ is called an *ℓ-isogeny* if
$$\varphi^*\mathcal{L}_{A'}^1 = \mathcal{L}_A^\ell.$$

2. Let K be a real quadratic field, and let $\beta \in \mathbb{Z}_K$ be a totally positive prime. Let (A, ι) and (A', ι') be principally polarized abelian surfaces over k with real multiplication by $\mathbb{Z}_K$. An isogeny $\varphi\colon A \to A'$ is called a *β-isogeny* if
$$\varphi^*\mathcal{L}_{A'}^1 = \mathcal{L}_A^{\iota(\beta)}$$
and
$$\forall \alpha \in \mathbb{Z}_K,\ \varphi \circ \iota(\alpha) = \iota'(\alpha) \circ \varphi.$$

In some sense, ℓ-isogenies are the simplest kind of isogenies that occur for a generic principally polarized abelian surface. They have degree ℓ^2. If we restrict to abelian surfaces with real multiplication by $\mathbb{Z}_K$, then β-isogenies are smaller: their degree is only $N_{K/\mathbb{Q}}(\beta)$ [15, Prop. 2.1].

From the point of view of moduli, ℓ-isogenies make sense on the Siegel threefold $\mathcal{A}_2$, and β-isogenies make sense on the Hilbert surface $\mathcal{A}_{2,K}$. They are easily described over $\mathbb{C}$: see [4, 8.3.1]. For $t = (t_1, t_2) \in \mathcal{H}_1^2$, write

$$t/\beta := \big(t_1/\beta, t_2/\overline{\beta}\big).$$

Proposition 2.23.

1. *For every $\tau \in \mathcal{H}_2$, the identity map on $\mathbb{C}^2$ induces an ℓ-isogeny*

$$A(\tau) \to A(\tau/\ell).$$

Let A, A' be principally polarized abelian surfaces over $\mathbb{C}$, and $\varphi\colon A \to A'$ an ℓ-isogeny. Then there exists $\tau \in \mathcal{H}_2$ such that there is a commutative diagram

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & A' \\ \downarrow\wr & & \downarrow\wr \\ A(\tau) & \xrightarrow{z\mapsto z} & A(\tau/\ell). \end{array}$$

2. *For every $t \in \mathcal{H}_1^2$, the identity map on $\mathbb{C}^2$ induces a β-isogeny*

$$\big(A_K(t), \iota_K(t)\big) \to \big(A_K(t/\beta), \iota_K(t/\beta)\big).$$

Let (A, ι), (A', ι') be principally polarized abelian surfaces over $\mathbb{C}$ with real multiplication by $\mathbb{Z}_K$, and let $\varphi\colon (A, \iota) \to (A', \iota')$ be a β-isogeny. Then there exists $t \in \mathcal{H}_1^2$ such that there is a commutative diagram

$$\begin{array}{ccc} (A, \iota) & \xrightarrow{\varphi} & (A', \iota') \\ \downarrow\wr & & \downarrow\wr \\ \big(A_K(t), \iota_K(t)\big) & \xrightarrow{z\mapsto z} & \big(A_K(t/\beta), \iota_K(t/\beta)\big). \end{array}$$

2.6 Modular equations

Modular equations encode the presence of an isogeny between principally polarized abelian surfaces, as the classical modular polynomial does for elliptic curves. To define them, we use the fact that the extension of the field $\mathbb{C}\big(j_1(\tau), j_2(\tau), j_3(\tau)\big)$ constructed by adjoining $j_1(\tau/\ell)$, $j_1(\tau/\ell)$, and $j_3(\tau/\ell)$ is finite and generated by $j_1(\tau/\ell)$. A similar statement holds for Igusa invariants at t/β [32, Prop. 4.11].

Definition 2.24.

1. Let $\ell \in \mathbb{N}$ be a prime. We call the *Siegel modular equations of level ℓ* the data of the three polynomials $\Phi_{\ell,1}, \Psi_{\ell,2}, \Psi_{\ell,3} \in \mathbb{C}(J_1, J_2, J_3)[J_1']$ defined as follows:

   - $\Phi_{\ell,1}$ is the univariate minimal polynomial of the function $j_1(\tau/\ell)$ over the field $\mathbb{C}\big(j_1(\tau), j_2(\tau), j_3(\tau)\big)$.
   - For $i \in \{2, 3\}$, we have

$$\forall \tau \in \mathcal{H}_2,\ j_i(\tau/\ell) = \Psi_{\ell,i}\big(j_1(\tau), j_2(\tau), j_3(\tau), j_1(\tau/\ell)\big).$$

2. Let K be a real quadratic field, and let $\beta \in \mathbb{Z}_K$ be a totally positive prime. We call the *Hilbert modular equations of level β* the data of the three polynomials $\Phi_{\beta,1}, \Psi_{\beta,2}, \Psi_{\beta,3}$ defined as follows:

- $\Phi_{\beta,1}$ is the univariate minimal polynomial of the function $j_1(t/\beta)$ over the field $\mathbb{C}\big(j_1(t), j_2(t), j_3(t)\big)$.
- For $i \in \{2,3\}$, we have

$$\forall t \in \mathcal{H}_1^2,\ j_i(t/\beta) = \Psi_{\beta,i}\big(j_1(t), j_2(t), j_3(t), j_1(t/\beta)\big).$$

In the Hilbert case, since Igusa invariants are symmetric by Corollary 2.19, the modular equations encode β- and $\overline{\beta}$-isogenies simulaneously [32, Ex.4.17]. It would be better to consider modular equations with non-symmetric invariants; however, we know of no good choice of such invariants in general.

These modular equations also have coefficients in $\mathbb{Z}$. However, the situation is not as good as in genus 1, because Igusa invariants have poles on $\mathcal{A}_2$ and $\mathcal{A}_{2,K}$. This causes the modular equations in genus 2 to have denominators [32, Rem. 4.20].

Unfortunately, modular equations in genus 2 are very large. This is especially true for Siegel modular equations of level ℓ. The degree in J_1' is $\ell^3+\ell^2+\ell+1$, and the degree in J_1, J_2, J_3 has the same order of magnitude, not mentioning the denominators or the size of the coefficients in $\mathbb{Z}$. The situation is less desperate for Hilbert modular equations of level β, whose degree in J_1' is $2N_{K/\mathbb{Q}}(\beta)+2$ [32, Ex. 4.17]. Modular equations have been computed for $\ell = 2$ and 3 in the Siegel case, up to $N(\beta) = 41$ in the Hilbert case with $K = \mathbb{Q}(\sqrt{5})$ using Gundlach invariants, and even up to $N(\beta) = 97$ for $K = \mathbb{Q}(\sqrt{2})$ using theta constants as invariants [30].

Remark 2.25. Although we will only consider modular equations in Igusa invariants in the sequel, the algorithm would work in the same way with modular equations arising from another presentation for the ideal or another choice of invariants. Imagine, for instance, that we want to compute an isogeny to a product of elliptic curves. Then we cannot use Igusa invariants, as they have a pole, but we can use another set of invariant given by

$$h_1 = \frac{\psi_6^2}{\psi_4^3}, \quad h_2 = \frac{\chi_{12}}{\psi_4^3}, \quad h_3 = \frac{\chi_{10}\psi_6}{\psi_4^4}$$

and change the modular equations accordingly.

3 Explicit identifications of modular forms

A nonsingular hyperelliptic equation $\mathcal{C} : v^2 = f_{\mathcal{C}}(u)$, with $\deg f_{\mathcal{C}} \in \{5,6\}$, naturally encodes a basis of differential forms $\omega(\mathcal{C})$ on the principally polarized abelian surface $\mathrm{Jac}(\mathcal{C})$ (§3.1). Let f be a Siegel modular function; this gives rise to a rational map

$$\mathrm{Cov}(f)\colon \mathcal{C} \mapsto f\big(\mathrm{Jac}(\mathcal{C}), \omega(\mathcal{C})\big).$$

Then, $\mathrm{Cov}(f)$ has an expression in terms of the coefficients of the curve, and we give an algorithm to obtain this expression from the q-expansion of f (§3.2). Finally we apply it to the modular functions which are of interest in the algorithm, namely derivatives of Igusa invariants (§3.3).

3.1 Hyperelliptic equations

Let k be a field, and let $\mathcal{C}$ be a nonsingular hyperelliptic *equation* of genus 2 over k:

$$\mathcal{C} \,:\, v^2 = E_{\mathcal{C}}(u),$$

with $\deg E_{\mathcal{C}} \in \{5, 6\}$. Then $\mathcal{C}$ is naturally endowed with the basis of differential forms

$$\omega(\mathcal{C}) = \Big(\frac{u\,du}{v}, \frac{du}{v}\Big).$$

Recall that the Jacobian $\mathrm{Jac}(\mathcal{C})$ is a principally polarized abelian surface over k [34, 1.1 and 6.11]. Choose a base point P on $\mathcal{C}$, possibly after a field extension. This gives an embedding

$$\eta_P \colon \mathcal{C} \hookrightarrow \mathrm{Jac}(\mathcal{C}), \quad Q \mapsto [Q - P].$$

Proposition 3.1 ([34, 2.2])**.** *The map*

$$\eta_P^* \colon \Omega^1\big(\mathrm{Jac}(\mathcal{C})\big) \to \Omega^1(\mathcal{C})$$

is an isomorphism and is independent of P.

By Proposition 3.1, we can see $\omega(\mathcal{C})$ as a basis of differential forms on $\mathrm{Jac}(\mathcal{C})$. This basis depends on the particular hyperelliptic equation chosen.

Lemma 3.2. *Let $\mathcal{C}$ be a genus 2 hyperelliptic equation over k, and let*

$$r = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(k).$$

Let $E_{\mathcal{C}'}$ be the image of $E_{\mathcal{C}}$ by $\det^{-2}\mathrm{Sym}^6(r)$, and let $\mathcal{C}'$ be the curve with equation $y'^2 = E_{\mathcal{C}'}(x')$. Let $\eta \colon \mathcal{C} \to \mathcal{C}'$ be the isomorphism defined by

$$\eta^{-1}(x', y') = \left(\frac{ax' + c}{bx' + d},\ \frac{(\det r)\, y'}{(bx' + d)^3}\right).$$

Then we have

$$\eta^*\omega(\mathcal{C}') = r^{-t}\omega(\mathcal{C}).$$

Proof. Write $(x, y) = \eta^{-1}(x', y')$. A simple calculation shows that

$$\frac{dx}{y} = (bx' + d)\frac{dx'}{y'} \quad \text{and} \quad \frac{x\,dx}{y} = (ax' + c)\frac{dx'}{y'},$$

so the result follows. □

Corollary 3.3. *Let A be a principally polarized abelian surface over k that is not a product of two elliptic curves, and let ω be a basis of $\Omega^1(A)$. Then there exists a unique hyperelliptic curve equation $\mathcal{C}$ of genus 2 over k such that*

$$\big(\mathrm{Jac}(\mathcal{C}), \omega(\mathcal{C})\big) \simeq (A, \omega).$$

Proof. By Torelli's theorem [26, Appendice], there is a curve equation $\mathcal{C}_0$ over k such that A is isomorphic to $\mathrm{Jac}(\mathcal{C}_0)$. Then ω differs from $\omega(\mathcal{C}_0)$ by a linear transformation in $\mathrm{GL}_2(k)$. By Lemma 3.2, we can make a suitable change of variables to find the correct $\mathcal{C}$. It is unique because every isomorphism between hyperelliptic curves comes from a matrix r as in Lemma 3.2. □

Definition 3.4.

1. Let $\tau \in \mathcal{H}_2$, and assume that $\chi_{10}(\tau) \neq 0$. Then, by Corollary 3.3, there exists a unique hyperelliptic equation $\mathcal{C}(\tau)$ over $\mathbb{C}$ such that

$$\Big(\mathrm{Jac}\big(\mathcal{C}(\tau)\big), \omega\big(\mathcal{C}(\tau)\big)\Big) \simeq \big(A(\tau), \omega(\tau)\big).$$

   We call $\mathcal{C}(\tau)$ the *standard curve* attached to τ. Define the meromorphic functions $a_i(\tau)$ to be the coefficients of $\mathcal{C}(\tau)$:

$$\mathcal{C}(\tau) \,:\, y^2 = \sum_{i=0}^{6} a_i(\tau) x^i.$$

2. Let $t \in \mathcal{H}_1^2$, and assume that $\chi_{10}(H(t)) \neq 0$, where H is the Hilbert embedding. Then, by Corollary 3.3, there exists a unique hyperelliptic equation $\mathcal{C}_K(t)$ over $\mathbb{C}$ such that

$$\Big(\mathrm{Jac}\big(\mathcal{C}_K(t)\big), \omega\big(\mathcal{C}_K(t)\big)\Big) \simeq \big(A_K(t), \omega_K(t)\big).$$

   We call $\mathcal{C}_K(t)$ the *standard curve* attached to t.

Proposition 3.5. *The function $\tau \mapsto \mathcal{C}(\tau)$ is a Siegel modular function of weight $\det^{-2}\mathrm{Sym}^6$ which has no poles on the open set $\{\chi_{10} \neq 0\}$.*

Proof. Over $\mathbb{C}$, the Torelli map is biholomorphic, so this function is clearly meromorphic. By Corollary 3.3, it is defined everywhere on $\{\chi_{10} \neq 0\}$. Combining Proposition 2.1 with Lemma 3.2 shows the transformation rule. □

Finally, for $t \in \mathcal{H}_1^2$, we can relate the standard curves $\mathcal{C}_K(t)$ and $\mathcal{C}\big(H(t)\big)$.

Proposition 3.6. *For every $t \in \mathcal{H}_1^2$, we have*

$$\mathcal{C}_K(t) = \det{}^{-2}\mathrm{Sym}^6(R)\,\mathcal{C}\big(H(t)\big).$$

Proof. Use Proposition 2.16 and Lemma 3.2. □

3.2 Covariants

If f is a Siegel modular form, then we have a map

$$\mathrm{Cov}(f)\colon \mathcal{C} \mapsto f\big(\mathrm{Jac}(\mathcal{C}), \omega(\mathcal{C})\big).$$

We show that $\mathrm{Cov}(f)$ is a covariant of the curve equation. A recent reference for covariants is Mestre's article [29].

Definition 3.7. Let $\rho\colon \mathrm{GL}_2(\mathbb{C}) \to \mathrm{GL}(V)$ be a finite-dimensional holomorphic representation of $\mathrm{GL}_2(\mathbb{C})$. A *covariant*, or *polynomial covariant*, of weight ρ is a map

$$C\colon \mathbb{C}_6[x] \to V$$

which is polynomial in the coefficients, and such that the following transformation rule holds: for every $r \in \mathrm{GL}_2(\mathbb{C})$ and $W \in \mathbb{C}_6[x]$,

$$C\big(\det{}^{-2}\operatorname{Sym}^6(r)\, W\big) = \rho(r)\, C(W).$$

If $\dim V \geq 2$, C is said to be *vector-valued*, and otherwise *scalar-valued*. A *fractional covariant* is a map satisfying the same transformation rule which is only required to have a rational expression in terms of the coefficients.

It is enough to consider covariants of weight $\det^k \operatorname{Sym}^n$ for $k \in \mathbb{Z}$, $n \in \mathbb{N}$. What we call a vector-valued covariant of weight $\det^k \operatorname{Sym}^n$ is in Mestre's paper a covariant of order n and index $k + n/2$; what we call a scalar-valued covariant of weight $\det^k$ is in Mestre's paper an invariant of index k. The reason for this change of terminology is the following.

Proposition 3.8. *If f be a Siegel modular function of weight ρ, then $\mathrm{Cov}(f)$ is a fractional covariant of weight ρ. Conversely, if F is a fractional covariant of weight ρ, then the meromorphic function $\tau \mapsto F\big(\mathcal{C}(\tau)\big)$ is a Siegel modular function of weight ρ. These operations are inverse of each other.*

Proof. $\mathrm{Cov}(f)$ is well defined on a Zariski open set of $\mathbb{C}_6[x]$ and is algebraic, so must have a fractional expression in terms of the coefficients. Let us check the transformation rule. Let $\mathcal{C}$ be a hyperelliptic equation over $\mathbb{C}$, let $r \in \mathrm{GL}_2(\mathbb{C})$, and let $\mathcal{C}'$ be the image of $\mathcal{C}$ under $\det^{-2}\operatorname{Sym}^6(r)$. Then

$$\begin{aligned}
\mathrm{Cov}(f)(\mathcal{C}') &= f\big(\mathrm{Jac}(\mathcal{C}'), \omega(\mathcal{C}')\big) && \text{by definition}\\
&= f\big(\mathrm{Jac}(\mathcal{C}), r^{-t}\omega(\mathcal{C})\big) && \text{by Lemma 3.2}\\
&= \rho(r)\,\mathrm{Cov}(f)(\mathcal{C}).
\end{aligned}$$

This shows that $\mathrm{Cov}(f)$ is a fractional covariant of weight ρ. The converse comes from Proposition 3.5; the rest of the proof is easy and omitted. □

Unlike for Siegel modular forms, the graded $\mathbb{C}$-algebra generated by polynomial covariants is finitely generated.

Theorem 3.9 ([11, p. 296])**.** *The graded $\mathbb{C}$-algebra of covariants has 26 generators defined over $\mathbb{Z}$, where the number of generators of weight $\det^k \operatorname{Sym}^n$ is indicated in the following table:*

$n \setminus k$	-3	-2	-1	0	1	2	3	4	5	6	7	8	9	10	11	15
0						1		1		1				1		1
2						1		1		1	1		1		1	
4				1		1	1		1		1					
6		1		1	1		2									
8		1	1		1											
10			1													
12	1															

We only need to manipulate a small subset of these generators. Take our scalar generators of even weight to be the Igusa–Clebsch invariants I_2, I_4, I_6, I_{10}, in Mestre's notation A', B', C', D' [29], and set

$$I_6' := (I_2 I_4 - 3I_6)/2.$$

Denote by y_1, y_2, y_3 the generators of weights $\det^2 \mathrm{Sym}^2$, $\det^4 \mathrm{Sym}^2$, and $\det^6 \mathrm{Sym}^2$ respectively as defined in Mestre's paper. Finally, the generator of weight $\det^{-2} \mathrm{Sym}^6$, denoted by X, is the degree 6 polynomial itself. All these generators have explicit expressions in terms of the coefficients of the curve.

Proposition 3.8 gives a bijection between Siegel modular *functions* and *fractional* covariants, but we need more. The following theorem establishes a relation between Siegel modular *forms* and *polynomial* covariants, and was first proved in [12, §4].

Theorem 3.10. *Let f be a holomorphic Siegel modular form. Then $\mathrm{Cov}(f)$ is a polynomial covariant. Moreover, if f is a cusp form, then $\mathrm{Cov}(f/\chi_{10})$ is also a polynomial covariant.*

The main difficulty is that nonsingular hyperelliptic equations only form a codimension 1 subset of all degree 6 polynomials. However, if f is a Siegel modular form, then f extends to the so-called toroidal compactification of $\mathcal{A}_2$ by Koecher's principle, and this shows that $\mathrm{Cov}(f)$ is well defined on all curve equations with at most one node. Since this set has codimension 2, the result follows.

3.3 Explicit identifications of Siegel modular forms

We now explain how to compute the polynomial covariant associated with a Siegel modular form whose q-expansion is known up to a certain precision. We start by computing the q-expansion of the standard curve $\mathcal{C}(\tau)$. Recall the Siegel modular form $f_{8,6}$ of weight $\det^8 \mathrm{Sym}^6$ introduced in Example 2.11.

Proposition 3.11. *There is a nonzero constant $\lambda \in \mathbb{C}^\times$ such that*

$$\forall \tau \in \mathcal{H}_2,\ \mathcal{C}(\tau) = \lambda \frac{f_{8,6}(\tau)}{\chi_{10}(\tau)}.$$

Proof. Since $f_{8,6}$ is a cusp form, by Theorem 3.10, $\mathrm{Cov}(f_{8,6}/\chi_{10})$ is a polynomial covariant of weight $\det^{-2} \mathrm{Sym}^6$. By Theorem 3.9, this space of covariants of dimension 1, generated by X. Since both $f_{8,6}/\chi_{10}$ and X are nonzero, we can find $\lambda \in \mathbb{C}^\times$ such that $X = \lambda \,\mathrm{Cov}(f_{8,6}/\chi_{10})$, and the result follows. □

In particular, the q-expansions of the coefficients $a_i(\tau)$ of $\mathcal{C}(\tau)$ are given by

$$\begin{aligned}
a_0(\tau) &= 4\lambda\frac{(q_2-1)^2}{q_2}(q_3+\cdots)\\
a_1(\tau) &= 12\lambda\frac{(q_2-1)(q_2+1)}{q_2}(q_3+\cdots)\\
a_2(\tau) &= \lambda\big(-1+12(q_2+q_2^{-1})q_3+\cdots\big)\\
a_3(\tau) &= 2\lambda\frac{q_2+1}{q_2-1}\big(-1+2(q_2-2+q_2^{-1})(q_1+q_3)+\cdots\big)\\
a_4(\tau) &= \lambda\big(-1+12(q_2+q_2^{-1})q_1+\cdots\big)\\
a_5(\tau) &= 12\lambda\frac{(q_2-1)(q_2+1)}{q_2}(q_1+\cdots)\\
a_6(\tau) &= 4\lambda\frac{(q_2-1)^2}{q_2}(q_1+\cdots),
\end{aligned}$$

where we listed all terms with total degree in q_1, q_3 at most 1.

Given a Siegel modular form f of weight ρ whose q-expansion can be computed, the following algorithm recovers the expression of $\mathrm{Cov}(f)$ up to a power of λ in terms of the coefficients of the curve.

Algorithm 3.12.
1. Compute a basis $\mathcal{B}$ of the vector space of polynomial covariants of weight ρ using Theorem 3.9.
2. Choose a precision ν.
3. Compute the q-expansion of f modulo (q_1^ν, q_3^ν).
4. For every $B \in \mathcal{B}$, compute the q-expansion of the Siegel modular function $\tau \mapsto B\big(\mathcal{C}(\tau)\big)$ using Proposition 3.11.
5. Do linear algebra; if the matrix does not have full rank, go back to step 3 with a larger ν.

Remark 3.13. Sturm-type bounds [10] provide a theoretical limit for the precision ν that we need to consider; for the examples given in this article, $\nu = 3$ is enough.

Algorithm 3.12 allows us to recover, up to a multiplicative constant, the well known formulæ for scalar-valued forms.

Theorem 3.14 ([23])**.** *We have*

$$\begin{aligned}
4\ \mathrm{Cov}(\psi_4) &= I_4,\\
4\ \mathrm{Cov}(\psi_6) &= I_6',\\
-2^{14}\ \mathrm{Cov}(\chi_{10}) &= I_{10},\\
2^{17}\cdot 3\ \mathrm{Cov}(\chi_{12}) &= I_2 I_{10}.
\end{aligned}$$

Therefore, the Igusa invariants are given by

$$\mathrm{Cov}(j_1) = \frac{I_4 I_6'}{I_{10}}, \quad \mathrm{Cov}(j_2) = \frac{I_2 I_4^2}{I_{10}}, \quad \mathrm{Cov}(j_3) = \frac{I_4^5}{I_{10}^2}.$$

We now apply Algorithm 3.12 to derivatives of Igusa invariants. Recall from Proposition 2.10 that for $1 \le k \le 3$, the partial derivative

$$\frac{dj_k}{d\tau} := \frac{\partial j_k}{\partial \tau_1} x^2 + \frac{\partial j_k}{\partial \tau_2} x + \frac{\partial j_k}{\partial \tau_3}$$

is a Siegel modular function of weight Sym^2.

Theorem 3.15. *There is a nonzero constant $\mu \in \mathbb{C}^\times$ such that the following equalities hold:*

$$\begin{aligned}
\mathrm{Cov}\Big(\frac{dj_1}{d\tau}\Big) &= \frac{\mu}{I_{10}}\Big(\frac{153}{8} I_2^2 I_4 y_1 - \frac{135}{2} I_2 I_6 y_1 + \frac{135}{2} I_4^2 y_1 + \frac{46575}{4} I_2 I_4 y_2 \\
&\qquad - 30375\, I_6 y_2 + 1366875\, I_4 y_3\Big), \\
\mathrm{Cov}\Big(\frac{dj_2}{d\tau}\Big) &= \frac{\mu}{I_{10}}\big(90\, I_2^2 I_4 y_1 + 900\, I_2^2 y_1 + 40500\, I_2 I_4 y_2\big), \\
\mathrm{Cov}\Big(\frac{dj_3}{d\tau}\Big) &= \frac{\mu}{I_{10}^2}\big(225\, I_2 I_4^4 y_1 + 101250\, I_4^4 y_2\big).
\end{aligned}$$

Proof. Let $1 \le k \le 3$. By Definition 2.8, $\chi_{10}^2 j_k$ has no poles on $\mathcal{A}_2$. Therefore, the Siegel modular function

$$f_k = \chi_{10}^3 \frac{dj_k}{d\tau}$$

is holomorphic on $\mathcal{A}_2$. Its q-expansion can be computed from the q-expansion of j_k by formal differentiation. Since, up to scalar,

$$\frac{\partial}{\partial \tau_i} = q_i \frac{\partial}{\partial q_i}$$

for $1 \le i \le 3$, we check that f_k is a cusp form. Therefore, by Theorem 3.10, $\mathrm{Cov}(f_k/\chi_{10})$ is a polynomial covariant of weight $\det^{20} \mathrm{Sym}^2$. Looking at the table in Theorem 3.9, we find that a basis of this space of covariants is given by covariants of the form Iy where $y \in \{y_1, y_2, y_3\}$ and I is a scalar-valued covariant of the appropriate even weight. Algorithm 3.12 succeeds with $p = 3$; the computations were done using Pari/GP [41]. □

Remark 3.16. Theorems 3.14 and 3.15 can be checked numerically. Computing big period matrices of hyperelliptic curves [36] provides pairs $\big(\tau, \mathcal{C}(\tau)\big)$ with $\tau \in \mathcal{H}_2$. We can evaluate Igusa invariants at a given τ to high precision, using their expression in terms of theta functions [16]. Therefore we can also evaluate their derivatives numerically with a high precision and compute the associated covariant using floating-point linear algebra. The computations were done using the libraries `hcperiods` [35] and `cmh` [18].

Such numerical computations do not provide a proof of Theorem 3.15, unless we show that the coefficients are rational numbers with bounded denominators, but they provide a nice consistency check.

Remark 3.17. From Theorem 3.15, we can easily obtain similar formulæ for derivatives of other invariants, as soon as their algebraic expression in terms of Igusa invariants is known (or the other way around): differentiating this algebraic expression yields a linear relation between derivatives.

It is convenient to introduce a matrix notation.

Definition 3.18. For $\tau \in \mathcal{H}_2$, we define

$$\Big(\frac{dj}{d\tau}\Big)(\tau) = \left(\frac{\partial j_k}{\partial \tau_l}(\tau)\right)_{1\le k,l\le 3}$$

and we denote by

$$\mathcal{C} \mapsto \Big(\frac{dj}{d\tau}\Big)(\mathcal{C})$$

the associated fractional covariant.

Proposition 3.19. *Let $\mathcal{C}$ be a genus 2 hyperelliptic equation over $\mathbb{C}$. Choose $\tau \in \mathcal{H}_2$ and $r \in \mathrm{GL}_2(\mathbb{C})$ such that there is an isomorphism*

$$\big(\mathrm{Jac}(\mathcal{C}), \omega(\mathcal{C})\big) \simeq \big(A(\tau), r\,\omega(\tau)\big).$$

Then

$$\Big(\frac{dj}{d\tau}\Big)(\mathcal{C}) = \Big(\frac{dj}{d\tau}\Big)(\tau) \cdot \mathrm{Sym}^2(r^{-t})^t$$

where the right hand side is a multiplication of 3×3 matrices.

Proof. By Proposition 2.10, each $dj_k/d\tau$ has weight Sym^2; the result follows with an easy matrix calculation. □

Theorem 3.15 expresses the entries of $\Big(\frac{dj}{d\tau}\Big)(\mathcal{C})$ up to a constant in terms of the coefficients of $\mathcal{C}$.

3.4 Explicit identification of Hilbert modular forms

Similarly, we can express Hilbert modular forms in terms of coefficients of suitable hyperelliptic equations. Let k be a field, and choose a value of $\sqrt{\Delta}$ in k; this defines a morphism $\mathbb{Z}_K \to k$.

Definition 3.20. Let $\mathcal{C}$ be a genus 2 hyperelliptic equation over k with real multiplication $\iota\colon \mathbb{Z}_K \hookrightarrow \mathrm{End}^{\mathrm{sym}}\big(\mathrm{Jac}(\mathcal{C})\big)$. We say that $\mathcal{C}$ has *diagonal real endomorphisms* if for every $\alpha \in \mathbb{Z}_K$, the matrix of $\iota(\alpha)^*$ in the basis $\omega(\mathcal{C})$ is diagonal.

This definition is independent of the choice of real multiplication embedding.

Definition 3.21. Let $\mathcal{C}$ be a hyperelliptic equation of genus 2 over k, and assume that $\mathcal{C}$ has diagonal real endomorphisms. Then we define the real multiplication embedding

$$\iota(\mathcal{C})\colon \mathbb{Z}_K \hookrightarrow \mathrm{End}^{\mathrm{sym}}\big(\mathrm{Jac}(\mathcal{C})\big)$$

to be such that

$$\forall \alpha \in \mathbb{Z}_K,\ \iota(\mathcal{C})(\alpha)^* = \mathrm{Diag}(\alpha, \overline{\alpha}) \quad \text{in the basis } \omega(\mathcal{C}).$$

If $\mathcal{C}'$ is the curve obtained from $\mathcal{C}$ after the change of variables $x \mapsto 1/x$, then $\mathcal{C}'$ also has diagonal real endomorphisms, and $\iota(\mathcal{C}')$ is the conjugate of $\iota(\mathcal{C})$.

If $\mathcal{C}$ has diagonal real endomorphisms, then $\big(\mathrm{Jac}(\mathcal{C}), \iota(\mathcal{C}), \omega(\mathcal{C})\big)$ is Hilbert-normalized as in Definition 2.15. Therefore, it makes sense to evaluate Hilbert modular forms in terms of coefficients of $\mathcal{C}$. We only use derivatives of Igusa invariants; as above, we introduce a matrix notation.

Definition 3.22. For $t \in \mathcal{H}_2$, we define

$$\Big(\frac{dj}{dt}\Big)(\tau) = \left(\frac{\partial j_k}{\partial t_l}(\tau)\right)_{1\le k\le 3, 1\le l\le 2}$$

and we denote by

$$\mathcal{C} \mapsto \Big(\frac{dj}{dt}\Big)(\mathcal{C})$$

the associated fractional covariant on curves with diagonal endomorphisms.

Proposition 3.23. *Let $\mathcal{C}$ be a genus 2 hyperelliptic equation over $\mathbb{C}$ with diagonal real endomorphisms. Choose $t \in \mathcal{H}_1^2$ and a diagonal matrix $r \in \mathrm{GL}_2(\mathbb{C})$ such that there is an isomorphism*

$$\big(\mathrm{Jac}(\mathcal{C}), \iota(\mathcal{C}), \omega(\mathcal{C})\big) \simeq \big(A_K(t), \iota_K(t), r\,\omega_K(t)\big).$$

Then

$$\Big(\frac{dj}{dt}\Big)(\mathcal{C}) = \Big(\frac{dj}{dt}\Big)(t) \cdot r^{-2}.$$

Proof. By Proposition 2.14, derivatives with respect to t_1 and t_2 are Hilbert modular functions of weight $(2,0)$ and $(0,2)$ respectively. □

Proposition 3.24. *Let $\mathcal{C}$ be a hyperelliptic equation of genus 2 over k with diagonal real endomorphisms. Then*

$$\Big(\frac{dj}{dt}\Big)(\mathcal{C}) = \Big(\frac{dj}{d\tau}\Big)(\mathcal{C}) \cdot T \qquad \textit{where}\ \ T = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Proof. It is sufficient to prove this over $\mathbb{C}$. Let $t \in \mathcal{H}_1^2$ such that

$$\big(\mathrm{Jac}(\mathcal{C}), \iota(\mathcal{C}), \omega(\mathcal{C})\big) \simeq \big(A(t), \iota, r\,\omega(t)\big)$$

where r is a diagonal matrix. Write $\tau = H(t)$. By Proposition 2.16, we have

$$\big(\mathrm{Jac}(\mathcal{C}), \omega(\mathcal{C})\big) \simeq \big(A(\tau), rR^{-t}\omega(\tau)\big).$$

Using the expression of the Hilbert embedding, we compute that

$$\Big(\frac{dj}{dt}\Big)(t) = \Big(\frac{dj}{d\tau}\Big)(\tau) \cdot \mathrm{Sym}^2(R)^t \cdot T.$$

Therefore

$$\begin{aligned}
\Big(\frac{dj}{dt}\Big)(\mathcal{C}) &= \Big(\frac{dj}{dt}\Big)(t) \cdot r^{-2} && \text{by 3.23} \\
&= \Big(\frac{dj}{d\tau}\Big)(\tau) \cdot \mathrm{Sym}^2(R)^t \cdot T \cdot r^{-2} \\
&= \Big(\frac{dj}{d\tau}\Big)(\mathcal{C}) \cdot \mathrm{Sym}^2(R^{-1}r)^t \cdot \mathrm{Sym}^2(R)^t \cdot T \cdot r^{-2} && \text{by 3.19} \\
&= \Big(\frac{dj}{d\tau}\Big)(\mathcal{C}) \cdot T. && \square
\end{aligned}$$

It is natural that the matrix R defining the Hilbert embedding does not appear in Proposition 3.24: evaluating derivatives of Igusa invariants on a curve has an intrinsic interpretation in terms of the Kodaira–Spencer isomorphism, and the choice of Hilbert embedding does not matter. Proposition 3.24 and Theorem 3.15 give an explicit expression of the fractional covariant

$$\mathcal{C} \mapsto \Big(\frac{dj}{dt}\Big)(\mathcal{C})$$

on curves with diagonal real endomorphisms.

4 Description of the algorithm

4.1 Input and output

Let k be a field, and let $\mathcal{J}$, $\mathcal{J}'$ be Jacobians of genus 2 curves over k. Assume that we are in one of the two following cases:

- The *Siegel case*: $\mathcal{J}$ and $\mathcal{J}'$ are ℓ-isogenous, where $\ell \in \mathbb{Z}$ is a prime.
- The *Hilbert case*: $\mathcal{J}$ and $\mathcal{J}'$ have real multiplication by $\mathbb{Z}_K$ where K is a real quadratic field, and are β-isogenous, where β is a totally positive prime element of $\mathbb{Z}_K$.

In the Hilbert case, we fix a morphism $\mathbb{Z}_K \to k$. The input of the isogeny algorithm consists of

- The Igusa invariants of $\mathcal{J}$ and $\mathcal{J}'$ in k, denoted by (j_1, j_2, j_3) and (j'_1, j'_2, j'_3) respectively.
- An algorithm EV that evaluates derivatives of Siegel modular equations of level ℓ (resp. Hilbert modular equations of level β) at a given point over k, within $C_{\mathrm{ev}}(\ell)$ (resp. $C_{\mathrm{ev}}(\beta)$) operations in k.

In particular, in the Hilbert case, the real multiplication embeddings are not part of the input. The choice is made during the algorithm; depending on it, we compute either a β- or a $\overline{\beta}$-isogeny. In the algorithm, we have to make genericity assumptions on $\mathcal{J}$ and $\mathcal{J}'$.

In order to describe the output, we explain how to describe an isogeny explicitly. Let $\mathcal{C}$, $\mathcal{C}'$ be hyperelliptic equations over k such that $\mathcal{J} \simeq \mathrm{Jac}(\mathcal{C})$ and $\mathcal{J}' \simeq \mathrm{Jac}(\mathcal{C}')$. Choose a base point P on $\mathcal{C}$. This gives an embedding

$$\eta_P : \mathcal{C} \hookrightarrow \mathrm{Jac}(\mathcal{C}), \quad Q \mapsto [Q - P].$$

By [34, §5], $\mathrm{Jac}(\mathcal{C}')$ is birationally equivalent to the symmetric square ${\mathcal{C}'}^{2,\mathrm{sym}}$.

Proposition 4.1. *There is a unique morphism φ_P making the following diagram commute:*

$$\begin{array}{ccccc} & \overset{\varphi_P}{\nearrow} & & & {\mathcal{C}'}^{2,\mathrm{sym}} \\ & & & & \downarrow \wr \\ \mathcal{C} & \xrightarrow{\eta_P} & \mathrm{Jac}(\mathcal{C}) & \xrightarrow{\varphi} & \mathrm{Jac}(\mathcal{C}'). \end{array}$$

Proof. The compositum of the other arrows is a rational map. It extends to a morphism since $\mathcal{C}$ is a smooth curve and ${\mathcal{C}'}^{2,\mathrm{sym}}$ is proper. □

Consider the coordinates on ${\mathcal{C}'}^{2,\mathrm{sym}}$ given by

$$s = x_1 + x_2, \quad p = x_1 x_2, \quad q = y_1 y_2, \quad r = \frac{y_2 - y_1}{x_2 - x_1}$$

as expressed at an unordered pair of points $\{(x_1, y_1), (x_2, y_2)\}$ on $\mathcal{C}'$.

Definition 4.2. We call the tuple (s, p, q, r) of rational fractions describing φ_P the *rational expression of φ at the base point P*.

This representation was introduced in [14], and the representation of φ as a correspondence is easily derived from it.

The output of the isogeny algorithm consists of

- Curve equations $\mathcal{C}$, $\mathcal{C}'$ over a quadratic extension k'/k such that

$$\mathrm{Jac}(\mathcal{C}) \simeq \mathcal{J} \quad \text{and} \quad \mathrm{Jac}(\mathcal{C}') \simeq \mathcal{J}'.$$

- A base point $P \in \mathcal{C}(k')$.
- The rational expression (s, p, q, r) of $\pm\varphi$ at the base point P.

A key step in the algorithm is to compute the action of the isogeny φ on differential forms.

Definition 4.3. Let $\omega(\mathcal{C})$, $\omega(\mathcal{C}')$ be the bases of differential forms associated with the hyperelliptic equations $\mathcal{C}$, $\mathcal{C}'$. The *normalization matrix* of φ with respect to these curve equations is the unique matrix $m \in \mathrm{GL}_2(\overline{k})$ such that

$$\varphi^* \omega(\mathcal{C}') = m\, \omega(\mathcal{C}).$$

To compute the normalization matrix m of φ, we use the results from §3 about modular forms and covariants, as well as the evaluation algorithm EV. In the Hilbert case, we need the curve equations to have diagonal real endomorphisms. The algorithm runs as follows:

1. (§4.2) Reconstruct suitable curve equations $\mathcal{C}$ and $\mathcal{C}'$ over k'.
2. (§4.3) Compute the normalization matrix of φ.
3. (§4.4) Choose a base point P on $\mathcal{C}$ and compute φ_P locally around P by solving a differential system.
4. (§4.5) Recover the rational expression for φ at P from this local data.

In §4.6, we summarize the algorithm and prove Theorem 1.1.

Remark 4.4. Using other invariants as in Remark 2.25 would allow us to compute ℓ- or β-isogenies to, or from, products of two elliptic curves. In the algorithm, step 2 remains the same modulo the change of invariants as in Remark 3.17. However, we have to choose another explicit description to the isogeny, and the differential system changes accordingly.

4.2 Constructing suitable curve equations

In this subsection, we assume that we are in the Hilbert case; in the Siegel case, all curve equations will do in the rest of the algorithms, so it is sufficient to apply Mestre's algorithm [29].

Proposition 4.5. *Let $\mathcal{C}$ be a hyperelliptic curve equation of genus 2 over k with real multiplication by $\mathbb{Z}_K$. Denote its Igusa invariants by (j_1, j_2, j_3). Then the curve $\mathcal{C}$ has diagonal real endomorphisms if and only if the two columns of the 3×2 matrix*

$$\left(\frac{dj}{d\tau}\right)(\mathcal{C}) \cdot T \qquad \text{where } T = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix}$$

define tangent vectors to the Humbert surface at (j_1, j_2, j_3).

Proof. We can assume that $k = \mathbb{C}$. Let $t \in \mathcal{H}_1^2$ such that $\mathrm{Jac}(\mathcal{C})$ is isomorphic to $A_K(t)$, and write $\tau = H(t)$. Let $r \in \mathrm{GL}_2(\mathbb{C})$ such that

$$\omega(\mathcal{C}) = r\,\omega(t) = rR^{-t}\,\omega(\tau).$$

By Proposition 3.19, we have

$$\left(\frac{dj}{d\tau}\right)(\mathcal{C}) \cdot T = \left(\frac{dj}{d\tau}\right)(\tau) \cdot \mathrm{Sym}^2(r^{-t}R)^t \cdot T.$$

We compute that the two columns of this matrix contain the derivatives of Igusa invariants along the two directions in $\mathcal{H}_2$ given by

$$R^t r^{-1} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} r^{-t} R \quad \text{and} \quad R^t r^{-1} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} r^{-t} R.$$

These directions are tangent to the image of H if and only if r is is either diagonal or anti-diagonal. This ends the proof. □

Assume that the equation of the Humbert surface for K in terms of Igusa invariants is given: this precomputation depends only on K. Given Igusa invariants (j_1, j_2, j_3) on the Humbert surface, the algorithm to reconstruct a curve equation with diagonal real endomorphisms runs as follows.

Algorithm 4.6.
1. Reconstruct any curve equation $\mathcal{C}_0$ with Igusa invariants (j_1, j_2, j_3) using Mestre's algorithm.
2. Find $r \in \mathrm{GL}_2(\bar{k})$ such that the two columns of the matrix
$$\Big(\frac{dj}{d\tau}\Big)(\mathcal{C}) \cdot \mathrm{Sym}^2(r)^t \cdot T$$
are tangent to the Humbert surface at (j_1, j_2, j_3).
3. Output $\det^{-2} \mathrm{Sym}^6(r)\mathcal{C}_0$.

Proposition 4.7. *Algorithm 4.6 costs $O_K(1) + O(C_{\mathrm{sqrt}})$ operations in k. The output is a curve equation with diagonal real endomorphisms, defined over a quadratic extension k'/k.*

Proof. Mestre's algorithm costs $O(1)$ operations in k, and returns a curve equation defined over k. In step 2, if a, b, c, d denote the entries of r, we have to solve a quadratic equation in a, c, and a quadratic equation in b, d; this can be done in $O(C_{\mathrm{sqrt}})$ operations in k, and the output is defined over a quadratic extension. By Proposition 3.19, we have
$$\Big(\frac{dj}{d\tau}\Big)(\mathcal{C}) = \Big(\frac{dj}{d\tau}\Big)(\mathcal{C}_0) \cdot \mathrm{Sym}^2(m)^t,$$
hence the output is valid by Proposition 4.5. □

4.3 Computing the normalization matrix

Let $\mathcal{C}$, $\mathcal{C}'$ be hyperelliptic curve equations over k such that
$$\mathrm{Jac}(\mathcal{C}) \simeq \mathcal{J} \quad \text{and} \quad \mathrm{Jac}(\mathcal{C}') \simeq \mathcal{J}'.$$
In the Siegel case, we have an ℓ-isogeny
$$\varphi\colon \mathrm{Jac}(\mathcal{C}) \to \mathrm{Jac}(\mathcal{C}').$$
In the Hilbert case, we assume that $\mathcal{C}$ and $\mathcal{C}'$ have diagonal real endomorphisms. For simplicity, we assume that the real multiplication embeddings of $\mathrm{Jac}(\mathcal{C})$ and $\mathrm{Jac}(\mathcal{C}')$ are compatible under the φ. Then
$$\varphi\colon \big(\mathrm{Jac}(\mathcal{C}), \iota(\mathcal{C})\big) \to \big(\mathrm{Jac}(\mathcal{C}'), \iota(\mathcal{C}')\big).$$

is either a β- or a $\overline{\beta}$-isogeny. Let m be the normalization matrix of φ with respect to the curve equations $\mathcal{C}$, $\mathcal{C}'$.

Write Φ_1, Φ_2, Φ_3 for the Siegel modular equations of level ℓ (resp. the Hilbert modular equations of level β) in Igusa invariants, and consider them as elements in the ring $\mathbb{Q}(J_1, J_2, J_3)[J_1', J_2', J_3']$. Define

$$D\Phi_L = \left(\frac{\partial \Phi_n}{\partial J_k}\right)_{1\le n,k\le 3} \quad \text{and} \quad D\Phi_R = \left(\frac{\partial \Phi_n}{\partial J_k'}\right)_{1\le n,k\le 3}.$$

Write j as a shorthand for the Igusa invariants (j_1, j_2, j_3) of $\mathrm{Jac}(\mathcal{C})$, and j' for the invariants (j_1', j_2', j_3') of $\mathrm{Jac}(\mathcal{C}')$. We now state our genericity hypothesis on $\mathcal{J}$ and $\mathcal{J}'$.

Definition 4.8. We say that $\mathcal{J}$ and $\mathcal{J}'$ are *generic* if the following conditions are satisfied:

- The denominators of modular equations do not vanish at j.
- The 3×3 matrices $D\Phi_L(j, j')$, $D\Phi_R(j, j')$, $\left(\frac{dj}{d\tau}\right)(\mathcal{C})$ and $\left(\frac{dj}{d\tau}\right)(\mathcal{C}')$ are invertible.

This definition does not depend on the choice of the equations $\mathcal{C}$ and $\mathcal{C}'$; by Propositions 2.9 and 2.20, the conditions above indeed hold on an open set of the moduli space.

Proposition 4.9. *Assume that $\mathcal{J}$, $\mathcal{J}'$ are generic in the sense of Definition 4.8.*

1. *In the Siegel case, we have*

$$D\Phi_L(j, j') \cdot \left(\frac{dj}{d\tau}\right)(\mathcal{C}) = \frac{-1}{\ell} D\Phi_R(j, j') \cdot \left(\frac{dj}{d\tau}\right)(\mathcal{C}') \cdot \mathrm{Sym}^2(m^t)^t.$$

2. *In the Hilbert case, m is diagonal, and we have*

$$D\Phi_L(j, j') \cdot \left(\frac{dj}{dt}\right)(\mathcal{C}) = -D\Phi_R(j, j') \cdot \left(\frac{dj}{dt}\right)(\mathcal{C}') \cdot \mathrm{Diag}(1/\zeta, 1/\overline{\zeta}) \cdot m^2$$

with $\zeta = \beta$ or $\zeta = \overline{\beta}$ depending on whether φ is a β- or a $\overline{\beta}$-isogeny.

Proof. We can assume that $k = \mathbb{C}$.

1. *The Siegel case.* By Proposition 2.23, we can find $\tau \in \mathcal{H}_2$ such that there is a commutative diagram

$$\begin{array}{ccc} \mathrm{Jac}(\mathcal{C}) & \xrightarrow{\varphi} & \mathrm{Jac}(\mathcal{C}') \\ \downarrow \wr & & \downarrow \wr \\ A(\tau) & \xrightarrow{z \mapsto z} & A(\tau/\ell). \end{array}$$

Let r, $r' \in \mathrm{GL}_2(\mathbb{C})$ be such that

$$\omega(\mathcal{C}) = r\, \eta^* \omega(\tau), \quad \omega(\mathcal{C}') = r'\, \eta'^* \omega(\tau/\ell).$$

Then we have $m = r'r^{-1}$.

By the definition of modular equations, we have

$$\Phi_n\big(j_1(\tau), j_2(\tau), j_3(\tau), j_1(\tau/\ell), j_2(\tau/\ell), j_3(\tau/\ell)\big) = 0 \quad \text{for } 1 \le n \le 3.$$

Differentiating this equation with respect to τ_1, τ_2, τ_3 gives three linear relations between derivatives; in matrix notation, we obtain

$$D\Phi_L(j, j') \cdot \Big(\frac{dj}{d\tau}\Big)(\tau) + \frac{1}{\ell} D\Phi_R(j, j') \cdot \Big(\frac{dj}{d\tau}\Big)(\tau/\ell) = 0.$$

By Proposition 3.19, we have

$$\Big(\frac{dj}{d\tau}\Big)(\tau) = \Big(\frac{dj}{d\tau}\Big)(\mathcal{C}) \cdot \mathrm{Sym}^2(r^t)^t, \quad \Big(\frac{dj}{d\tau}\Big)(\tau/\ell) = \Big(\frac{dj}{d\tau}\Big)(\mathcal{C}') \cdot \mathrm{Sym}^2(r'^t)^t$$

so the result follows.

2. *The Hilbert case.* Without loss of generality, we can assume that φ is a β-isogeny. By Proposition 2.23, we can find $t \in \mathcal{H}_1^2$ such that there is a commutative diagram

$$\begin{array}{ccc} \big(\mathrm{Jac}(\mathcal{C}), \iota(\mathcal{C})\big) & \xrightarrow{\varphi} & \big(\mathrm{Jac}(\mathcal{C}'), \iota(\mathcal{C}')\big) \\ \downarrow\wr & & \downarrow\wr \\ \big(A_K(t), \iota_K(t)\big) & \xrightarrow{z \mapsto z} & \big(A_K(t/\beta), \iota_K(t/\beta)\big). \end{array}$$

Let r, $r' \in \mathrm{GL}_2(\mathbb{C})$ be such that

$$\omega(\mathcal{C}) = r\, \eta^* \omega(\tau), \quad \omega(\mathcal{C}') = r'\, \eta'^* \omega(\tau/\beta).$$

Since $\big(\mathrm{Jac}(\mathcal{C}), \iota(\mathcal{C})\big)$ and $\big(\mathrm{Jac}(\mathcal{C}'), \iota(\mathcal{C}')\big)$ are Hilbert-normalized, the matrices r, r' are diagonal. We have $m = r'r^{-1}$.

Differentiating the modular equations with respect to t_1, t_2, we obtain

$$D\Phi_L(j, j') \cdot \Big(\frac{dj}{dt}\Big)(t) + D\Phi_R(j, j') \cdot \Big(\frac{dj}{dt}\Big)(\tau/\beta) \cdot \mathrm{Diag}(1/\beta, 1/\overline{\beta}) = 0$$

By Proposition 3.23, we have

$$\Big(\frac{dj}{dt}\Big)(t) = \Big(\frac{dj}{dt}\Big)(\mathcal{C}) \cdot r^2, \quad \Big(\frac{dj}{dt}\Big)(t/\beta) = \Big(\frac{dj}{dt}\Big)(\mathcal{C}') \cdot r'^2$$

and the result follows. □

Remark 4.10. These computations can be interpreted as follows. Fixing a basis of differential forms on A defines a basis of $\mathrm{Sym}^2(\Omega^1(A))$. Hence, by the Kodaira–Spencer isomorphism, it defines a basis for the tangent space of $\mathcal{A}_2$ at A. In other words, it defined a deformation of A over the ring $k[\varepsilon_1, \varepsilon_2, \varepsilon_3]/(\varepsilon_1^2 = \varepsilon_2^2 = \varepsilon_3^2 = 0)$. Differentiation shows that the modular equations are satisfied *over* $k[\varepsilon_1, \varepsilon_2, \varepsilon_3]$ if and only if the normalization matrix has the standard form $\mathrm{Diag}(\ell, \ell)$ or $\mathrm{Diag}(\beta, \overline{\beta})$. Proposition 4.9 allows to deduce the normalization matrix from the *defect* of being isogenous over $k[\varepsilon_1, \varepsilon_2, \varepsilon_3]$.

Given $\mathcal{C}$ and $\mathcal{C}'$, and assuming genericity in the sense of Definition 4.8, the following algorithms allow us to compute the normalization matrix m of $\pm\varphi$. In the Hilbert case, we find a list of four possible candidates.

Algorithm 4.11 (Siegel case)**.**

1. Use Theorem 3.15 to compute $\left(\frac{dj}{d\tau}\right)(\mathcal{C})$ and $\left(\frac{dj}{d\tau}\right)(\mathcal{C}')$ up to the same constant λ.
2. Compute $D\Phi_L(j, j')$ and $D\Phi_R(j, j')$ using the evaluation algorithm EV.
3. Compute $\mathrm{Sym}^2(m^t)$ using Proposition 4.9; note that λ disappears.
4. Deduce m up to sign using the fact that

$$\mathrm{Sym}^2\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \begin{pmatrix} a^2 & 2ab & b^2 \\ ac & ad+bc & bd \\ c^2 & 2cd & d^2 \end{pmatrix}.$$

Algorithm 4.12 (Hilbert case)**.**

1. Use Theorem 3.15 and Proposition 3.24 to compute $\left(\frac{dj}{dt}\right)(\mathcal{C})$, $\left(\frac{dj}{dt}\right)(\mathcal{C}')$ up to the same constant λ.
2. Compute $D\Phi_L(g, g')$ and $D\Phi_R(g, g')$ using the evaluation algorithm EV.
3. Compute two candidates for m^2 using Proposition 4.9; by the genericity hypothesis and Proposition 3.24, the 3×2 matrices that appear there have full rank.
4. Extract square roots of the entries to obtain four candidates $m_{\beta,\pm}$, $m_{\overline{\beta},\pm}$ for the normalization matrix of φ up to sign.

In Algorithm 4.12, if the real multiplication embeddings $\iota(\mathcal{C})$ and $\iota(\mathcal{C}')$ are not compatible under φ, then we find an antidiagonal matrix in step 3. We can make the change of variables $x \mapsto 1/x$ in either $\mathcal{C}$ or $\mathcal{C}'$ to come back to diagonal matrices. The cost estimate is immediate.

Proposition 4.13. *Algorithms 4.11 and 4.12 cost respectively* $O\big(C_{\mathrm{ev}}(\ell)+C_{\mathrm{sqrt}}\big)$ *and* $O\big(C_{\mathrm{ev}}(\beta)+C_{\mathrm{sqrt}}\big)$ *operations in* k*. Their output is defined over a quadratic extension* k'/k*.*

Remark 4.14. The algorithms presented in this section are easy to adapt to other models of modular equations using Remark 3.17. If we use nonsymmetric invariants in the Hilbert case, then giving invariants also encodes a choice of real multiplication embedding; if we are able to reconstruct curve equations with the correct real multiplication embedding, then the uncertainty between β and $\overline{\beta}$ in Algorithm 4.12 disappears.

4.4 Solving the differential system

We now want to compute the rational representation of $\varphi_P \colon \mathcal{C} \to \mathcal{C}'^{2,\mathrm{sym}}$, for some base point P on $\mathcal{C}(k)$, knowing the normalization matrix m of φ. Let k be a common field of definition for $\mathcal{C}$, $\mathcal{C}'$, P and m. We write a differential system satisfied by φ_P, which we solve locally around P using power series.

Step 1: choosing the power series. Up to a change of variables, we can assume that P is not a point at infinity. Since $\varphi_P(P)$ is the zero point in $\mathrm{Jac}(\mathcal{C}')$, it must be of the form

$$\varphi_P(P) = \{Q, i(Q)\}$$

for some $Q \in \mathcal{C}'$, where i denotes the hyperelliptic involution. We say that φ_P is of *Weierstrass type* if Q is a Weierstrass point of $\mathcal{C}'$, and of *generic type* otherwise.

Lemma 4.15. *Let z be a uniformizer of $\mathcal{C}$ at P.*

1. *If φ_P is of generic type, then there is a local lift*

$$\begin{array}{ccc} \operatorname{Spec} k'[[z]] & \xrightarrow{(x_1,y_1),(x_2,y_2)} & \mathcal{C}'^2 \\ \downarrow & & \downarrow \\ \mathcal{C} & \xrightarrow{\varphi_P} & \mathcal{C}'^{2,\mathrm{sym}}. \end{array}$$

   for some suitable quadratic extension k' of k.

2. *If φ_P is of Weierstrass type, then such a lift exists if we replace $k[[z]]$ by $k'[[\sqrt{z}]]$ for some suitable quadratic extension k'/k.*

Proof. There is a degree 2 covering $\mathcal{C}'^2 \to \mathcal{C}'^{2,\mathrm{sym}}$; it is étale at $\big(Q, i(Q)\big)$ when φ_P is of generic type. The completed local ring of $\mathcal{C}$ at P is $k[[z]]$, so the result comes from the two following facts:

1. Eevery unramified extension of degree 2 of $k[[z]]$ is contained in $k'[[z]]$ for some quadratic extension k' of k;
2. Every extension of degree 2 of $k[[z]]$ of $\mathcal{C}$ at P is contained in $k'[[\sqrt{z}]]$ for some quadratic extension k' of k. □

Write the equations $\mathcal{C}$, $\mathcal{C}'$ and the normalization matrix as

$$\mathcal{C} \,:\, v^2 = E_{\mathcal{C}}(u), \quad \mathcal{C}' \,:\, y^2 = E_{\mathcal{C}'}(x), \quad m = \begin{pmatrix} m_{1,1} & m_{1,2} \\ m_{2,1} & m_{2,2} \end{pmatrix}.$$

Then, the power series (x_1, y_1), (x_2, y_2) from Lemma 4.15 satisfy the differential system

$$\left\{ \begin{array}{rcl} \dfrac{x_1\,dx_1}{y_1} + \dfrac{x_2\,dx_2}{y_2} & = & (m_{1,1}u + m_{1,2})\dfrac{du}{v} \\ \dfrac{dx_1}{y_1} + \dfrac{dx_2}{y_2} & = & (m_{2,1}u + m_{2,2})\dfrac{du}{v} \\ y_1^2 = E_{\mathcal{C}'}(x_1) & & \\ y_2^2 = E_{\mathcal{C}'}(x_2) & & \end{array} \right. \tag{S}$$

We can complete Lemma 4.15 as follows.

Lemma 4.16. *Assume that φ_P is of Weierstrass type, and that P is a Weierstrass point on $\mathcal{C}$. Then there is a local lift*

$$\begin{array}{ccc} \operatorname{Spec} k'[[z]] & \xrightarrow{(x_1,y_1),(x_2,y_2)} & \mathcal{C}'^2 \\ \downarrow & & \downarrow \\ \mathcal{C} & \xrightarrow{\varphi_P} & \mathcal{C}'^{2,\mathrm{sym}}. \end{array}$$

for some suitable quadratic extension k'/k.

Proof. Let $(x_1, x_2), (y_1, y_2)$ be the lift given by Lemma 4.15. Since P is Weierstrass, $k[[z]]$ is already a ramified extension of the completed local ring on the Kummer surface. Therefore x_1 and x_2, which as a pair are defined on the Kummer surface, belong to $k'[[z]]$ for some quadratic extension k'/k. The system (S) can be written as

$$\begin{pmatrix} 1/y_1 \\ 1/y_2 \end{pmatrix} = \begin{pmatrix} x_1 x_1' & x_2 x_2' \\ x_1' & x_2' \end{pmatrix}^{-1} \begin{pmatrix} R_1(z) \\ R_2(z) \end{pmatrix}$$

for some series $R_1, R_2 \in k[[z]]$, hence y_1 and y_2 belong to $k'[[z]]$ as well. □

We now consider the tangent space $T_{(Q,i(Q))}\,\mathcal{C}'^2$ of $\mathcal{C}'^2$ at $\big(Q, i(Q)\big)$. It decomposes as

$$T_{(Q,i(Q))}\,\mathcal{C}'^{\,2} = T_Q\,\mathcal{C}' \oplus T_{i(Q)}\,\mathcal{C}' \simeq (T_Q\,\mathcal{C}')^2$$

where the last map is given by the hyperelliptic involution on the second term.

Lemma 4.17. *Assume that a lift $\widetilde{\varphi}_P = (x_1, y_1, x_2, y_2)$ of φ_P to $k'[[z]]$ exists. Then the tangent vector $d\widetilde{\varphi}_P/dz$ at $z = 0$ cannot be of the form (v, v) where $v \in T_Q\,\mathcal{C}'$.*

Proof. Assume the contrary. The direction (v, v) is contracted to zero in the Jacobian, so every differential form on the Jacobian is pulled back to zero via φ_P. This is a contradiction because φ^* is nonzero. □

When solving (S), we want to avoid Weierstrass type. Using the following lemma, it is easy to choose P such that the associated Q is not Weierstrass.

Proposition 4.18. *The point Q is uniquely determined by the property that, up to a scalar factor,*

$$\varphi^*\omega_Q' = \omega_P$$

where ω_P (resp. ω_Q') is a nonzero differential form on $\mathcal{C}$ (resp. $\mathcal{C}'$) vanishing at P (resp. Q).

Proof. First, assume that a local lift $\widetilde{\varphi}_P = (x_1, x_2, y_1, y_2)$ exists in $k'[[z]]$. By Lemma 4.17, the tangent vector $d\widetilde{\varphi}_P/dz$ at $z = 0$ cannot be of the form (v, v) where $v \in T_Q\,\mathcal{C}'$, so it has a nonzero component of the form $(v, 0)$. Let ω' be the

unique nonzero differential form pulling back to ω_P by φ. Then ω' must vanish in the direction $(v,0)$ of $T_{(Q,i(Q))}\mathcal{C}'^2$, in other words ω' must vanish at Q.

Second, assume that *no* such lift exists. By Lemmas 4.15 and 4.16, Q is a Weierstrass point on $\mathcal{C}'$, and P is not a Weierstrass point on $\mathcal{C}$. After a change of variables, we may assume that Q is not at infinity. Write $P=(u_0,v_0)$ with $v_0\neq 0$, and $Q=(x_0,0)$. We have to show that

$$x_0=\frac{m_{1,1}u_0+m_{1,2}}{m_{2,1}u_0+m_{2,2}}.$$

Let (x_1,y_1,x_2,y_2) be a lift to $k'[[\sqrt{z}]]$ as in Lemma 4.15, and look at the differential system (S). Write the lift as

$$y_1=v_1\sqrt{z}+t_1z+\cdots\,,\quad y_2=v_2\sqrt{z}+t_2z+\cdots\,.$$

Then the relation $y^2=E_{\mathcal{C}'}(x)$ forces x_1,x_2 to have no term in $\sqrt{z}$, so that

$$x_1=x_0+w_1z+\cdots\,,\quad x_2=x_0+w_2z+\cdots\,.$$

Using the relation $dx/y=2dy/E'_{\mathcal{C}'}(x)$, we have

$$\begin{cases}2x_1\dfrac{dy_1}{E'_{\mathcal{C}'}(x_1)}+2x_2\dfrac{dy_2}{E'_{\mathcal{C}'}(x_2)}=(m_{1,1}u+m_{1,2})\dfrac{du}{v},\\[2ex] 2\dfrac{dy_1}{E'_{\mathcal{C}'}(x_1)}+2\dfrac{dy_2}{E'_{\mathcal{C}'}(x_2)}=(m_{2,1}u+m_{2,2})\dfrac{du}{v}.\end{cases}$$

Inspection of the $(\sqrt{z})^{-1}$ term gives the relation $v_1=-v_2$. Write $e=E'_{\mathcal{C}'}(x_0)$. Then the constant term of the series on the left hand side are respectively

$$2x_0\Big(\frac{t_1}{e}+\frac{t_2}{e}\Big)\quad\text{and}\quad 2\Big(\frac{t_1}{e}+\frac{t_2}{e}\Big).$$

Therefore $m_{2,1}u_0+m_{2,2}$ must be nonzero, because the differential forms on the right hand side do not vanish simultaneously at P. Taking the quotient of the two lines gives the result. □

Using Proposition 4.18 and the value of the normalization matrix m, we can choose a base point P on $\mathcal{C}$ such that φ_P is of generic type. Then, by Lemma 4.15, a lift $\widetilde{\varphi}_P=(x_1,y_1,x_2,y_2)$ exists, and these power series are elements of $k'[[z]]$ for some quadratic extension k' of k. Let U, D be the power series in z with respective constant terms u_0, d_0 such that $u=U(z)$ and $du/v=D(z)\,dz$. Then we can rewrite (S) as follows:

$$\begin{cases}\dfrac{x_1x_1'}{y_1}+\dfrac{x_2x_2'}{y_2} &=& (m_{1,1}U+m_{2,1})D\\[2ex] \dfrac{x_1'}{y_1}+\dfrac{x_2'}{y_2} &=& (m_{2,1}U+m_{2,2})D\\ y_1^2=E_{\mathcal{C}'}(x_1)\\ y_2^2=E_{\mathcal{C}'}(x_2).\end{cases}\qquad(S)$$

Step 2: initialization. We now explain how to compute the power series x_1, x_2, y_1, y_2 up to $O(z^2)$ by looking at the system (S). We can compute the point $Q = (x_0, y_0)$ using Proposition 4.18. Write

$$x_1 = x_0 + v_1 z + O(z^2), \quad x_2 = x_0 + v_2 z + O(z^2).$$

Then, using the curve equations, the series y_1, y_2 also have expressions up to $O(z^2)$ in terms of v_1, v_2 respectively. Taking constant terms in (S) gives

$$v_1 + v_2 = \frac{y_0}{x_0}(m_{1,1}u_0 + m_{2,1})d_0 = y_0(m_{2,1}u_0 + m_{2,2})d_0. \tag{1}$$

Combining the two lines, we also obtain

$$(x_1 - x_0)\frac{x_1'}{y_1} + (x_2 - x_0)\frac{x_2'}{y_2} = R,$$

where $R = R_1 z + O(z^2)$ has no constant term. At order 1, this yields

$$v_1^2 + v_2^2 = y_0 R_1. \tag{2}$$

Equalities (1) and (2) yield a quadratic equation satisfied by v_1, v_2. This gives the values of v_1 and v_2 in a quadratic extension k'/k.

Step 3: Newton iterations. Assume that the series x_1, x_2, y_1, y_2 are known up to $O(z^n)$ for some $n \geq 2$. The system (S) is satisfied up to $O(z^{n-1})$ for the first two lines, and $O(z^n)$ for the last two lines. We attempt to double the precision, and write

$$x_1 = x_1^0(z) + \delta x_1(z) + O(z^{2n}), \text{ etc.}$$

where x_1^0 is the polynomial of degree at most $n-1$ that has been computed. The series δx_i and δy_i start at the term z^n.

Proposition 4.19. *The power series δx_1, δx_2 satisfy a linear first-order differential equation*

$$M(z)\begin{pmatrix}\delta x_1' \\ \delta x_2'\end{pmatrix} + N(z)\begin{pmatrix}\delta x_1 \\ \delta x_2\end{pmatrix} = R(z) + O(z^{2n-1}) \tag{E_n}$$

where $M, N, R \in \mathcal{M}_2\big(k[[z]]\big)$ have explicit expressions in terms of x_1^0, x_2^0, y_1^0, y_2^0, D, U, $E_{\mathcal{C}}$ and $E_{\mathcal{C}'}$. In particular,

$$M(z) = \begin{pmatrix} x_1^0/y_1^0 & x_2^0/y_2^0 \\ 1/y_1^0 & 1/y_2^0 \end{pmatrix}$$

and, writing $e = E'_{\mathcal{C}'}(x_0)$, the constant term of N is

$$\begin{pmatrix} \dfrac{v_1}{y_0} - \dfrac{x_0 v_1}{2y_0^3}e & \dfrac{v_2}{y_0} - \dfrac{x_0 v_2}{2y_0^3}e \\ -\dfrac{v_1}{2y_0^3}e & -\dfrac{v_2}{2y_0^3}e \end{pmatrix}.$$

Proof. Linearize the system (S). We omit the calculations. □

In order to solve (S) in quasi-linear time in the precision, it is enough to solve equation (E_n) in quasi-linear time in n. One difficulty here, that does not appear in similar works [14, 13], is that the matrix M is not invertible in $k'[[z]]$. Still, we can adapt the generic divide-and-conquer algorithm from [5, §13.2].

Lemma 4.20. *The determinant*

$$\det\big(M(z)\big) = \frac{x_1^0 - x_2^0}{y_1^0 y_2^0}$$

has valuation exactly one.

Proof. We know that y_1^0 and y_2^0 have constant term $\pm y_0 \neq 0$. The polynomials x_1^0 and x_2^0 have the same constant term x_0, but they do not coincide at order 1: if they did, then so would y_1 and y_2 because of the curve equation, contradicting Lemma 4.17. □

By Lemma 4.20, we can find $I \in \mathcal{M}_2\big(k[[z]]\big)$ such that $IM = z$.

Lemma 4.21. *Let $\kappa \geq 1$, and assume that $\operatorname{char} k > \kappa + 1$. Let $A = IN$. Then the matrix $A + \kappa$ has an invertible constant term.*

Proof. By Lemma 4.20, the leading term of $\det(M)$ is λz for some nonzero $\lambda \in k'$. Using Proposition 4.19, we compute that the constant term of $\det(A+\kappa)$ is $\lambda^2\kappa(\kappa+1)$. We omit the calculations. □

Proposition 4.22. *Let $1 \leq \nu \leq 2n-1$, and assume that $\operatorname{char} k > \nu$. Then we can solve (E_n) to compute δx_1 and δx_2 up to precision $O(z^\nu)$ using $\widetilde{O}(\nu)$ operations in k'.*

Proof. Write $\theta = \begin{pmatrix} \delta x_1 \\ \delta x_2 \end{pmatrix}$. Multiplying (E_n) by I, we obtain a differential equation of the form

$$z\theta' + (A+\kappa)\theta = B + O(z^d), \quad \text{where } d = 2n-1,\ \kappa = 0.$$

We show that θ can be computed from this kind of equation up to $O(z^d)$ using a divide-and-conquer strategy. If $d > 1$, write $\theta = \theta_1 + z^{d_1}\theta_2$ where $d_1 = \lfloor d/2 \rfloor$. Then we have

$$z\theta_1' + (A+\kappa)\theta_1 = B + O(z^{d_1})$$

for some other B. By induction, we can recover θ_1 up to $O(z^d)$. Then

$$z\theta_2' + (A+\kappa+d_1)\theta_2 = E + O(z^{d-d_1})$$

where E has an expression in terms of θ_1. This is enough to recover θ_2 up to $O(z^{n-1-d})$, so we can recover θ up to $O(z^{n-1})$. We initialize the induction with the case $d = 1$, where we have to solve for the constant term in

$$(A+\kappa)\theta = B.$$

Since θ starts at z^2, the values of κ that occur are $2, \dots, \nu - 1$ when computing the solution of (S) up to precision $O(z^\nu)$. By Lemma 4.21, the constant term of $A + \kappa$ is invertible. This concludes the induction, and the result follows from standard lemmas in computer algebra [5, Lemme 1.12]. □

Proposition 4.23. *Let $\nu \geq 1$, and assume that $\operatorname{char} k > \nu$. Then we can compute the lift $\widetilde{\varphi}_P$ up to precision $O(z^\nu)$ within $\widetilde{O}(\nu)$ operations in k'.*

Proof. This is a consequence of Proposition 4.22 and [5, Lemme 1.12]. □

4.5 Rational reconstruction

Finally, we want to recover the rational representation (s, p, q, r) of φ at P from its power series expansion $\widetilde{\varphi}_P$ at some finite precision. First, we estimate the degrees of the rational fractions we want to compute; second, we present the reconstruction algorithm.

Degree estimates. The degrees of s, p, q, r as morphisms from $\mathcal{C}$ to $\mathbb{P}^1$ can be computed as intersection numbers of divisors on $\operatorname{Jac}(\mathcal{C}')$, namely $\varphi_P(\mathcal{C})$ and the polar divisors of s, p, q and r as functions on $\operatorname{Jac}(\mathcal{C}')$. They are already known in the Siegel case.

Proposition 4.24 ([29, §6.1])**.** *Let $\varphi\colon \operatorname{Jac}(\mathcal{C}) \to \operatorname{Jac}(\mathcal{C}')$ be an ℓ-isogeny, and let $P \in \mathcal{C}(k)$. Let (s, p, q, r) be the rational representation of φ at the base point P. Then the degrees of s, p, q and r as morphisms from $\mathcal{C}$ to $\mathbb{P}^1$ are 4ℓ, 4ℓ, 12ℓ, and 8ℓ respectively.*

Hence we concentrate on the Hilbert case, where $\operatorname{Jac}(\mathcal{C})$ and $\operatorname{Jac}(\mathcal{C}')$ have real multiplication by $\mathbb{Z}_K$ given by embeddings ι, ι', and where

$$\varphi\colon \big(\operatorname{Jac}(\mathcal{C}), \iota\big) \to \big(\operatorname{Jac}(\mathcal{C}'), \iota'\big)$$

is a β-isogeny. Denote the Theta divisors on $\operatorname{Jac}(\mathcal{C})$ and $\operatorname{Jac}(\mathcal{C}')$ by Θ and Θ' respectively; in particular, $\eta_P(\mathcal{C})$ is algebraically equivalent to Θ.

Lemma 4.25. *The polar divisors of s, p, q, r as rational functions on $\operatorname{Jac}(\mathcal{C}')$ are algebraically equivalent to $2\Theta'$, $2\Theta'$, $6\Theta'$ and $4\Theta'$ respectively.*

Proof. This comes from the expression of s, p, q, r. For instance, $s = x_1 + x_2$ has a pole of order 1 along each of the two divisors $\big\{(\infty_\pm, Q) \mid Q \in \mathcal{C}\big\}$, where $\infty_\pm$ are the two points at infinity on $\mathcal{C}$, assuming that we choose a degree 6 hyperelliptic model for $\mathcal{C}'$. Each of these divisors is algebraically equivalent to Θ'. The proof for p, q, and r is similar. □

Recall that divisor classes on $\operatorname{Jac}(\mathcal{C}')$ are in bijective correspondence with isomorphism classes of line bundles. By Theorem 2.21, if (A, ι) is a principally polarized abelian surface with real multiplication by $\mathbb{Z}_K$, then there is a bijection $\alpha \mapsto \mathcal{L}^{\iota(\alpha)}_{\operatorname{Jac}(\mathcal{C}')}$ between $\mathbb{Z}_K$ and the Néron–Severi group of A.

Lemma 4.26. *In the Hilbert case, the divisor $\varphi_P(\mathcal{C})$ is algebraically equivalent to the divisor corresponding to the line bundle $\mathcal{L}_{\mathrm{Jac}(\mathcal{C}')}^{\iota'(\overline{\beta})}$.*

Proof. By Theorem 2.21, there exists $\alpha \in \mathbb{Z}_K$ such that the divisor $\varphi_P(\mathcal{C})$ corresponds to the line bundle $\mathcal{L}_{\mathrm{Jac}(\mathcal{C}')}^{\iota'(\alpha)}$ up to algebraic equivalence. Look at the pullback $\varphi^*\big(\varphi_P(\mathcal{C})\big)$ as a divisor on $\mathrm{Jac}(\mathcal{C})$: by definition, we have

$$\varphi^*\big(\varphi_P(\mathcal{C})\big) = \sum_{x \in \ker \varphi} \big(x + \eta_P(\mathcal{C})\big)$$

and therefore, up to algebraic equivalence,

$$\varphi^*\big(\varphi_P(\mathcal{C})\big) = (\#\ker\varphi)\Theta = N_{K/\mathbb{Q}}(\beta)\Theta.$$

Since φ is a β-isogeny, by Definition 2.22, the pullback $\varphi^*\Theta'$ corresponds to $\mathcal{L}_{\mathrm{Jac}(\mathcal{C})}^{\iota(\beta)}$ up to algebraic equivalence. Therefore, for every $\gamma \in \mathbb{Z}_K$,

$$\varphi^* \mathcal{L}_{\mathrm{Jac}(\mathcal{C}')}^{\iota'(\gamma)} = \mathcal{L}_{\mathrm{Jac}(\mathcal{C})}^{\iota(\gamma\beta)}.$$

By Theorem 2.21 applied on $\mathrm{Jac}(\mathcal{C})$, we have $\alpha\beta = N_{K/\mathbb{Q}}(\beta)$, so $\alpha = \overline{\beta}$. □

The next step is to compute the intersection number between Θ' and the divisor corresponding to $\mathcal{L}_{\mathrm{Jac}(\mathcal{C}')}^{\iota(\alpha)}$ for $\alpha \in \mathbb{Z}_K$.

Proposition 4.27 ([25, Rem. 16])**.** *Let (A, ι) be a principally polarized abelian surface with real multiplication by $\mathbb{Z}_K$, and let Θ be its Theta divisor. Then the quadratic form*

$$D \mapsto (D \cdot \Theta)^2 - 2(D \cdot D)$$

on $\mathrm{NS}(A)$ corresponds to the quadratic form on $\mathbb{Z}_K$ given by

$$\alpha \mapsto 2\,\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^2) - \frac{1}{2}\,\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)^2.$$

Corollary 4.28. *Let (A, ι) be a principally polarized abelian surface with real multiplication by $\mathbb{Z}_K$, and let Θ be its Theta divisor. Then for every $\alpha \in \mathbb{Z}_K$, we have*

$$\big(\mathcal{L}_A^{\iota(\alpha)} \cdot \Theta\big)^2 = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha)^2.$$

Proof. Write $\alpha = a + b\sqrt{\Delta}$. By Proposition 4.27, we can compute

$$\big(\mathcal{L}_A^{\iota(\alpha)} \cdot \Theta\big)^2 - 2\,\big(\mathcal{L}_A^{\iota(\alpha)} \cdot \mathcal{L}_A^{\iota(\alpha)}\big) = 2\,\mathrm{Tr}(\alpha^2) - \frac{1}{2}\,\mathrm{Tr}(\alpha)^2 = 4b^2\Delta.$$

On the other hand, the Riemann–Roch theorem [33, 11.1] gives

$$\big(\mathcal{L}_A^{\iota(\alpha)} \cdot \mathcal{L}_A^{\iota(\alpha)}\big) = 2\,\chi\big(\mathcal{L}_A^{\iota(\alpha)}\big) = 2\sqrt{\deg \iota(\alpha)} = 2(a^2 - b^2\Delta).$$

The result follows. □

Proposition 4.29. *In the Hilbert case, let (s, p, q, r) be the rational representation of φ at P. Then, considered as morphisms from $\mathcal{C}$ to $\mathbb{P}^1$, the respective degrees of s, p, q, and r are $2\,\mathrm{Tr}(\beta)$, $2\,\mathrm{Tr}(\beta)$, $6\,\mathrm{Tr}(\beta)$ and $4\,\mathrm{Tr}(\beta)$.*

Proof. The degrees of s, p, q, r can be computed as the intersection of the polar divisors from Lemma 4.25 and the divisor $\varphi_P(\mathcal{C})$. By Lemma 4.26, the line bundle associated with $\varphi_P(\mathcal{C})$, up to algebraic equivalence, is $\mathcal{L}^{\overline{\beta}}$. Its intersection number with Θ is nonnegative, hence by Corollary 4.28, we have

$$\left(\varphi_P(\mathcal{C}) \cdot \Theta'\right) = \mathrm{Tr}_{K/\mathbb{Q}}(\overline{\beta}) = \mathrm{Tr}_{K/\mathbb{Q}}(\beta).$$

The result follows by Lemma 4.25. □

Rational reconstruction. We now explain how to recover the rational representation of φ at P from the power series expansion $\widetilde{\varphi}_P$ in the uniformizer z, and we compute the necessary precision. Write the equation $\mathcal{C}$ as

$$\mathcal{C} \,:\, v^2 = E_{\mathcal{C}}(u), \qquad \text{with } \deg(E_{\mathcal{C}}) \in \{5, 6\}.$$

The hyperelliptic involution is denoted by i. Let k be a field of definition for all these objects.

Lemma 4.30. *Let $s\colon \mathcal{C} \to \mathbb{P}^1$ be a morphism of degree d.*

1. *If s is invariant under i, then we can write*

$$s(u, v) = X(u)$$

and the degree of X is bounded by $d/2$.

2. *In general, let X, Y be the rational fractions such that*

$$s(u, v) = X(u) + v\,Y(u).$$

Then the degrees of X and Y are bounded by d and $d + 3$ respectively.

Proof. 1. The function u itself has degree 2.

2. We have

$$s(u, v) + s(u, -v) = 2X(u), \quad \frac{s(u, v) - s(u, -v)}{v} = 2Y(u).$$

These morphisms have degree at most $2d$ and $2d + 6$ respectively, and we can apply 1. □

Proposition 4.31. *Let $\widetilde{\varphi}_P$ and $\widetilde{\varphi}_{i(P)}$ be the power series expansion of φ_P around P and $i(P)$ in the uniformizers z and $i(z)$. Let $\nu = 8\ell + 7$ in the Siegel case, and $\nu = 4\,\mathrm{Tr}_{K/\mathbb{Q}}(\beta) + 7$ in the Hilbert case. Then, given $\widetilde{\varphi}_P$ and $\widetilde{\varphi}_{i(P)}$ at precision $O(z^\nu)$, we can compute the rational representation of φ at P within $\widetilde{O}(\nu)$ operations in k.*

Proof. It is enough to recover the rational fractions s and p; afterwards, q and r can be deduced from the equation of $\mathcal{C}'$.

First, assume that P is a Weierstrass point on $\mathcal{C}$. Then s, p are invariant under the hyperelliptic involution, because the value of φ_P at $i(Q)$ is $-\varphi_P(Q)$. Therefore we have to recover univariate rational fractions in u of degree $d \leq 2\ell$ (resp. $d \leq \mathrm{Tr}(\beta)$). This can be done in quasi-linear time from their power series expansion up to precision $O(u^{2d+1})$ [5, §7.1]. Since u has valuation 2 in z, we need to compute $\widetilde{\varphi}$ at precision $O(z^{4d+1})$.

Second, assume that P is not a Weierstrass point on $\mathcal{C}$. Then the series defining $s(u,-v)$ and $p(u,-v)$ are given by $\widetilde{\varphi}_{i(P)}$. We now have to compute rational fractions of degree $d \leq 4\ell+3$ (resp. $d \leq 2\,\mathrm{Tr}(\beta)+3$) in u. Since u has valuation 1 in z, this can be done in quasi-linear time if $\widetilde{\varphi}_P$ and $\widetilde{\varphi}_{i(P)}$ are known up to precision $O(z^{2d+1})$. □

4.6 Summary of the algorithm

Given an input as described in §4.1 in either the Siegel case or the Hilbert case, the isogeny algorithm runs as follows.

Algorithm 4.32.

1. Use Mestre's algorithm [29] or Algorithm 4.6 to reconstruct curve equations $\mathcal{C}$, $\mathcal{C}'$.
2. Compute at most 4 candidates for the normalization matrix of φ using Algorithm 4.11 or Algorithm 4.12. Run the rest of the algorithm for all the candidates; only one will produce meaningful results.
3. Choose a base point P on $\mathcal{C}$ such that φ_P is of generic type, and compute the power series $\widetilde{\varphi}_P$ and $\widetilde{\varphi}_{i(P)}$ up to precision $O\big(z^{8\ell+7}\big)$, respectively $O\big(z^{4\,\mathrm{Tr}(\beta)+7}\big)$ using Proposition 4.23.
4. Recover the rational representation of φ at P using Proposition 4.31.

We can finally state and prove a more precise version of Theorem 1.1.

Theorem 4.33. *Let K be a real quadratic field, and let $\beta \in \mathbb{Z}_K$ be a totally positive prime. Let k be a field such that*

$$\mathrm{char}\, k > 4\,\mathrm{Tr}_{K/\mathbb{Q}}(\beta) + 7.$$

Assume that there is an algorithm that can evaluate derivatives of modular equations of level β at a given point over k, using $C_{\mathrm{ev}}(\beta)$ operations in k; also assume that there is an algorithm that can compute square roots in field extensions of k of degree at most 4 using C_{sqrt} operations in k.

Then, given Igusa invariants of two Jacobians of genus 2 curves over k with real multiplication by $\mathbb{Z}_K$ that are β-isogenous and generic in the sense of Definition 4.8, Algorithm 4.32 returns the rational representation of this isogeny at some base point on $\mathcal{C}$, within

$$O\big(C_{\mathrm{ev}}(\beta)\big) + \widetilde{O}\big(\mathrm{Tr}_{K/\mathbb{Q}}(\beta)\big) + O_K(1) + O(C_{\mathrm{sqrt}})$$

operations in k. The output is defined over an extension of k of degree 8.

Proof. In the algorithm, we take at most 3 quadratic extensions. Hence, up to replacing k by an extension of degree 8, we can assume that all computations take place over k. The cost of each step in Algorithm 4.32 in the Hilbert case is

1. $O_K(1) + O(C_{\mathrm{sqrt}})$ operations in k, by Proposition 4.7.
2. $O\big(C_{\mathrm{ev}}(\beta)\big) + O(C_{\mathrm{sqrt}})$ operations in k, by Proposition 4.13. This is where we use the genericity hypothesis.
3. $\widetilde{O}\big(\mathrm{Tr}(\beta)\big)$ operations in k, by Proposition 4.23. This is where we use the hypothesis on $\mathrm{char}\, k$.
4. $\widetilde{O}\big(\mathrm{Tr}(\beta)\big)$ operations in k, by Proposition 4.31. □

The Siegel version is as follows. The proof is very similar, and omitted.

Theorem 4.34. *Let $\ell \in \mathbb{N}$ be a prime, and let k be a field such that*

$$\mathrm{char}\, k > 8\ell + 7.$$

Assume that there is an algorithm that can evaluate derivatives of modular equations of level ℓ at a given point over k, using $C_{\mathrm{ev}}(\ell)$ operations in k.

Then, given Igusa invariants of two Jacobians of genus 2 curves over k that are ℓ-isogenous and generic in the sense of Definition 4.8, Algorithm 4.32 returns the rational representation of this isogeny at some base point on $\mathcal{C}$, within

$$O\big(C_{\mathrm{ev}}(\ell)\big) + \widetilde{O}(\ell) + O(C_{\mathrm{sqrt}})$$

operations in k. The output is defined over an extension of k of degree 4.

References

[1] Y. André. On the Kodaira-Spencer map of abelian schemes. *Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)*, 17(4):1397–1416, 2017.

[2] W. L. Baily, Jr. and A. Borel. Compactification of arithmetic quotients of bounded symmetric domains. *Ann. of Math. (2)*, 84:442–528, 1966.

[3] S. Ballentine, A. Guillevic, E. Lorenzo García, C. Martindale, M. Massierer, B. Smith, and J. Top. Isogenies for point counting on genus two hyperelliptic curves with maximal real multiplication. In *Algebraic Geometry for Coding Theory and Cryptography*, volume 9, pages 63–94, Los Angeles, 2016. Springer.

[4] C. Birkenhake and H. Lange. *Complex Abelian Varieties*. Springer-Verlag, Berlin, second edition, 2004.

[5] A. Bostan, F. Chyzak, M. Giusti, R. Lebreton, G. Lecerf, B. Salvy, and E. Schost. *Algorithmes efficaces en calcul formel*. Published by the authors, 2017.

[6] A. Bostan, F. Morain, B. Salvy, and É. Schost. Fast algorithms for computing isogenies between elliptic curves. *Math. Comp.*, 77(263):1755–1778, 2008.

[7] N. Bourbaki. *Groupes et algèbres de Lie. Chapitres II et III*, volume 1349 of *Actualités Scientifiques et Industrielles*. Hermann, Paris, 1972.

[8] N. Bourbaki. *Groupes et algèbres de Lie. Chapitres VII et VIII*, volume 1364 of *Actualités Scientifiques et Industrielles*. Hermann, Paris, 1975.

[9] J. H. Bruinier. Hilbert modular forms and their applications. In *The 1-2-3 of Modular Forms*, Universitext, pages 105–179. Springer, Berlin, 2008.

[10] J. I. Burgos Gil and A. Pacetti. Hecke and Sturm bounds for Hilbert modular forms over real quadratic fields. *Math. Comp.*, 86(306):1949–1978, 2017.

[11] A. Clebsch. *Theorie der binären algebraischen Formen*. B. G. Teubner, Leipzig, 1872.

[12] F. Cléry, C. Faber, and G. van der Geer. Covariants of binary sextics and vector-valued Siegel modular forms of genus two. *Math. Ann.*, 369(3-4):1649–1669, 2017.

[13] E. Costa, N. Mascot, J. Sijsling, and J. Voight. Rigorous computation of the endomorphism ring of a Jacobian. *Math. Comp.*, 88(317):1303–1339, 2019.

[14] J.-M. Couveignes and T. Ezome. Computing functions on Jacobians and their quotients. *Lond. Math. Soc. J. Comput. Math.*, 18(1):555–577, 2015.

[15] A. Dudeanu, D. Jetchev, D. Robert, and M. Vuille. Cyclic isogenies for abelian varieties with real multiplication. Preprint, 2017.

[16] R. Dupont. Fast evaluation of modular functions using Newton iterations and the AGM. *Math. Comput.*, 80(275):1823–1847, 2011.

[17] N. D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational Perspectives on Number Theory (Chicago, IL, 1995)*, volume 7 of *AMS/IP Stud. Adv. Math.*, pages 21–76. Amer. Math. Soc., Providence, RI, 1998.

[18] A. Enge and E. Thomé. CMH: Computation of Igusa class polynomials, 2014. http://cmh.gforge.inria.fr/.

[19] P. Gaudry, D. Kohel, and B. Smith. Counting points on genus 2 curves with real multiplication. In *ASIACRYPT 2011*, volume 7073 of *Lecture Notes in Computer Science*, pages 504–519, Seoul, South Korea, 2011. Springer.

[20] P. Gaudry and É. Schost. Genus 2 point counting over prime fields. *J. Symb. Comput.*, 47(4):368–400, 2012.

[21] D. Gruenewald. Computing Humbert surfaces and applications. In *Arithmetic, Geometry, Cryptography and Coding Theory 2009*, volume 521 of *Contemp. Math.*, pages 59–69. Amer. Math. Soc., Providence, RI, 2010.

[22] T. Ibukiyama. Vector-valued Siegel modular forms of symmetric tensor weight of small degrees. *Comment. Math. Univ. St. Pauli*, 61(1):51–75, 2012.

[23] J.-I. Igusa. On Siegel modular forms of genus two. *Amer. J. Math.*, 84:175–200, 1962.

[24] J.-I. Igusa. Modular forms and projective invariants. *Amer. J. Math.*, 89:817–855, 1967.

[25] E. Kani. Elliptic subcovers of a curve of genus 2. I. The isogeny defect. *Ann. Math. Qué.*, 43(2):281–303, 2019.

[26] K. Lauter and J.-P. Serre. Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields. *J. Algebraic Geom.*, 10(1):19–36, 2001.

[27] K. Lauter and T. Yang. Computing genus 2 curves from invariants on the Hilbert moduli space. *J. Number Theory*, 131(5):936–958, 2011.

[28] C. Martindale. *Isogeny Graphs, Modular Polynomials, and Applications*. PhD thesis, Universiteit Leiden and Université de Bordeaux, 2018.

[29] J.-F. Mestre. Construction de courbes de genre 2 à partir de leurs modules. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, page 313–334. Birkhäuser, Boston, 1991.

[30] E. Milio. Modular polynomials. https://members.loria.fr/EMilio/modular-polynomials.

[31] E. Milio. A quasi-linear time algorithm for computing modular polynomials in dimension 2. *LMS J. Comput. Math.*, 18:603–632, 2015.

[32] E. Milio and D. Robert. Modular polynomials on Hilbert surfaces. Preprint, 2017.

[33] J. S. Milne. Abelian varieties. In *Arithmetic Geometry (Storrs, Conn., 1984)*, pages 103–150. Springer, New York, 1986.

[34] J. S. Milne. Jacobian varieties. In *Arithmetic Geometry (Storrs, Conn., 1984)*, pages 167–212. Springer, New York, 1986.

[35] P. Molin. Hcperiods: Period matrices and Abel-Jacobi maps of hyperelliptic and superperelliptic curves, 2018. https://github.com/pascalmolin/hcperiods.

[36] P. Molin and C. Neurohr. Computing period matrices and the {A}bel-{J}acobi map of superelliptic curves. *Math. Comp.*, 88(316):847–888, 2019.

[37] S. Nagaoka. On the ring of Hilbert modular forms over $\mathbb{Z}$. *J. Math. Soc. Japan*, 35(4):589–608, 1983.

[38] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, 44(170):483–494, 1985.

[39] R. Schoof. Counting points on elliptic curves over finite fields. *J. Théorie Nr. Bordx.*, 7(1):219–254, 1995.

[40] M. Streng. *Complex Multiplication of Abelian Surfaces*. PhD thesis, Universiteit Leiden, 2010.

[41] The PARI group. Pari/GP version 2.11.0, 2019. http://pari.math.u-bordeaux.fr/.

[42] G. van der Geer. *Hilbert Modular Surfaces*. Springer-Verlag, Berlin, 1988.

[43] G. van der Geer. Siegel modular forms and their applications. In *The 1-2-3 of Modular Forms*, Universitext, pages 181–245. Springer, Berlin, 2008.

A The case $K = \mathbb{Q}(\sqrt{5})$

We present a variant of our algorithm in the case of principally polarized abelian varieties with real multiplication by $\mathbb{Z}_K$ where $K = \mathbb{Q}(\sqrt{5})$. In this case, the structure of the ring of Hilbert modular form is well known, and the Hilbert surface is rational: its function field can be generated by only two elements called *Gundlach invariants*. Having only two coordinates reduces the size of modular equations. We illustrate our algorithm with an example of cyclic isogeny of degree 11.

A.1 Hilbert modular forms for $K = \mathbb{Q}(\sqrt{5})$

We keep the notation used to describe the Hilbert embedding (§2.4). Hilbert modular forms have Fourier expansions in terms of

$$w_1 = \exp\big(2\pi i(e_1 t_1 + \overline{e_1} t_2)\big) \quad \text{and} \quad w_2 = \exp\big(2\pi i(e_2 t_1 + \overline{e_2} t_2)\big).$$

We use this notation and the term *w-expansions* to avoid confusion with expansions of Siegel modular forms.

Remark A.1. Apart from the constant term, a term in $w_1^a w_2^b$ can only appear when $ae_1 + be_2$ is a totally positive element of $\mathbb{Z}_K$. Since $e_1 = 1$ and e_2 has negative norm, for a given a, only finitely many b's appear. Therefore we can consider truncations of w-expansions as elements of $\mathbb{C}(w_2)[[w_1]]$ modulo an ideal of the form (w_1^ν).

Theorem A.2 ([37])**.** *The graded $\mathbb{C}$-algebra of symmetric Hilbert modular forms of even parallel weight for $K = \mathbb{Q}(\sqrt{5})$ is generated by three elements G_2, F_6, F_{10} of respective weights 2, 6 and 10, with w-expansions*

$$\begin{aligned} G_2(t) &= 1 + (120w_2 + 120)w_1 \\ &\quad + \big(120w_2^3 + 600w_2^2 + 720w_2 + 600 + 120w_2^{-1}\big)w_1^2 + \cdots \\ F_6(t) &= (w_2 + 1)w_1 + \big(w_2^3 + 20w_2^2 - 90w_2 + 20 + w_2^{-1}\big)w_1^2 + \cdots \\ F_{10}(t) &= (w_2^2 - 2w_2 + 1)w_1^2 + \cdots \end{aligned}$$

Definition A.3. We define the *Gundlach invariants* for $K = \mathbb{Q}(\sqrt{5})$ to be

$$g_1 = \frac{G_2^5}{F_{10}} \quad \text{and} \quad g_2 = \frac{G_2^2 F_6}{F_{10}}.$$

Proposition A.4. *The Gundlach invariants define a birational map*

$$\mathcal{A}_{2,K}(\mathbb{C})/\sigma \to \mathbb{C}^2.$$

Proof. This is a consequence of [2, 10.11] and Theorem A.2. □

By Proposition 2.18, the pullbacks of the Siegel modular forms ψ_4, ψ_6, χ_{10} and χ_{12} via the Hilbert embedding H are symmetric Hilbert modular forms of even weight, so they have expressions in terms of G_2, F_6, F_{10}. These expressions can be computed using linear algebra on Fourier expansions [32, Prop. 2.12]: in our case, the Hilbert embedding is defined by $e_1 = 1$, $e_2 = (1-\sqrt{5})/2$, so

$$q_1 = w_1, \quad q_2 = w_2, \quad q_3 = w_1 w_2.$$

As a corollary, we obtain the expression for the pullback of Igusa invariants.

Proposition A.5 ([32, Cor. 2.14])**.** *In the case $K = \mathbb{Q}(\sqrt{5})$, we have*

$$\begin{aligned}
H^* j_1 &= 8 g_1 \Big(3\frac{g_2^2}{g_1} - 2\Big)^5, \\
H^* j_2 &= \frac{1}{2} g_1 \Big(3\frac{g_2^2}{g_1} - 2\Big)^3, \\
H^* j_3 &= \frac{1}{8} g_1 \Big(3\frac{g_2^2}{g_1} - 2\Big)^2 \Big(4\frac{g_2^2}{g_1} + 2^5 3^2 \frac{g_2}{g_1} - 3\Big).
\end{aligned}$$

Definition A.6. Let $\beta \in \mathbb{Z}_K$ be a totally positive prime. We call the *Hilbert modular equations of level β* in Gundlach invariants the data of the two polynomials $\Phi_{\beta,1}, \Psi_{\beta,2} \in \mathbb{C}(G_1, G_2)[G_1']$ defined as follows:

- $\Phi_{\beta,1}$ is the univariate minimal polynomial of the function $g_1(t/\beta)$ over the field $\mathbb{C}\big(g_1(t), g_2(t)\big)$.
- We have
$$\forall t \in \mathcal{H}_1^2,\ g_2(t/\beta) = \Psi_{\beta,2}\big(g_1(t), g_2(t), g_1(t/\beta)\big).$$

Modular equations using Gundlach invariants for $K = \mathbb{Q}(\sqrt{5})$ also have denominators. They have been computed up to $N_{K/\mathbb{Q}}(\beta) = 41$ [30].

A.2 Variants in the isogeny algorithm

Constructing curves with diagonal real endomorphisms. We give another method to reconstruct such curves using the pullback of the modular form $f_{8,6}$ from Example 2.11 as a Hilbert modular form.

Proposition A.7. *Define the functions $b_i(t)$ for $0 \le i \le 6$ on $\mathcal{H}_1^2$ by*

$$\forall t \in \mathcal{H}_1^2,\ \det{}^8 \operatorname{Sym}^6(R) f_{8,6}\big(H(t)\big) = \sum_{i=0}^{6} b_i(t)\, x^i.$$

Then b_2 and b_4 are identically zero, and

$$\begin{aligned} b_3^2 &= 4F_{10}F_6^2, \\ b_1b_5 &= \frac{36}{25}F_{10}F_6^2 - \frac{4}{5}F_{10}^2G_2, \\ b_0b_6 &= \frac{-4}{25}F_{10}F_6^2 + \frac{1}{5}F_{10}^2G_2, \\ b_3\big(b_0^2b_5^3 + b_1^3b_6^2\big) &= 123F_{10}^3F_6 - \frac{32}{25}F_{10}^2F_6^2G_2^2 + \frac{288}{125}F_{10}F_6^4G_2 - \frac{3456}{3125}F_6^6. \end{aligned}$$

Proof. By Proposition 2.18, each coefficient b_i is a Hilbert modular form of weight $(8+i, 14-i)$. We can check using the action of M_σ that σ exchanges b_i and b_{6-i}. From the Siegel q-expansion for $f_{8,6}$, we can compute the w-expansions of the b_i's; then, we use linear algebra to identify symmetric combinations of the b_i's of parallel even weight in terms of the generators G_2, F_6, F_{10}. □

By Propositions 3.6 and 3.11, the standard curve $\mathcal{C}_K(t)$ attached to $t \in \mathcal{H}_1$ is proportional to the curve $y^2 = \sum_{i=0}^6 b_i(t)\, x^i$. The algorithm to compute a curve $\mathcal{C}$ with diagonal real endomorphisms from its Igusa invariants (j_1, j_2, j_3) runs as follows.

Algorithm A.8.
1. Compute Gundlach invariants (g_1, g_2) mapping to the Igusa invariants (j_1, j_2, j_3) via H using Proposition A.5.
2. Compute values for the generators G_2, F_6, F_{10} giving these Gundlach invariants, choosing for instance $G_2 = 1$ in Definition A.3.
3. Compute b_3^2, b_1b_5, etc. using Proposition A.7.
4. Recover values for the coefficients: choose any square root for b_3; choose any value for b_1, which gives b_5; finally, solve a quadratic equation to find b_0 and b_6.

We can always choose values G_2, F_6, F_{10} such that b_3^2 is a square in k; then, the output is defined over a quadratic extension of k. The choices made in the algorithm do not change the fact that the curve obtained has diagonal real endomorphisms.

Computing the normalization matrix. Write Φ_1, Φ_2 for the Hilbert modular equations of level β in Gundlach invariants, and consider them as elements of the ring $\mathbb{Q}(G_1, G_2)[G_1', G_2']$. Define

$$D\Phi_L = \left(\frac{\partial \Phi_n}{\partial G_k}\right)_{1\le n,k\le 2} \quad \text{and} \quad D\Phi_R = \left(\frac{\partial \Phi_n}{\partial G_k'}\right)_{1\le n,k\le 2}.$$

Denote by g the Gundlach invariants of $\mathcal{J}$, and by g the Gundlach invariants of $\mathcal{J}'$. The genericity hypothesis is now that the 2×2 matrices $D\Phi_L(g, g')$ and $D\Phi_R(g, g')$ are invertible. To compute the normalization matrix, we replace derivatives of Igusa invariants in Proposition 4.9 by derivatives of Gundlach invariants. The relation between these derivatives is given by Proposition A.5.

A.3 An example of cyclic isogeny

We illustrate our algorithm in the Hilbert case with $K = \mathbb{Q}(\sqrt{5})$ by computing a β-isogeny between Jacobians with real multiplication by $\mathbb{Z}_K$, where

$$\beta = 3 + \frac{1+\sqrt{5}}{2} \in \mathbb{Z}_K, \quad N_{K/\mathbb{Q}}(\beta) = 11, \quad \mathrm{Tr}_{K/\mathbb{Q}}(\beta) = 7.$$

We work over the prime finite field $k = \mathbb{F}_{56311}$, whose characteristic is large enough for our purposes. The image of β in k is 26213.

The Igusa–Streng invariants

$$(j_1, j_2, j_3) = \big(14030, 9041, 56122\big), \quad (j_1', j_2', j_3') = \big(13752, 42980, 12538\big)$$

lie on the Humbert surface, and the associated Gundlach invariants are

$$(g_1, g_2) = \big(23, 56260\big), \quad (g_1', g_2') = \big(8, 36073\big).$$

In order to reconstruct a Hilbert-normalized curve, we apply Algorithm A.8. We obtain the curve equations

$$\begin{aligned} \mathcal{C} &: v^2 = 13425u^6 + 34724u^5 + 102u^3 + 54150u + 11111 \\ \mathcal{C}' &: y^2 = 47601x^6 + 35850x^5 + 40476x^3 + 24699x + 40502. \end{aligned}$$

The derivatives of Gundlach invariants are given by

$$\Big(\frac{dg}{dt}\Big)(\mathcal{C}) = \begin{pmatrix} 43658 & 17394 \\ 16028 & 26656 \end{pmatrix}, \quad \Big(\frac{dg}{dt}\Big)(\mathcal{C}') = \begin{pmatrix} 15131 & 739 \\ 50692 & 49952 \end{pmatrix}.$$

Computing derivatives of the modular equations as in Proposition 4.9, we find that the isogeny is compatible with the real embeddings $\iota(\mathcal{C})$ and $\iota(\mathcal{C}')$. We still do not known whether φ is a β or a $\overline{\beta}$-isogeny, so we have four candidates for the normalization matrix up to sign:

$$\begin{aligned} m_{\beta,\pm} &= \begin{pmatrix} 38932\alpha + 19466 & 0 \\ 0 & \pm(53318\alpha + 26659) \end{pmatrix}, \\ m_{\overline{\beta},\pm} &= \begin{pmatrix} 50651\alpha + 53481 & 0 \\ 0 & \pm(11076\alpha + 5538) \end{pmatrix} \end{aligned}$$

where $\alpha^2 + \alpha + 2 = 0$. We see that the isogeny is only defined over a quadratic extension of k.

The curve $\mathcal{C}$ has a rational Weierstrass point $\big(36392, 0\big)$. We can bring it to $(0, 0)$, so that $\mathcal{C}$ is of the standard form

$$\mathcal{C} : v^2 = 33461u^6 + 7399u^5 + 16387u^4 + 34825u^3 + 14713u^2 + u.$$

This multiplies the normalization matrix on the right by

$$\begin{pmatrix} 44206 & 18649 \\ 0 & 7615 \end{pmatrix}.$$

Choose $P = (0, 0)$ as a base point on $\mathcal{C}$, and $z = \sqrt{u}$ as a uniformizer; it is a Weierstrass point, and we check that φ_P is of generic type. We solve the differential system up to precision $O(z^{35})$, or any higher precision. It turns out that the correct normalization matrix is $m_{\overline{\beta},+}$ as the other series do not come from rational fractions of the prescribed degree. We obtain

$$s(u) = \frac{50255u^6 + 40618u^5 + 17196u^4 + 9527u^3 + 22804u^2 + 49419u + 11726}{u^6 + 40883u^5 + 22913u^4 + 41828u^3 + 18069u^2 + 14612u + 7238},$$
$$p(u) = \frac{35444u^6 + 9569u^5 + 52568u^4 + 3347u^3 + 9325u^2 + 32206u + 7231}{u^6 + 40883u^5 + 22913u^4 + 41828u^3 + 18069u^2 + 14612u + 7238}.$$

The degrees agree with Proposition 4.29. The isogeny is k-rational at the level of Kummer surfaces, but not on the Jacobians themselves: α appears on the numerator of $r(u, v)$.