Computing isogenies from modular equations in genus two

Jean Kieffer, Aurel Page and Damien Robert

Abstract

We present an algorithm solving the following problem: given two genus 2 curves over a field k with isogenous Jacobians, compute such an isogeny explicitly. This isogeny can be either an ℓ-isogeny or, in the real multiplication case, an isogeny with cyclic kernel; our algorithm uses modular equations of either Siegel or Hilbert type, respectively. As an essential step of independent interest, we construct an explicit Kodaira–Spencer isomorphism for principally polarized abelian surfaces, by giving an explicit expression for derivatives of Igusa invariants in terms of the coefficients of a genus 2 curve equation.

1. Introduction

The problem of computing isogenies between principally polarized (p.p.) abelian varieties has attracted considerable interest in recent years. Two cases of particular interest are abelian varieties over finite fields, especially in relation with the development of isogeny-based cryptography; and abelian varieties over number fields, which are central objects in number theory.

Since the pioneering work of Vélu [Vél71] in the case of elliptic curves, several algorithms are available to solve instance of the following problem: given a p.p. abelian variety A and an explicitly described torsion subgroup K of A such that A/K is also principally polarizable, compute the isogeny $A \to A/K$. Among algorithms that apply to general K (as opposed to Richelot isogenies for instance), some work with Jacobians of curves, of genus 2 in particular [CR15; CE15]; others are based on theta functions and apply in any dimension [LR15; DJR+17].

This raises the question of how to obtain such a subgroup K in the first place. From a practical point of view, the previous algorithms suffer from the fact that torsion subgoups $A[\ell]$ are difficult to describe in full as ℓ grows, due to their sheer size $\ell^{2\dim A}$.

In this paper, we are interested in the inverse question: given two p.p. abelian varieties A and A' that are known to be isogenous, compute an isogeny $\varphi\colon A \to A'$ explicitly. The input to such an algorithm could be provided by *modular equations*, which are explicit equations for moduli spaces parametrizing such isogenies. For abelian surfaces specifically, van Wamelen [vWam00; vWam06] describes an answer using complex approximations; however, this approach is inherently restricted to subfields of $\mathbb{C}$ and lacks clear complexity estimates.

Our main result follows a different and completely algebraic approach, generalizing Elkies's isogeny algorithm for elliptic curves [Elk98] which uses equations for the modular curves of level $\Gamma_0(\ell)$. We describe a complete algorithm in the case of p.p. abelian surfaces; a similar strategy would apply to compute isogenies in any dimension. Let us state a simplified version in the

2020 Mathematics Subject Classification 14K02, 14K10, 14Q20
Keywords: abelian varieties, isogenies, modular equations, algorithms
The authors were supported by the ANR grant CIAO (French Agence Nationale de la Recherche).

case of ℓ-isogenies (of degree ℓ^2) where ℓ is a prime, described by modular equations of Siegel type [BL09; Mil15].

Theorem 1.1. *Let ℓ be a prime, and let k be a field such that $\operatorname{char} k = 0$ or $\operatorname{char} k > 8\ell + 7$. Then, given the data of*

(i) two sufficiently generic ℓ-isogenous p.p. abelian surfaces A and A' over k, and
(ii) the values of derivatives of modular equations of Siegel type and level ℓ at (A, A'),

one can compute an explicit description of an ℓ-isogeny $\varphi\colon A \to A'$. This description consists of

(i) a tower k'/k of at most three quadratic extensions,
(ii) hyperelliptic curve equations $\mathcal{C}, \mathcal{C}'$ over k' whose Jacobians are isomorphic to A, A' respectively,
(iii) a point $P \in \mathcal{C}(k')$,
(iv) rational fractions $s, p, q, r \in k'(\mathcal{C})$,

such that (s, p, q, r) equals the composite map

$$\mathcal{C} \xhookrightarrow{Q \mapsto [Q-P]} \operatorname{Jac}(\mathcal{C}) \xrightarrow{\varphi} \operatorname{Jac}(\mathcal{C}') \dashrightarrow \mathcal{C}'^{2,\mathrm{sym}} \xrightarrow{m} \mathbb{A}^4$$

where m is the rational map given by

$$\{(x_1, y_1), (x_2, y_2)\} \mapsto \left(x_1 + x_2,\ x_1 x_2,\ y_1 y_2,\ \frac{y_2 - y_1}{x_2 - x_1}\right).$$

The cost of the algorithm $\widetilde{O}(\ell)$ elementary operations and $O(1)$ square roots in k'.

A more precise statement including the precise genericity assumptions appears in §6. We also describe a similar result in the case of cyclic isogenies in the setting of p.p. abelian surfaces with fixed real multiplication, based on modular equations of Hilbert type [MR20; Mar18].

From a practical point of view, the isogeny algorithm itself is extremely cheap. The bulk of the cost is hidden in the evaluation of modular equations of Siegel type and their derivatives. Still, manipulating modular equations is often cheaper than manipulating the full torsion subgroups, both in the case of elliptic curves [Eng09; Sut13] and abelian surfaces [Kie21].

As a consequence, Theorem 1.1 provides an efficient way of obtaining maximally isotropic subgroups in $A[\ell]$, as kernels of ℓ-isogenies. In the case of elliptic curves, this remark is at the heart of the Schoof–Elkies–Atkin (or SEA) point-counting algorithm [Sch85]. Similarly, the isogeny algorithms presented here can be used to improve the asymptotic complexity of point-counting for p.p. abelian surfaces over finite fields [Kie22a], compared to previous methods relying only of kernels of endomorphisms to construct rational subgroups [GKS11; GS12]. Under standard heuristics on the distribution of Elkies primes, isogeny-based point counting methods achieve an asymptotic complexity of $\widetilde{O}(\log^6 q)$ binary operations on average (instead of $\widetilde{O}(\log^8 q)$) for a fixed abelian surface over a number field modulo sufficiently many primes. If one considers abelian surfaces with fixed real multiplication, they achieve a complexity of $\widetilde{O}(\log^4 q)$ (instead of $\widetilde{O}(\log^5 q)$) even for a single instance, thus reaching the same asymptotic complexity as the SEA algorithm up to constant factors.

Let us outline our algorithm to compute ℓ-isogenies from a geometric point of view, in any dimension g. The central object is the map

$$\Phi_\ell = (\Phi_{\ell,1}, \Phi_{\ell,2})\colon \mathcal{A}_g(\ell) \to \mathcal{A}_g \times \mathcal{A}_g$$

where $\mathcal{A}_g(\ell)$ denotes the stack of p.p. abelian schemes of dimension g endowed with the kernel of an ℓ-isogeny, and $\mathcal{A}_g$ denotes the stack of p.p. abelian schemes of dimension g; this map is given

by $(A, K) \mapsto (A, A/K)$. Both $\Phi_{\ell,1}$ and $\Phi_{\ell,2}$ are étale maps. Let $\varphi\colon A \to A'$ be an ℓ-isogeny, so that (A, A') lies in the image of Φ_ℓ. Denote the tangent space of $\mathcal{A}_g$ at A by $T_A(\mathcal{A}_g)$, and the tangent space of A at its neutral point by $T_0(A)$. Then there is a close relation between two maps:

- the *deformation map* $\mathscr{D}(\varphi)\colon T_A(\mathcal{A}_g) \to T_{A'}(\mathcal{A}_g)$ defined as $\mathscr{D}(\varphi) \coloneqq d\Phi_{\ell,2} \circ d\Phi_{\ell,1}{}^{-1}$;
- the *tangent map* $d\varphi\colon T_0(A) \to T_0(A')$.

This relation stems from a canonical Kodaira–Spencer isomorphism between $T_A(\mathcal{A}_g)$ and $\mathrm{Sym}^2 T_0(A)$. Therefore, in any dimension g, an isogeny algorithm could run as follows.

(i) Compute the deformation map by differentiating certain modular equations giving a local model of $\mathcal{A}_g(\ell)$ and $\mathcal{A}_g$.

(ii) Compute $d\varphi$ from the deformation map by using an explicit version of the Kodaira–Spencer isomorphism, that is, an explicit way to map a pair (A, w) where w is an element of $\mathrm{Sym}^2 T_0(A)$ to the corresponding point of $T_A(\mathcal{A}_g)$ in the local model of $\mathcal{A}_g$.

(iii) Finally, reconstruct φ itself by solving a differential system in the formal group of A and performing a multivariate rational reconstruction, following [CE15; CMS+19]. In this last step, the characteristic of k should be large compared to ℓ. Otherwise, a standard solution is to use étaleness of the modular correspondence to lift the isogeny in characteristic zero.

The whole method, when applied to elliptic curves, is a reformulation of Elkies's algorithm.

In practice, working with stacks would involve adding an additional level structure and keeping track of automorphisms, which is not computationally convenient. Therefore, in order to make everything explicit in the case $g = 2$, we choose to replace the stack $\mathcal{A}_2$ by its coarse moduli scheme $\mathbf{A}_2$. We even work up to birationality, by considering the birational map from $\mathbf{A}_2$ to $\mathbb{A}^3$ defined by the three Igusa invariants (j_1, j_2, j_3), which are only defined for Jacobians of genus 2 curves. These modifications have the drawback of introducing the genericity assumptions in Theorem 1.1. When they are not satisfied, one would have to work at the level of stacks, or choose different coordinates, for instance when A or A' is a product of elliptic curves.

Thus, in the setting of abelian surfaces, the local model of $\mathcal{A}_g(\ell)$ in Step (i) is given by modular equations of Siegel type in Igusa invariants. In Step (ii), we assume that A is the Jacobian of a hyperelliptic genus 2 curve $\mathcal{C}$, as products of elliptic curves would simply reduce to the dimension 1 case. We encode a basis of $T_0(A)$ in the choice of an equation of $\mathcal{C}$; then, the explicit Kodaira–Spencer isomorphism is simply an expression for certain Siegel modular forms, namely derivatives of Igusa invariants, in terms of the coefficients of the curve. We compute these explicit formulas explicitly, building on work of Cléry, Faber, and van der Geer: see Theorem 3.14. This result of independent interest generalizes the classical formula

$$\frac{1}{2\pi i}\frac{dj}{d\tau} = -\frac{E_4^2 E_6}{\Delta}$$

in the case of elliptic curves. In Step (iii), we take advantage of the fact that the curve $\mathcal{C}$ embeds in its Jacobian to compute with power series in one variable only.

This paper is organized as follows. In Sections 2 and 3, we work over $\mathbb{C}$: Section 2 is devoted to the necessary background on modular forms and isogenies, and Section 3 is devoted to the explicit Kodaira–Spencer isomorphism and the computation of the tangent map. In Section 4, we call upon the language of algebraic stacks to show that the calculations over $\mathbb{C}$ remain valid over any base. We present the computation of the isogeny from its tangent map in Section 5, and review the whole algorithm in Section 6. Finally, in Appendix A, we present variants in the algorithm in the case of real multiplication by $\mathbb{Q}(\sqrt{5})$ and compute an example of cyclic isogeny of degree 11.

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 [vdGee08] for Siegel modular forms, and [Bru08] for Hilbert modular forms, where the general case is treated.

We write 4×4 matrices in block notation using 2×2 blocks. We write m^t for the transpose of a matrix m, and use the notations

$$m^{-t} = (m^{-1})^t, \qquad \mathrm{Diag}(x, y) = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}.$$

2.1 Siegel modular forms

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

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

is naturally endowed with the structure of a principally polarized abelian surface over $\mathbb{C}$. A basis of differential forms on $A(\tau)$ is given by

$$\omega(\tau) = (2\pi i\, dz_1, 2\pi i\, dz_2)$$

where z_1, z_2 are the coordinates on $\mathbb{C}^2$. Recall that the symplectic group $\mathrm{Sp}_4(\mathbb{Z})$ acts on $\mathbb{H}_2$ in the following way:

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

Proposition 2.1 [BL04, Rem. 8.1.4]. *Let $\tau \in \mathbb{H}_2$, and let $\gamma \in \mathrm{Sp}_4(\mathbb{Z})$ with blocks a, b, c, d. Then there is an isomorphism*

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

Theorem 2.2 [BL04, Prop. 8.1.3]. *Let A be a principally polarized abelian surface over $\mathbb{C}$. Then there exists $\tau \in \mathbb{H}_2$ 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 $\mathbf{A}_2(\mathbb{C}) = \mathrm{Sp}_4(\mathbb{Z})\backslash\mathbb{H}_2$ is the set of complex points of the coarse moduli space $\mathbf{A}_2$ alluded to in the introduction.

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 $f \colon \mathbb{H}_2 \to V$ satisfying the transformation rule

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

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

If A is a principally polarized abelian surface over $\mathbb{C}$ endowed with a basis ω of $\Omega^1(A)$ (the space of global differential forms on A), and if f is a Siegel modular form of weight ρ, then it makes sense to evaluate f on the pair (A, ω). We refer to §4 for a geometric interpretation of this fact. To compute this quantity, choose $\tau \in \mathbb{H}_2$ and an isomorphism $\eta \colon A \to A(\tau)$ as in Theorem 2.2.

Let $r \in \mathrm{GL}_2(\mathbb{C})$ be the matrix of the pullback map $\eta^* \colon \Omega^1(A(\tau)) \to \Omega^1(A)$ in the bases $\omega(\tau), \omega$. Then

$$f(A, \omega) = \rho(r) f(\tau).$$

We can check using Proposition 2.1 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

Classification of weights. Finite-dimensional holomorphic representations of $\mathrm{GL}_2(\mathbb{C})$ are well known. Let $n \geqslant 0$ 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

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

We take $(x^n, \ldots, x, 1)$ as the standard basis of $\mathbb{C}_n[x]$, so that we can write an endomorphism of $\mathbb{C}_n[x]$ as a matrix; in particular we have

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

Proposition 2.3. *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 $\mathfrak{sl}_2(\mathbb{C})$ [Bou72, Ch. III, §6.1, Th. 1]. By [Bou75, Ch. VIII, §1.3, Th. 1], irreducible representations of $\mathfrak{sl}_2(\mathbb{C})$ are classified by their highest weight; on the Lie group side, this shows that the holomorphic finite-dimensional irreducible representations of $\mathrm{SL}_2(\mathbb{C})$ are exactly the representations 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 f is of the form $\det^k$ for some $k \in \mathbb{Z}$, and in fact $k \geqslant 0$. We also say that f is a scalar-valued Siegel modular form of weight k. 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 $\mathbb{H}_2$ of any weight, with underlying vector space V. If $s \in \mathcal{M}_2(\mathbb{Z})$ is symmetric, then $f(\tau + s) = f(\tau)$ for every $\tau \in \mathbb{H}_2$. Hence, if we write

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

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 $n_1 \geqslant 0$, $n_3 \geqslant 0$, and $n_2^2 \leqslant 4 n_1 n_3$. Note that n_2 can still be negative.

When computing with q-expansions, we consider them as elements of the power series ring $\mathbb{C}[q_2, q_2^{-1}][[q_1, q_3]]$. 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 $\nu \geqslant 0$.

Structure of scalar-valued forms. The full graded $\mathbb{C}$-algebra of Siegel modular forms in genus 2 is not finitely generated [vdGee08, Lem. 4], but the subalgebra of scalar-valued modular forms is.

Theorem 2.4 [Igu62; Igu67]. *The graded $\mathbb{C}$-algebra of scalar-valued even-weight Siegel modular forms in genus 2 is generated by four algebraically independent elements $\psi_4, \psi_6, \chi_{10}$, and χ_{12} of respective weights 4, 6, 10, 12, and q-expansions*

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

The graded $\mathbb{C}$-algebra of scalar-valued Siegel modular forms in genus 2 is

$$\mathbb{C}[\psi_4, \psi_6, \chi_{10}, \chi_{12}] \oplus \chi_{35}\mathbb{C}[\psi_4, \psi_6, \chi_{10}, \chi_{12}]$$

where χ_{35} is a modular form of weight 35 and q-expansion

$$\chi_{35}(\tau) = q_1^2q_3^2(q_1 - q_3)(q_2 - q_2^{-1}) + O(q_1^4, q_3^4).$$

The q-expansions in Theorem 2.4 are easily computed from expressions in terms of theta functions, and their coefficients are integers. We warn the reader that different normalizations appear in the literature: our χ_{10} is -4 times the modular form χ_{10} appearing in Igusa's papers, our χ_{12} is 12 times Igusa's χ_{12}, and our χ_{35} is $4i$ times Igusa's χ_{35}.

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.

Following Streng [Str10, §2.1] and our choice of normalizations, we define the *Igusa invariants* to be

$$j_1 = 2^{-8}\frac{\psi_4\psi_6}{\chi_{10}}, \quad j_2 = 2^{-5}\frac{\psi_4^2\chi_{12}}{\chi_{10}^2}, \quad j_3 = 2^{-14}\frac{\psi_4^5}{\chi_{10}^2}.$$

They are Siegel modular functions of trivial weight, i.e. weight $\det^0$.

Proposition 2.5. *Igusa invariants define a birational map $\mathbf{A}_2(\mathbb{C}) \to \mathbb{C}^3$.*

Proof. By the theorem of Baily and Borel [BB66, Thm. 10.11], scalar-valued Siegel modular forms of sufficiently high even weight realize a projective embedding of $\mathbf{A}_2(\mathbb{C})$. Therefore, by Theorem 2.4, Igusa invariants generate the function field of $\mathbf{A}_2(\mathbb{C})$. □

Remark 2.6. Proposition 2.5 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 $\psi_4 = 0$. If one wants to consider these points nonetheless, it is best to make another choice of invariants: for instance one could use

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

which are generically well-defined on products of elliptic curves. See [Liu93, Thm. 1.V] for an interpretation of these invariants in terms of $j(E_1) + j(E_2)$ and $j(E_1)j(E_2)$ when evaluated on a product $E_1 \times E_2$.

Examples of vector-valued forms. Derivatives of Igusa invariants are modular function themselves; as explained in the introduction, this property stems from the existence of the Kodaira–Spencer isomorphism. It can also be seen as a special case of Rankin–Cohen operators [vdGee08, §25].

Proposition 2.7. *Let f be a Siegel modular function of trivial weight, and let*

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

Then $\dfrac{df}{d\tau}$ is a Siegel modular function of weight Sym^2.

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

We will use another vector-valued modular form in the sequel.

Example 2.8. Following Ibukiyama [Ibu12], let $E_8 \subset \mathbb{R}^8$ denote the lattice of half-integer vectors $v = (v_1, \dots, v_8)$ subject to the conditions

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

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 [CFvdG17] 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

In the context of Hilbert surfaces and abelian surfaces with real multiplication, we consistently use the following notation:

K	a real quadratic number field (embedded in $\mathbb{R}$)
Δ	the discriminant of K, so that $K = \mathbb{Q}(\sqrt{\Delta})$
$\mathbb{Z}_K$	the ring of integers in K
$\mathbb{Z}_K^\vee$	the trace dual of $\mathbb{Z}_K$, in other words $\mathbb{Z}_K^\vee = 1/\sqrt{\Delta}\ \mathbb{Z}_K$
$x \mapsto \bar{x}$	real conjugation in K
Σ	the embedding $x \mapsto (x, \bar{x})$ from K to $\mathbb{R}^2$.

Finally, we denote

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

A principally polarized abelian surface A over $\mathbb{C}$ has *real multiplication by* $\mathbb{Z}_K$ if it is endowed with an embedding

$$\iota \colon \mathbb{Z}_K \hookrightarrow \mathrm{End}^{\mathrm{sym}}(A),$$

where $\mathrm{End}^{\mathrm{sym}}(A)$ denotes the set of endomorphisms of A that are invariant under the Rosati involution.

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

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

is naturally endowed with the structure of a principally polarized abelian surface over $\mathbb{C}$, and has a real multiplication embedding $\iota_K(t)$ given by multiplication via Σ. It is also endowed with the basis of differential forms

$$\omega_K(t) = (2\pi i\, dz_1, 2\pi i\, dz_2).$$

The involution σ of $\mathbb{H}_1^2$ given by $\sigma\big((t_1, t_2)\big) = (t_2, t_1)$ exchanges the two differential forms in the basis, and exchanges the real multiplication embedding with its conjugate.

The embedding Σ induces a map $\Gamma_K \hookrightarrow \mathrm{SL}_2(\mathbb{R})^2$. Through this embedding, the group Γ_K acts on $\mathbb{H}_1^2$ by the usual action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathbb{H}_1$ on each coordinate.

Theorem 2.9 [BL04, §9.2]. *Let (A, ι) be a principally polarized abelian surface over $\mathbb{C}$ with real multiplication by $\mathbb{Z}_K$. Then there exists $t \in \mathbb{H}_1^2$ such that (A, ι) is isomorphic to $\big(A_K(t), \iota_K(t)\big)$, and t is uniquely determined up to action of Γ_K.*

The quotient $\mathbf{H}_2(\mathbb{C}) = \Gamma_K \backslash \mathbb{H}_1^2$ is the set of complex points of an algebraic variety $\mathbf{H}_2$ 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 $f \colon \mathbb{H}_1^2 \to \mathbb{C}$ satisfying the transformation rule

$$\forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_K,\ \forall t \in \mathbb{H}_1^2,\ f(\gamma t) = \big(c\, t_1 + d\big)^{k_1} \big(\bar{c}\, t_2 + \bar{d}\big)^{k_2} f(t).$$

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.

All irreducible finite-dimensional representations of $\mathrm{GL}_1(\mathbb{C})^2$ have dimension 1, so there is no need to consider vector-valued forms. The analogue of Proposition 2.7 for Hilbert modular forms is the following.

Proposition 2.10. *Let f be a Hilbert modular function of weight $(0,0)$. Then the partial derivatives $\partial f/\partial t_1$ and $\partial f/\partial t_2$ are Hilbert modular functions of weight $(2,0)$ and $(0,2)$ respectively.*

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

Let (A, ι) be a principally polarized abelian surface over $\mathbb{C}$ with real multiplication by $\mathbb{Z}_K$. As in the Siegel case, we would like to evaluate Hilbert modular forms when a basis of differential forms on A is given; this is possible if we restrict to bases of $\Omega^1(A)$ which behave well with respect to the real multiplication embedding.

Definition 2.11. Let ω be a basis of $\Omega^1(A)$. We say that (A, ι, ω) is *Hilbert-normalized* if for every $\alpha \in \mathbb{Z}_K$, the matrix of $\iota(\alpha)^* \colon \Omega^1(A) \to \Omega^1(A)$ in the basis ω is $\mathrm{Diag}(\alpha, \overline{\alpha})$.

If (A, ι, ω) is Hilbert-normalized and f is a Hilbert modular form of weight (k_1, k_2), then we compute the quantity $f(A, \iota, \omega)$ as follows. Choose $t \in \mathbb{H}_1^2$ and an isomorphism

$$\eta \colon (A, \iota) \to \big(A_K(t), \iota_K(t)\big)$$

as in Theorem 2.9, and let $r \in \mathrm{GL}_2(\mathbb{C})$ be matrix of η^* in the bases $\omega(t), \omega$. 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 $\mathbf{H}_2(\mathbb{C}) \to \mathbf{A}_2(\mathbb{C})$ from the Hilbert surface to the Siegel threefold. In fact, this forgetful map comes from a linear map

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

called the *Hilbert embedding*, which we now describe explicitly. Let (e_1, e_2) be the $\mathbb{Z}$-basis of $\mathbb{Z}_K$ given by $e_1 = 1$ and

$$e_2 = \frac{1 - \sqrt{\Delta}}{2} \quad \text{if } \Delta = 1 \bmod 4, \quad e_2 = \sqrt{\Delta} \quad \text{otherwise.}$$

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

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

Proposition 2.12. *For every $t \in \mathbb{H}_1^2$, left multiplication by R^t on $\mathbb{C}^2$ induces an isomorphism $A_K(t) \to A\big(H(t)\big)$.*

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

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

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

Proposition 2.13 [LY11, Prop. 3.1].

(i) Under H, the action of Γ_K on $\mathbb{H}_1^2$ is transformed into the action of $\mathrm{Sp}_4(\mathbb{Z})$ on $\mathbb{H}_2$ 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 $x^* = \mathrm{Diag}(x, \bar{x})$ for $x \in K$.

(ii) 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

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

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

Proposition 2.14. *Let $k \in \mathbb{Z}$, $n \in \mathbb{N}$, and let $f\colon \mathbb{H}_2 \to \mathbb{C}_n[x]$ be a Siegel modular form of weight $\rho = \det^k \mathrm{Sym}^n$. Define the functions $g_i\colon \mathbb{H}_1^2 \to \mathbb{C}$ for $0 \leqslant i \leqslant n$ by*

$$\forall t \in \mathbb{H}_1^2,\ \sum_{i=0}^{n} g_i(t)\, x^i = \rho(R) f\big(H(t)\big).$$

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

Proof. It is straightforward to check the transformation rule using Proposition 2.13. The heart of the computation is that 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 the quantity $(r_1 r_2)^k\, r_1^i\, r_2^{n-i}$. □

Corollary 2.15. *If f is a scalar-valued Siegel modular form of weight $\det^k$, then the function $H^*f : t \mapsto f\big(H(t)\big)$ is a symmetric Hilbert modular form of weight (k, k).*

Proof. Since $\det(R)^k$ is a nonzero constant, by Proposition 2.14, 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 2.13. □

The image of the Hilbert embedding in $\mathbf{A}_2(\mathbb{C})$ is called a *Humbert surface*. It can be described by an equation in terms of Igusa invariants, which grows quickly in size with the discriminant Δ, but can be computed in small cases [Gru10].

Proposition 2.16. *Igusa invariants generate the field of symmetric Hilbert modular functions of weight $(0, 0)$. They define a birational map from $\mathbf{H}_2(\mathbb{C})$ to the closed subset of $\mathbb{C}^3$ cut out by the Humbert equation.*

Proof. Let U the open set of $\mathbf{A}_2(\mathbb{C})$ defined by $\psi_4 \neq 0$ and $\chi_{10} \neq 0$. The Igusa invariants realize an isomorphism between U and an open set in $\mathbb{A}^3$. Therefore it is enough to show that the image of H intersects U, or in other words that both $H^*\chi_{10}$ and $H^*\psi_4$ via H are nonzero Hilbert modular forms. The pullback of χ_{10} is nonzero because a generic principally polarized abelian surface over $\mathbb{C}$ with real multiplication by $\mathbb{Z}_K$ is not a product of two elliptic curves [vdGee88, IX, Prop. 1.2]. Moreover the pullback of ψ_4 is nonzero, since its Fourier expansion as a Hilbert modular form has a nonzero constant term [LY11, Prop. 3.1]. □

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

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 $\pi\colon A \to A^\vee$. Recall that for every line bundle $\mathcal{L}$ on A, there is a

morphism $\phi_{\mathcal{L}}\colon A \to A^\vee$ defined by $\phi_{\mathcal{L}}(x) = T_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$, 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 2.17 [Mil86a, 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 $\phi_{\mathcal{L}_A^\xi} = \pi \circ \xi$. The map $\xi \mapsto \mathcal{L}_A^\xi$ 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 will consider two different isogeny types that we now define.

Definition 2.18. Let k be a field.

(i) 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

$$\varphi^*\mathcal{L}_{A'}^1 = \mathcal{L}_A^\ell.$$

(ii) 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

$$\forall \alpha \in \mathbb{Z}_K,\ \varphi \circ \iota(\alpha) = \iota'(\alpha) \circ \varphi.$$

For a generic principally polarized abelian surface, ℓ-isogenies are the simplest kind of isogenies that occur. 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 $N_{K/\mathbb{Q}}(\beta)$ [DJR+17, Prop. 2.1].

Both ℓ- and β-isogenies are easily described over $\mathbb{C}$. For $t = (t_1, t_2) \in \mathbb{H}_1^2$, write

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

The following well-known statement is a consequence of Theorems 2.2 and 2.9, using the facts that the kernel of an ℓ-isogeny is a maximal isotropic subgroup of the ℓ-torsion, and the kernel of a β-isogeny is a cyclic subgroup of the β-torsion.

Proposition 2.19.

(i) For every $\tau \in \mathbb{H}_2$, 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 let $\varphi\colon A \to A'$ be an ℓ-isogeny. Then there exists $\tau \in \mathbb{H}_2$ such that there is a commutative diagram

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

(ii) *For every $t \in \mathbb{H}_1^2$, 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 $t \in \mathbb{H}_1^2$ such that there is a commutative diagram

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

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 in the Hilbert case [MR20, Prop. 4.11].

Definition 2.20.

(i) Let $\ell \in \mathbb{N}$ be a prime. We call the *Siegel modular equations of level ℓ* the data of the three polynomials $\Psi_{\ell,1}, \Psi_{\ell,2}, \Psi_{\ell,3} \in \mathbb{C}(J_1, J_2, J_3)[J_1']$ defined as follows:
- $\Psi_{\ell,1}$ is the minimal polynomial of the function $j_1(\tau/\ell)$ over the field $\mathbb{C}\big(j_1(\tau), j_2(\tau), j_3(\tau)\big)$; in particular, $\Psi_{\ell,1}$ is monic.
- For $i \in \{2, 3\}$, we have the following equality of meromorphic functions:

$$j_i(\tau/\ell) = \Psi_{\ell,i}\big(j_1(\tau), j_2(\tau), j_3(\tau), j_1(\tau/\ell)\big).$$

(ii) 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 $\Psi_{\beta,1}, \Psi_{\beta,2}, \Psi_{\beta,3}$ defined as follows:
- $\Psi_{\beta,1}$ is the minimal polynomial of the function $j_1(t/\beta)$ over the field $\mathbb{C}\big(j_1(t), j_2(t), j_3(t)\big)$; in particular, $\Psi_{\beta,1}$ is monic.
- For $i \in \{2, 3\}$, we have the following equality of meromorphic functions:

$$j_i(t/\beta) = \Psi_{\beta,i}\big(j_1(t), j_2(t), j_3(t), j_1(t/\beta)\big).$$

In the Hilbert case, since Igusa invariants are symmetric by Corollary 2.15, the modular equations encode β- and $\overline{\beta}$-isogenies simulaneously [MR20, 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.

As explained in the introduction, modular equations really are equations for the image of a map defined at the level of algebraic stacks. As a consequence, they have coefficients in $\mathbb{Q}$. Since Igusa invariants have poles on $\mathbf{A}_2$ and $\mathbf{H}_2$, modular equations in genus 2 have denominators [MR20, §5]. If we multiply by these denominators, then we may consider modular polynomials as elements of $\mathbb{C}[J_1, J_2, J_3, J_1', J_2', J_3']$ that vanish on the Igusa invariants of isogenous Jacobians: this is what we do in the sequel.

From a practical point of view, modular equations in genus 2 are very large polynomials. This is especially true for Siegel modular equations of level ℓ. For each $1 \leqslant k \leqslant 3$, the degree of $\Psi_{\ell,k}$ in

each variable is $O(\ell^3)$, and the height of the coefficients is $O(\ell^3 \log \ell)$ [Kie22b]. The situation is less desperate for Hilbert modular equations of level β: the degree of each $\Psi_{\beta,k}$ in each variable is $O_K(N_{K/\mathbb{Q}}(\beta))$. Modular equations have been computed in full for $\ell = 2$ and 3 in the Siegel case, and up to $N(\beta) = 97$ in the Hilbert case for $K = \mathbb{Q}(\sqrt{2})$ using different invariants [Mil]. However, directly evaluating modular equations and their derivatives at a given point is much cheaper than writing down the modular equations in full [Kie21]. These evaluations are all we need to apply the isogeny algorithm.

3. Explicit Kodaira–Spencer over $\mathbb{C}$

A nonsingular hyperelliptic equation $\mathcal{C} : v^2 = E_{\mathcal{C}}(u)$ over $\mathbb{C}$ naturally encodes a basis of differential forms $\omega(\mathcal{C})$ on the principally polarized abelian surface $\mathrm{Jac}(\mathcal{C})$ (§3.1). If f is a Siegel modular function, this gives rise to a map

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

Then, $\mathrm{Cov}(f)$ is a *covariant* of the curve, and has an expression in terms of the coefficients. We give an algorithm to obtain this expression from the q-expansion of f (§3.2), and apply it to the derivatives of Igusa invariants (§3.3). The result is the explicit Kodaira–Spencer isomorphism. This allows us to compute the deformation map and the tangent map of a given ℓ-isogeny over $\mathbb{C}$ (§3.4). Finally, we adapt these methods to the Hilbert case (§3.5).

3.1 Hyperelliptic equations

Let $\mathcal{C}$ be a nonsingular hyperelliptic *equation* of genus 2 over $\mathbb{C}$:

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

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 $\mathbb{C}$ [Mil86b, Thm. 1.1 and Summary 6.11]. Choose a base point P on $\mathcal{C}$. This gives an embedding

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

Proposition 3.1 [Mil86b, Prop. 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 $\mathbb{C}$, and let*

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

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

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

Then the matrix of $\eta^* : \Omega^1(\mathcal{C}) \to \Omega^1(\mathcal{C}')$ in the bases $\omega(\mathcal{C}), \omega(\mathcal{C}')$ is r.

Proof. Write $(u, v) = \eta(x, y)$. A simple calculation shows that

$$\frac{du}{v} = (bx + d)\frac{dx}{y} \quad \text{and} \quad \frac{u\,du}{v} = (ax + c)\frac{dx}{y},$$

so the result follows. □

Corollary 3.3. *Let A be a principally polarized abelian surface over $\mathbb{C}$ 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 $\mathbb{C}$ such that*

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

Proof. By Torelli's theorem, there is a curve equation $\mathcal{C}_0$ over $\mathbb{C}$ such that A is isomorphic to $\mathrm{Jac}(\mathcal{C}_0)$. Then ω differs from $\omega(\mathcal{C}_0)$ by a linear transformation in $\mathrm{GL}_2(\mathbb{C})$. 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 such a matrix r. □

Definition 3.4. The bases of differential forms chosen in §2 allows us to define particular curve equations attached to a point of $\mathbb{H}_2$ or $\mathbb{H}_1^2$.

(i) Let $\tau \in \mathbb{H}_2$, 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. We define the meromorphic functions $a_i(\tau)$ for $0 \leqslant i \leqslant 6$ to be the coefficients of $\mathcal{C}(\tau)$:

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

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

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

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

Proof. Use Proposition 2.12 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 [Mes91].

Definition 3.7. Denote by $\mathbb{C}_6[x]$ the vector space of complex polynomials of degree at most 6. 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 which is compatible with the group action: for every $r \in \mathrm{GL}_2(\mathbb{C})$ and $W \in \mathbb{C}_6[x]$,

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

If $\dim V \geqslant 2$, then 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 fractional expression in terms of the coefficients.

It is enough to consider covariants of weight $\det^k \mathrm{Sym}^n$ for $k \in \mathbb{Z}$, $n \in \mathbb{N}$. What we call a vector-valued covariant of weight $\det^k \mathrm{Sym}^n$ is in Mestre's paper a covariant of order n and degree $k + n/2$; what we call a scalar-valued covariant of weight $\det^k$ is in Mestre's paper an invariant of degree 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 maps are inverse of each other.*

Proof. If f is a Siegel modular function, then $\mathrm{Cov}(f)$ 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. Lemma 3.2 and Proposition 3.5 give the transformation rules. □

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 [CFvdG17, §4].

Theorem 3.9. *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.*

Proof. The main difficulty is that singular hyperelliptic equations form a subset of codimension only 1 in the set of all degree 6 polynomials: if f is a Siegel modular form, then the proof of Proposition 3.8 only shows that $\mathrm{Cov}(f)$ is a polynomial divided by some power of the discriminant. However, one can show that f extends to the so-called toroidal compactification of $\mathbf{A}_2(\mathbb{C})$, and this proves that $\mathrm{Cov}(f)$ is well-defined on all curve equations with at most one node. Since the complement of this set has codimension 2, the result follows. □

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

Theorem 3.10 [Cle72, p. 296]. *The graded $\mathbb{C}$-algebra of covariants is generated by 26 elements defined over $\mathbb{Q}$. The number of generators of weight $\det^k \mathrm{Sym}^n$ 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 will 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' [Mes91], and set

$$I'_6 = (I_2 I_4 - 3I_6)/2.$$

Other generators are computed in [Mes91, §1] (in this reference, the integers m and n on page 315 should be the *orders* of f and g, and not their degrees). Denote the generator of weight $\det^{15}$ by R, and 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. Finally, the generator of weight $\det^{-2} \mathrm{Sym}^6$, denoted by X, is the degree 6 polynomial itself. To help the reader check their computations, we mention that the coefficient of $a_1^5 a_4^{10}$ in R is $2^{-2}3^{-6}5^{-10}$.

3.3 From q-expansions to covariants

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. The works of Igusa already provide the answer in the case of scalar covariants.

Theorem 3.11. *We have*

$$\begin{aligned} 4\ \mathrm{Cov}(\psi_4) &= I_4, \\ 4\ \mathrm{Cov}(\psi_6) &= I'_6, \\ 2^{12}\ \mathrm{Cov}(\chi_{10}) &= I_{10}, \\ 2^{15}\ \mathrm{Cov}(\chi_{12}) &= I_2 I_{10}, \\ 2^{37}3^{-9}5^{-10}\ \mathrm{Cov}(\chi_{35}) &= I_{10}^2 R. \end{aligned}$$

Proof. By [Igu62, p. 848], there exists a constant $\lambda \in \mathbb{C}^\times$ such that these relations hold up to a factor λ^k, for $k \in \{4, 6, 10, 12, 35\}$ respectively. Note that Igusa's covariant E is $-2^5 3^9 5^{10} R$. Then, Thomae's formulæ ([Mum84, Thm. IIIa.8.1] and [Tho70, pp. 216–217]) relating theta constants with the values of path integrals on the associated hyperelliptic curve imply that $\lambda = 1$. □

Therefore, the Igusa invariants satisfy

$$\mathrm{Cov}(j_1) = \frac{I_4 I'_6}{I_{10}}, \quad \mathrm{Cov}(j_2) = \frac{I_2 I_4^2}{I_{10}}, \quad \mathrm{Cov}(j_3) = \frac{I_4^5}{I_{10}^2}.$$

Let us compute 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 2.8.

Proposition 3.12. *We have* $\mathrm{Cov}(f_{8,6}/\chi_{10}) = X$. *In other words, for every* $\tau \in \mathbb{H}_2$ *such that* $\chi_{10}(\tau) \neq 0$, *we have*

$$\mathcal{C}(\tau) = \frac{f_{8,6}(\tau)}{\chi_{10}(\tau)}.$$

Proof. Since $f_{8,6}$ is a cusp form, by Theorem 3.9, $\mathrm{Cov}(f_{8,6}/\chi_{10})$ is a nonzero polynomial covariant of weight $\det^{-2}\mathrm{Sym}^6$. By Theorem 3.10, this space of covariants is of dimension 1 and generated by X, so the relation holds up to a factor $\lambda \in \mathbb{C}^\times$. This yields q-expansions for the coefficients $a_i(\tau)$ of $\mathcal{C}(\tau)$ up to a factor λ. Then, the relations from Theorem 3.11 imply $\lambda^4 = \lambda^6 = \lambda^{35} = 1$, hence $\lambda = 1$. □

Given a Siegel modular form f of weight ρ whose q-expansion can be computed, the following algorithm recovers the expression of $\mathrm{Cov}(f)$ as a polynomial.

Algorithm 3.13.

(i) Compute a basis $\mathcal{B}$ of the vector space of polynomial covariants of weight ρ using Theorem 3.10.

(ii) Choose a precision ν and compute the q-expansion of f modulo (q_1^ν, q_3^ν).

(iii) 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 3.12.

(iv) Do linear algebra; if the matrix does not have full rank, go back to step ii with a larger ν.

Sturm-type bounds [BP17] provide a theoretical limit for the precision ν that we need to consider; for the examples given in this article, $\nu = 3$ is enough.

We now apply Algorithm 3.13 to derivatives of Igusa invariants. Recall from Proposition 2.7 that for $1 \leqslant k \leqslant 3$, 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 3.14. *We have*

$$\begin{aligned}
\frac{1}{2\pi i}\mathrm{Cov}\Big(\frac{dj_1}{d\tau}\Big) &= \frac{1}{I_{10}}\Big(\frac{153}{8}I_2^2I_4y_1 - \frac{135}{2}I_2I_6y_1 + \frac{135}{2}I_4^2y_1 + \frac{46575}{4}I_2I_4y_2 \\
&\qquad - 30375\,I_6y_2 + 1366875\,I_4y_3\Big), \\
\frac{1}{2\pi i}\mathrm{Cov}\Big(\frac{dj_2}{d\tau}\Big) &= \frac{1}{I_{10}}\Big(90\,I_2^2I_4y_1 + 900\,I_2^2y_1 + 40500\,I_2I_4y_2\Big), \\
\frac{1}{2\pi i}\mathrm{Cov}\Big(\frac{dj_3}{d\tau}\Big) &= \frac{1}{I_{10}^2}\Big(225\,I_2I_4^4y_1 + 101250\,I_4^4y_2\Big).
\end{aligned}$$

Proof. Let $1 \leqslant k \leqslant 3$. The function $\chi_{10}^2 j_k$ has no poles on $\mathbf{A}_2(\mathbb{C})$. Therefore, the Siegel modular function

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

is holomorphic on $\mathbf{A}_2(\mathbb{C})$. Its q-expansion can be computed from the q-expansion of j_k by formal differentiation. Since

$$\frac{1}{2\pi i}\frac{\partial}{\partial \tau_i} = q_i\frac{\partial}{\partial q_i}$$

for $1 \leqslant i \leqslant 3$, we check that f_k is a cusp form. Therefore, by Theorem 3.9, $\mathrm{Cov}(f_k/\chi_{10})$ is a polynomial covariant of weight $\det^{20}\mathrm{Sym}^2$. Looking at the table in Theorem 3.10, 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 3.13 succeeds with $\nu = 3$; the computations were done using Pari/GP [The19]. □

Remark 3.15. Theorems 3.11 and 3.14 can be checked numerically. Computing big period matrices of hyperelliptic curves [MN19] provides pairs $(\tau, \mathcal{C}(\tau))$ with $\tau \in \mathbb{H}_2$. We can evaluate Igusa invariants at a given τ to high precision using their expression in terms of theta functions [Dup11]. Therefore we can also evaluate their derivatives numerically with high precision and compute the associated covariant using floating-point linear algebra. The computations were done using the libraries `hcperiods` [Mol18] and `cmh` [ET14]; they provide a nice consistency check to Theorem 3.14. Another consistency check is that we can recover the relations from Theorem 3.11.

Remark 3.16. From Theorem 3.14, we can easily obtain similar formulæ for derivatives of other invariants, or even invariants for abelian surfaces with extra structure such as theta constants. For instance, taking the invariants h_1, h_2, h_3 defined in Remark 2.6, we obtain

$$\begin{aligned}
\frac{1}{2\pi i}\mathrm{Cov}\Big(\frac{dh_1}{d\tau}\Big) &= \frac{1}{I_4^4}\Big(-\frac{297}{8}y_1I_4^2I_2^3 + -\frac{54675}{4}y_2I_4^2I_2^2 + \frac{1701}{8}y_1I_6I_4I_2^2 + \frac{135}{2}y_1I_4^3I_2 \\
&\quad + 1366875y_3I_4^2I_2 + \frac{346275}{4}y_2I_6I_4I_2 - \frac{1215}{4}y_1I_6^2I_2 + -\frac{405}{2}y_1I_6I_4^2 \\
&\quad - 4100625y_3I_6I_4 - \frac{273375}{2}y_2I_6^2\Big), \\
\frac{1}{2\pi i}\mathrm{Cov}\Big(\frac{dh_2}{d\tau}\Big) &= \frac{1}{I_4^4}\Big(-135y_1I_{10}I_2^2 - 60750y_2I_{10}I_2 + 900y_1I_{10}I_4\Big), \\
\frac{1}{2\pi i}\mathrm{Cov}\Big(\frac{dh_3}{d\tau}\Big) &= \frac{1}{I_4^5}\Big(-\frac{747}{8}y_1I_{10}I_4I_2^2 - \frac{155925}{4}y_2I_{10}I_4I_2 + 270y_1I_{10}I_6I_2 + \frac{135}{2}y_1I_{10}I_4^2 \\
&\quad + 1366875y_3I_{10}I_4 + 121500y_2I_{10}I_6\Big).
\end{aligned}$$

3.4 Deformation matrix and action on tangent spaces

Let $\mathcal{C}, \mathcal{C}'$ be equations of genus 2 hyperelliptic curves over $\mathbb{C}$, let A, A' be their Jacobians, and let $\varphi\colon A \to A'$ be an ℓ-isogeny. The choice of curve equations encodes a choice of bases of $\Omega^1(A)$ and $\Omega^1(A')$, or equivalently, by taking dual bases, a choice of bases of the tangent spaces $T_0(A)$ and $T_0(A')$. By an abuse of notation, we identify the tangent map $d\varphi\colon T_0(A) \to T_0(A')$ with its matrix written in these bases. Let us show how to compute $d\varphi$ from the data of the curve equations and modular equations of level ℓ.

Definition 3.17. It is convenient to introduce matrix notations.

– For $\tau \in \mathbb{H}_2$, we define

$$D_\tau J(\tau) = \left(\frac{1}{2\pi i}\frac{\partial j_k}{\partial \tau_l}(\tau)\right)_{1\leqslant k,l\leqslant 3} \cdot \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

In other words, if we set

$$v_1 = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad v_3 = \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix},$$

then the l-th column of $D_\tau J(\tau)$ contains (up to $2\pi i$) the derivatives of Igusa invariants at τ in the direction v_l. One can check that for $r \in \mathrm{GL}_2(\mathbb{C})$, the l-th column of $D_\tau J(\tau)\,\mathrm{Sym}^2(r)$ contains the derivatives of Igusa invariants at τ in the direction $r\,v_l\,r^t$.
Let (A,ω) be a principally polarized abelian surface over $\mathbb{C}$ with a basis of differential forms, let $\eta\colon A \to A(\tau)$ be an isomorphism for some $\tau \in \mathbb{H}_2$, and let r be the matrix of η^* in the bases $\omega(\tau), \omega$. Then the fact that derivatives of Igusa invariants have weight Sym^2 translates as

$$D_\tau J(A,\omega) = D_\tau J(\tau)\,\mathrm{Sym}^2(r^t).$$

We denote by

$$\mathcal{C} \mapsto D_\tau J(\mathcal{C})$$

the associated fractional covariant; Theorem 3.14 expresses the entries of this matrix up to a constant in terms of the coefficients of $\mathcal{C}$.

– Consider the Siegel modular equations $\Psi_{\ell,1}, \Psi_{\ell,2}, \Psi_{\ell,3}$ of level ℓ as elements of the ring $\mathbb{Q}[J_1, J_2, J_3, J_1', J_2', J_3']$. We define

$$D\Psi_{\ell,L} = \left(\frac{\partial \Psi_{\ell,n}}{\partial J_k}\right)_{1\leqslant n,k\leqslant 3} \quad \text{and} \quad D\Psi_{\ell,R} = \left(\frac{\partial \Psi_{\ell,n}}{\partial J_k'}\right)_{1\leqslant n,k\leqslant 3}.$$

Definition 3.18. Let φ be an ℓ-isogeny as above, write j as a shorthand for the Igusa invariants (j_1, j_2, j_3) of A, and j' for the invariants (j_1', j_2', j_3') of A'. We say that the isogeny φ is *generic* if the 3×3 matrices $D\Psi_{\ell,L}(j,j')$, $D\Psi_{\ell,R}(j,j')$, $D_\tau J(\mathcal{C})$ and $D_\tau J(\mathcal{C}')$ are invertible. In this case, we define the *deformation matrix* $\mathscr{D}(\varphi)$ of φ as

$$\mathscr{D}(\varphi) = -D_\tau J(\mathcal{C}')^{-1} \cdot D\Psi_{\ell,R}(j,j')^{-1} \cdot D\Psi_{\ell,L}(j,j') \cdot D_\tau J(\mathcal{C}).$$

In Section 4, we will interpret $\mathscr{D}(\varphi)$ as the matrix of the deformation map in the bases of $T_A(\mathcal{A}_2)$ and $T_{A'}(\mathcal{A}_2)$ associated with $\omega(\mathcal{C}), \omega(\mathcal{C}')$ via the Kodaira–Spencer isomorphism. Let us relate the deformation matrix $\mathscr{D}(\varphi)$ with the tangent matrix $d\varphi$.

Proposition 3.19. *Assume that φ is generic. Then we have*

$$\mathrm{Sym}^2(d\varphi) = \ell\,\mathscr{D}(\varphi).$$

Proof. By Proposition 2.19, we can find $\tau \in \mathbb{H}_2$ and isomorphisms η, η' such that there is a commutative diagram

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

Let r be the matrix of η^* in the bases $\omega(\tau), \omega(\mathcal{C})$, and define r' similarly. Then we have $d\varphi = r'^t r^{-t}$. By the definition of modular equations, we have

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

We differentiate with respect to τ_1, τ_2, τ_3 and obtain

$$D\Psi_{\ell,L}(j,j') \cdot D_\tau J(\tau) + \frac{1}{\ell} D\Psi_{\ell,R}(j,j') \cdot D_\tau J(\tau/\ell) = 0.$$

We rewrite this relation as

$$-\ell\, D\Psi_{\ell,L}(j,j') \cdot D_\tau J(\mathcal{C}) \cdot \mathrm{Sym}^2(r^t) = D\Psi_{\ell,R}(j,j') \cdot D_\tau J(\mathcal{C}') \cdot \mathrm{Sym}^2(r'^t),$$

and the result follows. □

Once we have $\mathscr{D}(\varphi)$, we easily obtain the matrix $d\varphi$ itself up to sign.

3.5 Explicit Kodaira–Spencer in the Hilbert case

We now explain how to recover the tangent matrix in the Hilbert case, in the same spirit as the Siegel case. An important difference is that we have to restrict to Hilbert-normalized bases of differential forms (recall Definition 2.11), so not all curve equations will do. For the moment, assume that we have a β-isogeny $\varphi\colon (A,\iota) \to (A',\iota')$ between abelian surfaces with real multiplication by $\mathbb{Z}_K$, and we are given curve equations $\mathcal{C}, \mathcal{C}'$ such that the associated bases $\omega(\mathcal{C})$ and $\omega(\mathcal{C}')$ are Hilbert-normalized. We address the question of constructing $\mathcal{C}, \mathcal{C}'$ in §3.6.

Definition 3.20.

- For $t \in \mathbb{H}_1^2$, we define
$$D_t J(t) = \left(\frac{1}{\pi i}\frac{\partial j_k}{\partial t_l}(t)\right)_{1\leqslant k\leqslant 3, 1\leqslant l\leqslant 2}.$$
If $\mathcal{C}$ is a curve equation such that $\omega(\mathcal{C})$ is Hilbert-normalized, we denote by $D_t J(\mathcal{C})$ the value of this modular form on $\mathcal{C}$.
- We define the 3×3 matrices $D\Psi_{\beta,L}$ and $D\Psi_{\beta,R}$ in the case of Hilbert modular equations of level β as in Definition 3.17.
- Write j as a shorthand for the Igusa invariants (j_1, j_2, j_3) of A, and j' for the invariants (j_1', j_2', j_3') of A'. We say that the isogeny φ is *generic* if the denominators of modular equations do not vanish at j and the 3×2 matrices
$$D\Psi_{\beta,L}(j,j')\cdot D_t J(\mathcal{C}) \quad \text{and} \quad D\Psi_{\beta,R}(j,j')\cdot D_t J(\mathcal{C}')$$
have rank 2.

Lemma 3.21. *Let (A,ι,ω) be Hilbert-normalized, and let $t \in \mathbb{H}_1^2$ such that there is an isomorphism $\eta\colon (A,\iota) \to (A_K(t), \iota_K(t))$. Let r be the matrix of η^* in the bases $\omega_K(t), \omega$. Then we have*
$$D_t J(A,\omega) = D_t J(t)\cdot r^2.$$

Proof. By Proposition 2.10, derivatives of Igusa with respect to t_1 and t_2 are Hilbert modular functions of weight $(2,0)$ and $(0,2)$ respectively. □

Proposition 3.22. *Let (A,ι,ω) be Hilbert-normalized. Then we have*
$$D_t J(A,\omega) = D_\tau J(A,\omega)\cdot T \qquad \text{where } T = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Proof. Let t, η, r as in Lemma 3.21, and write $\tau = H(t)$. By the expression of the Hilbert embedding, $D_t J(t)$ contains the derivatives of Igusa invariants at τ in the directions
$$\frac{1}{\pi i} R^t \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} R \quad \text{and} \quad \frac{1}{\pi i} R^t \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} R.$$
Hence we have
$$D_t J(t) = D_\tau J(\tau)\cdot \mathrm{Sym}^2(R^t)\cdot T.$$

By Proposition 2.12, we have an isomorphism $\zeta\colon A_K(t) \to A(\tau)$ such that the matrix of ζ^* in the bases $\omega(\tau), \omega_K(t)$ is R. Therefore

$$D_t J(A,\omega) = D_t J(t) r^2, \quad D_\tau J(A,\omega) = D_\tau J(\tau)\,\mathrm{Sym}^2((rR)^t).$$

The result follows. □

It is natural that the matrix R defining the Hilbert embedding does not appear in Proposition 3.22: evaluating derivatives of Igusa invariants on (A,ω) has an intrinsic meaning in terms of the Kodaira–Spencer isomorphism, and the choice of Hilbert embedding does not matter.

Proposition 3.23. *Let $\varphi\colon A \to A'$ be a β-isogeny and let $\mathcal{C}, \mathcal{C}'$ be Hilbert-normalized curve equations as above. Then the tangent matrix $d\varphi$ is diagonal, and we have*

$$D\Psi_{\beta,L}(j,j') \cdot D_t J(\mathcal{C}) = -D\Psi_{\beta,R}(j,j') \cdot D_t J(\mathcal{C}') \cdot \mathrm{Diag}(1/\beta, 1/\overline{\beta}) \cdot (d\varphi)^2.$$

Proof. By Proposition 2.19, we can find $t \in \mathbb{H}_1^2$ and isomorphisms η, η' such that there is a commutative diagram

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

Let r be the matrix of η^* in the bases $\omega_K(t), \omega$, and define r' similarly; they are diagonal. We have $d\varphi = r'^t r^{-t} = r' r^{-1}$. Differentiating the modular equations, we obtain

$$D\Psi_{\beta,L}(j,j') \cdot D_t J(t) + D\Psi_{\beta,R}(j,j') \cdot D_t J(t/\beta) \cdot \mathrm{Diag}(1/\beta, 1/\overline{\beta}) = 0.$$

By Lemma 3.21, we have

$$D_t J(t) = D_t J(\mathcal{C}) \cdot r^2, \quad D_t J(t/\beta) = D_t J(\mathcal{C}') \cdot r'^2$$

and the result follows. □

This relation allows us to compute $(d\varphi)^2$ from derivatives of modular equations when φ is generic. In contrast with the Siegel case, the knowledge of $(d\varphi)^2$ does not allow us to recover the diagonal matrix $d\varphi$ up to sign, as we have to perform two uncorrelated root extractions: we obtain two possible candidates.

3.6 Constructing Hilbert-normalized curves

Let (A,ι) be an abelian surface over $\mathbb{C}$ with real multiplication by $\mathbb{Z}_K$. Given the Igusa invariants (j_1, j_2, j_3) of A, we would like to construct a curve equation $\mathcal{C}$ such that $A = \mathrm{Jac}(\mathcal{C})$ and $(A, \iota, \omega(\mathcal{C}))$ is Hilbert-normalized. Our method is to compute a first curve equation using Mestre's algorithm [Mes91], and then look for a suitable homographic change of variables. However, we are missing some information, as the two pairs (A,ι) and $(A,\bar\iota)$, where $\bar\iota$ denotes the real conjugate of ι, have the same Igusa invariants. The best we can hope for is to obtain the following form.

Definition 3.24. A curve equation $\mathcal{C}$ such that $A = \mathrm{Jac}(\mathcal{C})$ is *potentially Hilbert-normalized* if $(A, \iota, \omega(\mathcal{C}))$ or $(A, \bar\iota, \omega(\mathcal{C}))$ is Hilbert-normalized.

This uncertainty is a consequence of our use of symmetric invariants on the Hilbert surface.

Proposition 3.25. *Let $\mathcal{C}$ be a hyperelliptic curve equation of genus 2 over $\mathbb{C}$ such that $\mathrm{Jac}(\mathcal{C})$ has real multiplication by $\mathbb{Z}_K$. Let (j_1, j_2, j_3) denote its Igusa invariants. Then the curve equation $\mathcal{C}$ is potentially Hilbert-normalized if and only if the two columns of the 3×2 matrix*

$$D_\tau J(\mathcal{C}) \cdot T \qquad \text{where } T = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix}$$

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

Proof. Let $t \in \mathbb{H}_1^2$ such that there is an isomorphism $\eta\colon \mathrm{Jac}(\mathcal{C}) \to A_K(t)$, and write $\tau = H(t)$. Let $r \in \mathrm{GL}_2(\mathbb{C})$ be the matrix of η^* in the bases $\omega_K(t), \omega$. Then the columns of $D_\tau J(\mathcal{C}) \cdot T$ contain, up to πi, the derivatives of Igusa invariants at τ in the directions

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

These directions are tangent to the Humbert surface if and only if r is is either diagonal or anti-diagonal. □

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 following algorithm reconstructs a potentially Hilbert-normalized curve equation.

Algorithm 3.26.

(i) Construct any curve equation $\mathcal{C}_0$ with Igusa invariants (j_1, j_2, j_3) using Mestre's algorithm.

(ii) Find $r \in \mathrm{GL}_2(\mathbb{C})$ such that the two columns of the matrix

$$D_\tau J(\mathcal{C}_0) \cdot \mathrm{Sym}^2(r^t) \cdot T$$

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

(iii) Output $\det{}^{-2} \mathrm{Sym}^6(r)\mathcal{C}_0$.

In step ii, if a, b, c, d denote the entries of r, we only have to solve a quadratic equation in a, c, and a quadratic equation in b, d. Therefore Algorithm 3.26 costs $O_K(1)$ square roots and field operations.

In practice, when computing a β-isogeny $\varphi\colon A \to A'$ in the Hilbert case, we are only given the Igusa invariants of A and A'. Constructing potentially Hilbert-normalized curves is then equivalent to making a choice of real multiplication embedding for each abelian surface. If these embeddings are incompatible via φ, we obtain antidiagonal matrices when computing the tangent matrix; in this case, we apply the change of variables $x \mapsto 1/x$ on one of the curve equations to make them compatible. Even if they are compatible, φ will be either a β- or a $\overline{\beta}$-isogeny depending on the choices of real multiplication embeddings. Therefore we really obtain four candidates for the tangent matrix, among which only one is correct.

4. Moduli spaces and the deformation map

In this section, we use the language of algebraic stacks to show how to compute the deformation map of a given isogeny φ, and to show its relation with the tangent map $d\varphi$, for abelian schemes of any dimension over any base.

We recommend to the reader who is only interested in abelian surfaces over fields, and who is satisfied with lifting arguments to apply the characteristic zero results of Section 3, and the genericity hypotheses used in Theorem 1.1, to directly skip to Section 5.

We start by recalling well-known and general facts about separated Deligne–Mumford stacks and their coarse moduli spaces (§4.1). Then we recall the properties of several moduli stacks for principally polarized abelian schemes of dimension g, namely $\mathcal{A}_g$ (abelian schemes with no extra structure), $\mathcal{A}_{g,n}$ (abelian schemes with a level n structure), $\mathcal{A}_g(\ell)$ (abelian schemes endowed with the kernel of an ℓ-isogeny), and their coarse moduli schemes $\mathbf{A}_g$, $\mathbf{A}_{g,n}$, $\mathbf{A}_g(\ell)$ (§4.2). In particular, we have a map at the level of algebraic stacks,

$$\Phi_\ell = (\Phi_{\ell,1}, \Phi_{\ell,2}) \colon \mathcal{A}_g(\ell) \to \mathcal{A}_g \times \mathcal{A}_g$$

sending (A, K) to $(A, A/K)$ such that both $\Phi_{\ell,1}$ and $\Phi_{\ell,2}$ are étale. Therefore, for an ℓ-isogeny φ seen as a point of $\mathcal{A}_g(\ell)$, the deformation map

$$\mathscr{D}(\varphi) = d\Phi_{\ell,2}(\varphi) \circ d\Phi_{\ell,1}(\varphi)^{-1}$$

is well-defined at the level of stacks. However, the induced maps at the level of coarse spaces,

$$(\mathbf{\Phi}_{\ell,1}, \mathbf{\Phi}_{\ell,2}) \ : \ \mathbf{A}_g(\ell) \to \mathbf{A}_g \times \mathbf{A}_g$$

are not étale everywhere, so that we can only recover the deformation map on an open set of the coarse spaces (see Corollary 4.10). In the genus 2 case, when we work with the modular polynomials $\Psi_{\ell,i}$ from Section 2.6, this phenomenon worsens; still, we can give precise conditions on the isogeny that ensure genericity in the sense of Definition 3.18 (see Proposition 4.13). We also extend these results to the Hilbert case.

After that, we give the general relation between the tangent map and the deformation map of a given ℓ- or β-isogeny (§4.3). Finally we show that in dimension 2, the relations between modular forms and covariants given in Proposition 3.12 hold over $\mathbb{Z}$ and not only over $\mathbb{C}$ (§4.4). This allows us to give an explicit version of the Kodaira–Spencer isomorphism over any base (§4.5), that we could use for instance to construct explicit families of abelian surfaces with real multiplication.

In summary, this section explains the relationship between the fine moduli space $\mathcal{A}_g(\ell)$ and its coarse moduli space $\mathbf{A}_g(\ell)$, and the geometric meaning of the genericity conditions of Theorem 1.1; moreover it gives a purely algebraic, rather than analytic, interpretation of the results of Section 3. Another way to extend the results of Section 3 over any base would be to lift the isogeny to characteristic zero (in the case of fields), then interpolate between fibers using rigidity; however, we find that the moduli-theoretic approach is superior as it provides more geometric insight.

4.1 Coarse moduli spaces

In this paper, we always assume stacks to be of finite type over a Noetherian base scheme S. Let $\mathscr{X}$ be a separated Deligne–Mumford stack over S; we recall that an Artin stack is Deligne–Mumford if and only if its diagonal is unramified [The18, Tag 06N3]. Here we summarize well-known results on the geometry of $\mathscr{X}$ and its coarse moduli space.

By a *point* x of $\mathscr{X}$, we mean a point of the underlying topological space $|\mathscr{X}|$, and we implicitly take a representative $\operatorname{Spec} k \to \mathscr{X}$ of x. For any scheme T, a *T-point* of $\mathscr{X}$ is a morphism $T \to \mathscr{X}$. We denote by $I_{\mathscr{X}}$ the inertia stack of $\mathscr{X}$, and if x is a point of $\mathscr{X}$, we denote by I_x the pullback of $I_{\mathscr{X}}$ to x; this pullback is simply the space $\operatorname{Aut}(x)$ of automorphisms, or stabilizers, of x. Since we assume $\mathscr{X}$ separated, I_x is in fact finite. The stabilizer I_x does not depend on the representative chosen since I_x is the pullback of the residual gerbe $G_x \to k(\xi)$ at x through $\operatorname{Spec} k \to \operatorname{Spec} k(\xi)$:

see [LM00, Ch. 11], [The18, Tag 06ML]. We identify open substacks of $\mathscr{X}$ with the underlying open topological spaces of $|\mathscr{X}|$ [The18, Tag 06FJ].

We recall that a map $f\colon \mathscr{X} \to \mathscr{Y}$ is representable if and only if the induced map $I_{\mathscr{X}} \to \mathscr{X} \times_{\mathscr{Y}} I_{\mathscr{Y}}$ is a monomorphism [The18, Tag 04YY]. Also, if f is unramified, then its diagonal is étale by [The18, Tag 0CIS] and [Ryd11]; hence the map $I_{\mathscr{X}} \to \mathscr{X} \times_{\mathscr{Y}} I_{\mathscr{Y}}$ is étale. Therefore, if f is representable and unramified, then the map $I_{\mathscr{X}} \to \mathscr{X} \times_{\mathscr{Y}} I_{\mathscr{Y}}$ is an open immersion.

A *coarse moduli space* X of $\mathscr{X}$ is an algebraic space X endowed with a map $\pi\colon \mathscr{X} \to X$ such that π is categorical and induces a bijection $\pi\colon \mathscr{X}(k) \to X(k)$ for every algebraically closed field k. We also use the following terminology from [MFK94] (see also [KM97, Def. 1.8] and [Ryd13, Defs. 2.2 and 6.1]): a map $q\colon \mathscr{X} \to Z$ is *topological* if q is a universal homeomorphism, and *geometric* if it is topological and furthermore $\mathcal{O}_Z \to q_*\mathcal{O}_{\mathscr{X}}$ is an isomorphism. A *GC quotient* is a geometric quotient that is also (uniformly) categorical; in particular, its image is a coarse moduli space ([KM97, Def. 1.8] and [Ryd13, Def. 3.17 and Rem. 3.18]).

Theorem 4.1. *Let $\mathscr{X} \to S$ be a separated Deligne–Mumford stack.*

(i) (Keel–Mori). There exists a coarse moduli space $\pi\colon \mathscr{X} \to X$, where X is of finite type over S. The map π is a GC quotient, is proper, quasi-finite and separated; moreover the construction is stable under flat base change.

(ii) Let $x \in X(k)$ be a point, and let I_x be the stabilizer of any point in $\mathscr{X}$ above x. Then étale-locally around x, $\mathscr{X}$ is a quotient stack by I_x and X is a geometric quotient by I_x. More precisely, there is an affine scheme U, an étale morphism $U \to X$ whose image contains x, and a finite morphism $V \to U$ with an action of I_x on V such that $\mathscr{X}_U := \mathscr{X} \times_X U = [V/I_x]$ is an I_x-quotient stack, and $U = V/I_x$.

Proof. Theorem 4.1.(i) is valid for Artin stacks with finite inertia; the original proof is in [KM97], and reformulations of the proof using the language of stacks rather than groupoids are given in [Con05], [Ryd13] and [The18, Tag 0DUK]. Since $\mathscr{X}$ is a separated Deligne–Mumford stack, its inertia $I_{\mathscr{X}}$ is finite, so the Keel–Mori theorem applies.

For Theorem 4.1.(ii), see [AV02, Lem. 2.2.3] which shows that $\mathscr{X}$ is locally a quotient, and [Ols06, Thm. 2.12] which shows that we can take the quotient to be a quotient by I_x. If $V = \operatorname{Spec} R$, then V/I_x is the affine scheme $\operatorname{Spec} R^{I_x}$. The fact that $U = (\operatorname{Spec} R)/I_x$ then follows easily from the theory of quotients of affine schemes: see for instance [Ryd13, §4] or [DR73, §I.8.2.2]. See also [The18, Tag 0DU0] for extensions of this result in the case of quasi-DM stacks, and [AHR19; AHR20] for a far reaching generalization. □

By Zariski's main theorem, the coarse moduli space X is characterized by the fact that $\pi\colon \mathscr{X} \to X$ is proper and quasi-finite, and $\mathcal{O}_X \simeq \pi_\star\mathcal{O}_{\mathscr{X}}$ on the étale site [Con05, §1].

The formation of coarse moduli spaces is not stable under base change in general. This causes problems when reducing coarse moduli spaces, defined for instance over $\mathbb{Z}$, modulo a prime p, as the morphism $\operatorname{Spec} \mathbb{F}_p \to \operatorname{Spec} \mathbb{Z}$ is not flat. Coarse moduli spaces have better properties in the case of *tame* stacks.

The stack $\mathscr{X}$ is said to be tame [AOV08] if the map $\pi\colon \mathscr{X} \to X$ is cohomologically affine; in particular it is a good moduli space in the sense of [Alp13]. A finite fppf group scheme G/S is *linearly reductive* if $BG \to S$ is tame ([MFK94], [AOV08, Def. 2.4], [Alp13, Def. 12.1]). In [AOV08], it is shown that G/S is linearly reductive if and only if its geometric fibers are geometrically reductive, if and only if its geometric fibers are locally (in the fppf topology) a split extension of a

constant tame group by a group of multiplicative type. If $x \in \mathscr{X}(k)$ is a geometric point of $\mathscr{X}$, we say that x is a *tame point* of $\mathscr{X}$ if x has a linearly reductive stabilizer.

Theorem 4.2. *Let $\mathscr{X} \to S$ be a separated Deligne–Mumford stack, and let $\pi\colon \mathscr{X} \to X$ be its coarse moduli space.*

(i) If every geometric point of $\mathscr{X}$ is tame, then $\mathscr{X}$ is tame. If $\mathscr{X}$ is tame, then the formation of its coarse space commutes with arbitrary base change.
(ii) More generally, if $x \in \mathscr{X}(k)$ is tame, then there is an open tame substack $\mathscr{U}$ of $\mathscr{X}$ containing x. Furthermore, the image of $\mathscr{U}$ in X is Cohen–Macaulay.
(iii) The map $\pi\colon \mathscr{X} \to X$ is always an adequate moduli space in the sense of [Alp14]. In particular, if $T \to S$ is a morphism of algebraic spaces, $\mathscr{X}_T$ denotes the base change of $\mathscr{X}$ to T and X_T denotes the coarse moduli space of $\mathscr{X}_T$, then the natural map $\mathsf{X}_T \to X \times_S T$ is an universal homeomorphism.

Proof. Theorems 4.2.(i) and 4.2.(ii) are proved in the case of Artin stacks with finite inertia in [AOV08]. The openness of tame points is the main result of this paper [AOV08, Thm. 3.2, Prop. 3.6]. Since we restrict to separated Deligne–Mumford stacks, it also follows from Theorem 4.1.(ii). Formation of the coarse moduli space commutes with pullbacks in the tame case by [AOV08, Cor. 3.3].

If x is a tame point of $\mathscr{X}$, then by the local structure theorem, étale-locally around x, there is an open substack of the form $\mathscr{U} = [V/I_x]$, and I_x is linearly reductive. By the Hochster–Roberts theorem [MFK94, Appendix 1.E], the affine scheme V/I_x is Cohen–Macaulay. Being Cohen–Macaulay is a local notion for the étale topology, so the image of $\mathscr{U}$ in X is also Cohen–Macaulay.

Finally, Theorem 4.2.(iii) is proved in [Alp14], which shows that the coarse moduli space of an Artin stack with finite inertia is always an adequate moduli space. The natural map $\mathsf{X}_T \to X \times_S T$ is then an adequate homeomorphism in the sense of [Alp14], and in particular is a universal homeomorphism [Alp14, Main Theorem]. □

Corollary 4.3. *Let $\mathscr{X}$ be a separated Deligne–Mumford stack.*

(i) The set $\mathscr{U}$ of points x such that I_x is trivial is an open substack of $\mathscr{X}$ (which may be empty), and $\pi\colon \mathscr{U} \to \pi(\mathscr{U})$ is an isomorphism.
(ii) Let $x \in \mathscr{X}(k)$ be a point, and let $\widehat{O}_{\mathscr{X},x}$ be the strict Hensel ring of $\mathscr{X}$ at x. Then

$$\widehat{O}_{X,x} = \widehat{O}_{\mathscr{X},x}^{I_x}. \tag{1}$$

In particular, if $\mathscr{X}$ is normal, then its coarse moduli space is normal.

Proof. These two statements are immediate consequences of Theorem 4.1.(ii). For Corollary 4.3.(ii), see also [DR73, §I.8.2.1] which states that the kernel of the action of I_x acting on $\widehat{O}_{\mathscr{X},x}$ is exactly the set of automorphisms of x that can be extended to $\operatorname{Spec} \widehat{O}_{\mathscr{X},x} \to \mathscr{X}$. □

Finally, we know when an étale map between algebraic stacks induces an étale map on their coarse moduli spaces.

Theorem 4.4 Luna's fundamental lemma. *Let $f\colon \mathscr{X} \to \mathscr{Y}$ be a representable and unramified morphism of separated Deligne–Mumford stacks. Then the set of points where f is* stabilizer preserving, *meaning that the monomorphism on inertia $I_x \to I_{f(x)}$ induced by f is an isomorphism, is an open substack $\mathscr{U}$ of $\mathscr{X}$. The morphism $I_{\mathscr{U}} \to I_{\mathscr{Y}} \times_{\mathscr{Y}} \mathscr{U}$ induced by f is an isomorphism.*

If f is étale and $\mathscr{U} = \mathscr{X}$, that is if f is stabilizer preserving at every point, then the induced map on coarse spaces $f_0\colon X \to Y$ is étale, and even strongly étale; in other words $\mathscr{X} = X \times_Y \mathscr{Y}$.

Proof. The fact that $\mathscr{U}$ is open is [The18, Tag 0DUA], [Ryd13, Prop. 3.5]. Since $\mathscr{X}$ and $\mathscr{Y}$ are separated Deligne–Mumford stacks, the induced map is étale by Corollary 4.3.(ii).

The general case of Artin stacks with finite inertia is treated in [Ryd13, Prop. 6.5 and Thm. 6.10]. In this reference, *stabilizer preserving* is called *fixed point reflecting*, but we prefer to use the terminology of the Stacks project [The18, Tag 0DU6]. The fact that f_0 is strongly étale comes from the cartesian diagram in [Ryd13, Thm. 6.10]. See also [AHR19, Thm. 3.14] where this is proved in a more general setting. □

Remark 4.5. If $f\colon \mathscr{X} \to \mathscr{Y}$ is proper (resp. finite), then the induced map $f_0\colon X \to Y$ is proper (resp. finite), because the maps from $\mathscr{X}$ and $\mathscr{Y}$ to their coarse moduli spaces are proper quasi-finite [The18, Tag 02LS], [Gro64, EGA IV.8.11.1]).

Remark 4.6. If x is a tame smooth k-point of $\mathscr{X}$, then by Luna's étale slice theorem ([Lun73], [AHR20, Thm 1.1 and Thm 2.1], [AHR19, Thm 19.4]), the étale local structure of Theorem 4.1.(ii) takes a particularly nice form. Indeed, taking an étale local presentation $\mathscr{X}_U = [V/I_x]$ as in Theorem 4.1.(ii), then (possibly after an étale extension of k and after shrinking V) there is a strongly étale morphism $[V/I_x] \to [T_x\mathscr{X}/I_x]$ which sends x to 0, where I_x acts via its natural linear action on $T_x\mathscr{X}$. In particular, étale locally around x the map $\pi\colon \mathscr{X} \to X$ is given by $[T_x\mathscr{X}/I_x] \to T_x\mathscr{X}/I_x$.

4.2 Moduli stacks of abelian varieties

In this section, we apply the general results gathered in §4.1 to the case of moduli spaces of abelian schemes. This allows us to investigate the properties of the map Φ_ℓ on coarse moduli spaces in the Siegel case, and its analogue Φ_β in the Hilbert case.

4.2.1 *Siegel stacks* Recall that we denote by $\mathcal{A}_g$ the moduli stack of principally polarized abelian varieties, and by $\mathcal{A}_{g,n}$ the moduli stack of principally polarized abelian varieties with a level n symplectic structure; here we mean a level $(\mathbb{Z}/n\mathbb{Z})^{2g}$ structure as in [FC90] rather than a $(\mathbb{Z}/n\mathbb{Z})^g \times \mu_n^g$ structure as in [Mum71; dJon93], so that $\mathcal{A}_{g,n}$ is defined over $\mathbb{Z}[1/n]$ rather than over $\mathbb{Z}$. Both $\mathcal{A}_g$ and $\mathcal{A}_{g,n}$ are separated Deligne–Mumford stacks, and moreover $\mathcal{A}_{g,n}$ is smooth over $\mathbb{Z}[1/n]$ with $\phi(n)$ geometrically irreducible fibers [FC90].

We denote by $\mathbf{A}_g$, $\mathbf{A}_{g,n}$ their corresponding coarse moduli spaces. By Mumford's Geometric Invariant Theory [MFK94], they are quasi-projective schemes. We can extend $\mathbf{A}_{g,n}$ over $\mathbb{Z}$ by taking the normalization of $\mathbf{A}_g$ in $\mathbf{A}_{g,n}/\mathbb{Z}[1/n]$, as in [Mum71; DR73; dJon93]. Over $\mathbb{C}$, the analytification of $\mathcal{A}_g$ is the Siegel space $\mathbb{H}_g/\operatorname{Sp}_{2g}(\mathbb{Z})$ seen as an orbifold.

If $n \geqslant 3$, then the inertia of the stack $\mathcal{A}_{g,n}$ is trivial. Therefore $\mathcal{A}_{g,n}$ is isomorphic to $\mathbf{A}_{g,n}$ by Corollary 4.3.(i), and $\mathbf{A}_{g,n}$ is smooth over $\mathbb{Z}[1/n]$. This shows in particular that there is a p_0 such that $\mathcal{A}_g$ is tame at every abelian variety defined over a field of characteristic $p \geqslant p_0$.

If $n \leqslant 2$, then the generic automorphism group on $\mathcal{A}_{g,n}$ is μ_2. We can rigidify $\mathcal{A}_{g,n}$ by μ_2 in such a way that $\mathcal{A}_{g,n} \to [\mathcal{A}_{g,n}/\mu_2]$ is a μ_2-gerbe [AOV08, Appendix A]. The map $\mathcal{A}_{g,n} \to \mathbf{A}_{g,n}$ factors through $[\mathcal{A}_{g,n}/\mu_2]$, so the coarse moduli space of $[\mathcal{A}_{g,n}/\mu_2]$ is still $\mathbf{A}_{g,n}$. By Theorem 4.1.(ii) or Theorem 4.2.(ii), there exists an affine étale open scheme U above $\mathbf{A}_{g,n}$ whose image is dense and contains all points with only generic automorphisms. Then $[\mathcal{A}_{g,n}/\mu_2] \to \mathbf{A}_{g,n}$ becomes an isomorphism over U by Corollary 4.3.(i). Since $[\mathcal{A}_{g,n}/\mu_2]$ is smooth, the image of U in $\mathbf{A}_{g,n}$ is also smooth by étale descent.

We now proceed to construct the moduli stack $\mathcal{A}_g(\ell)$ that parametrizes ℓ-isogenies. If Γ is a congruence subgroup of $\operatorname{Sp}_{2g}(\widehat{\mathbb{Z}})$, and n is an integer such that the congruence subgroup $\Gamma(n)$

is contained in Γ, we define $\mathcal{A}_{g,\Gamma}/\mathbb{Z}[1/n]$ as the quotient stack $[\mathcal{A}_{g,n}/\widetilde{\Gamma}]$ where $\widetilde{\Gamma}$ is the image of Γ in $\mathrm{Sp}_{2g}(\mathbb{Z}/n\mathbb{Z})$, and $\mathbf{A}_{g,\Gamma}$ the corresponding coarse moduli space. A T-point of $[\mathcal{A}_{g,n}/\widetilde{\Gamma}]$ corresponds to an abelian scheme A/T which is étale-locally endowed with a level n structure modulo the action of $\widetilde{\Gamma}$ [DR73, §IV.3.1]. The maps $\mathcal{A}_{g,n} \to \mathcal{A}_{g,\Gamma}$ and $\mathcal{A}_{g,\Gamma} \to \mathcal{A}_g$ are finite, étale, and representable [DR73, §IV.2, §IV.3]. We can extend $\mathbf{A}_{g,\Gamma}$ to $\mathbb{Z}$ by normalization, as we did for $\mathbf{A}_{g,n}$. We can check as in [DR73, §IV.3.6] that the definition does not depend on the integer n such that $\Gamma(n) \subset \Gamma$.

We apply this construction to $\Gamma = \Gamma_0(\ell)$, the standard congruence subgroup encoding ℓ-isogenies, and we denote by $\mathcal{A}_g(\ell) \coloneqq \mathcal{A}_{g,\Gamma_0(\ell)}$ the resulting stack. The stack $\mathcal{A}_g(\ell)$ is smooth over $\mathbb{Z}[1/\ell]$. We denote by

$$\Phi_\ell = (\Phi_{\ell,1}, \Phi_{\ell,2})\colon \mathcal{A}_g(\ell) \to \mathcal{A}_g \times \mathcal{A}_g$$

the map $(A, K) \mapsto (A, A/K)$.

Proposition 4.7.

(i) The maps $\Phi_{\ell,1}$ and $\Phi_{\ell,2}$ are finite, étale and representable.

(ii) Let $x \in \mathcal{A}_g(\ell)(k)$ be a point represented by (A, K), and let $K' \subset A/K$ be the kernel of the contragredient isogeny. Then $\Phi_{\ell,1}$ is stabilizer preserving at x if and only if all automorphisms of A stabilize K, and $\Phi_{\ell,2}$ is stabilizer preserving at x if and only if all automorphisms of A/K stabilize K'.

Proof. The automorphisms of x in $\mathcal{A}_g(\ell)$ are exactly the automorphisms of A stabilizing K. In particular $\Phi_{\ell,1}$ induces a monomorphism of the automorphism groups, and is therefore representable; it is stabilizer preserving if and only if all automorphisms of A stabilize K.

If α is an automorphism of (A, K), then α descends to $A' = A/K$, so $\Phi_{\ell,2}$ is representable as well. An automorphism of A' comes from an automorphism of A if and only if it stabilizes K', hence the condition for $\Phi_{\ell,2}$ to be stabilizer preserving.

Finally, the map $\Phi_{\ell,1}$ is finite étale because it is of the form $\mathcal{A}_{g,\Gamma} \to \mathcal{A}_g$ for $\Gamma = \Gamma_0(\ell)$. Denote by $\pi_1\colon \mathscr{X}_g \to \mathcal{A}_g$ the universal abelian scheme, and by $\pi_\ell\colon \mathscr{X}_g(\ell) \to \mathcal{A}_g(\ell)$ the universal abelian scheme with a $\Gamma_0(\ell)$-level structure. Then the universal isogeny $f\colon \mathscr{X}_g(\ell) \to \mathscr{X}_g \times_{\mathcal{A}_g} \mathcal{A}_g(\ell)$ is separable over $\mathbb{Z}[1/\ell]$. If we let $s_1\colon \mathcal{A}_g \to \mathscr{X}_g$ and $s_\ell\colon \mathcal{A}_g(\ell) \to \mathscr{X}_g(\ell)$ be the zero sections, then we have

$$\Phi_{\ell,2} = \Phi_{\ell,1} \circ \pi_1 \times_{\mathcal{A}_g} \mathcal{A}_g(\ell) \circ f \circ s_\ell.$$

Therefore $\Phi_{\ell,2}\colon \mathcal{A}_g(\ell) \to \mathcal{A}_g$ is finite étale as well. □

The map Φ_ℓ induces a map $\mathbf{\Phi}_\ell\colon \mathbf{A}_g(\ell) \to \mathbf{A}_g^2$ on the coarse moduli spaces. This map is not injective, but the same reasoning as in [DR73, §VI.6] shows that it is generically radicial, and even a birational isomorphism. The open subscheme U of $\mathbf{A}_g(\ell)$ where $\mathbf{\Phi}_\ell$ is an embedding is dense in every fiber of characteristic $p \nmid \ell$.

Proposition 4.8. *Let Ψ_0 denote the schematic image of $\mathbf{\Phi}_\ell$. Then $\mathbf{A}_g(\ell)$ is the normalization of Ψ_0. If x_0 lies in the image, then $\mathbf{\Phi}_\ell\colon \mathbf{A}_g(\ell) \to \Psi_0$ induces a local isomorphism around x_0 if and only if x_0 is normal in Ψ_0.*

Proof. The map $\mathbf{A}_g(\ell) \to \Psi_0$ is separated quasi-finite, and birational by the discussion above. Since $\mathbf{A}_g(\ell)$ is normal by Corollary 4.3.(ii), we deduce that $\mathbf{A}_g(\ell)$ is the normalization of Ψ_0 by Zariski's main theorem [Gro64, Cor. IV.8.12.11].

If $\mathbf{\Phi}_\ell$ induces a local isomorphism at x_0, then x_0 is normal since $\mathbf{A}_g(\ell)$ is normal. In fact it suffices to ask that $\mathbf{\Phi}_\ell\colon \mathbf{A}_g(\ell) \to \Psi_0$ is étale at x, because normality is a local notion in the smooth topology [The18, Tag 034F]. The converse also follows from Zariski's main theorem [Gro64, Cor. IV.8.12.10 and Cor. IV.8.12.12]: there exists an open neighborhood U of x_0 in Ψ_0 such that the map $\mathbf{\Phi}_\ell^{-1}(U) \to U$ is an isomorphism. □

If x is a point of $\mathcal{A}_g(\ell)$ or $\mathcal{A}_g$, we abuse notation by also calling x its reduction to the associated coarse moduli space.

Proposition 4.9. *Let x be a k-point of $\mathcal{A}_g(\ell)$.*

(i) Assume that $\Phi_{\ell,1}$ is stabilizer preserving at x. Then:
- *The map $\mathbf{\Phi}_{\ell,1}$ is strongly étale at x, and the point x is smooth in $\mathbf{A}_g(\ell)$ if and only if $\mathbf{\Phi}_{\ell,1}(x)$ is smooth in $\mathbf{A}_g$.*
- *The point $x_0 = \mathbf{\Phi}_\ell(x)$ is normal in Ψ_0 if and only if the projection $p_1\colon \Psi_0 \to \mathbf{A}_g$ is étale at x_0.*
- *If $\mathbf{\Phi}_{\ell,1}(x)$ is represented by an abelian variety A defined over k, then the isogeny $\varphi\colon A \to A'$ representing x is also defined over k.*

(ii) Assume that $\mathbf{\Phi}_{\ell,1}(x)$ only has generic automorphisms. Then $\Phi_{\ell,1}$ is stabilizer preserving at x, the point x is smooth in $\mathbf{A}_g(\ell)$, and the map $\mathcal{A}_g(\ell) \to \mathbf{A}_g(\ell)$ (resp. $\mathcal{A}_g \to \mathbf{A}_g$) is étale at x (resp. at $\Phi_{\ell,1}(x)$).

Proof. The first part of Item 1 comes from Theorem 4.4: in this case, the map $\mathbf{\Phi}_{\ell,1}$ is étale at x, and $\Phi_{\ell,1}$ is étale-locally around x the pullback of $\mathbf{\Phi}_{\ell,1}$ by the map $\mathcal{A}_g(\ell) \to \mathbf{A}_g(\ell)$.

For the second part, we know that $\mathbf{\Phi}_{\ell,1} = p_1 \circ \mathbf{\Phi}_\ell$ is étale at x, and we have seen in Proposition 4.8 that $\mathbf{\Phi}_\ell$ is étale at x if and only if x_0 is normal in Ψ_0. Therefore x_0 is normal in Ψ_0 if and only if p_1 is étale at x_0.

The final part of Item 1 comes from [DR73, §VI.3.1]. Indeed, if (A, K) represents x over $\overline{k}$, the obstruction for (A, K) to descend over k is given by an element in $H^2(\operatorname{Spec} k, \operatorname{Aut}(x))$ in the sense of Giraud. But this obstruction vanishes since $\mathbf{\Phi}_{\ell,1}(x)$ is represented by A/k, and the automorphism groups of x and $\mathbf{\Phi}_{\ell,1}(x)$ are equal. The set of isomorphism classes over k is then canonically given by $H^1(\operatorname{Spec} k, \operatorname{Aut}(x))$.

If $y = \Phi_{\ell,1}(x)$ only has generic automorphisms, then x too, so $\Phi_{\ell,1}$ is stabilizer preserving at x. The rigidification $\mathcal{A}_g \to [\mathcal{A}_g/\mu_2]$ is étale (it is a μ_2-gerbe) and $[\mathcal{A}_g/\mu_2] \to \mathbf{A}_g$ is an isomorphism above y by Corollary 4.3.(i). Therefore $\mathcal{A}_g \to \mathbf{A}_g$ is étale at y, and y is smooth in $\mathbf{A}_g$. By the same reasoning, the map $\mathcal{A}_g(\ell) \to \mathbf{A}_g(\ell)$ is étale at x. □

Proposition 4.9 also holds for $\mathbf{\Phi}_{\ell,2}$ in place of $\mathbf{\Phi}_{\ell,1}$.

Corollary 4.10. *Let x be a k-point of $\mathcal{A}_g(\ell)$ such that both $\mathbf{\Phi}_{\ell,1}(x)$ and $\mathbf{\Phi}_{\ell,2}(x)$ only have generic automorphisms. Then x is a smooth k-point of $\mathbf{A}_g(\ell)$, the points $\mathbf{\Phi}_{\ell,1}(x)$ and $\mathbf{\Phi}_{\ell,2}(x)$ are both smooth k-points of $\mathbf{A}_g$, and we have a commutative diagram*

$$\begin{array}{ccccc}
T_{\Phi_{\ell,1}(x)}(\mathcal{A}_g) & \xleftarrow{d\Phi_{\ell,1}} & T_x(\mathcal{A}_g(\ell)) & \xrightarrow{d\Phi_{\ell,2}} & T_{\Phi_{\ell,2}(x)}(\mathcal{A}_g) \\
\downarrow & & \downarrow & & \downarrow \\
T_{\mathbf{\Phi}_{\ell,1}(x)}(\mathbf{A}_g) & \xleftarrow{d\mathbf{\Phi}_{\ell,1}} & T_x(\mathbf{A}_g(\ell)) & \xrightarrow{d\mathbf{\Phi}_{\ell,2}} & T_{\mathbf{\Phi}_{\ell,2}(x)}(\mathbf{A}_g)
\end{array}$$

where the vertical arrows are isomorphisms induced by the maps $\mathcal{A}_g(\ell) \to \mathbf{A}_g(\ell)$ and $\mathcal{A}_g \to \mathbf{A}_g$. In particular, the deformation map of the isogeny φ representing x is $\mathscr{D}(\varphi) = d\mathbf{\Phi}_{\ell,2}(x) \circ d\mathbf{\Phi}_{\ell,1}{}^{-1}(x)$.

Furthermore, let $\Psi_0 \subset \mathbf{A}_g \times \mathbf{A}_g$ be the image of $\mathbf{\Phi}_\ell$, denote by $p_1, p_2 \colon \Psi_0 \to \mathbf{A}_g$ the two projections, and let $x_0 = \mathbf{\Phi}_\ell(x)$. If Ψ_0 is normal at x_0, then the deformation map $\mathscr{D}(\varphi)$ is given by $dp_2(x_0) \circ dp_1(x_0)^{-1}$.

Proof. For the first part, apply Proposition 4.9 for both $\Phi_{\ell,1}$ and $\Phi_{\ell,2}$. For the second part, if Ψ_0 is normal at y, then $\mathbf{\Phi}_\ell \colon \mathbf{A}_g(\ell) \to \Psi_0$ is an isomorphism around x_0 by Proposition 4.8. □

Remark 4.11. Let x be a k-point of $\mathcal{A}_g(\ell)$ such that both $\Phi_{\ell,1}$ and $\Phi_{\ell,2}$ are stabilizer preserving at x. Let $y_1 = \mathbf{\Phi}_{\ell,1}(x)$, $y_2 = \mathbf{\Phi}_{\ell,2}(x)$, and let y_1', y_2' be lifts of y_1, y_2 to $\mathcal{A}_g$. Let $G = I_x$ be the common automorphism group of these objects. Even if G contains non-generic automorphisms, strong étaleness still allows us to compute the deformation map by looking at the coarse spaces, as follows.

Indeed, suppose that x is smooth in $\mathbf{A}_g(\ell)$ (equivalently, by Proposition 4.9, y_1, or y_2, is smooth in $\mathbf{A}_g$). Then, the same reasoning as in Corollary 4.10 holds for x, except that in the commutative diagram the vertical maps are not isomorphisms, since the maps to the coarse moduli spaces are not étale at x and its images. From strong étaleness, the maps on the bottom are isomorphisms, and it remains to explain how to recover the maps on the top from them.

Let B_1 be the completed local ring of $\mathcal{A}_g$ at y_1'. Then by Corollary 4.3.(ii), the completed local ring of $\mathbf{A}_g$ at y_1 is B_1^G. Therefore, given $m = g(g+1)/2$ uniformizers $u_1', \dots, u_m'$ of $\mathcal{A}_g$ at y_1', we obtain $g(g+1)/2$ uniformizers of $\mathbf{A}_g$ at y_1 as G-invariant polynomials in $u_1', \dots, u_m'$. Knowing these polynomials and proceeding in the same way at y_2 allows us to recover the deformation map at the level of stacks up to an action of non-generic elements of G, which amounts to changing the lifts y_1' and y_2'.

In practice, it may be more convenient to work at the level of stacks to recover the deformation map directly, rather than using G-invariants uniformizers on $\mathbf{A}_g$. Algorithmically, the choice depends on the degree of the field extension one has to take to add enough level structure to rigidify the stack. For instance, if $g = 2$ and k is a finite field, we only need an extension of degree at most 6 to get the 2-torsion, whereas over a number field this could take an extension of degree up to 720.

Remark 4.12. Let k be a field. Then Proposition 4.9 and Corollary 4.10 also apply to the map $\mathbf{A}_g(\ell)^{(k)} \to \mathbf{A}_g^{(k)} \times \mathbf{A}_g^{(k)}$, where $\mathbf{A}_g(\ell)^{(k)}$ and $\mathbf{A}_g^{(k)}$ are the coarse moduli space of $\mathcal{A}_g(\ell) \otimes k$ and $\mathcal{A}_g \otimes k$ respectively. In practice this does not change the results much, since at points x with generic automorphisms, we know that $\mathbf{A}_g^{(k)}$ is isomorphic to $\mathbf{A}_g \otimes k$ locally around x by Theorem 4.2.(ii). Moreover, if the characteristic of k is large enough, then all points above k are tame, so $\mathbf{A}_g^{(k)} = \mathbf{A}_g \otimes k$ by Theorem 4.2.(i).

Now assume that we are in the situation of Remark 4.11, with x a k-point of $\mathcal{A}_g(\ell)$ such that both $\Phi_{\ell,1}$ and $\Phi_{\ell,2}$ are stabilizer preserving at x. Assume furthermore that x is a tame point, and that the characteristic of k is p. Let $x_0 = \mathbf{\Phi}_\ell(x)$. If $\mathbf{\Phi}_\ell$ is étale at x, or equivalently x_0 is normal in Ψ_0, then $\mathbf{\Phi}_\ell$ is étale above lifts in characteristic 0 of x. The converse is also true: if x_0 is not normal, then it must come from a singular point in characteristic zero. Indeed, normality is equivalent to Serre's conditions S_2 and R_1; since $\Psi_0 \otimes k$ is reduced, and therefore satisfies S_1 and R_0, it suffices to check normality at lifts of characteristic zero. This generalizes the remark of [Sch95, p. 248].

4.2.2 *Birational invariants for abelian surfaces* In the case $g = 2$, the structure of the coarse moduli space $\mathbf{A}_2$ and the possible automorphism groups have been worked out explicitly.

Recall that the Jacobian locus, denoted by $\mathbf{M}_2$, is the open locus in $\mathbf{A}_2$ consisting of Jacobians of hyperelliptic curves. Igusa showed in [Igu60] that

$$\mathbf{M}_2 = \mathrm{Proj}[J_2, J_4, J_6, J_8, J_{10}]/(J_2J_6 - J_4^2 - 4J_8)_{(J_{10})},$$

and that $\mathbf{M}_2$ has only one singular point over $\mathbb{Z}$, given by the hyperelliptic curve $\mathcal{C}_0 : y^2 = x^5 - 1$, which corresponds to the point $J_2 = J_4 = J_6 = J_8 = 0$. Over $\mathbb{C}$, in [Igu62], Igusa shows that $\mathbf{A}_2$ has also in its singular locus two projective lines which represent products of elliptic curves, one of which being isomorphic to $y^2 = x^3 - 1$ or to $y^2 = x^4 - 1$. Finally, the structure of $\mathbf{A}_2$ over $\mathbb{Z}$ is described in [Igu79], but the singular locus is not determined.

The possible (reduced) groups of automorphisms of genus 2 curves over an algebraic closure are determined in [Igu60, §VIII]; see also [Liu93, §4.1]. We restrict to a characteristic different from 2. Define

$$\mathcal{C}_0 : y^2 = x^5 - 1 \text{ and } \mathcal{C}_1 : y^2 = x^5 - x.$$

Then every curve $\mathcal{C}$ not isomorphic to $\mathcal{C}_0$ or $\mathcal{C}_1$ satisfies $\#\operatorname{Aut}(\mathcal{C}) \in \{2, 4, 6\}$. In characteristic different from 5, we have $\operatorname{Aut}\mathcal{C}_0 = \mathbb{Z}/10\mathbb{Z}$ and $\#\operatorname{Aut}\mathcal{C}_1 \in \{6, 8\}$. In characteristic 5, $\operatorname{Aut}\mathcal{C}_1$ is an extension of $\mathrm{PGL}_2(\mathbb{F}_5)$, which has cardinality 120, by $\mathbb{Z}/2\mathbb{Z}$. In particular we see that in characteristic 0 and $p > 5$ all curves have a tame automorphism group.

From [Igu60; Str10; GL12], the covariants I_2, I_4, I_6', I_{10} are defined over $\mathbb{Z}$. They are zero modulo 2, and I_2, I_4, I_6' are all polynomials in J_2 modulo 3. Therefore the Igusa invariants j_1, j_2, j_3 have bad reduction modulo 2 and do not generate the function field of $\mathbf{M}_2$ modulo 3. Over $\mathbb{Z}[1/6]$ however, they are birational invariants, and determine an isomorphism from $U = \{I_4 \neq 0\} \subset \mathbf{M}_2$ to $\{j_3 \neq 0\} \subset \mathbb{A}^3$. Every point with $I_4 = 0$ maps to $(j_1, j_2, j_3) = (0, 0, 0)$.

The modular polynomials $\Psi_{\ell,i}$ from §2.6 are equations for the image $\Psi_0 \subset \mathbf{A}_g \times \mathbf{A}_g$ of $\mathbf{\Phi}_\ell$ intersected with $U \times U$ in $\mathbb{A}^3 \times \mathbb{A}^3$ via j_1, j_2, j_3.

Proposition 4.13. *Let Ψ_1 denote the normalization of the variety cut out by the modular polynomials $\Psi_{\ell,i}$. Let $\varphi\colon A \to A'$ be an ℓ-isogeny over a field k of caracteristic $p > 5$ or zero, and let x be the k-point of Ψ_1 corresponding to φ. Assume that A and A' are Jacobians with no extra automorphisms and that $A, A' \in U$. Then the deformation map $\mathscr{D}(\varphi)$ of φ is given by $dp_2(x) \circ dp_1(x)^{-1}$, where p_1, p_2 denotes the projections $\Psi_1 \otimes k \to \mathbb{A}^3_k$.*

Proof. By assumption, the three Igusa invariants induce an isomorphism between the tangent spaces $T_A(\mathbf{A}_g)$ and $T_{j(A)}(\mathbb{A}^3_k)$, and similarly for A'. Since A and A' have no extra automorphisms, $\Phi_{\ell,1}$ and $\Phi_{\ell,2}$ are automatically stabilizer preserving. The normalization Ψ_1 is isomorphic to the preimage of $U \times U$ in the coarse moduli space $\mathbf{A}_g(\ell)$ by Proposition 4.8. Since φ is a tame point, by Theorem 4.2.(ii), $\Psi_1 \otimes k$ is still the coarse moduli space of $\mathcal{A}_{g,\Gamma_0(\ell)} \otimes k$ locally around φ, so we conclude by Proposition 4.9. □

Remark 4.14. We summarize different incarnations of the deformation map.

- At the level of stacks, the two projections $\Phi_{\ell,1}, \Phi_{\ell,2}\colon \mathcal{A}_g(\ell) \to \mathcal{A}_g$ are always étale and we can always compute the deformation map at an isogeny φ as $d\Phi_{\ell,2}(\varphi) \circ d\Phi_{\ell,1}(\varphi)^{-1}$.
- At the level of the coarse moduli space $\mathbf{A}_g(\ell)$, we can still compute the deformation map at the points where $\Phi_{\ell,1}$ and $\Phi_{\ell,2}$ are stabilizer preserving. If this is not the case, we must add a level structure that kills the automorphisms that do not stabilize the kernel of the isogeny.
- We may then replace $\mathbf{A}_g(\ell)$ by its birational image in $\mathbf{A}_g^2$. We recover the deformation map at points $x \in \mathbf{A}_g^2$ where there is a local isomorphism $\Phi_\ell^{-1}(U) \to U$ for some open set U containing x. If this is not the case, we may instead recover $\mathbf{A}_g(\ell)$ from its birational image

by computing the normalization. It is usually enough to compute the normalization once and for all over $\mathbb{Z}$, since by Theorem 4.2 the formation of $\mathbf{A}_g(\ell)$ commutes with arbitrary base change at tame points.

– Finally, when $g = 2$, we can use the birational morphism from $\mathbf{A}_2$ to $\mathbb{A}^3$ given by the three Igusa invariants. Modular polynomials are usually given in this form. With Streng's version of Igusa invariants, they can be used as long as $I_4 \neq 0$, i.e. $j_3 \neq 0$. Otherwise, one has to compute the modular polynomials for another set of invariants which are defined at A and A'.

As we go down the list, modular equations become algorithmically more tractable, at the expense of introducing more exceptions; but if we find such an exception, we can always spend more computation time if needed in order to recover the deformation map.

4.2.3 *Hilbert–Blumenthal stacks* We now briefly describe Hilbert–Blumenthal stacks, and refer to [Rap78; Cha90] for more details. Let K be a real number field of dimension g, and let $\mathbb{Z}_K$ be its maximal order. We say that an abelian scheme $A \to S$ has *real multiplication by* $\mathbb{Z}_K$ (or, for short, is RM) if it is endowed with a morphism $\iota\colon \mathbb{Z}_K \to \mathrm{End}(A)$ such that $\mathrm{Lie}(A)$ is a locally free $\mathbb{Z}_K \otimes \mathcal{O}_S$-module of rank 1. This last condition can be checked on geometric fibers [Rap78, Rem. 1.2] and is automatic on fibers of characteristic zero [Rap78, Prop. 1.4].

We let $\mathscr{H}_g$ be the stack of principally polarized abelian schemes with real multiplication by $\mathbb{Z}_K$. It is algebraic and smooth of relative dimension g over $\operatorname{Spec}\mathbb{Z}$ [Rap78, Thm. 1.14]. Moreover, $\mathscr{H}_g$ is connected and its generic fiber is geometrically connected [Rap78, Thm. 1.28]. Forgetting the real multiplication embedding ι yields a map $\mathscr{H}_g \to \mathcal{A}_g$, called the *Hilbert embedding*, which is an $\mathrm{Isom}(\mathbb{Z}_K, \mathbb{Z}_K) \simeq \mathrm{Aut}(K)$-gerbe over its image, the *Humbert stack*. We described the analytification of $\mathscr{H}_g$ and the Hilbert embedding in Section 2. The map from $\mathscr{H}_g \to \mathcal{A}_g$ is finite by [Gro64, EGA IV.15.5.9], [DR73, Lem 1.19] (or by looking at the compactifications of [Rap78], [FC90]).

One can define the stack $\mathscr{H}_{g,n} \to \mathbb{Z}[1/n]$ of RM abelian schemes with a level n structure in the usual way. The map $\mathscr{H}_{g,n} \to \mathscr{H}_g$ is étale over $\mathbb{Z}[1/n]$ [Rap78, Thm. 1.22], its generic fiber is connected, and geometrically has $\phi(n)$ components defined over $\mathbb{Q}(\zeta_n)$ [Rap78, Thm. 1.28]. If β is a totally positive prime of $\mathbb{Z}_K$, this allows us to construct, in a similar fashion to $\mathcal{A}_g(\ell)$, the stack $\mathscr{H}_g(\beta) = \mathscr{H}_{g,\Gamma_0(\beta)}$ of RM abelian schemes endowed with a subgroup K which is maximal isotropic for the β-pairing. We have a map

$$\Phi_\beta = (\Phi_{\beta,1}, \Phi_{\beta,2})\colon \mathscr{H}_g(\beta) \to \mathscr{H}_g \times \mathscr{H}_g$$

given by forgetting the extra structure and taking the isogeny respectively. The condition on β ensures that $\Phi_{\beta,2}$ sends $\mathscr{H}_g(\beta)$ to $\mathscr{H}_g$.

The methods of Section 4.2.1 also apply to compute the Hilbert deformation map. We have the following analogue of Corollary 4.10, with a similar proof.

Proposition 4.15. *Let x be a k-point of $\mathscr{H}_g(\beta)$ such that $\Phi_{\beta,1}(x)$ and $\Phi_{\beta,2}(x)$ only have generic automorphisms. Then x maps to a smooth point of the coarse moduli space $\mathbf{H}_g(\beta)$, both $\Phi_{\beta,1}(x)$ and $\Phi_{\beta,2}(x)$ map to smooth points of the coarse moduli space $\mathbf{H}_g$, and we have a commutative diagram*

$$\begin{array}{ccccc}
T_{\Phi_{\beta,1}(x)}(\mathscr{H}_g) & \xleftarrow{d\Phi_{\beta,1}} & T_x(\mathscr{H}_g(\beta)) & \xrightarrow{d\Phi_{\beta,2}} & T_{\Phi_{\beta,2}(x)}(\mathscr{H}_g) \\
\downarrow & & \downarrow & & \downarrow \\
T_{\mathbf{\Phi}_{\beta,1}(x)}(\mathbf{H}_g) & \xleftarrow{d\mathbf{\Phi}_{\beta,1}} & T_x(\mathbf{H}_g(\beta)) & \xrightarrow{d\mathbf{\Phi}_{\beta,2}} & T_{\mathbf{\Phi}_{\beta,2}(x)}(\mathbf{H}_g)
\end{array}$$

where the vertical arrows are isomorphisms induced by the maps $\mathcal{A}_g(\ell) \to \mathbf{A}_g(\ell)$ and $\mathcal{A}_g \to \mathbf{A}_g$, and $\mathbf{\Phi}_{\beta,i}$ is the map induced by $\Phi_{\beta,i}$ at the level of coarse spaces. In particular, the deformation map of the isogeny φ representing x is given by $\mathscr{D}(\varphi) = d\mathbf{\Phi}_{\beta,2}(x) \circ d\mathbf{\Phi}_{\beta,1}{}^{-1}(x)$.

Corollary 4.16. *Let x be a k-point of $\mathscr{H}_g(\beta)$ such that both $x_1 = \Phi_{\beta,1}(x)$ and $x_2 = \Phi_{\beta,2}(x)$ only have generic automorphisms. Assume furthermore that (x_1, x_2) does not lie in $\Phi_{\overline{\beta}}(\mathscr{H}_g(\overline{\beta}))$: this means that the corresponding abelian varieties are β-isogenous but not $\overline{\beta}$-isogenous.*

Let $\Psi_\beta \subset \mathbf{H}_g \times \mathbf{H}_g$ be the image of $\mathbf{\Phi}_\beta$. Let $\Psi_{\beta,\overline{\beta}} \subset \mathbf{A}_g \times \mathbf{A}_g$ be the image of Ψ_β, and let $y = (y_1, y_2)$ the image of (x_1, x_2) by the forgetful morphism $\mathbf{H}_g \times \mathbf{H}_g \to \mathbf{A}_g \times \mathbf{A}_g$. Denote by $p_1, p_2 \colon \Psi_{\beta,\overline{\beta}} \to \mathbf{A}_g$ the two projections. If $\Psi_{\beta,\overline{\beta}}$ is normal at y, then the deformation map $\mathscr{D}(\varphi)$ is given by $dp_2(y) \circ dp_1(y)^{-1}$.

Proof. The map $\mathscr{H}_g \to \mathcal{A}_g$ is finite étale, and under our assumptions the maps $\mathscr{H}_g \to \mathbf{H}_g$ and $\mathcal{A}_g \to \mathbf{A}_g$ are étale at x_1 and x_2 (resp. at their images y_1, y_2 in $\mathcal{A}_g$). Therefore the map $\mathbf{H}_g \times \mathbf{H}_g \to \mathbf{A}_g \times \mathbf{A}_g$ is étale at $x' = (x_1, x_2)$. Furthermore the pullback of $\Psi_{\beta,\overline{\beta}}$ by $\mathbf{H}_g \times \mathbf{H}_g \to \mathbf{A}_g \times \mathbf{A}_g$ is $\Psi_\beta \cup \Psi_{\overline{\beta}} \subset \mathbf{H}_g \times \mathbf{H}_g$, so the map $\Psi_\beta \cup \Psi_{\overline{\beta}} \to \Psi_{\beta,\overline{\beta}}$ is étale at x'. Since $\Phi_{\overline{\beta}}$ is finite, its image $\Psi_{\overline{\beta}} \subset \mathbf{H}_g \times \mathbf{H}_g$ is closed. By our assumption on x, there is an open subscheme containing x which does not intersect Ψ_β, so the map $\Psi_\beta \to \Psi_{\beta,\overline{\beta}}$ is étale at x'. In particular, Ψ_β is normal at x' if and only if $\Psi_{\beta,\overline{\beta}}$ is normal at x. The same proof as in Corollary 4.10 shows that the projections maps $\Psi_\beta \to \mathbf{H}_g$ are étale at x', and can be used to compute the deformation matrix. Since $\mathbf{H}_g \to \mathbf{A}_g$ is étale at x_1 and x_2, the projections p_1 and p_2 are also étale at y, and can be used to compute the deformation matrix as well. □

4.3 The deformation and tangent maps

In this section, we present the Kodaira–Spencer isomorphism, which for a principally polarized abelian variety A identifies $T_A(\mathcal{A}_g)$ with $\mathrm{Sym}^2(T_0(A))$. This yields a relation between the deformation and tangent maps of a given ℓ-isogeny (Proposition 4.19). We also present an analogous result in the Hilbert case.

4.3.1 *The Siegel case* The Kodaira-Spencer morphism was first introduced in [KS58]; we refer to [FC90, §III.9] and [And17, §1.3] for more details.

Let $p \colon A \to S$ be a proper abelian scheme, and assume for simplicity that S is smooth. Then, using the Gauss-Manin connection

$$\nabla \colon R^1 p_* \Omega_{A/S} \to R^1 p_* \Omega_{A/S} \otimes \Omega^1_S,$$

one can define the *Kodaira–Spencer morphism*

$$\kappa \colon T_S \to R^1 p_* T_{A/S},$$

where $T_{A/S}$ is the dual of $\Omega^1_{A/S}$.

Recall that $\mathrm{Lie}_S A = p_* T_{A/S}$ is the dual of $p_* \Omega^1_{A/S}$, and is canonically identified with $s^* T_{A_S}$ where $s \colon S \to A$ is the zero section [MvdGE12, Prop. 3.15]. By the projection formula [FGI+05, Thm. 8.3.2], [The18, Tag 0943], we have

$$R^1 p_* T_{A/S} = \mathrm{Lie}_S(A) \otimes_{\mathcal{O}_S} R^1 p_* \mathcal{O}_A.$$

Moreover, $R^1 p_* \mathcal{O}_A$ is naturally isomorphic to $\mathrm{Lie}_S(A^\vee)$, where $A^\vee \to S$ is the dual of A. Therefore, we can also write the Kodaira–Spencer map as

$$\kappa \colon T_S \to R^1 p_* T_{A/S} \simeq \mathrm{Lie}_S(A) \otimes_{\mathcal{O}_S} \mathrm{Lie}_S(A^\vee).$$

The Kodaira-Spencer map κ is invariant by duality. A polarization $A \to A^\vee$ induces another version of the Kodaira–Spencer map:

$$\kappa\colon T_S \to \operatorname{Sym}^2 \operatorname{Lie}_S(A) = \operatorname{Hom}_{\operatorname{Sym}}(\Omega^1_{A/S}, \Omega^{1\vee}_{A^\vee/S}) = \operatorname{Hom}_{\operatorname{Sym}}\big(\operatorname{Lie}_S(A)^\vee, \operatorname{Lie}_S(A^\vee)\big).$$

If we apply this construction to the universal abelian scheme $\mathscr{X}_g \to \mathcal{A}_g$ (or rather, the pullback of $\mathscr{X}_g$ to an étale presentation S of $\mathcal{A}_g$), the Kodaira–Spencer map is an isomorphism [And17, §2.1.1]. Its analytification can be described explicitly.

Proposition 4.17. *Let V be the trivial vector bundle $\mathbb{C}^g$ on $\mathbb{H}_g$, identified with the tangent space at 0 of the universal abelian variety $A(\tau)$ over $\mathbb{H}_g$. Then the pullback of the Kodaira–Spencer map $\kappa\colon T_{\mathcal{A}_g} \to \operatorname{Sym}^2 \operatorname{Lie}_S \mathscr{X}_g$ by $\mathbb{H}_g \to {\mathcal{A}_g}^{\mathrm{an}}$ is an isomorphism $T_{\mathbb{H}_g} \simeq \operatorname{Sym}^2 V$ given by*

$$\kappa\Big(\frac{1+\delta_{jk}}{2\pi i}\frac{\partial}{\partial \tau_{jk}}\Big) = \frac{1}{(2\pi i)^2}\frac{\partial}{\partial z_j} \otimes \frac{\partial}{\partial z_k}.$$

for each $1 \leqslant j, k \leqslant g$, where δ_{jk} is the Kronecker symbol.

Proof. The fact that the pullback is an isomorphism is [And17, §2.2]. The identification itself can be derived by looking at the deformation of a section s of the line bundle on $\mathscr{X}_g$ giving the principal polarization. On $\mathbb{H}_g \times \mathbb{C}^g \to \mathbb{H}_g$, we can take the theta function θ as a section, and its deformation along τ is given by the heat equation [CvdG00, p. 9]:

$$2\pi i(1+\delta_{jk})\frac{\partial \theta}{\partial \tau_{jk}} = \frac{\partial^2 \theta}{\partial z_j \partial z_k}.$$ □

When identifying the tangent space at τ with the symmetric matrices, the action of Sym^2 at a matrix U on the tangent space is given by $M \mapsto MUM^t$. It is then easy to check that this action is indeed compatible with the action of $\operatorname{Sp}_{2g}(\mathbb{Z})$ on τ and U. From Proposition 4.17, we recover that derivatives of Siegel modular invariants have weight Sym^2 in the sense of §2; moreover the basis of differential forms $\omega(\tau)$ from §2.1 and the matrix $D_\tau J$ defined in §3.4 are correctly normalized.

To sum up, if $x\colon \operatorname{Spec} k \to \mathcal{A}_g$ is a point represented by a principally polarized abelian variety A/k, we have a canonical isomorphism $T_x\mathcal{A}_g \simeq \operatorname{Sym}^2(T_0(A))$.

Definition 4.18. Let k be a field of characteristic distinct from ℓ, let $\varphi\colon A \to A'$ be an ℓ-isogeny representing a point of $\mathcal{A}_g(\ell)(k)$, and fix bases of $T_0(A)$ and $T_0(B)$ as k-vector spaces. We call the matrix of the tangent map $d\varphi$ in these bases the *tangent matrix* of φ.

By functoriality, this choice of bases induces bases of $T_A(\mathcal{A}_g)$ and $T_{A'}(\mathcal{A}_g)$ over k. We call the matrix of the deformation map $\mathscr{D}(\varphi)$ in these bases the *deformation matrix* of φ.

We still denote these matrices by $d\varphi$ and $\mathscr{D}(\varphi)$, but this abuse of notation should cause no confusion.

We can now extend the relation that we gave in Proposition 3.19 between the tangent and deformation matrices, as follows.

Proposition 4.19. *Let φ be as in Definition 4.18, and let $d\varphi$ (resp. $\mathscr{D}(\varphi)$) be its tangent (resp. deformation) matrix. Then we have $\operatorname{Sym}^2(d\varphi) = \ell\mathscr{D}(\varphi)$.*

Proof. It suffices to prove it for the universal ℓ-isogeny

$$\varphi\colon \mathscr{X}_g(\ell) \to \mathscr{X}_g \times_{\mathcal{A}_g} \mathcal{A}_g(\ell)$$

over $\mathbb{Z}[1/\ell]$. All line bundles involved in the relation we have to prove are locally free on smooth stacks, so are flat over $\mathbb{Z}$; therefore, since $\mathbb{Z} \to \mathbb{C}$ is injective, it suffices to prove the relation over $\mathbb{C}$. By rigidity [MFK94, Prop. 6.1 and Thm. 6.14], it suffices to prove the relation on each fiber.

Hence we may assume that $\varphi\colon A \to A'$ is an ℓ-isogeny over $\mathbb{C}$. There exists $\tau \in \mathbb{H}_g$ such that A is isomorphic to $\mathbb{C}^g/(\mathbb{Z}^g + \tau\mathbb{Z}^g)$ and A' is isomorphic to $\mathbb{C}^g/(\mathbb{Z}^g + \tau/\ell\mathbb{Z}^g)$, with φ induced by the identity on $\mathbb{C}^g$. Then, the deformation map at φ is given by $\tau \to \tau/\ell$, so the result follows. □

4.3.2 *The Hilbert case* In the Hilbert case, the Kodaira–Spencer isomorphism is as follows.

Proposition 4.20. *Let $A \to S$ be an abelian scheme in $\mathscr{H}_g$. Then we have canonical isomorphisms*

$$T_A(\mathscr{H}_g) \simeq \mathrm{Hom}_{\mathbb{Z}_K \otimes \mathcal{O}_S}(\mathrm{Lie}(A)^\vee, \mathrm{Lie}(A^\vee)) = \mathrm{Lie}(A^\vee) \otimes_{\mathbb{Z}_K \otimes \mathcal{O}_S} \mathrm{Lie}(A) \otimes_{\mathbb{Z}_K} \mathbb{Z}_K^\vee.$$

Proof. Combine [Rap78, Prop. 1.6] with [Rap78, Prop. 1.9]. □

Proposition 4.20 shows that for Hilbert–Blumenthal stacks, the deformation map is actually represented by an element of $\mathbb{Z}_K \otimes \mathcal{O}_S$ rather than a matrix in $\mathcal{O}_S$. The action of the Hilbert embedding on tangent spaces is also easy to describe.

Proposition 4.21. *Let A be a k-point of $\mathscr{H}_g$. Then the map $T_A(\mathscr{H}_g) \to T_A(\mathcal{A}_g)$ induced by the forgetful functor fits in the commutative diagram*

$$\begin{array}{ccc} T_A(\mathscr{H}_g) & \longrightarrow & T_A(\mathcal{A}_g) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{\mathbb{Z}_K \otimes \mathcal{O}_k}(\mathrm{Lie}(A)^\vee, \mathrm{Lie}(A^\vee)) & \longrightarrow & \mathrm{Hom}_{\mathrm{Sym}}(\mathrm{Lie}(A)^\vee, \mathrm{Lie}(A^\vee)). \end{array}$$

where the vertical arrows are the Kodaira–Spencer isomorphisms.

Proof. The bottom arrow is well-defined: $\mathrm{Lie}(A)$ is a projective $\mathbb{Z}_K \otimes \mathcal{O}_k$-sheaf of rank 1, so its image in $\mathrm{Hom}_{\mathcal{O}_k}(\mathrm{Lie}(A)^\vee, \mathrm{Lie}(A^\vee))$ obtained by forgetting the $\mathbb{Z}_K$-structure is automatically symmetric. We omit the proof of commutativity. □

Combining Proposition 4.21 with the analytic description of the Kodaira–Spencer in the Siegel case (Proposition 4.17) and the analytic description of the forgetful map (§2.4), we obtain the following analytic description of the Kodaira–Spencer isomorphism in the Hilbert case.

Corollary 4.22. *The pullback of $\kappa\colon T_{\mathscr{H}_g} \to \mathrm{Sym}^2 \mathit{Lie}_S X_g$ by $\mathbb{H}_1^g \to \mathscr{H}_g^{\mathrm{an}}$ is given by*

$$\kappa\Big(\frac{1}{\pi i}\frac{\partial}{\partial t_j}\Big) = \frac{1}{(2\pi i)^2}\frac{\partial}{\partial z_j} \otimes \frac{\partial}{\partial z_j}$$

for every $1 \leqslant j \leqslant g$.

This result gives an algebraic interpretation of Proposition 3.22: in genus 2, the part of $T_A(\mathcal{A}_2)$ that comes from the Hilbert space corresponds to the span of $dz_1 \otimes dz_1$ and $dz_2 \otimes dz_2$.

We obtain the analogue of Proposition 4.19 in the Hilbert case by a similar proof; in this statement, we see $\mathscr{D}(\varphi)$ as an element of a $\mathbb{Z}_K \otimes \mathcal{O}_S$-module.

Proposition 4.23. *Let $\varphi\colon A \to A'$ be a β-isogeny. Then $\mathrm{Sym}^2(d\varphi) = \beta\mathscr{D}(\varphi)$.*

Remark 4.24. We give an algebraic interpretation of the notion of Hilbert-normalized bases from §2.3, and the reduction to diagonal matrices that we used in §3.5 to compute the tangent matrix in the Hilbert case.

Let k be a field, and let A be an abelian variety representing a k-point of $\mathscr{H}_g$. Then $\mathrm{Lie}(A)$ is a free $\mathbb{Z}_K \otimes k$-module of rank 1, and any choice of basis v induces an isomorphism with $\mathbb{Z}_K \otimes k$ itself. Provided that $\mathrm{char}\, k \nmid \mathrm{Discr}(K)$, and up to taking an étale extension of k, we may assume that k splits $\mathbb{Z}_K$:

$$\mathbb{Z}_K \otimes k = \oplus_{i=1}^{g} k^{\sigma_i}$$

where $k^{\sigma_i} \simeq k$ has a $\mathbb{Z}_K$-module structure induced by the i-th morphism $\sigma_i \colon \mathbb{Z}_K \to k$. We fixed such a trivialization in §2.3 in the case $k = \mathbb{C}$. Then, v induces a basis of $\mathrm{Lie}(A)$ as a k-vector space on which $\mathbb{Z}_K$ acts diagonally, in other words a Hilbert-normalized basis of $\mathrm{Lie}(A)$. With such choices of trivializations, the deformation map is given by a $g \times g$ matrix in the basis $(v_1 \otimes v_1, \dots, v_g \otimes v_g)$ of the tangent spaces to $\mathscr{H}_g$.

Let us discuss, as a generalization of §3.6, the construction of Hilbert-normalized basis when only the Humbert equation is given. Assume that k splits $\mathbb{Z}_K$ and fix a trivialization; let $(v_1, \dots, v_g)$ be a Hilbert-normalized basis of $\mathrm{Lie}(A)$, let $(w_1, \dots, w_g)$ be another k-basis and let M be the base-change matrix. Then $w_1 \otimes w_1, \dots, w_g \otimes w_g$ are tangent to the Humbert variety if and only if they are in the image of the map

$$\mathrm{Hom}_{\mathbb{Z}_K \otimes k}(\mathrm{Lie}(A)^\vee, \mathrm{Lie}(A^\vee)) \to \mathrm{Hom}_{\mathrm{Sym}}(\mathrm{Lie}(A)^\vee, \mathrm{Lie}(A^\vee)).$$

Via the trivialization, the left hand side is isomorphic to $\oplus_{i=1}^{g} \mathrm{Hom}_k(k^{\sigma_i}, k^{\sigma_i})$. Therefore, the vectors $w_1 \otimes w_1, \dots, w_g \otimes w_g$ are tangent to the Humbert variety if and only if M is diagonal up to a permutation. When $g = 2$, $\mathrm{Gal}(K/\mathbb{Q})$ is the full symmetric group $\mathfrak{S}_2$, so this is enough in general to ensure that the basis $(w_1, \dots, w_g)$ is potentially Hilbert-normalized.

As a final remark, assume that $\varphi \colon A \to A'$ is an isogeny compatible with the real multiplication, and assume that we are given bases of $\mathrm{Lie}(A)$ and $\mathrm{Lie}(A')$ as $\mathbb{Z}_K \otimes k$-modules (which we assume is étale for simplicity). Then, knowing $\mathrm{Sym}^2(d\varphi)$, the number of possibilities for $d\varphi$ is 2^s where s is the number of connected components of the étale algebra $\mathbb{Z}_K \otimes k$. For instance, if $g = 2$ and $k = \mathbb{F}_p$ there are 2 or 4 possibilities according to whether p is inert or split in $\mathbb{Z}_K$.

4.4 Modular forms and covariants

In this section, we give an algebraic interpretation of modular forms and covariants over $\mathbb{Z}$, as well as a completely algebraic proof of Theorem 3.9. This yields an explicit version of the Kodaira–Spencer isomorphism in the model of $\mathbf{A}_g$ given by Igusa invariants over $\mathbb{Z}[1/2]$ and not only over $\mathbb{C}$.

Let $\pi \colon \mathscr{X}_g \to \mathcal{A}_g$ be the universal abelian variety. The vector bundle

$$\mathsf{H} = \pi_* \Omega^1_{\mathscr{X}_g/\mathcal{A}_g}$$

over $\mathcal{A}_g$, which is dual to $\mathrm{Lie}_{\mathscr{X}_g/\mathcal{A}_g}$, is called the *Hodge bundle*. If ρ is a representation of GL_g, a Siegel modular form of weight ρ is a section of $\rho(\mathsf{H})$; in particular, a scalar-valued modular form of weight k is a section of $\Lambda^g \mathsf{H}^{\otimes k}$. In other words, a Siegel modular form f can be seen as a map

$$(A, \omega) \mapsto f(A, \omega)$$

where A is a point of $\mathcal{A}_g$ and ω is a basis of differential forms on A, with the following property: if $\eta \colon A \to A'$ is an isomorphism, and $r \in \mathrm{GL}_g$ is the matrix of η^* in the bases ω', ω, then $f(A', \omega) = \rho(r) f(A, \omega')$. The link with classical modular forms over $\mathbb{C}$ is the following: if $\tau \in \mathbb{H}_g$, then we define

$$f(\tau) = f\big(\mathbb{C}^g/(\mathbb{Z}^g + \tau\mathbb{Z}^g), (2\pi i\, dz_1, \dots, 2\pi i\, dz_g)\big).$$

This choice of basis is made so that the q-expansion principle holds [FC90, p. 141]. We already used it to define $f(A, \omega)$ over $\mathbb{C}$ in §2.1. The canonical line bundle $\Lambda^g \mathsf{H}$ is ample, so modular forms give local coordinates on $\mathbf{A}_g$.

The link between modular forms and covariants comes from the Torelli morphism

$$\tau_g \colon \mathscr{M}_g \to \mathcal{A}_g$$

where $\mathscr{M}_g$ denotes the moduli stack of smooth curves of genus g. Let $\mathscr{C}_g \to \mathscr{M}_g$ denote the universal curve; then the pullback $\tau_g^* \mathsf{H}$ of the Hodge bundle by the Torelli morphism is $\pi_* \Omega^1 \mathscr{C}_g / \mathscr{M}_g$, with both having canonical action by GL_g. In other words a Siegel modular form of weight ρ induces a Teichmuller modular form of weight ρ.

Now assume that $g = 2$. Over $\mathbb{Z}[1/2]$, the moduli stack $\mathscr{M}_2$ is identified with the moduli stack of nondegenerate binary forms of degree 6. Let $V = \mathbb{Z}x \oplus \mathbb{Z}y$, let $X = \det^{-2} V \otimes \mathrm{Sym}^6 V$, and let U be the open locus determined by the discriminant. Then $U \to \mathscr{M}_2$ is naturally identified with the Hodge frame bundle on $\mathscr{M}_2$: in other words, U is the moduli space of genus 2 hyperelliptic curves $\pi \colon C \to S$ endowed with a rigidification $\mathcal{O}_S^{\oplus 2} \simeq \pi_* \Omega^1_{C/S}$. In this identification, we send the binary form $f(x, y)$ to the curve $v^2 = f(u, 1)$ with a basis of differential forms given by $(u\,du/v, du/v)$ [CFvdG17, §4]. The natural action of GL_2 on the Hodge bundle corresponds to the action of GL_2 on U that we describe in Section 3.2. This shows why a Siegel modular form of weight ρ pulls back to a fractional covariant of weight ρ, at least over $\mathbb{Z}[1/2]$. In fact, one can show as in Theorem 3.9, by considering suitable compactifications, that a Siegel modular form pulls back to a polynomial covariant over any ring R in which 2 is invertible. Using Igusa's universal form [Igu60, §2], one can also use binary forms of degree 6 to describe the moduli stack of genus 2 curves even in characteristic two.

Proposition 4.25. *The equality* $\mathrm{Cov}(f_{8,6}) = \mathrm{Cov}(\chi_{10})X$ *from Proposition 3.12 holds over* $\mathbb{Z}$.

Proof. By the q-expansion principle, $f_{8,6}$ is defined over $\mathbb{Z}[1/2, 1/3, 1/5, 1/43]$; the covariants I_{10} and X are defined over $\mathbb{Z}[1/2]$ since they have integral coefficients. Checking the value of $\mathrm{Cov}(\chi_{10})X$ on Igusa's universal hyperelliptic curve as in [Igu60, §3] shows that this covariant is even defined over $\mathbb{Z}$. Since the Hodge bundle is without torsion, it is enough to check equality over $\mathbb{C}$, which is the content of Proposition 3.12. □

This suggests another, entirely algebraic proof of Proposition 3.12. By dimension considerations, we have $\mathrm{Cov}(f_{8,6}) = \lambda\,\mathrm{Cov}(\chi_{10})X$ for some $\lambda \in \mathbb{Q}^\times$. We have seen above that $\mathrm{Cov}(\chi_{10})X$ is defined over $\mathbb{Z}$ and primitive; therefore, if we can show that the Fourier coefficients of $f_{8,6}$ are integers with gcd 1, we will have $\lambda = \pm 1$. In order to obtain $\lambda = 1$, we can use Thomae's formula on one curve, perform a certified numerical evaluation over $\mathbb{C}$, or study degenerations from hyperelliptic curves to elliptic curves using the formula from [Liu93, Thm. 1.II].

As a consequence of Proposition 4.25, the identification of derivatives of Igusa invariants as explicit covariants (Theorem 3.14) still holds over $\mathbb{Z}[1/2]$.

For the algebraic interpretation of Hilbert modular forms as sections of the Hodge bungle on $\mathscr{H}_g$, the Koecher principle and the q-expansion principle for Hilbert modular forms, we refer to [Cha90, §4] and [Rap78, Thm. 6.7]. We can check that the relation between derivatives of Igusa invariants on the Hilbert and Siegel sides (Proposition 3.22) and the characterization of potentially Hilbert-normalized curves (Proposition 3.25) are still valid over $\mathbb{Z}[1/2]$.

4.5 Computing the tangent map in dimension 2

In this section, we work over a field k of characteristic different from 2 and 3; this restriction is not essential and comes from our choice of invariants. We have seen that derivatives of Igusa invariants are defined over $\mathbb{Z}[1/2]$, and hence make sense over k. We keep the matrix notations from §3.4.

Proposition 4.26. *Let U be the open set of $\mathcal{A}_2$ over k consisting of abelian surfaces A such that $\mathrm{Aut}(A) = \{\pm 1\}$ and $j_3(A) \neq 0$. Let $\varphi\colon A \to A'$ be an ℓ-isogeny over k. Assume that A, A' lie in U, and denote their Igusa invariants by j, j'. Assume further that the subvariety of $\mathbb{A}^3 \times \mathbb{A}^3$ cut out by modular equations is normal at $(j(A), j(A'))$. Let $\mathcal{C}, \mathcal{C}'$ be hyperelliptic equations over k whose Jacobians are isomorphic to A, A' respectively. Then*

(i) The isogeny φ is generic in the sense of Definition 3.18, in other words the 3×3 matrices

$$D\Psi_{\ell,L}(j,j'), \quad D\Psi_{\ell,R}(j,j'), \quad D_\tau J(\mathcal{C}) \quad \text{and} \quad D_\tau J(\mathcal{C}')$$

are invertible.

(ii) Let $d\varphi$ be the tangent matrix of φ with respect to $\mathcal{C}, \mathcal{C}'$. Then

$$\mathrm{Sym}^2(d\varphi) = -\ell D_\tau J(\mathcal{C}')^{-1} \cdot D\Psi_{\ell,R}(j,j')^{-1} \cdot D\Psi_{\ell,L}(j,j') \cdot D_\tau J(\mathcal{C}).$$

Proof. By Corollary 4.10, both A and A' are smooth points of $\mathbf{A}_g$, and the deformation map $\mathscr{D}(\varphi)$ is $d\mathbf{\Phi}_{\ell,2}(\varphi) \circ d\mathbf{\Phi}_{\ell,1}(\varphi)^{-1}$. Since A has generic automorphisms, A is not a product of elliptic curves; moreover $j_3(A) \neq 0$, so the birational map $(j_1, j_2, j_3)\colon \mathbf{A}_g \to \mathbb{A}^3$ is well-defined and étale at A. The map $\mathcal{A}_g \to \mathbf{A}_g$ is also étale at A, so the Igusa invariants are local uniformizers around A in $\mathcal{A}_g$. This shows that φ is generic in the sense of Definition 3.18. We obtain the expression of $\mathrm{Sym}^2(d\varphi)$ by Proposition 4.19. □

If A lies in the open set U defined in Proposition 4.26 and $\mathcal{C}$ is a hyperelliptic equation for A, then giving an element of $T_A(\mathcal{A}_g)$ is equivalent to giving one of the following:

(i) A deformation $\mathcal{C}_\epsilon$ of $\mathcal{C}$ over $k[\epsilon]/(\epsilon^2)$,

(ii) The Igusa invariants $j_1(\mathcal{C}_\epsilon), j_2(\mathcal{C}_\epsilon), j_3(\mathcal{C}_\epsilon)$ in $k[\epsilon]/(\epsilon^2)$,

(iii) A vector $v = \alpha w_1^2 + \beta w_1 w_2 + \gamma w_2^2$ in $\mathrm{Sym}^2 \Omega^1(\mathcal{C})$ where $(w_1, w_2) = (x\,dx/y, dx/y)$ is the canonical basis of differential forms on $\mathcal{C}$.

Switching from one representation to another can be done at the cost of $O(1)$ operations in k using the formulæ for Igusa invariants, the expression of their derivatives as a covariant, and linear algebra.

In the Hilbert case, it is more difficult to ensure genericity in the sense of Definition 3.20 because the Hilbert embedding $\mathscr{H}_g \to \mathcal{A}_g$ comes into play. We assume that k splits $\mathbb{Z}_K$, and fix a trivialization of $\mathbb{Z}_K \otimes k$.

Proposition 4.27. *Let A, A' be abelian varieties representing k-points of $\mathscr{H}_g$, and let $\mathcal{C}, \mathcal{C}'$ be hyperelliptic equations over k whose Jacobians are isomorphic to A, A' respectively; assume that $\mathcal{C}, \mathcal{C}'$ are Hilbert-normalized and that there exists a β-isogeny $\varphi\colon A \to A'$. Then we have*

$$D\Psi_{\beta,L}(j,j') \cdot D_t J(\mathcal{C}) = -D\Psi_{\beta,R}(j,j') \cdot D_t J(\mathcal{C}') \cdot \mathrm{Diag}(1/\beta, 1/\overline{\beta}) \cdot (d\varphi)^2.$$

Proof. This comes from the relation between the deformation and tangent matrices (Proposition 4.23). □

The equality in Proposition 4.27 only allows to compute $(d\varphi)^2$ when φ is generic. Even in this case, we get several possible candidates for $d\varphi$ up to sign. The discussion of Remark 4.24 shows that Proposition 3.25, which gives an algorithm to construct potentially Hilbert-normalized curve equations in genus 2, is still valid over k.

Remark 4.28. The 3×2 matrices $D_t J(\mathcal{C})$ and $D_t J(\mathcal{C}')$ have rank two when the Igusa invariants contain uniformizers of $\mathscr{H}_g$ at A and A' by [Gro64, p. IV.17.11.3]. Given the relation between derivatives of Igusa invariants on the Hilbert and Siegel sides (Proposition 3.25, which is valid over k by Proposition 4.21), this will be the case at soon as the images of A and A' in $\mathbf{A}_g$ lie in the open set U from Proposition 4.26.

Assume that generators of the ring of Hilbert modular forms are known, and the expression of Igusa invariants in terms of these generators is given. Since modular forms realize a projective embedding of $\mathbf{H}_g$, one can compute from this data an open set V in $\mathbf{H}_g$ where the Igusa invariants contain local uniformizers. Then, if A lies in V and $\mathrm{Aut}(A) \simeq \{\pm 1\}$, the Igusa invariants will contain local uniformizers of $\mathscr{H}_g$, hence $D_t J(\mathcal{C})$ will have rank 2.

In the Hilbert case, if Igusa invariants contain local uniformizers of $\mathscr{H}_g$ at A and if $\mathcal{C}$ is a Hilbert-normalized curve equation for A, then giving an element of $T_A(\mathscr{H}_g)$ is equivalent to giving

(i) A deformation $\mathcal{C}_\epsilon$ of $\mathcal{C}$ over $k[\epsilon]/(\epsilon^2)$ with real multiplication by $\mathbb{Z}_K$,
(ii) Igusa invariants $j_1(\mathcal{C}_\epsilon), j_2(\mathcal{C}_\epsilon), j_3(\mathcal{C}_\epsilon)$ in $k[\epsilon]/(\epsilon^2)$ lying on the Humbert surface (if $j_1(\mathcal{C}) \neq 0$),
(iii) A vector $v = \alpha w_1^2 + \gamma w_2^2$ in $\mathrm{Sym}^2 \Omega^1(\mathcal{C})$ where $(w_1, w_2) = (x\,dx/y, dx/y)$ is the canonical basis of differential forms on $\mathcal{C}$.

Switching from one representation to another can be done at the cost of $O(1)$ operations in k.

5. Computing the isogeny from its tangent map

5.1 General strategy

Assume that we are given the tangent map $d\varphi$ of a separable isogeny $\varphi\colon A \to A'$ of principally polarized abelian varieties of dimension g defined over a field k. In general, the task of *computing* φ *explicitly* may be specified as follows: given models of A and A', that is given very ample line bundles $\mathcal{L}_A$ and $\mathcal{L}_{A'}$ on A and A' and a choice of global sections (a_i) (resp. (a'_j)) which give a projective embedding of A (resp. A'), express the functions $\varphi^* a'_j$ on A as rational fractions in terms the coordinates (a_i).

One method to determine φ given $d\varphi$ is to work over the formal groups of A and A'. Let $x_1, \ldots, x_g$ be uniformizers at 0_A, and let $y_1, \ldots, y_g$ be uniformizers at $0_{A'}$. Knowing the map $d\varphi$ allows us to express the differential form $\varphi^* dy_j$ in term of the differential forms dx_i on A, so the functions $\varphi^* a'_j$ satisfy a differential system. A possible strategy to solve this differential system is to use a multivariate Newton algorithm, possibly over a finite free extension of the formal group. If this algorithm is successful, we recover the functions $\varphi^* a'_j$ as power series in $k[[x_1, \ldots, x_g]]$ up to some precision. The next step is to use multivariate rational reconstruction to obtain φ as a rational map. In order for the rational reconstruction algorithm to succeed, the power series precision must be large enough with respect to the degrees of the result in the variables (a_i).

This strategy to compute φ is not new: the idea of using a differential equation to compute isogenies in genus 1 appears in [Elk98], and [BMS+08] uses a Newton algorithm to solve this differential equation. To the best of our knowledge, the first article to extend these ideas to genus 2 is [CE15]. The method is further extended to compute endomorphisms of Jacobians

over a number field in [CMS+19]. In [CMS+19, §6], the endomorphism is represented as a divisorial correspondence; the interpolation of this divisor is done differently, via linear algebra on Riemann–Roch spaces.

A necessary condition for the whole method to work is that φ be completely determined by its tangent map. In general, this will be the case when $\operatorname{char} k$ is large with respect to the degree of φ. For instance, we have the following statement in the case of ℓ-isogenies.

Lemma 5.1. *Let A and A' be two principally polarized abelian varieties over a field k, let $M\colon T_0(A) \to T_0(A')$ be a linear map, and let $N > 0$ be an integer. Assume that that $\operatorname{char} k = 0$ or $\operatorname{char} k > 4N$. Then there is at most one ℓ-isogeny $\varphi\colon A \to A'$ with $\ell \leqslant N$ such that $d\varphi = M$.*

Proof. Let φ_1 and φ_2 be two such isogenies. Then $\varphi_1 = \varphi_2 + \psi$ where ψ is inseparable. If $\operatorname{char} k = 0$, this implies $\psi = 0$ and hence $\varphi_1 = \varphi_2$. Otherwise, write $p = \operatorname{char} k$ and denote by $\overline{\varphi_1}$ the contragredient isogeny. Then if $\psi \neq 0$, we have

$$\psi\overline{\psi} = \varphi_2\overline{\varphi_2} + \varphi_1\overline{\varphi_1} - \varphi_1\overline{\varphi_2} - \varphi_2\overline{\varphi_1}.$$

But $\psi\overline{\psi}$ is equal to p^m for some $m \geqslant 1$, and $\varphi_1\overline{\varphi_1} = \ell_1$, $\varphi_2\overline{\varphi_2} = \ell_2$ with $\ell_1, \ell_2 \leqslant N$ by hypothesis. Therefore we obtain $p^m \leqslant 2N + 2\sqrt{N}\sqrt{N} = 4N$. □

In practice, Newton iterations fail to reach sufficiently high power series precision if $\operatorname{char} k$ is too small, hence the larger bound $8\ell + 7$ given in Theorem 1.1.

In the rest of this section, we carry out this strategy in detail when A, A' are the Jacobians of genus 2 hyperelliptic curves $\mathcal{C}, \mathcal{C}'$, and we assume for simplicity that the characteristic is different from two. Concretely, we are given the matrix of $d\varphi$ in the bases of $T_0(A)$ and $T_0(A')$ that are dual to $\omega(\mathcal{C})$ and $\omega(\mathcal{C}')$ respectively (see §3.1). In this case, a nice simplification occurs: the isogeny φ is completely determined by the composite map

$$\mathcal{C} \xhookrightarrow{Q \mapsto [Q-P]} \operatorname{Jac}(\mathcal{C}) \xrightarrow{\varphi} \operatorname{Jac}(\mathcal{C}') \dashrightarrow \mathcal{C}'^{2,\mathrm{sym}} \xrightarrow{m} \mathbb{A}^4$$

where P is any point on $\mathcal{C}$, and m is the rational map given by

$$\{(x_1, y_1), (x_2, y_2)\} \mapsto \left(x_1 + x_2,\ x_1x_2,\ y_1y_2,\ \frac{y_2 - y_1}{x_2 - x_1}\right).$$

This composite map is a quadruple rational fractions $s, p, q, r \in k(u, v)$ that we call the *rational representation of φ at the base point P*. We choose a uniformizer z of $\mathcal{C}$ around P and perform the Newton iterations and rational reconstruction over the *univariate* power series ring $k[[z]]$.

We explain how we choose the base point P and solve the differential system in Section 5.2. One difficulty is that the differential system we obtain is singular (Lemma 5.6), so we need to use the geometry of the curves (Proposition 5.4) to find the first few terms in the series before switching to Newton iterations (Proposition 5.8). In Section 5.3, we estimate the degrees of the rational fractions that we want to compute and present the rational reconstruction step.

5.2 Solving the differential system

We keep the notation used in §5.1, and assume that the characteristic of k is not 2. Write the curve equations $\mathcal{C}, \mathcal{C}'$ and the tangent matrix as

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

We assume that φ is separable, so that $d\varphi$ is invertible. If P is a base point on $\mathcal{C}$, we denote by φ_P the associated map $\mathcal{C} \to \mathcal{C}'^{2,\mathrm{sym}}$.

Step 1: choice of base point and power series. Let P be a point on $\mathcal{C}$ which is not at a point at infinity; enlarging k if necessary, we assume that $P \in \mathcal{C}(k)$. Since $\varphi_P(P)$ is zero in $\mathrm{Jac}(\mathcal{C}')$, we have

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

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. If z is a local uniformizer of $\mathcal{C}$ at P, and R is a finite free extension of $k[[z]]$, we define a *local lift of φ_P at P with coefficients in R* to be a tuple $\widetilde{\varphi}_P = (x_1, x_2, y_1, y_2) \in R^4$ such that we have a commutative diagram

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

If the power series x_1, x_2, y_1, y_2 define a local lift of φ_P, then they satisfy the differential system (S) given by

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

where we consider the coordinates u, v on $\mathcal{C}$ as elements of $k[[z]]$, and the symbol d/dz denotes differentiation with respect to z.

When solving (S), we want φ_P to be of generic type. Proposition 5.4 shows how to choose P to enforce this condition; in order to prove it, we first study the existence of local lifts for arbitrary base points.

Lemma 5.2. *Let z be a uniformizer of $\mathcal{C}$ at P. Then there is a quadratic extension k'/k such that a local lift of φ_P at P with coefficients in $R = k'[[\sqrt{z}]]$ exists. Moreover, if φ_P is of generic type, or if P is a Weierstrass point of $\mathcal{C}$, then the same statement holds with $R = k'[[z]]$.*

Proof. First assume that φ_P is of generic type. Since the unordered pair $\{Q, i(Q)\}$ is Galois-invariant, there is a quadratic extension k'/k such that Q is defined over k'. The map $\mathcal{C}'^2 \to \mathcal{C}'^{2,\mathrm{sym}}$ is étale at $\big(Q, i(Q)\big)$, and therefore induces an isomorphism of completed local rings. Therefore a local lift exists over $k'[[z]]$.

Second, assume that φ_P is of Weierstrass type. The map $\operatorname{Spec} k[[z]] \to \mathcal{C}'^{2,\mathrm{sym}}$ defines a $k((z))$-point of $\mathcal{C}'^{2,\mathrm{sym}}$, and there exists a preimage of this point defined over an extension $K/k((z))$ of degree 2. Let R be the integral closure of $k[[z]]$ in K. Then R is contained in $k'[[\sqrt{z}]]$ for some quadratic extension k'/k [The18, Tag 09E8]. By the valuative criterion of properness, our K-point of $\mathcal{C}'^2$ extends to an R-point uniquely, so a local lift exists over R.

Finally, assume that φ_P is of Weierstrass type and that P is a Weierstrass point of $\mathcal{C}$. Let (x_1, x_2, y_1, y_2) be a local lift of φ_P over $k'[[\sqrt{z}]]$. The completed local ring of the Kummer line of $\mathcal{C}$ at P is $k[[z^2]]$, and the unordered pair $\{x_1, x_2\}$ is defined on the Kummer line; by the same

argument as above, x_1 and x_2 are defined over $k'[[z]]$. The system (S) can be written as

$$\begin{pmatrix} 1/y_1 \\ 1/y_2 \end{pmatrix} = \begin{pmatrix} x_1\,dx_1/dz & x_2\,dx_2/dz \\ dx_1/dz & dx_2/dz \end{pmatrix}^{-1} \begin{pmatrix} R_1(z) \\ R_2(z) \end{pmatrix}$$

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

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 5.3. *Assume that a local lift $\widetilde{\varphi}_P$ 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. □

Proposition 5.4. *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 $\widetilde{\varphi}_P$ exists over $k'[[z]]$. By Lemma 5.3, the tangent vector $d\widetilde{\varphi}_P/dz$ at $z = 0$ is of the form $(v + w, w)$ for some $v, w \in T_Q\mathcal{C}'$ such that $v \neq 0$. Let ω' be the unique nonzero differential form pulled back to ω_P by φ. Then ω' must vanish on $(v, 0)$, in other words ω' must vanish at Q.

Second, assume that no such lift exists. By Lemma 5.2, 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 over $k'[[\sqrt{z}]]$ as in Lemma 5.2, and look at the differential system (S). Write the lift as

$$y_1 = v_1\sqrt{z} + t_1 z + O(z^{3/2}), \quad y_2 = v_2\sqrt{z} + t_2 z + O(z^{3/2}).$$

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

$$x_1 = x_0 + w_1 z + O(z^{3/2}), \quad x_2 = x_0 + w_2 z + O(z^{3/2}).$$

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

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

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

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

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

Using Proposition 5.4, we choose a base point P on $\mathcal{C}$ such that φ_P is of generic type. By Lemma 5.2, a local lift $\widetilde{\varphi}_P = (x_1, x_2, y_1, y_2)$ of φ_P exists over $k'[[z]]$, where k' is a quadratic extension of k.

Step 2: initialization. Now we explain how to compute the power series x_1, x_2, y_1, y_2 up to $O(z^2)$. We can compute the point $Q = (x_0, y_0)$ using Proposition 5.4. 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, we can compute y_1, y_2 up to $O(z^2)$ in terms of v_1, v_2 respectively. Let u_0 (resp. d_0) be the constant term of the power series u (resp. $1/v \cdot du/dz$). Then (S) gives

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

Combining the two lines, we also obtain

$$(x_1 - x_0)\frac{dx_1}{y_1} + (x_2 - x_0)\frac{dx_2}{y_2} = R,$$

where $R = r_1 z + O(z^2)$ has no constant term. At order 1, this yields

$$v_1^2 + v_2^2 = y_0 r_1. \tag{3}$$

Equalities (2) and (3) 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 $n \geqslant 2$. 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 5.5. *The power series δx_1, δx_2 satisfy a linear differential equation of the first order*

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

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, u, v, $E_{\mathcal{C}}$ 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 [CE15; CMS+19], is that the matrix M is not invertible in $k'[[z]]$. Still, we can adapt the generic divide-and-conquer algorithm from [BCG+17, §13.2].

Lemma 5.6. *The determinant*

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

has valuation 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 2: if they did, then so would y_1 and y_2 because of the curve equation, contradicting Lemma 5.3. □

By Lemma 5.6, we can find $I \in \mathcal{M}_2\big(k[[z]]\big)$ such that $IM = \begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix}$.

Lemma 5.7. *Let $\kappa \geqslant 1$, and assume that $\operatorname{char} k > \kappa + 1$. Let $A = IN$. Then the matrix $A + \kappa$ has an invertible constant term.*

Proof. By Lemma 5.6, the leading term of $\det(M)$ is λz for some nonzero $\lambda \in k'$. Using Proposition 5.5, we compute that the constant term of $\det(A + \kappa)$ is $\lambda^2 \kappa(\kappa + 1)$. We omit the calculations. □

Proposition 5.8. *Let $1 \leqslant \nu \leqslant 2n - 1$, 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 the equation

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

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

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

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

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

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 5.7, the constant term of $A + \kappa$ is invertible. This concludes the induction, and the result follows from standard lemmas in computer algebra [BCG+17, Lem. 1.12]. □

Proposition 5.9. *Let $\nu \geqslant 1$, 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 5.8 and [BCG+17, Lem. 1.12]. □

5.3 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 $\mathrm{Jac}(\mathcal{C}')$, namely $\varphi_P(\mathcal{C})$ and the polar divisors of s, p, q and r as functions on $\mathrm{Jac}(\mathcal{C}')$. They are already known in the case of an ℓ-isogeny.

Proposition 5.10 [CE15, §6.1]. *Let $\varphi\colon \mathrm{Jac}(\mathcal{C}) \to \mathrm{Jac}(\mathcal{C}')$ 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.*

Now assume that $\mathrm{Jac}(\mathcal{C})$ and $\mathrm{Jac}(\mathcal{C}')$ have real multiplication by $\mathbb{Z}_K$ given by embeddings ι, ι', and that

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

is a β-isogeny. Denote the theta divisors on $\mathrm{Jac}(\mathcal{C})$ and $\mathrm{Jac}(\mathcal{C}')$ by Θ and Θ' respectively, and denote by $\eta_P\colon \mathcal{C} \to \mathrm{Jac}(\mathcal{C})$ the map $Q \mapsto [Q - P]$. Then $\eta_P(\mathcal{C})$ is algebraically equivalent to Θ.

Lemma 5.11. *The polar divisors of s, p, q, r as rational functions on $\mathrm{Jac}(\mathcal{C}')$ are algebraically equivalent to $2\Theta'$, $2\Theta'$, $6\Theta'$ and $4\Theta'$ respectively.*

Proof. See [CE15, §6.1]. For instance, $s = x_1 + x_2$ has a pole of order 1 along each of the two divisors $\big\{(\infty_\pm, Q) \,|\, Q \in \mathcal{C}\big\}$, 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 $\mathrm{Jac}(\mathcal{C}')$ are in bijective correspondence with isomorphism classes of line bundles. By Theorem 2.17, if (A, ι) is a principally polarized abelian surface with real multiplication by $\mathbb{Z}_K$, then there is a bijection $\alpha \mapsto \mathcal{L}_A^{\iota(\alpha)}$ between $\mathbb{Z}_K$ and the Néron–Severi group of A.

Lemma 5.12. *Let φ be a β-isogeny as above. Then the divisor $\varphi_P(\mathcal{C})$ is algebraically equivalent to the divisor corresponding to the line bundle $\mathcal{L}_{\mathrm{Jac}(\mathcal{C}')}^{\iota'(\bar{\beta})}$.*

Proof. By Theorem 2.17, there exists an $\alpha \in \mathbb{Z}_K$ 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 2.18, the pullback $\varphi^*\Theta'$ corresponds to the line bundle $\mathcal{L}_{\mathrm{Jac}(\mathcal{C})}^{\iota(\beta)}$ 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 2.17 applied on $\mathrm{Jac}(\mathcal{C})$, we have $\alpha\beta = N_{K/\mathbb{Q}}(\beta)$, so $\alpha = \bar{\beta}$. □

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

Proposition 5.13 [Kan19, 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 via the isomorphism of Theorem 2.17 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 5.14. *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*

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

Proof. Write $\alpha = a + b\sqrt{\Delta}$. By Proposition 5.13, we can compute

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

On the other hand, the Riemann–Roch theorem [Mil86a, Thm. 11.1] gives

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

The result follows. □

Proposition 5.15. *Let φ be a β-isogeny as above, and 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 5.11 and the divisor $\varphi_P(\mathcal{C})$. By Lemma 5.12, the line bundle associated with $\varphi_P(\mathcal{C})$, up to algebraic equivalence, is $\mathcal{L}_{\mathrm{Jac}(\mathcal{C}')}^{\bar{\beta}}$. Its intersection number with Θ' is nonnegative, hence by Corollary 5.14, we have

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

The result follows by Lemma 5.11. □

Rational reconstruction. Now we present the rational reconstruction algorithm, and compute the power series precision that is precisely needed.

Lemma 5.16. *Let $s\colon \mathcal{C} \to \mathbb{P}^1$ be a morphism of degree d.*

(i) If s is invariant under the hyperelliptic involution i, then we can write $s(u, v) = X(u)$ where the degree of X is bounded by $d/2$.

(ii) 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. For item 1, use the fact that the function u itself has degree 2. For item 2, write

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

The degrees of these morphisms are bounded by $2d$ and $2d + 6$ respectively. □

Proposition 5.17. *Let $\widetilde{\varphi}_P$ and $\widetilde{\varphi}_{i(P)}$ be local lifts of φ_P at P and $i(P)$ in the uniformizers z and $i(z)$. Let $\nu = 8\ell + 7$ in the Siegel case, and $\nu = 4\operatorname{Tr}_{K/\mathbb{Q}}(\beta) + 7$ 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 of $\mathcal{C}$. Then s, p are invariant under the hyperelliptic involution. Therefore we have to recover univariate rational fractions in u of degree $d \leqslant 2\ell$ (resp. $d \leqslant \operatorname{Tr}(\beta)$). This can be done in quasi-linear time from their power series expansion up to precision $O(u^{2d+1})$ [BCG+17, §7.1]. Since u has valuation 2 in z, we need to compute $\widetilde{\varphi}_P$ at precision $O(z^{4d+1})$.

Second, assume that P is not a Weierstrass point of $\mathcal{C}$. 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 $d \leqslant 4\ell + 3$ (resp. $d \leqslant 2\operatorname{Tr}(\beta) + 3$) 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 $O(z^{2d+1})$. □

6. Summary of the algorithm

In this final section, we summarize the isogeny algorithm and prove Theorem 1.1. We also state the analogous result in the case of β-isogenies (Theorem 6.3).

Algorithm 6.1. Let j, j' the Igusa invariants of principally polarized abelian varieties A, A' over k. Assume that A, A' are ℓ-isogenous (the Siegel case), or that A, A' have real multiplication by $\mathbb{Z}_K$ and are β-isogenous (the Hilbert case).

(i) Use Mestre's algorithm [Mes91] to construct curve equations $\mathcal{C}, \mathcal{C}'$ whose Jacobians are isomorphic to A, A'. In the Hilbert case, use Algorithm 3.26 to ensure that $\mathcal{C}, \mathcal{C}'$ are potentially Hilbert-normalized.

(ii) Compute at most 4 candidates for the tangent matrix of the isogeny φ using Proposition 4.26 in the Siegel case, or Proposition 4.27 in the Hilbert case. Run the rest of the algorithm for all the candidates.

(iii) 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 $O\big(z^{4\operatorname{Tr}(\beta)+7}\big)$ using Proposition 5.9.

(iv) Try to recover the rational representation of φ at P using Proposition 5.17. Output the result if rational fractions of the correct degrees are found.

In general, only one candidate will produce meaningful results in step iv. We recall the statement of Theorem 1.1 from the introduction.

Theorem 6.2. *Let ℓ be a prime, and let k be a field such that $\operatorname{char} k = 0$ or $\operatorname{char} k > 8\ell + 7$. Let $U \subset \mathbf{A}_2(k)$ be the open set consisting of abelian surfaces A such that $\operatorname{Aut}(A) \simeq \{\pm 1\}$ and $j_3(A) \neq 0$. Let $A, A' \in U$, and let $j(A), j(A')$ be their Igusa invariants. Assume that A and A' are ℓ-isogenous over k, and that the subvariety of $\mathbb{A}^3 \times \mathbb{A}^3$ cut out by the modular equations $\Psi_{\ell,i}$ for $1 \leqslant i \leqslant 3$ is normal at $(j(A), j(A'))$. Then, given $j(A)$ and $j(A')$ as well as the values of derivatives of Siegel modular equations of level ℓ at (A, A'), Algorithm 6.1 succeeds and returns*

(i) a tower k'/k of at most three quadratic extensions,

(ii) hyperelliptic curve equations $\mathcal{C}, \mathcal{C}'$ over k' whose Jacobians are isomorphic to A, A' respectively,

(iii) *a point* $P \in \mathcal{C}(k')$,

(iv) *the rational representation* $(s,p,q,r) \in k'(u,v)^4$ *of an* ℓ*-isogeny* $\varphi\colon \mathrm{Jac}(\mathcal{C}) \to \mathrm{Jac}(\mathcal{C}')$ *at* P.

The cost of this algorithm is $\widetilde{O}(\ell)$ *elementary operations and* $O(1)$ *square roots in* k'.

Proof. Mestre's algorithm returns curve equations $\mathcal{C},\mathcal{C}'$ defined over extensions of k of degree at most 2, and costs $O(1)$ operations in k and $O(1)$ square roots. Under our hypotheses, Proposition 4.26 applies and allows us to recover $\mathrm{Sym}^2(d\varphi)$ using $O(1)$ operations in k. We recover $d\varphi$ up to sign using $O(1)$ square roots and elementary operations; since φ is defined over k, extending the base field is not necessary. We choose the base point P on $\mathcal{C}$ such that φ_P is of generic type using Proposition 5.4, perhaps taking another extension of degree 2. By Proposition 5.9, we can compute the local lifts $\widetilde{\varphi}_P$ and $\widetilde{\varphi}_{i(P)}$ up to precision $8\ell+7$ within $\widetilde{O}(\ell)$ field operations; this is where we use the hypothesis on $\mathrm{char}\, k$. Finally, we recover the rational representation at P using a further $\widetilde{O}(\ell)$ field operations by Proposition 5.17. The result is defined over an extension of k of degree dividing 8. □

We conclude with the analogue of Theorem 6.2 in the Hilbert case.

Theorem 6.3. *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* $\mathrm{char}\, k = 0$ *or* $\mathrm{char}\, k > 4\,\mathrm{Tr}_{K/\mathbb{Q}}(\beta)+7$. *Let* A, A' *be principally polarized abelian surfaces over* k *with real multiplication by* $\mathbb{Z}_K$ *whose Igusa invariants* $j(A), j(A')$ *are well-defined, and assume that there exists a* β*-isogeny* $\varphi\colon A \to A'$ *defined over* k *which is generic in the sense of Definition 3.18. Then, given* $j(A)$ *and* $j(A')$, *as well of the values of derivatives of Hilbert modular equations of level* β *at* (A, A'), *Algorithm 6.1 succeeds and returns*

(i) *a tower* k'/k *of at most three quadratic extensions,*

(ii) *hyperelliptic curve equations* $\mathcal{C},\mathcal{C}'$ *over* k' *whose Jacobians are isomorphic to* A, A' *respectively,*

(iii) *a point* $P \in \mathcal{C}(k')$,

(iv) *at most* 4 *possible values for the rational representation* $(s,p,q,r) \in k'(u,v)^4$ *of a* β*- or* $\overline{\beta}$*-isogeny* $\varphi\colon \mathrm{Jac}(\mathcal{C}) \to \mathrm{Jac}(\mathcal{C}')$ *at* P.

The cost of Algorithm 6.1 in the Hilbert case is $\widetilde{O}\big(\mathrm{Tr}_{K/\mathbb{Q}}(\beta)\big) + O_K(1)$ *elementary operations and* $O(1)$ *square roots in* k'; *the implied constants, except in* $O_K(1)$, *are independent of* K.

We expect that the algorithm returns only one answer for the rational representation of φ at P; if the algorithm outputs several answers, we could implements tests for correctness, but they might be more expensive than the isogeny algorithm itself.

Proof. We use Algorithm 3.26 to construct the curve equations $\mathcal{C},\mathcal{C}'$. By Remark 4.24, we obtain potentially Hilbert-normalized curves, and each of them is defined over an extension of k of degree at most 4. This requires $O_K(1)$ elementary operations and $O(1)$ square roots in k. We may assume that $\mathcal{C},\mathcal{C}'$ are Hilbert-normalized for some choice of real multiplication embeddings that are compatible via φ, which becomes either a β- or a $\overline{\beta}$-isogeny.

Under our hypotheses, Proposition 4.27 applies, so we recover two possible values for $(d\varphi)^2$ within $O(1)$ operations in k, and hence 4 possible values for $d\varphi$, using $O(1)$ square roots. We can now make a change of variables to the (not necessarily Hilbert-normalized) curves output by Mestre's algorithm, so that each curve is defined over an extension of k of degree 2. The end of the algorithm is similar to the Siegel case: we take an extension of degree 2 to find the base point, then try to compute the rational representation for each value of $d\varphi$ using $\widetilde{O}(\mathrm{Tr}_{K/\mathbb{Q}}(\beta))$ operations

in k. For the correct value of $d\varphi$, rational reconstruction will succeed and output fractions of the correct degrees. □

References

[AOV08] D. Abramovich, M. Olsson, and A. Vistoli. "Tame stacks in positive characteristic". In: *Ann. Inst. Fourier (Grenoble)* 58.4 (2008), pp. 1057–1091.

[AV02] D. Abramovich and A. Vistoli. "Compactifying the space of stable maps". In: *J. Amer. Math. Soc.* 15.1 (2002), pp. 27–75.

[Alp13] J. Alper. "Good moduli spaces for Artin stacks". In: *Ann. Inst. Fourier (Grenoble)* 63.6 (2013), pp. 2349–2402.

[Alp14] J. Alper. "Adequate moduli spaces and geometrically reductive group schemes". In: *Algebr. Geom.* 1.4 (2014), pp. 489–531.

[AHR19] J. Alper, J. Hall, and D. Rydh. "The étale local structure of algebraic stacks". 2019.

[AHR20] J. Alper, J. Hall, and D. Rydh. "A Luna étale slice theorem for algebraic stacks". In: *Ann. Math.* 191.3 (2020), pp. 675–738.

[And17] Y. André. "On the Kodaira–Spencer map of abelian schemes". In: *Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)* 17.4 (2017), pp. 1397–1416.

[BB66] W. L. Baily Jr. and A. Borel. "Compactification of arithmetic quotients of bounded symmetric domains". In: *Ann. of Math. (2)* 84 (1966), pp. 442–528.

[BL04] C. Birkenhake and H. Lange. *Complex abelian varieties*. 2nd ed. Springer, 2004.

[BCG+17] A. Bostan, F. Chyzak, M. Giusti, R. Lebreton, G. Lecerf, B. Salvy, and É. Schost. *Algorithmes efficaces en calcul formel*. CreateSpace, 2017.

[BMS+08] A. Bostan, F. Morain, B. Salvy, and É. Schost. "Fast algorithms for computing isogenies between elliptic curves". In: *Math. Comp.* 77.263 (2008), pp. 1755–1778.

[Bou72] N. Bourbaki. *Groupes et algèbres de Lie. Chapitres II et III*. Hermann, 1972.

[Bou75] N. Bourbaki. *Groupes et algèbres de Lie. Chapitres VII et VIII*. Hermann, 1975.

[BL09] R. Bröker and K. Lauter. "Modular polynomials for genus 2". In: *LMS J. Comp. Math.* 12 (2009), pp. 326–339.

[Bru08] J. H. Bruinier. "Hilbert modular forms and their applications". In: *The 1-2-3 of modular forms*. Springer, 2008, pp. 105–179.

[BP17] J. I. Burgos Gil and A. Pacetti. "Hecke and Sturm bounds for Hilbert modular forms over real quadratic fields". In: *Math. Comp.* 86.306 (2017), pp. 1949–1978.

[Cha90] C.-L. Chai. "Arithmetic minimal compactification of the Hilbert–Blumenthal moduli spaces". In: *Ann. of Math. (2)* 131.3 (1990), pp. 541–554.

[CvdG00] C. Ciliberto and G. van der Geer. "The moduli space of abelian varieties and the singularities of the theta divisor". In: *Surveys in differential geometry*. Vol. 7. Surv. Differ. Geom. Int. Press, 2000, pp. 61–81.

[Cle72] A. Clebsch. *Theorie der binären algebraischen Formen*. B. G. Teubner, 1872.

[CFvdG17] F. Cléry, C. Faber, and G. van der Geer. "Covariants of binary sextics and vector-valued Siegel modular forms of genus two". In: *Math. Ann.* 369.3-4 (2017), pp. 1649–1669.

[Con05] B. Conrad. "The Keel–Mori theorem via stacks". 2005.

[CR15] R. Cosset and D. Robert. "Computing (ℓ, ℓ)-isogenies in polynomial time on Jacobians of genus 2 curves". In: *Math. Comp.* 84.294 (2015), pp. 1953–1975.

[CMS+19] E. Costa, N. Mascot, J. Sijsling, and J. Voight. "Rigorous computation of the endomorphism ring of a Jacobian". In: *Math. Comp.* 88.317 (2019), pp. 1303–1339.

[CE15] J.-M. Couveignes and T. Ezome. "Computing functions on Jacobians and their quotients". In: *Lond. Math. Soc. J. Comput. Math.* 18.1 (2015), pp. 555–577.

[dJon93] A. J. de Jong. "The moduli spaces of polarized abelian varieties". In: *Math. Ann.* 295.3 (1993), pp. 485–503.

[DR73] P. Deligne and M. Rapoport. "Les schémas de modules de courbes elliptiques". In: *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, 1972)*. Springer, 1973, pp. 143–316.

[DJR+17] A. Dudeanu, D. Jetchev, D. Robert, and M. Vuille. "Cyclic isogenies for abelian varieties with real multiplication". 2017.

[Dup11] R. Dupont. "Fast evaluation of modular functions using Newton iterations and the AGM". In: *Math. Comp.* 80.275 (2011), pp. 1823–1847.

[Elk98] N. D. Elkies. "Elliptic and modular curves over finite fields and related computational issues". In: *Computational perspectives on number theory (Chicago, 1995)*. Vol. 7. Amer. Math. Soc., 1998, pp. 21–76.

[Eng09] A. Enge. "Computing modular polynomials in quasi-linear time". In: *Math. Comp.* 78.267 (2009), pp. 1809–1824.

[ET14] A. Enge and E. Thomé. *CMH: Computation of Igusa class polynomials*. 2014. URL: https://gitlab.inria.fr/cmh/cmh/.

[FC90] G. Faltings and C.-L. Chai. *Degeneration of abelian varieties*. Springer, 1990.

[FGI+05] B. Fantechi, L. Göttsche, L. Illusie, S. L. Kleiman, N. Nitsure, and A. Vistoli. *Fundamental algebraic geometry*. Mathematical Surveys and Monographs 123. American Mathematical Society, 2005.

[GKS11] P. Gaudry, D. Kohel, and B. Smith. "Counting points on genus 2 curves with real multiplication". In: *Advances in Cryptology – Asiacrypt 2011*. Seoul: Springer, 2011, pp. 504–519.

[GS12] P. Gaudry and É. Schost. "Genus 2 point counting over prime fields". In: *J. Symb. Comput.* 47.4 (2012), pp. 368–400.

[GL12] E. Z. Goren and K. E. Lauter. "Genus 2 curves with complex multiplication". In: *IMRN* 5 (2012), pp. 1068–1142.

[Gro64] A. Grothendieck. "Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. I". In: *Inst. Hautes Études Sci. Publ. Math.* 20 (1964).

[Gru10] D. Gruenewald. "Computing Humbert surfaces and applications". In: *Arithmetic, geometry, cryptography and coding theory 2009*. Amer. Math. Soc., 2010, pp. 59–69.

[Ibu12] T. Ibukiyama. "Vector-valued Siegel modular forms of symmetric tensor weight of small degrees". In: *Comment. Math. Univ. St. Pauli* 61.1 (2012), pp. 51–75.

[Igu60] J.-I. Igusa. "Arithmetic variety of moduli for genus two". In: *Ann. of Math. (2)* 72 (1960), pp. 612–649.

[Igu62] J.-I. Igusa. "On Siegel modular forms of genus two". In: *Amer. J. Math.* 84 (1962), pp. 175–200.

[Igu79] J.-I. Igusa. "On the ring of modular forms of degree two over $\mathbb{Z}$". In: *Amer. J. Math.* 101.1 (1979), pp. 149–183.

[Igu67] J.-I. Igusa. "Modular forms and projective invariants". In: *Amer. J. Math.* 89 (1967), pp. 817–855.

[Kan19] E. Kani. "Elliptic subcovers of a curve of genus 2. I. The isogeny defect". In: *Ann. Math. Qué.* 43.2 (2019), pp. 281–303.

[KM97] S. Keel and S. Mori. "Quotients by groupoids". In: *Ann. of Math. (2)* 145.1 (1997), pp. 193–213.

[Kie21] J. Kieffer. "Evaluating modular equations for abelian surfaces". 2021.

[Kie22a] J. Kieffer. "Counting points on abelian surfaces over finite fields with Elkies's method". 2022.

[Kie22b] J. Kieffer. "Degree and height estimates for modular equations on PEL Shimura varieties". In: *J. London Math. Soc.* (2022).

[KS58] K. Kodaira and D. C. Spencer. "On deformations of complex analytic structures, I". In: *Ann. of Math. (2)* 67 (1958), pp. 328–401.

[LM00] G. Laumon and L. Moret-Bailly. *Champs algébriques*. Springer, 2000.

[LY11] K. Lauter and T. Yang. "Computing genus 2 curves from invariants on the Hilbert moduli space". In: *J. Number Theory* 131.5 (2011), pp. 936–958.

[Liu93] Q. Liu. "Courbes stables de genre 2 et leur schéma de modules". In: *Math. Ann.* 295.2 (1993), pp. 201–222.

[LR15] D. Lubicz and D. Robert. "Computing separable isogenies in quasi-optimal time". In: *LMS J. Comp. Math.* 18.1 (2015), pp. 198–216.

[Lun73] D. Luna. "Slices étales". In: *Sur les groupes algébriques*. 1973, 81–105. Bull. Soc. Math. France, Paris, Mémoire 33.

[Mar18] C. Martindale. "Isogeny graphs, modular polynomials, and applications". Universiteit Leiden and Université de Bordeaux, 2018.

[Mes91] J.-F. Mestre. "Construction de courbes de genre 2 à partir de leurs modules". In: *Effective methods in algebraic geometry (Castiglioncello, 1990)*. Birkhäuser, 1991, pp. 313–334.

[Mil15] E. Milio. "A quasi-linear time algorithm for computing modular polynomials in dimension 2". In: *LMS J. Comput. Math.* 18 (2015), pp. 603–632.

[Mil] E. Milio. *Database of modular polynomials*. URL: https://members.loria.fr/EMilio/modular-polynomials.

[MR20] E. Milio and D. Robert. "Modular polynomials on Hilbert surfaces". In: *J. Number Theory* 216 (2020), pp. 403–459.

[Mil86a] J. S. Milne. "Abelian varieties". In: *Arithmetic geometry (Storrs, 1984)*. Springer, 1986, pp. 103–150.

[Mil86b] J. S. Milne. "Jacobian varieties". In: *Arithmetic geometry (Storrs, 1984)*. Springer, 1986, pp. 167–212.

[Mol18] P. Molin. *Hcperiods: Period matrices and Abel-Jacobi maps of hyperelliptic and superperelliptic curves*. 2018. URL: https://github.com/pascalmolin/hcperiods.

[MN19] P. Molin and C. Neurohr. "Computing period matrices and the Abel-Jacobi map of superelliptic curves". In: *Math. Comp.* 88.316 (2019), pp. 847–888.

[MvdGE12] B. Moonen, G. van der Geer, and B. Edixhoven. *Abelian varieties*. 2012.

[Mum84] D. Mumford. *Tata lectures on theta. II*. Birkhäuser, 1984.

[MFK94] D. Mumford, J. Fogarty, and F. Kirwan. *Geometric invariant theory*. 3rd ed. Springer, 1994.

[Mum71] D. Mumford. "The structure of the moduli spaces of curves and abelian varieties". In: *Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 1*. 1971, pp. 457–465.

[Nag83] S. Nagaoka. "On the ring of Hilbert modular forms over $\mathbb{Z}$". In: *J. Math. Soc. Japan* 35.4 (1983), pp. 589–608.

[Ols06] M. C. Olsson. "Hom-stacks and restriction of scalars". In: *Duke Math. J.* 134.1 (2006), pp. 139–164.

[Rap78] M. Rapoport. "Compactifications de l'espace de modules de Hilbert-Blumenthal". In: *Compositio Math.* 36.3 (1978), pp. 255–335.

[Ryd11] D. Rydh. "The canonical embedding of an unramified morphism in an étale morphism". In: *Math. Z.* 268.3-4 (2011), pp. 707–723.

[Ryd13] D. Rydh. "Existence and properties of geometric quotients". In: *J. Algebraic Geom.* 22.4 (2013), pp. 629–669.

[Sch85] R. Schoof. "Elliptic curves over finite fields and the computation of square roots mod p". In: *Math. Comp.* 44.170 (1985), pp. 483–494.

[Sch95] R. Schoof. "Counting points on elliptic curves over finite fields". In: *J. Théorie Nr. Bordx.* 7.1 (1995), pp. 219–254.

[Str10] M. Streng. "Complex multiplication of abelian surfaces". Universiteit Leiden, 2010.

[Sut13] A. V. Sutherland. "On the evaluation of modular polynomials". In: *Proceedings of the 10th Algorithmic Number Theory Symposium*. San Diego: Math. Sci. Publ., 2013, pp. 531–555.

[The19] The PARI group. *Pari/GP version 2.11.0*. 2019. URL: http://pari.math.u-bordeaux.fr/.

[The18] The Stacks project authors. *The Stacks Project*. 2018. URL: https://stacks.math.columbia.edu/.

[Tho70] J. Thomae. "Beitrag zur Bestimmung von $\vartheta(0,0,\dots 0)$ durch die Klassenmoduln algebraischer Functionen". In: *J. Reine Angew. Math.* 71 (1870), pp. 201–222.

[vdGee88] G. van der Geer. *Hilbert modular surfaces*. Springer, 1988.

[vdGee08] G. van der Geer. "Siegel modular forms and their applications". In: *The 1-2-3 of modular forms*. Springer, 2008, pp. 181–245.

[vWam00] P. van Wamelen. "Poonen's question concerning isogenies between Smart's genus 2 curves". In: *Math. Comp.* 69.232 (2000), pp. 1685–1697.

[vWam06] P. van Wamelen. "Computing with the analytic Jacobian of a genus 2 curve". In: *Discovering Mathematics with Magma*. Springer, 2006, pp. 117–135.

[Vél71] J. Vélu. "Isogénies entre courbes elliptiques". In: *C. R. Acad. Sci. Paris* A273 (1971), pp. 238–241.

Appendix 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 Humbert 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 work over $\mathbb{C}$, but the methods of §4 show that the computations are valid in general. We illustrate our algorithm with an example of cyclic isogeny of degree 11 over a finite field.

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. 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.1 [Nag83]. *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*

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

The *Gundlach invariants* for $K = \mathbb{Q}(\sqrt{5})$ are

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

Recall that we denote by σ the involution $(t_1, t_2) \mapsto (t_2, t_1)$ of $\mathbf{H}_2(\mathbb{C})$

Proposition A.2. *The Gundlach invariants define a birational map*

$$\mathbf{H}_2(\mathbb{C})/\sigma \to \mathbb{C}^2.$$

Proof. This is a consequence of the Baily–Borel Theorem [BB66, Thm. 10.11] and Theorem A.1. □

By Proposition 2.14, 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 [LY11, Prop. 3.2]: 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.3 [LY11, Prop. 4.5]. *In the case $K = \mathbb{Q}(\sqrt{5})$, we have*

$$H^* j_1 = 8g_1\left(3\frac{g_2^2}{g_1} - 2\right)^5,$$
$$H^* j_2 = \frac{1}{2}g_1\left(3\frac{g_2^2}{g_1} - 2\right)^3,$$
$$H^* j_3 = \frac{1}{8}g_1\left(3\frac{g_2^2}{g_1} - 2\right)^2\left(4\frac{g_2^2}{g_1} + 2^5 3^2\frac{g_2}{g_1} - 3\right).$$

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 $\Psi_{\beta,1}, \Psi_{\beta,2} \in \mathbb{C}(G_1, G_2)[G_1']$ defined as follows:

- $\Psi_{\beta,1}$ 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 the following equality of meromorphic functions on $\mathbf{H}_2(\mathbb{C})$:

$$g_2(t/\beta) = \Psi_{\beta,2}\big(g_1(t), g_2(t), g_1(t/\beta)\big).$$

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

A.2 Variants in the isogeny algorithm

Constructing potentially Hilbert-normalized curves. We give another method to reconstruct such curves using the pullback of the modular form $f_{8,6}$ from Example 2.8 as a Hilbert modular form. Let $H\colon \mathbb{H}_1^2 \to \mathbb{H}_2$ be the Hilbert embedding from §2.4.

Proposition A.4. *Define the functions $b_i(t)$ for $0 \leqslant i \leqslant 6$ on $\mathbb{H}_1^2$ by*

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

Then b_2 and b_4 are identically zero, and

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

Proof. By Proposition 2.14, 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 3.12, the standard curve $\mathcal{C}_K(t)$ attached to $t \in \mathbb{H}_1^2$ is proportional to the curve $y^2 = \sum b_i(t)x^i$. The algorithm to compute a potentially Hilbert-normalized curve $\mathcal{C}$ from its Igusa invariants (j_1, j_2, j_3) runs as follows.

Algorithm A.5.

(i) Compute Gundlach invariants (g_1, g_2) mapping to the Igusa invariants (j_1, j_2, j_3) via H using Proposition A.3, and compute values for the generators G_2, F_6, F_{10} giving these invariants.

(ii) Compute b_3^2, $b_1 b_5$, etc. using Proposition A.4.

(iii) 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. Even if arbitrary choices are made during Algorithm A.5, the output will be potentially Hilbert-normalized.

Computing the tangent matrix. Consider $\Psi_{\beta,1}$ and $\Psi_{\beta,2}$ as elements of the ring $\mathbb{Q}(G_1, G_2)[G_1', G_2']$. Define the 2×2 matrices

$$D\Psi_{\beta,L} = \left(\frac{\partial \Psi_n}{\partial G_k}\right)_{1 \leqslant n,k \leqslant 2} \quad \text{and} \quad D\Psi_{\beta,R} = \left(\frac{\partial \Psi_n}{\partial G_k'}\right)_{1 \leqslant n,k \leqslant 2}.$$

Then we have an analogue of Proposition 4.27, where we replace derivatives of Igusa invariants in Proposition 3.19 by derivatives of Gundlach invariants. The relation between these derivatives is given by Proposition A.3. This time, using the formalism of §4, we can prove that all 2×2 matrices will be invertible if the abelian varieties A, A' have only $\mathbb{Z}_K^\times$ as automorphisms, have $g_1 \neq 0$, and if the modular equations in Gundlach invariants cut out a normal subvariety of $\mathbb{A}^2 \times \mathbb{A}^2$ at $(g(A), g(A'))$.

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. We choose a trivialization of $\mathbb{Z}_K \otimes k$, in other words a square root of 5 in k, so that $\beta = 26213$.

Consider the Gundlach invariants

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

In order to reconstruct a Hilbert-normalized curve, we apply Algorithm A.5. We obtain the curve equations

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

The derivatives of Gundlach invariants are given by

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

Computing derivatives of the modular equations as in Proposition 3.19, we find that the isogeny is compatible with the real multiplication embeddings for which $\mathcal{C}, \mathcal{C}'$ are Hilbert-normalized. We do not known whether φ is a β- or a $\overline{\beta}$-isogeny, so we have four candidates for the tangent matrix

up to sign:

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

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 tangent 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 tangent matrix is $d\varphi_{\bar{\beta},+}$ 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 5.15. The isogeny is k-rational at the level of Kummer surfaces, but not on the Jacobians themselves: α appears on the numerator of $r(u, v)$.

Jean Kieffer kieffer@math.harvard.edu
Harvard University Mathematics Department, 1 Oxford St., Cambridge, MA 02140, United States

Aurel Page aurel.page@math.u-bordeaux.fr
Institut de Mathématiques de Bordeaux, Université de Bordeaux, 351 cours de la Libération, 33400 Talence, France

Damien Robert damien.robert@math.u-bordeaux.fr
Institut de Mathématiques de Bordeaux, Université de Bordeaux, 351 cours de la Libération, 33400 Talence, France