COMPUTING ISOGENIES FROM MODULAR EQUATIONS IN GENUS TWO

JEAN KIEFFER, AUREL PAGE, AND DAMIEN ROBERT

Abstract. Consider two genus 2 curves over a field whose Jacobians are linked by an isogeny of known type: either an ℓ-isogeny or, in the real multiplication case, an isogeny with cyclic kernel. We present a completely algebraic algorithm to compute this isogeny using modular equations of either Siegel or Hilbert type. An essential step of independent interest is to construct an explicit Kodaira–Spencer isomorphism for principally polarized abelian surfaces.

1. Introduction

Since the pioneering work of Vélu [Vél71] in the case of elliptic curves, several algorithms are available to solve the following problem: given a principally polarized (p.p.) abelian variety A and a torsion subgroup K of A such that A/K is also principally polarizable, compute the quotient isogeny $A \to A/K$. Some of these algorithms work with Jacobians of curves, of genus 2 in particular [CR15; CE15]; others use theta functions and apply in every dimension [LR15; DJR+22; LR22].

In this paper, we are interested in the reverse question: given two p.p. abelian varieties A and A' linked by an isogeny φ of a known type and degree but unknown kernel, compute φ. We present a completely algebraic algorithm for this task that generalizes Elkies's isogeny algorithm for elliptic curves [Elk98], and thus solve a longstanding open problem in isogeny computations [BGL+16, ğ1.1.2].

1.1. Main results.

Elkies's algorithm uses an explicit equation for the modular curve of level $\Gamma_0(\ell)$ to compute ℓ-isogenies between elliptic curves, where ℓ is a prime. More generally, we explain how algebraic equations encoding the presence of isogenies of a given type between abelian varieties, called *modular equations*, can be used to compute isogenies in every dimension. In the case of Jacobians of genus 2 curves, we describe the resulting algorithm completely. Let us state a simplified version of our main result (Theorem 6.2) in the 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 $\operatorname{char} k > 8\ell + 1$. Then, given the data of*

(1) two generic ℓ-isogenous p.p. abelian surfaces A and A' over k, and

(2) the derivatives of modular equations of Siegel type and level ℓ at (A, A'),

one can compute an ℓ-isogeny $\varphi\colon A \to A'$. This algorithm costs $\widetilde{O}(\ell)$ elementary operations and $O(1)$ square roots in k.

2020 *Mathematics Subject Classification.* 14K02, 14K10, 14Q20.

Key words and phrases. Abelian varieties, isogenies, modular equations, algorithms.

The authors were supported by the ANR grant CIAO (French Agence Nationale de la Recherche).

We also obtain a similar result (Theorem 6.3) for cyclic isogenies between p.p. abelian surfaces with real multiplication. The algorithm is then based on modular equations of Hilbert type [Mar20; MR20]. Note that, as in the case of elliptic curves, computing roots of modular equations (over finite fields in particular) is a typical way of generating suitable input for our isogeny algorithms.

1.2. **Comparison with previous works.** Other polynomial-time algorithms to compute an isogeny $\varphi\colon A \to A'$ exist, in every dimension g. For instance, one could compute k-rational subgroups of the ℓ-torsion group $A[\ell]$ and apply an algorithm to compute quotient isogenies. However, the torsion subgoups $A[\ell]$ are difficult to manipulate as ℓ grows, due to their large size ℓ^{2g}. In another direction, for abelian surfaces specifically, van Wamelen [vWam00; vWam06] describes an isogeny algorithm using complex approximations; these ideas were later generalized to Jacobians of arbitrary dimensions in [CMS+19]. However, this numerical approach is inherently restricted to subfields of $\mathbb{C}$ and lacks clear complexity estimates. In comparison, the isogeny algorithm of Theorem 1.1 reconstructs the tangent map of the isogeny exactly, and is extremely efficient. Its practical cost is hidden in the evaluation of modular equations and their derivatives, but these evaluations are still less costly than manipulating the full torsion subgroups, both in the case of elliptic curves [Eng09; Sut13] and p.p. abelian surfaces [Kie22c]. In fact, computing ℓ-isogenies provides an efficient way of obtaining maximal isotropic subgroups in $A[\ell]$. This remark is at the heart of the Schoof–Elkies–Atkin (or SEA) point-counting algorithm [Sch85] for elliptic curves over finite fields. In genus 2, one can similarly obtain asymptotic speedups over point-counting methods that only rely on kernels of endomorphisms to construct rational subgroups [GKS11; GS12]: we refer to [Kie22a] for a detailed analysis.

1.3. **Outline of the algorithm.** From a geometric point of view, we compute ℓ-isogenies in arbitrary dimension g as follows. Denote by $\mathcal{A}_g(\ell)$ the moduli stack of p.p. abelian schemes of dimension g endowed with the kernel of an ℓ-isogeny, and by $\mathcal{A}_g$ the moduli stack of p.p. abelian schemes of dimension g. Consider the map

$$\begin{aligned} \Phi_\ell = (\Phi_{\ell,1}, \Phi_{\ell,2})\colon \mathcal{A}_g(\ell) &\to \mathcal{A}_g \times \mathcal{A}_g \\ (A, K) &\mapsto (A, A/K). \end{aligned}$$

Both $\Phi_{\ell,1}$ and $\Phi_{\ell,2}$ are étale maps. Let $\varphi\colon A \to A'$ be an ℓ-isogeny, and let x, x' be the points of $\mathcal{A}_g$ corresponding to A and A'. Then the *Kodaira–Spencer isomorphism* between $T_x(\mathcal{A}_g)$ and $\operatorname{Sym}^2 T_0(A)$ yields a close relation between two maps:

- the *deformation map* $\mathscr{D}(\varphi) := d\Phi_{\ell,2} \circ d\Phi_{\ell,1}{}^{-1}\colon T_x(\mathcal{A}_g) \to T_{x'}(\mathcal{A}_g)$, and
- the *tangent map* $d\varphi\colon T_0(A) \to T_0(A')$.

Therefore, in any dimension g, an isogeny algorithm could run as follows.

(1) Compute the deformation map by differentiating certain modular equations giving a local model of $\mathcal{A}_g(\ell)$ and $\mathcal{A}_g$.
(2) Compute $d\varphi$ from the deformation map by using an explicit version of the Kodaira–Spencer isomorphism.
(3) Finally, compute φ by solving a differential system in the formal group of A and performing a rational reconstruction, as in [CE15; CMS+19].

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

In practice, working with stacks would involve adding a 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 replace the stack $\mathcal{A}_2$ by its coarse moduli scheme $\mathbf{A}_2$. We even work up to birationality, by considering the map from $\mathbf{A}_2$ to $\mathbb{A}^3$ defined by the three Igusa invariants (j_1, j_2, j_3). These modifications simplify the computations considerably, but have the drawback of introducing the genericity assumptions in Theorem 1.1. In particular, we only consider abelian surfaces A that are the Jacobian of a genus 2 curve $\mathcal{C}$.

Working with genus 2 curves allows us to encode a basis of $T_0(A)$ in the choice of an equation of $\mathcal{C}$. Then, the explicit Kodaira–Spencer isomorphism of Step (2) is simply an expression for certain Siegel modular functions, namely the derivatives of the Igusa invariants, in terms of the coefficients of the curve equation. We compute these formulas building on work of Cléry, Faber, and van der Geer [CFvdG17]: see Theorem 3.10. This result of independent interest generalizes the classical formula

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

used in Elkies's isogeny algorithm for elliptic curves.

Finally, in Step (3), we use the fact that $\mathcal{C}$ embeds in its Jacobian to compute with power series in one variable only, and use Newton iterations to solve the differential system in quasi-linear time. The hypothesis on $\operatorname{char} k$ appears in this step, but is not essential: a standard workaround in small characteristic would be to lift the isogeny to characteristic zero, following [Eid21].

1.4. **Organization of the paper.** 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. In Section 4, we adopt the language of algebraic stacks to show that the calculations over $\mathbb{C}$ remain in fact 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 Section 7, 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 forms 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

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

2.1. **Siegel modular forms.** 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

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

is naturally endowed with the structure of a principally polarized (p.p.) abelian surface over $\mathbb{C}$. A basis of $\Omega^1(A(\tau))$ is given by

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

where z_1, z_2 are the coordinates on $\mathbb{C}^2$.

The symplectic group $\mathrm{Sp}_4(\mathbb{Z})$ acts on $\mathbb{H}_2$ as follows: for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{Sp}_4(\mathbb{Z})$ and $\tau \in \mathbb{H}_2$, we write

$$\gamma\tau \coloneqq (a\tau + b)(c\tau + d)^{-1}.$$

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 $\mathbf{A}_2$ mentioned in the introduction: for every p.p. abelian surface A over $\mathbb{C}$, there exists $\tau \in \mathbb{H}_2$, unique up to the action of $\mathrm{Sp}_4(\mathbb{Z})$, such that A and $A(\tau)$ are isomorphic [BL04, Prop. 8.1.3]. For $\gamma \in \mathrm{Sp}_4(\mathbb{Z})$ as above, the linear map $z \mapsto (c\tau + d)^{-t} z$ yields an isomorphism $A(\tau) \to A(\gamma\tau)$ [BL04, Rem. 8.1.4]

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

$$f(\gamma\tau) = \rho(c\tau + d) f(\tau).$$

for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{Sp}_4(\mathbb{Z})$ and $\tau \in \mathbb{H}_2$. We say that f is *scalar-valued* if $\dim V = 1$, and *vector-valued* otherwise. A *Siegel modular form* is a holomorphic Siegel modular function.

If A is a p.p. abelian surface over $\mathbb{C}$ endowed with a basis ω of $\Omega^1(A)$ and f is a Siegel modular form of weight ρ, then one can evaluate f on the pair (A, ω): see [FC90, p. 141] or ğ4.1 for a geometric interpretation of this fact. To compute $f(A, \omega)$, choose $\tau \in \mathbb{H}_2$ and an isomorphism $\eta\colon A \to A(\tau)$. 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 $\omega(\tau)$ and ω. Then

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

One can directly check that $f(A, \omega)$ does not depend on the choice of τ and η.

2.2. **An explicit view on Siegel modular forms in genus 2.** In genus 2, the possible weights of Siegel modular forms can be listed explicitly: each representation ρ as above is isomorphic to $\det^k \otimes \mathrm{Sym}^n$ for some $k \in \mathbb{Z}$ and $n \geq 0$ [FH91, Prop. 15.47]. We will omit the tensor symbol. Explicitly, Sym^n is a representation on the vector space $V = \mathbb{C}_n[x]$ of polynomials of degree at most n, and for all $E \in \mathbb{C}_n[X]$ and $r = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{C})$, we have

$$\mathrm{Sym}^n(r)\, E = (bx + d)^n \ E\left(\frac{ax + c}{bx + d}\right).$$

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

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

The weight of a nonzero scalar-valued Siegel modular form f is of the form $\det^k$ for a unique $k \in \mathbb{Z}$, and in fact $k \geq 0$. 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. Thus, the graded vector space generated by Siegel modular forms is also naturally a graded $\mathbb{C}$-algebra, called the *graded algebra of Siegel modular forms.*[1]

[1]Under our definitions, not all elements of this graded algebra are modular forms: for instance, if f_1 and f_2 are nonzero modular forms of distinct weights, then $f_1 + f_2$ is not a modular form.

In order to represent a modular form explicitly, we use Fourier expansions. Let f be a Siegel modular form on $\mathbb{H}_2$ of weight $\det^k \mathrm{Sym}^n$, with underlying vector space $V = \mathbb{C}^{n+1}$. If we write

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

then f has a Fourier expansion of the form

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

The Fourier coefficients $c_f(n_1, n_2, n_3)$ belong to V, and can be nonzero only when $n_1 \geq 0, n_3 \geq 0$ and $n_2^2 \leq 4n_1n_3$ (note that n_2 can still be negative). To compute with q-expansions, we work in the power series ring $\mathbb{C}[q_2, q_2^{-1}][[q_1, q_3]]$ modulo an ideal of the form $\big(q_1^\nu, q_3^\nu\big)$ for some precision $\nu \geq 0$.

Now we can describe the structure of the graded $\mathbb{C}$-algebra of Siegel modular forms. While the full algebra is not finitely generated [vdGee08, Lem. 4], the subalgebra of scalar-valued modular forms is.

Theorem 2.1 ([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

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

The q-expansions in Theorem 2.1 are easily computed from expressions in terms of theta functions [Str14, ğ7.1], [Bol87, p. 493], and their Fourier coefficients are integers. We warn the reader that different normalizations appear in the literature: for instance, our χ_{10} is 4 times the modular form χ_{10} appearing in Igusa's papers, and our χ_{12} is 12 times Igusa's χ_{12}.

The equality $\chi_{10}(\tau) = 0$ occurs exactly when $A(\tau)$ is isomorphic to a product of elliptic curves (with the product polarization). When $\chi_{10}(\tau) \neq 0$, the p.p. abelian surface $A(\tau)$ is isomorphic to the Jacobian of a hyperelliptic curve. Following [Str14, ğ2.1] and our choice of normalizations, we define the *Igusa invariants* to be

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

The Igusa invariants j_1, j_2, j_3 are Siegel modular functions of weight 0, and together define a birational map $\mathbf{A}_2(\mathbb{C}) \to \mathbb{C}^3$.

Remark 2.2. Generically, giving $(j_1, j_2, j_3) \in \mathbb{C}^3$ uniquely specifies an isomorphism class of p.p. abelian surfaces over $\mathbb{C}$. This correspondence only holds on an open set: the Igusa invariants are not defined on products of elliptic curves, and do not represent a unique isomorphism class when $\psi_4 = 0$. To consider these points nonetheless, it is best to use other invariants: for instance the invariants

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

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

We conclude this paragraph by describing key examples of vector-valued forms. First, if f is a Siegel modular function of weight 0, then its derivative

$$Df := \frac{1}{2\pi i}\Big(\frac{\partial f}{\partial \tau_1}x^2 + \frac{\partial f}{\partial \tau_2}x + \frac{\partial f}{\partial \tau_3}\Big) : \mathbb{H}_2 \to \mathbb{C}_2[x]$$

is a Siegel modular function of weight Sym^2. 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, ğ25], or be checked directly by differentiating the relation $f(\gamma\tau) = f(\tau)$ with respect to τ.

The second key example is the modular form $\chi_{6,8}$ of weight $\det^8 \mathrm{Sym}^6$ [Ibu12; CFvdG17], with Fourier expansion

$$\begin{aligned} \chi_{6,8}(\tau) = \ & \big((4q_2^2 - 16q_2 + 24 - 16q_2^{-1} + 4q_2^{-2})q_1^2q_3 + \cdots\big)\, x^6 \\ & + \big((12q_2^2 - 24q_2 + 24q_2^{-1} - 12q_2^{-2})q_1^2q_3 + \cdots\big)\, x^5 \\ & + \big((-q_2 + 2 - q_2^{-1})q_1q_3 + \cdots\big)\, x^4 \\ & + \big((-2q_2 + 2q_2^{-1})q_1q_3 + \cdots\big)\, x^3 \\ & + \big((-q_2 + 2 - q_2^{-1})q_1q_3 + \cdots\big)\, x^2 \\ & + \big((12q_2^2 - 24q_2 + 24q_2^{-1} - 12q_2^{-2})q_1q_3^2 + \cdots\big)\, x \\ & + \big((4q_2^2 - 16q_2 + 24 - 16q_2^{-1} + 4q_2^{-2})q_1q_3^2 + \cdots\big)\, . \end{aligned}$$

The modular form $\chi_{6,8}$ is in a sense "universal", as it provides a link with equations of genus 2 curves: see Section 3.

2.3. **Hilbert modular forms.** In the context of Hilbert surfaces and abelian surfaces with real multiplication, we consistently use the following notation:

$\mathbb{H}_1$	the upper half plane in $\mathbb{C}$
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 $\mathbb{R}^2$
σ	the involution $(t_1, t_2) \mapsto (t_2, t_1)$ of $\mathbb{H}_1^2$.

Finally, the Hilbert modular group Γ_K is defined as follows:

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

Let A be a p.p. abelian surface. We denote by $\mathrm{End}^\dagger(A)$ the set of endomorphisms of A that are invariant under the Rosati involution (see [Mil86a, ğ17] for a definition). A *real multiplication structure* by $\mathbb{Z}_K$ on A is an embedding

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

We say that A has *real multiplication by* $\mathbb{Z}_K$ if it is endowed with a real multiplication structure. We sometimes use this terminology when ι is not explicitly given: we then make an implicit choice of a real multiplication embedding.

As in the Siegel case, the coarse moduli space of p.p. abelian surfaces over $\mathbb{C}$ with real multiplication by $\mathbb{Z}_K$ can be constructed complex-analytically. For each $t = (t_1, t_2) \in \mathbb{H}_1^2$, the complex torus

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

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

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

The embedding Σ induces a map $\Gamma_K \hookrightarrow \mathrm{SL}_2(\mathbb{R})^2$. The group Γ_K thus acts on $\mathbb{H}_1^2$ by the usual action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathbb{H}_1$ on each coordinate. The quotient $\mathbf{H}_2(\mathbb{C}) = \Gamma_K\backslash\mathbb{H}_1^2$ is the moduli space we are looking for: for each (A, ι) as above, 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 the action of Γ_K [BL04, ğ9.2]. The involution σ descends to $\mathbf{H}_2(\mathbb{C})$ and exchanges the real multiplication embedding with its conjugate. In fact, the quotient $\mathbf{H}_2(\mathbb{C})$ is the set of complex points of an algebraic variety $\mathbf{H}_2$ defined over $\mathbb{Q}$, called the *Hilbert surface* attached to K.

Let $k_1, k_2 \in \mathbb{Z}$. A *Hilbert modular function* of weight (k_1, k_2) is a meromorphic function $f\colon \mathbb{H}_1^2 \to \mathbb{C}$ such that for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_K$ and all $t \in \mathbb{H}_1^2$,

$$f(\gamma t) = \big(c\,t_1 + d\big)^{k_1} \big(\bar{c}\,t_2 + \bar{d}\big)^{k_2} f(t).$$

Note that 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. 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 form* is a holomorphic Hilbert modular function.

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. 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 a $\mathbb{Z}$-basis of $\mathbb{Z}_K$. To make a deterministic choice, we take $e_1 = 1$ and $e_2 = \frac{1}{2}(1 - \sqrt{\Delta})$ (resp. $e_2 = \sqrt{\Delta}$) when Δ is 1 mod 4 (resp. 0 mod 4). Set $R = \left(\begin{smallmatrix} e_1 & e_2 \\ \bar{e}_1 & \bar{e}_2 \end{smallmatrix}\right)$, and define

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

Then, for every $t \in \mathbb{H}_1^2$, the left multiplication by R^t on $\mathbb{C}^2$ induces an isomorphism $A_K(t) \to A\big(H(t)\big)$ [vdGee88, p. 209]. Indeed we have

$$\Lambda_K(t) = R^{-t}\mathbb{Z}^2 \oplus R^{-t}\big(R^t\,\mathrm{Diag}(t_1, t_2) R\big)\mathbb{Z}^2 = R^{-t}\Lambda(H(t)).$$

The Hilbert embedding is compatible with the actions of the modular groups, as follows. Let Γ_K act on $\mathbb{H}_2$ by means of the morphism $\Gamma_K \to \mathrm{Sp}_4(\mathbb{Z})$ given by

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

where we write $x^* = \mathrm{Diag}(x, \bar{x})$ for $x \in K$. The Hilbert embedding H is then equivariant for the actions of Γ_K on $\mathbb{H}_1^2$ and $\mathbb{H}_2$. The involution σ of $\mathbb{H}_1^2$ also corresponds via H to an element $M_\sigma \in \mathrm{Sp}_4(\mathbb{Z})$, namely

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

where $\delta = 1$ if $\Delta = 1 \bmod 4$, and $\delta = 0$ otherwise [LY11, Prop. 3.1].

Using this compatibility, we can directly check that pulling back a Siegel modular form via the Hilbert embedding yields Hilbert modular forms.

Proposition 2.3. *Let $k \in \mathbb{Z}$, $n \in \mathbb{Z}_{\geq 0}$, and let $f : \mathbb{H}_2 \to \mathbb{C}_n[x]$ be a Siegel modular form of weight $\rho = \det^k \mathrm{Sym}^n$. Define the functions $g_i : \mathbb{H}_1^2 \to \mathbb{C}$ for $0 \leq i \leq n$ by*

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

Then each g_i for $0 \leq i \leq n$ is a Hilbert modular form of weight $(k+i,\, k+n-i)$, and we have $g_i \circ \sigma = g_{n-i}$. In particular, if $n = 0$ and 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 parallel weight (k, k).

The image of the Hilbert embedding H in $\mathbf{A}_2(\mathbb{C})$ is called the *Humbert surface* attached to K. The pullback of χ_{10} by the Hilbert embedding is nonzero because a generic p.p. 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]. As a consequence, the Igusa invariants define a birational map from the Humbert surface to its image in $\mathbb{C}^3$. The squarefree polynomial cutting out this image is called the *Humbert equation*. This equation grows quickly in size with the discriminant Δ, but can be computed in small cases [Gru10].

2.5. **Isogenies between abelian surfaces.** Let A be a p.p. abelian surface over k. Denote its dual by $A^\vee$ and its principal polarization by $\pi : A \to A^\vee$. For every line bundle $\mathcal{L}$ on A, there is a morphism $\phi_{\mathcal{L}} : A \to A^\vee$ defined by $\phi_{\mathcal{L}}(x) = t_x^* \mathcal{L} \otimes \mathcal{L}^{-1}$, where t_x denotes translation by x on A. Let $\mathrm{NS}(A)$ denote the Néron–Severi group of A, consisting of algebraic equivalence classes of line bundles. A fundamental fact is that $\mathrm{NS}(A)$ is completely described in terms of endomorphisms of A over k.

Theorem 2.4 ([Mum70, Thm. 2 p. 188, Thm. 3 p. 231 and Application III p. 209])**.** *For every $\xi \in \mathrm{End}^\dagger(A)$, there exists a line bundle $\mathcal{L}_A(\xi)$ (possibly defined over an extension of k) such that $\phi_{\mathcal{L}_A(\xi)} = \pi \circ \xi$. The map $\xi \mapsto \mathcal{L}_A(\xi)$ induces an isomorphism of groups $(\mathrm{End}^\dagger(A), +) \simeq (\mathrm{NS}(A), \otimes)$. The morphism $\phi_{\mathcal{L}_A(\xi)}$ is a polarization on A if and only if $\xi \in \mathrm{End}^\dagger(A)$ is totally positive.*

In this notation, $\mathcal{L}_A(1)$ is the line bundle associated with the polarization π.

Now, let $\varphi : A \to A'$ be an isogeny between p.p. abelian surfaces. The line bundle $\varphi^*\mathcal{L}_{A'}(1)$ defines another polarization on A, hence is algebraically equivalent to $\mathcal{L}_A(\xi)$ for some totally positive $\xi \in \mathrm{End}^\dagger(A)$. Provided that A is simple, there are two possibilities [Mum70, p. 202]: either $\mathbb{Q}(\xi) = \mathbb{Q}$, in which case ξ is a positive integer; or $\mathbb{Q}(\xi)$ is a real quadratic field K. For simplicity, we assume in this paper that ξ is a prime, and A has real multiplication by the maximal order $\mathbb{Z}_K$ in the latter case. These assumptions often hold in practice, and our techniques would also apply with suitable modifications to more exotic cases. Then $\varphi : A \to A'$ is an isogeny of one of the two following types.

Definition 2.5. Let k be a field, and let A, A' be p.p. abelian surfaces over k.

(1) Let $\ell \in \mathbb{Z}_{\geq 0}$. An isogeny $\varphi\colon A \to A'$ is called an *ℓ-isogeny* if
$$\varphi^*\mathcal{L}_{A'}(1) = \mathcal{L}_A(\ell) \quad \text{in } \mathrm{NS}(A).$$

(2) Let K be a real quadratic field, and let $\beta \in \mathbb{Z}_K$ be a totally positive prime. Assume that A, A' have real multiplication by $\mathbb{Z}_K$, given by embeddings ι and ι'. An isogeny $\varphi\colon A \to A'$ is called a *β-isogeny* if
$$\varphi^*\mathcal{L}_{A'}(1) = \mathcal{L}_A(\,\iota(\beta)) \quad \text{in } \mathrm{NS}(A)$$
and the real multiplication embeddings ι and ι' are compatible under φ, meaning that for all $\alpha \in \mathbb{Z}_K$, we have $\varphi \circ \iota(\alpha) = \iota'(\alpha) \circ \varphi$.

An ℓ-isogeny $\varphi : A \to A'$ has degree ℓ^2; its kernel is a maximal isotropic subgroup in the ℓ-torsion subgroup $A[\ell]$ for the Weil pairing, and isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$ as an abstract group [Mum70, (1) p. 228 and Thm. 4 p. 233]. In the real multiplication case, β-isogenies are even smaller. The kernel of a β-isogeny $\varphi : A \to A'$ is maximal isotropic in $A[\beta]$, thus $\deg(\varphi) = N_{K/\mathbb{Q}}(\beta)$, and $\ker(\varphi)$ is cyclic when the ideal (β) lies above a split prime in $K/\mathbb{Q}$.

Both ℓ- and β-isogenies are easily described over $\mathbb{C}$. Up to isomorphism, every ℓ-isogeny is of the form
$$A(\tau) \to A(\tau/\ell)$$
(induced by the identity on $\mathbb{C}^2$) for some $\tau \in \mathbb{H}_2$ [BL09, Thm. 3.2]. Similarly, write $t/\beta \coloneqq \big(t_1/\beta, t_2/\overline{\beta}\big)$ for $t = (t_1, t_2) \in \mathbb{H}_1^2$. Then every β-isogeny is of the form
$$\big(A_K(t), \iota_K(t)\big) \to \big(A_K(t/\beta), \iota_K(t/\beta)\big)$$
for some choice of t [Mar20, Lem. 4.9].

2.6. **Modular equations.** Modular equations encode the presence of an isogeny between p.p. abelian surfaces, and generalize the classical modular polynomials that are widely used to compute isogenies between elliptic curves.

In the Siegel case, let $\Gamma^0(\ell) \subset \mathrm{Sp}_4(\mathbb{Z})$ be the subgroup consisting of matrices whose upper right 2×2 block is divisible by ℓ, and consider the map
$$\begin{aligned} \mathbf{\Phi}_{\ell,\mathbb{C}} : \Gamma^0(\ell)\backslash\mathbb{H}_2 &\to \mathbf{A}_2(\mathbb{C}) \times \mathbf{A}_2(\mathbb{C}) \\ \tau &\mapsto (\tau, \tau/\ell). \end{aligned}$$
The map $\mathbf{\Phi}_{\ell,\mathbb{C}}$ is the analytification of the map $\mathit{\Phi}_\ell$ described in the introduction, which exists at the level of algebraic stacks over $\mathbb{Q}$. The Siegel modular equations are equations for the image of $\mathbf{\Phi}_{\ell,\mathbb{C}}$ in $\mathbb{C}^3 \times \mathbb{C}^3$ via the Igusa invariants; we consider them as elements of $\mathbb{Q}[J_1, J_2, J_3, J_1', J_2', J_3']$. Any such set of equations

would work in the context of the isogeny algorithm. We can nonetheless define the Siegel modular equations uniquely, using 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 $j_1(\tau/\ell)$ [BL09, Lem. 4.2].

Definition 2.6. Let ℓ be a prime. The *Siegel modular equations of level* ℓ are the three following irreducible polynomials $\Psi_{\ell,1}, \Psi_{\ell,2}, \Psi_{\ell,3} \in \mathbb{Q}[J_1, J_2, J_3, J_1', J_2', J_3']$:

- $\Psi_{\ell,1} \in \mathbb{Q}[J_1, J_2, J_3, J_1']$ is the (non-monic) minimal polynomial of the function $j_1(\tau/\ell)$ over $\mathbb{C}\big(j_1(\tau), j_2(\tau), j_3(\tau)\big)$.
- For $i \in \{2, 3\}$, we have $\Psi_{\ell,i} \in \mathbb{Q}[J_1, J_2, J_3, J_1', J_i']$, with $\deg_{J_i'} \Psi_{\ell,i} = 1$, and an equality of meromorphic functions
$$\Psi_{\ell,i}\big(j_1(\tau), j_2(\tau), j_3(\tau), j_1(\tau/\ell), j_i(\tau/\ell)\big) = 0.$$

In the Hilbert case, we let $\Gamma^0(\beta) \subset \Gamma_K$ be the subgroup of matrices whose upper right entry b lies in $\beta(\mathbb{Z}_K^\vee)^{-1}$, and consider the map
$$\begin{aligned} \mathbf{\Phi}_{\beta,\mathbb{C}} : \Gamma^0(\beta)\backslash\mathbb{H}_1^2 &\to \mathbf{A}_2(\mathbb{C}) \times \mathbf{A}_2(\mathbb{C}) \\ t &\mapsto \big(H(t), H(t/\beta)\big). \end{aligned}$$

We call *Hilbert modular equations of level* β any set of three irreducible polynomials $\Psi_{\beta,k} \in \mathbb{Q}[J_1, J_2, J_3, J_1', J_2', J_3']$ for $1 \leq k \leq 3$ which, together with the Humbert equation in $\mathbb{Q}[J_1, J_2, J_3]$, are equations for the image of $\mathbf{\Phi}_{\beta,\mathbb{C}}$ in $\mathbb{C}^3 \times \mathbb{C}^3$ via the Igusa invariants. One can adapt Definition 2.6 to also define the Hilbert modular equations uniquely: see [MR20, Prop. 4.11] and [Kie22b, ğ3.2].

Since the Igusa invariants are symmetric by Proposition 2.3, the Hilbert modular equations encode β- and $\overline{\beta}$-isogenies simulaneously [MR20, Ex. 4.17]. It would be better to consider modular equations in terms non-symmetric invariants; however, we know of no explicit choice of such invariants in general.

From a practical point of view, modular equations in genus 2 are very large polynomials. This is especially true for the Siegel modular equations of level ℓ. For each $1 \leq k \leq 3$, the degree of $\Psi_{\ell,k}$ in each variable is $O(\ell^3)$, and the height of the coefficients is $O(\ell^3 \log \ell)$, for a total size of $O(\ell^{15} \log \ell)$ [Kie22b]. The situation is less desperate for Hilbert modular equations of level β: their total size is $O_K(\ell^4 \log \ell)$ where $\ell = N_{K/Q}(\beta)$. Modular equations have only been computed in full (using different invariants) up to $\ell = 7$ in the Siegel case, and up to $N(\beta) = 97$ in the Hilbert case for $K = \mathbb{Q}(\sqrt{2})$ [Mil16].

Luckily, directly evaluating modular equations and their derivatives at a given point is much cheaper than writing them down in full [Kie22c]: for example, over a prime finite field $\mathbb{F}_p$, the evaluation cost is only $\widetilde{O}(\ell^6 \log p)$ and $\widetilde{O}(\ell^2 \log p)$ binary operations for the Siegel and Hilbert modular equations, respectively. These evaluations are all we need to apply the isogeny algorithm.

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

In ğ3.1, we explain how a choice of genus 2 curve equation $\mathcal{C}_E\colon y^2 = E(x)$ over $\mathbb{C}$ naturally encodes a basis ω_E of differential forms on the Jacobian of $\mathcal{C}_E$. If f is a Siegel modular form, this gives rise to a map
$$\mathrm{Cov}(f)\colon E \mapsto f\big(\mathrm{Jac}(\mathcal{C}_E), \omega_E\big)$$
Following [CFvdG17], we show that $\mathrm{Cov}(f)$ is a polynomial in the coefficients of E in ğ3.2. We describe an algorithm to obtain this polynomial from the q-expansion

of f in ğ3.3, and apply it to the derivatives of the Igusa invariants to obtain the explicit Kodaira–Spencer isomorphism. This allows us to compute the deformation map and the tangent map of a generic ℓ-isogeny over $\mathbb{C}$ in ğ3.4. Finally, we adapt these methods to the Hilbert case in ğ3.5.

3.1. **Genus 2 curve equations.** Let $E \in \mathbb{C}_6[x]$ be a polynomial with six distinct roots in $\mathbb{P}^1(\mathbb{C})$ (hence $\deg(E) \in \{5, 6\}$). We associate to E the genus 2 curve

$$\mathcal{C}_E : y^2 = E(x).$$

We refer to E as a *genus* 2 *curve equation.* Choosing E not only specifies $\mathcal{C}_E$ up to isomorphism: indeed, $\mathcal{C}_E$ is also endowed with the basis of differential forms

$$\omega_E \coloneqq \Big(\frac{x\,dx}{y}, \frac{dx}{y}\Big).$$

Any choice of base point P on a genus 2 curve $\mathcal{C}$ gives an embedding $\eta_P \colon \mathcal{C} \hookrightarrow \mathrm{Jac}(\mathcal{C})$ sending Q to the divisor class $[Q - P]$. Then $\eta_P^* : \Omega^1(\mathrm{Jac}(\mathcal{C})) \to \Omega^1(\mathcal{C})$ is an isomorphism and is independent of P [Mil86b, Prop. 5.3]. Throughout, we identify $\Omega^1(\mathrm{Jac}(\mathcal{C}))$ and $\Omega^1(\mathcal{C})$ via this isomorphism, so that we may also view ω_E as a basis of differential forms on $\mathrm{Jac}(\mathcal{C}_E)$. The following lemma (a simple calculation: see [CFvdG17, ğ4]) justifies why our choice of ω_E is convenient.

Lemma 3.1. *Let E be a genus 2 curve equation, and let $r = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{C})$. Let $E' = \det^{-2} \mathrm{Sym}^6(r)\, E$, and let $\eta \colon \mathcal{C}_{E'} \to \mathcal{C}_E$ 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 $\eta^* \colon \Omega^1(\mathcal{C}_E) \to \Omega^1(\mathcal{C}_{E'})$ in the bases ω_E and $\omega_{E'}$ is r.

By Lemma 3.1 and Torelli's theorem, if A is a p.p. abelian surface over $\mathbb{C}$ that is not the product of two elliptic curves, and if ω be a basis of $\Omega^1(A)$, then there exists a unique genus 2 curve equation E such that the pairs $\big(\mathrm{Jac}(\mathcal{C}_E), \omega_E\big)$ and (A, ω) are isomorphic. We can thus make the following definition.

Definition 3.2. Let $\tau \in \mathbb{H}_2$, and assume that $\chi_{10}(\tau) \neq 0$. We define $E(\tau)$ to be the unique genus 2 curve equation such that

$$\big(\mathrm{Jac}(\mathcal{C}_{E(\tau)}), \omega_{E(\tau)}\big) \simeq \big(A(\tau), \omega(\tau)\big),$$

and call it the *standard curve equation* attached to τ. We define the meromorphic functions $a_i(\tau)$ for $0 \leq i \leq 6$ to be the coefficients of $E(\tau)$:

$$E(\tau) = \sum_{i=0}^{6} a_i(\tau) x^i.$$

Lemma 3.3. *The function $\tau \mapsto E(\tau)$ is a vector-valued Siegel modular function of weight* $\det^{-2} \mathrm{Sym}^6$ *which has no poles on the open set $\{\chi_{10} \neq 0\}$.*

Proof. The function $\tau \mapsto E(\tau)$ is well-defined on $\{\chi_{10} \neq 0\}$ and is holomorphic on this open set. To prove the transformation rule, fix $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{Sp}_4(\mathbb{Z})$ and $\tau \in \mathbb{H}_2$ such that $\chi_{10}(\tau) \neq 0$. Let $\eta : A(\tau) \to A(\gamma\tau)$ be the isomorphism $z \mapsto (c\tau + d)^{-t} z$. Then the matrix of $\eta^* : \Omega^1(A(\gamma\tau)) \to \Omega^1(A(\tau))$ in the bases $\omega(\gamma\tau)$ and $\omega(\tau)$ is $(c\tau + d)^{-1}$. On the other hand, writing $E' = \det^{-2} \mathrm{Sym}^6(c\tau + d) E(\tau)$, we have an isomorphism $\eta' : \mathrm{Jac}(\mathcal{C}_{E(\tau)}) \to \mathrm{Jac}(\mathcal{C}_{E'})$ such that the matrix of η'^* in the bases $\omega_{E'}$ and $\omega_{E(\tau)}$ is $(c\tau + d)^{-1}$ by Lemma 3.1. Thus E' satisfies the equality of Definition 3.2 at $\gamma\tau$, so $E(\gamma\tau) = E' = \det^{-2} \mathrm{Sym}^6(c\tau + d)E(\tau)$. □

3.2. **Covariants.** Let f be a Siegel modular form of weight ρ. The construction of ğ3.1 yields an algebraic map

$$\mathrm{Cov}(f) : E \mapsto f\big(\mathrm{Jac}(\mathcal{C}_E), \omega_E\big).$$

The map $\mathrm{Cov}(f)$ is then a *covariant* of E. These are classical objects, studied in the 19th century by Clebsch [Cle72]. A more modern reference for covariants is Mestre's article [Mes91]. In light of Lemma 3.1, we use the following terminology.

Definition 3.4. Let $\rho : \mathrm{GL}_2(\mathbb{C}) \to \mathrm{GL}(V)$ be a finite-dimensional holomorphic representation of $\mathrm{GL}_2(\mathbb{C})$ on a vector space V. A *fractional covariant* of weight ρ is a rational map $C \colon \mathbb{C}_6[x] \to V$ that satisfies the following transformation rule: for all $r \in \mathrm{GL}_2(\mathbb{C})$ and $E \in \mathbb{C}_6[x]$,

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

If $\dim V \geq 2$, then C is said to be *vector-valued*, and otherwise *scalar-valued*. A *covariant* is a fractional covariant that is also a polynomial map.

It is enough to consider covariants of weight $\det^k \mathrm{Sym}^n$, for $k \in \mathbb{Z}$ and $n \in \mathbb{Z}_{\geq 0}$. As in the case of Siegel modular forms, multiplication of polynomials allows us to consider (fractional) covariants as elements of a graded $\mathbb{C}$-algebra. 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.

A precise correspondence between Siegel modular forms and covariants is established in [CFvdG17] by studying how modular forms and covariants extend to the toroidal compactification of $\mathbf{A}_2$. We reformulate some of these results as follows.

Theorem 3.5 ([CFvdG17, ğ4 and ğ6])**.** *The map $f \mapsto \mathrm{Cov}(f)$ induces a weight-preserving bijection between the graded algebras of Siegel modular functions and fractional covariants. Its inverse bijection is*

$$C \mapsto \big(f : \tau \mapsto C(E(\tau))\big).$$

Further, if f is a Siegel modular form, then $\mathrm{Cov}(f)$ is a covariant. If f is a cusp form, then $\mathrm{Cov}(f/\chi_{10})$ is a also a covariant.

A second key input is the structure of the graded algebra of covariants which, unlike the graded algebra of Siegel modular forms, is finitely generated.

Theorem 3.6 ([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 manipulate a small number 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', and set

$$I_6' \coloneqq (I_2 I_4 - 3I_6)/2.$$

Other generators can be computed following [Mes91, ğ1] (in this reference, the integers m and n on page 315 should be the orders of f and g, not their degrees). Denote the generator of weight $\det^{15}$ by S, 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 $\det^{-2} \mathrm{Sym}^6$ 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 S 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 of known q-expansion. The works of Igusa already provide the answer in the scalar-valued case.

Theorem 3.7. *We have*

$$\begin{aligned} 4\ \mathrm{Cov}(\psi_4) &= I_4, & 4\ \mathrm{Cov}(\psi_6) &= I_6', \\ -2^{12}\ \mathrm{Cov}(\chi_{10}) &= I_{10}, & 2^{15}\ \mathrm{Cov}(\chi_{12}) &= I_2 I_{10}, \\ 2^{32}3^{-9}5^{-10}\ \mathrm{Cov}(\chi_{35}) &= I_{10}^2 S. \end{aligned}$$

Proof. By [Igu67, 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 $2^5 3^9 5^{10} S$.) To determine λ, we apply Thomae's formula [Mum84, Thm. IIIa.8.1] on the genus 2 curve[2]

$$\mathcal{C}_E : y^2 = E(x) = x \prod_{j=2}^{6} (x - j)$$

whose Weierstrass points are ordered in the obvious way. Let $\tau \in \mathbb{H}_2$ be a period matrix of $\mathrm{Jac}(\mathcal{C}_E)$, choose an isomorphism $\eta : \mathrm{Jac}(\mathcal{C}_E) \to A(\tau)$, and let σ be the matrix of η^* in the bases $\omega(\tau)$ and ω. By [Mum84, Thm. IIIa.8.1], up to a common factor $\mu \in \mathbb{C}^\times$ with $\mu^2 = \det(\sigma)$, the ten even theta constants at τ are

$$2\sqrt[4]{30},\ 3\sqrt{2},\ 2\sqrt[4]{18},\ 2\sqrt[4]{15},\ 2\sqrt{3},\ \sqrt[4]{60},\ \sqrt[4]{180},\ 2\sqrt[4]{6}\ \text{(twice)},\ \sqrt[4]{12}.$$

(The correct roots of unity can be computed by noticing that these values are positive real numbers [Tho70, pp. 216–217], or by analytic computations as in Remark 3.11 below.) Using the formulas from [Str14, ğ7.1] and [Bol87, p. 493], the values of the modular forms $\psi_4, \ldots, \chi_{35}$ at τ are

$$\begin{aligned} \psi_4(\tau) &= 345168 \det(\sigma)^4, & \psi_6(\tau) &= 78382080 \det(\sigma)^6, \\ \chi_{10}(\tau) &= -128595600 \det(\sigma)^{10}, & \chi_{12}(\tau) &= 129720811500 \det(\sigma)^{12}, \\ \chi_{35}(\tau) &= 5704668843331078393733600640000 \det(\sigma)^{35}. \end{aligned}$$

On the other hand, using the formulas in [Mes91], we obtain

$$\begin{aligned} I_4(E) &= 1380672, & I_6'(E) &= 313528320, \\ I_{10}(E) &= 526727577600, & I_2 I_{10}(E) &= 4250691551232000, \\ I_{10}^2 S(E) &= 398335475146953279910550645086617 6/3125. \end{aligned}$$

[2] The even more obvious choice $y^2 = \prod_{j=1}^{6} (x - j)$ has a vanishing S.

Thus $\lambda^4 = \lambda^6 = \lambda^{10} = \lambda^{12} = \lambda^{35} = 1$, hence $\lambda = 1$. □

Therefore, the Igusa invariants satisfy, in accordance with [Str14, §2.1]:

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

In order to obtain similar formulas for vector-valued modular forms, we first compute the q-expansion of the standard curve $\mathcal{C}(\tau)$ from Definition 3.2.

Proposition 3.8. *The following equality of Siegel modular functions holds:*

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

Proof. The modular form $\chi_{6,8}$ introduced in §2.2 is a cusp form. By Theorem 3.5, $\mathrm{Cov}(\chi_{6,8}/\chi_{10})$ is a covariant of weight $\det^{-2}\mathrm{Sym}^6$, and this space of covariants is 1-dimensional by Theorem 3.6. Therefore, the claimed equality holds up to a certain 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, Theorem 3.7 implies that $\lambda^4 = \lambda^6 = \lambda^{35} = 1$, hence $\lambda = 1$. □

Proposition 3.8 improves slightly on [CFvdG17, §6] (which follows the same proof strategy) in that we determine the correct scalar factor.

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

Algorithm 3.9.

(1) Compute a generating family for the vector space of polynomial covariants of weight ρ using Theorem 3.6, and extract a basis $\mathcal{B}$ using the embedding into $\mathbb{C}[a_0, \dots, a_6]$.
(2) Choose a precision ν and compute the q-expansion of f modulo (q_1^ν, q_3^ν).
(3) For every $B \in \mathcal{B}$, compute the q-expansion of the Siegel modular function $\tau \mapsto B\big(\mathcal{C}(\tau)\big)$ modulo (q_1^ν, q_3^ν) using Proposition 3.8.
(4) Solve a linear system to write $\mathrm{Cov}(f)$ as a linear combination of the elements of $\mathcal{B}$; if the matrix does not have full rank, go back to step 2 with a larger ν.

We now apply Algorithm 3.9 to the derivatives of the Igusa invariants, denoted by Dj_k for $1 \le k \le 3$ following the notation of §2.1.

Theorem 3.10. *We have*

$$\begin{aligned}\mathrm{Cov}(Dj_1) &= \frac{1}{8I_{10}}\big(153\, I_2^2 I_4 y_1 - 540\, I_2 I_6 y_1 + 540\, I_4^2 y_1 + 93150\, I_2 I_4 y_2 \\ &\qquad - 243000\, I_6 y_2 + 10935000\, I_4 y_3\big), \\ \mathrm{Cov}(Dj_2) &= \frac{1}{I_{10}}\big(90\, I_2^2 I_4 y_1 + 900\, I_2^2 y_1 + 40500\, I_2 I_4 y_2\big), \\ \mathrm{Cov}(Dj_3) &= \frac{1}{I_{10}^2}\big(225\, I_2 I_4^4 y_1 + 101250\, I_4^4 y_2\big).\end{aligned}$$

Proof. Let $1 \le k \le 3$. The function $\chi_{10}^2 j_k$ has no poles on $\mathbf{A}_2(\mathbb{C})$, so $f_k \coloneqq \chi_{10}^3\, Dj_k$ is a Siegel modular form. Its q-expansion can be computed from the q-expansion of j_k by formal differentiation. Since

$$\frac{1}{2\pi i}\frac{\partial}{\partial \tau_l} = q_l \frac{\partial}{\partial q_l}$$

for $1 \leq l \leq 3$, we check that f_k is a cusp form. By Theorem 3.5, $\mathrm{Cov}(f_k/\chi_{10})$ is a polynomial covariant of weight $\det^{20}\mathrm{Sym}^2$, and by Theorem 3.6, 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 3.9 succeeds with $\nu = 3$; the computations were done using Pari/GP [PARI19]. ☐

Remark 3.11. Theorems 3.7 and 3.10 can be checked numerically. Computing big period matrices of genus 2 curves (see for instance [MN19]) provides pairs $\big(\tau, \mathcal{C}(\tau)\big)$ with $\tau \in \mathbb{H}_2$. We can evaluate the Igusa invariants at a given τ to high precision using their expression in terms of theta functions [LT16]. Therefore, we can also evaluate their derivatives numerically with high precision and compute the associated covariant using floating-point linear algebra. We used the libraries `hcperiods` [Mol18] and `cmh` [ET14] for these computations.

Using Theorem 3.10 and linear algebra, one can obtain similar formulas for the derivatives of other invariants such as the invariants h_k defined in Remark 2.2.

3.4. **Deformation matrix and action on tangent spaces.** Let E and F be genus 2 curve equations over $\mathbb{C}$, let A and A' be the Jacobians of $\mathcal{C}_E$ and $\mathcal{C}_F$, and let $\varphi\colon A \to A'$ be an ℓ-isogeny. Taking the dual bases of ω_E and ω_F defines bases of the tangent spaces $T_0(A)$ and $T_0(A')$. If the pair (A, A') is sufficiently generic, then there exists only one ℓ-isogeny $\varphi : A \to A'$ up to sign, and we show how to compute, up to sign, the matrix of the tangent map $d\varphi\colon T_0(A) \to T_0(A')$ in the above bases from the data of the curve equations and modular equations of level ℓ. First, we introduce the following matrix notations.

Definition 3.12. For $\tau \in \mathbb{H}_2$, we define

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

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 for each $1 \leq l \leq 3$, the l-th column of $DJ(\tau)$ contains (up to dividing by $2\pi i$) the derivatives of the Igusa invariants at τ in the direction v_l.

The next two lemmas summarize the properties of the matrix-valued function DJ.

Lemma 3.13. *Let $\tau \in \mathbb{H}_2$ be a point where the Igusa invariants are defined, and let $r \in \mathrm{GL}_2(\mathbb{C})$. Then the columns of $DJ(\tau)\,\mathrm{Sym}^2(r)$ contain the derivatives of the three Igusa invariants at τ in the directions rv_lr^t for $1 \leq l \leq 3$, divided by $2\pi i$.*

Proof. This relation comes from the fact that the representation of $\mathrm{GL}_2(\mathbb{C})$ on the space of symmetric 2×2 matrices for which r acts by $v \mapsto rvr^t$ is isomorphic to Sym^2. Here we check it by a direct calculation. Write $r = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. We have

$$\begin{aligned} rv_1r^t &= a^2v_1 + 2acv_2 + c^2v_3, \\ rv_2r^t &= abv_1 + (ad+bc)v_2 + cdv_3, \\ rv_3r^t &= b^2v_1 + 2bdv_2 + d^2v_3. \end{aligned}$$

This matches the entries of the matrix $\mathrm{Sym}^2(r)$ defined in ğ2.2. ☐

Lemma 3.14. *Let ρ be the representation of $\mathrm{GL}_2(\mathbb{C})$ on $V = \mathrm{Mat}_{3\times 3}(\mathbb{C})$ given by*

$$\rho(r) : M \mapsto M \,\mathrm{Sym}^2(r^t), \quad \textit{for all } r \in \mathrm{GL}_2(\mathbb{C}).$$

Then DJ is a vector-valued Siegel modular function on V of weight ρ.

Proof. We know that for each $1 \le k \le 3$, the function Dj_k is a vector-valued modular function of weight Sym^2 as defined in ğ2.2. Hence each column of the matrix $DJ(\tau)^t$ is a vector-valued modular form for the representation

$$\rho : r \mapsto \mathrm{Diag}(2,1,2)\,\mathrm{Sym}^2(r)\,\mathrm{Diag}(2,1,2)^{-1} = \mathrm{Sym}^2(r^t)^t,$$

and the conclusion follows by transposing. □

We also denote by $\mathrm{Cov}(DJ)$ the associated "matrix-valued" fractional covariant. For a given curve equation E, Theorem 3.10 expresses the entries of the 3×3 matrix $\mathrm{Cov}(DJ)(E)$ in terms of the coefficients of E.

Definition 3.15. 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

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

They are 3×3 matrices with coefficients in $\mathbb{Q}[J_1, J_2, J_3, J_1', J_2', J_3']$.

With these notations in place, we can define what a generic isogeny is in the context of Theorem 1.1, and define its attached deformation matrix $\mathscr{D}(\varphi)$.

Definition 3.16. Let $\varphi : A \to A'$ 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 Igusa invariants (j_1', j_2', j_3') of A'. We say that (A, A') is *generic*, or that φ is generic, when the complex 3×3 matrices $D\Psi_{\ell,L}(j,j')$, $D\Psi_{\ell,R}(j,j')$, $\mathrm{Cov}(DJ)(E)$ and $\mathrm{Cov}(DJ)(F)$ are invertible. In this case, we define the *deformation matrix* $\mathscr{D}(\varphi)$ of φ as

$$\mathscr{D}(\varphi) \coloneqq -\,\mathrm{Cov}(DJ)(F)^{-1} \cdot D\Psi_{\ell,R}(j,j')^{-1} \cdot D\Psi_{\ell,L}(j,j') \cdot \mathrm{Cov}(DJ)(E).$$

The deformation matrix $\mathscr{D}(\varphi)$ has a geometric interpretation that we detail in Section 4: if x, x' are the points of $\mathcal{A}_2$ corresponding to A, A', then $\mathscr{D}(\varphi)$ is the matrix of the deformation map of φ in the bases of $T_x(\mathcal{A}_2)$ and $T_{x'}(\mathcal{A}_2)$ associated with ω_E and ω_F via the Kodaira–Spencer isomorphism.

Now we can relate the deformation matrix $\mathscr{D}(\varphi)$ to the tangent map $d\varphi$, also identified with its matrix in the specified bases of $T_0(A)$ and $T_0(A')$.

Proposition 3.17. *With the above notation, assume that (A, A') is generic. Then there exists only one ℓ-isogeny $\varphi : A \to A'$ up to sign, and we have*

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

Proof. Choose $\tau \in \mathbb{H}_2$ and isomorphisms η, η' giving a commutative diagram

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, "\eta"] & A' \arrow[d, "\eta'"] \\ A(\tau) \arrow[r, "z\mapsto z"] & A(\tau/\ell). \end{tikzcd}$$

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

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

We differentiate these equalities with respect to τ_i for $1 \leq i \leq 3$. This yields

$$\sum_{n=1}^{3} \frac{\partial \Psi_{\ell,k}}{\partial J_n}(j,j')\frac{\partial j_n}{\partial \tau_i}(\tau) + \frac{1}{\ell}\sum_{n=1}^{3} \frac{\partial \Psi_{\ell,k}}{\partial J'_n}(j,j')\frac{\partial j_n}{\partial \tau_i}(\tau/\ell) = 0$$

for all $1 \leq i, k \leq 3$, which corresponds to the coefficient (k,i) of the matrix relation

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

We rewrite this last relation as

$$-\ell\, D\Psi_{\ell,L}(j,j') \cdot \mathrm{Cov}(DJ)(E) \cdot \mathrm{Sym}^2(r^t) = D\Psi_{\ell,R}(j,j') \cdot \mathrm{Cov}(DJ)(F) \cdot \mathrm{Sym}^2(r'^t),$$

and the expression of $\mathrm{Sym}^2(d\varphi)$ follows.

This determines $d\varphi$ up to sign, so $\pm\varphi$ are the only ℓ-isogenies from A to A', as all isogenies in characteristic zero are separable. $\square$

3.5. **The Hilbert case.** We now adapt our methods to recover the tangent matrix of a generic isogeny in the Hilbert case, for any real multiplication field K. If the attached ring of Hilbert modular forms is known, several improvements to this general strategy can be made: see Section 7 for the case $K = \mathbb{Q}(\sqrt{5})$.

A crucial difference with the Siegel case is that we cannot directly compute the tangent matrix of a β-isogeny, where $\beta \in \mathbb{Z}_K$ is a totally positive prime, from an arbitrary choice of curve equations attached to A and A': the real multiplication embedding has to play a role. The convenient notion for us will be the following.

Definition 3.18. Let (A, ι) be a p.p. abelian surface with real multiplication by $\mathbb{Z}_K$. We say that a basis ω of $\Omega^1(A)$ is *Hilbert-normalized* if for every $\alpha \in \mathbb{Z}_K$, the matrix of $\iota(\alpha)^* : \Omega^1(A) \to \Omega^1(A)$ in the basis ω is $\mathrm{Diag}(\alpha, \overline{\alpha})$. We say that a genus 2 curve equation E such that $A = \mathrm{Jac}(\mathcal{C}_E)$ is *Hilbert-normalized* if ω_E is.

In other words, a basis ω of $\Omega^1(A)$ is Hilbert-normalized if and only if its dual basis consists of eigenvectors for the action of $\mathbb{Z}_K$ on $T_0(A)$. Hilbert-normalized bases are the right notion to consider in the context of evaluating a Hilbert modular form on a pair (A, ω), in analogy with covariants in the Siegel case: we refer to Section 7 for a detailed discussion.

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 that we are given Hilbert-normalized curve equations E and F. We use the notation $D\Psi_{\beta,L}$ and $D\Psi_{\beta,R}$ in the Hilbert case in analogy with Definition 3.15. We also write

$$T \coloneqq \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Lemma 3.19. *Let E be a genus 2 curve equation such that $\mathrm{Jac}(\mathcal{C}_E)$ has real multiplication by $\mathbb{Z}_K$. Choose an isomorphism $\eta : \mathrm{Jac}(\mathcal{C}_E) \to A_K(t)$ for some $t \in \mathbb{H}_1^2$, and let $r \in \mathrm{GL}_2(\mathbb{C})$ be the matrix of $\eta^* : \Omega^1(A_K(t)) \to \Omega^1(\mathrm{Jac}(\mathcal{C}_E))$ in the bases $\omega_K(t)$ and ω_E. Finally, let $\tau = H(t)$. Then we have*

$$\mathrm{Cov}(DJ)(E) = DJ(\tau)\, \mathrm{Sym}^2(R^t r^t).$$

In other words, by Lemma 3.13, the columns of $\mathrm{Cov}(DJ)(E)$ *contain the derivatives of the Igusa invariants at* τ *in the directions*

$$\frac{1}{\pi i} R^t r^t \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} rR, \quad \frac{1}{2\pi i} R^t r^t \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} rR \quad \text{and} \quad \frac{1}{\pi i} R^t r^t \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} rR.$$

Proof. Let $\zeta : A_K(t) \to A(\tau)$ be the isomorphism induced by left multiplication by R^t on $\mathbb{C}^2$. The matrix of ζ^* in the bases $\omega(\tau)$ and $\omega_K(t)$ is R, so the action of $(\zeta \circ \eta)^*$ on differential forms is given by the matrix rR. The conclusion follows from the definition of covariants and Lemma 3.14. $\square$

Proposition 3.20. *Let* $\varphi \colon A \to A'$ *be a* β*-isogeny and* E, F *be Hilbert-normalized curve equations as above. Then the tangent matrix* $d\varphi$ *is diagonal, and we have*

$$D\Psi_{\beta,L}(j,j') \cdot \mathrm{Cov}(DJ)(E) \cdot T \,\mathrm{Diag}(\beta, \overline{\beta}) = -D\Psi_{\beta,R}(j,j') \cdot \mathrm{Cov}(DJ)(F) \cdot T\,(d\varphi)^2.$$

Proof. Choose $t \in \mathbb{H}_1^2$ and isomorphisms η, η' giving a commutative diagram

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

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

$$\Psi_{\beta,k}\big(j_1(H(t)), j_2(H(t)), j_3(H(t)), j_1(H(t/\beta)), j_2(H(t/\beta)), j_3(H(t/\beta))\big) = 0$$

with respect to $t \in \mathbb{H}_1^2$. Using Lemma 3.19, the resulting equality can be written as

$$\begin{aligned} &D\Psi_{\beta,L}(j,j') \cdot \mathrm{Cov}(DJ)(E) \cdot \mathrm{Sym}^2(r^t) \cdot T \\ &\quad + D\Psi_{\beta,R}(j,j') \cdot \mathrm{Cov}(DJ)(F) \cdot \mathrm{Sym}^2(r'^t) \cdot T \cdot \mathrm{Diag}(1/\beta, 1/\overline{\beta}) = 0. \end{aligned}$$

We can reorganize this equality into the claimed result as r and r' are diagonal. $\square$

In view of Proposition 3.20, we say that the pair (A, A') is *generic* if the 3×2 matrices $D\Psi_{\beta,L}(j,j') \cdot \mathrm{Cov}(DJ)(E) \cdot T$ and $D\Psi_{\beta,R}(j,j') \cdot \mathrm{Cov}(DJ)(F) \cdot T$ have rank 2. In this case, we can indeed recover $(d\varphi)^2$ from the derivatives of modular equations. However, in contrast with the Siegel case, we obtain two possible candidates for $\pm d\varphi$ as we have to extract two uncorrelated square roots.

We now address the question of constructing a Hilbert-normalized curve equation from the input of the Igusa invariants (j_1, j_2, j_3) of a p.p. abelian surface (A, ι) with real multiplication by $\mathbb{Z}_K$. Note that we are missing some information, as the two pairs (A, ι) and $(A, \overline{\iota})$, where $\overline{\iota}$ denotes the real conjugate of ι, have the same Igusa invariants. The best we can hope for is thus to obtain a *potentially Hilbert-normalized* curve in the following sense.

Definition 3.21. We say that a genus 2 curve equation E is *potentially Hilbert-normalized* if there exists a real multiplication embedding $\iota : \mathbb{Z}_K \hookrightarrow \mathrm{End}^\dagger(\mathrm{Jac}(\mathcal{C}_E))$ such that $(\mathrm{Jac}(\mathcal{C}_E), \iota, \omega_E)$ is Hilbert-normalized.

Generically, we can use the derivatives of the Igusa invariants to characterize potentially Hilbert-normalized curve equations.

Proposition 3.22. *Let E be a genus 2 curve equation such that $\operatorname{Jac}(\mathcal{C}_E)$ has real multiplication by $\mathbb{Z}_K$. Let (j_1, j_2, j_3) denote its Igusa invariants, and assume that the matrix $\operatorname{Cov}(DJ)(E)$ is invertible. Then E is potentially Hilbert-normalized if and only if the two columns of the 3×2 matrix $\operatorname{Cov}(DJ)(E) \cdot T$ are tangent vectors to the Humbert surface at (j_1, j_2, j_3).*

Proof. Let t, τ, η and r be as in Lemma 3.19. Since $\operatorname{Cov}(DJ)(E)$ is invertible, the directions

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

are tangent to the Humbert surface at τ (i.e. lie inside the image of $\mathbb{H}_1^2$ by the Hilbert embedding) if and only if the two columns $\operatorname{Cov}(DJ)(E) \cdot T$ are tangent to the algebraic Humbert surface at (j_1, j_2, j_3). By the expression of the Hilbert embedding, this happens if and only if both $r\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)r^t$ and $r\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)r^t$ are diagonal. This is equivalent to saying that r is is either diagonal or anti-diagonal, in other words E is potentially Hilbert-normalized. $\square$

Assume that we are given the equation of the Humbert surface for K in terms of the Igusa invariants: this precomputation depends only on K. Given a tuple of Igusa invariants (j_1, j_2, j_3) on the Humbert surface such that the genericity condition of Proposition 3.22 is satisfied, the following algorithm reconstructs a potentially Hilbert-normalized curve equation; its correctness follows from Lemma 3.1.

Algorithm 3.23.

(1) Construct a curve equation E_0 such that $\operatorname{Jac}(\mathcal{C}_{E_0})$ has Igusa invariants (j_1, j_2, j_3) using Mestre's algorithm [Mes91].

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

$$\operatorname{Cov}(DJ)(E_0) \cdot \operatorname{Sym}^2(r^t) \cdot T$$

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

(3) Output $\det^{-2} \operatorname{Sym}^6(r)\, E_0$.

In step 2, 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 3.23 costs $O_K(1)$ field operations and $O(1)$ square roots.

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', or possibly a genus 2 curve equation. Constructing potentially Hilbert-normalized curve equations E, F then amounts to making a choice of real multiplication embedding for each abelian surface (namely, the embeddings for which E and F are Hilbert-normalized). If these embeddings are incompatible via φ, we obtain antidiagonal matrices when attempting to compute the tangent matrix with Proposition 3.20; in this case, we apply the change of variables $x \mapsto 1/x$ on E or F to make them compatible. After that, φ will be either a β- or a $\overline{\beta}$-isogeny depending on the choices of real multiplication embeddings. In total, we obtain four possible candidates for the tangent matrix up to sign.

4. Moduli spaces and the deformation map

In this section, we use the language of moduli stacks to give an algebraic interpretation of the results in Section 3 and to generalize them to isogenies between abelian schemes of any dimension over any base. We also give precise conditions guaranteeing genericity in the sense of Definition 3.16.

Another way to generalize the previous computations to arbitrary fields (say) would be to lift the isogeny to characteristic zero and invoke the complex-analytic computations there. The reader who is satisfied with this direct argument (and the genericity assumption) may directly skip to Section 5. However, we think that the moduli-theoretic approach provides more geometric insight.

In ğ4.1, we recall general facts on moduli stacks of p.p. abelian varieties. In ğ4.2, we formally define the deformation map attached to an isogeny and compare its incarnations at the levels of stacks and coarse spaces, thereby obtaining precise conditions for genericity. In ğ4.3, we introduce the Kodaira–Spencer isomorphism and use it to reinterpret results from Section 3, in particular the relation between the tangent and deformation matrices (Proposition 3.17). In ğ4.4, we recast the definition of covariants in the algebraic setting to show that the formulas to evaluate $\mathrm{Cov}(DJ)(E)$ hold over any base. Finally, we treat the Hilbert case in ğ4.5.

4.1. **Moduli stacks of abelian varieties.** We denote by $\mathcal{A}_g$ the moduli stack of p.p. abelian varieties of dimension g, and by $\mathcal{A}_{g,n}$ the moduli stack of p.p. abelian varieties of dimension g with a level n symplectic structure, defined over $\mathbb{Z}[1/n]$ [FC90]. Both $\mathcal{A}_g$ and $\mathcal{A}_{g,n}$ are separated Deligne–Mumford stacks, and $\mathcal{A}_{g,n}$ is smooth over $\mathbb{Z}[1/n]$ with $\phi(n)$ geometrically irreducible fibers.

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, generalizing the setting of ğ2.1. If $n \geq 3$, then $\mathcal{A}_{g,n}$ has trivial inertia, so $\mathcal{A}_{g,n}$ is isomorphic to its coarse space $\mathbf{A}_{g,n}$, and $\mathbf{A}_{g,n}$ is smooth over $\mathbb{Z}[1/n]$. If $n \leq 2$, then the generic inertia group on $\mathcal{A}_{g,n}$ is $\mu_2 = \{\pm 1\}$.

The moduli stack $\mathcal{A}_g(\ell)$ parametrizing ℓ-isogenies can be constructed as follows. Let $\Gamma^0(\ell) \subset \operatorname{Sp}_{2g}(\widehat{\mathbb{Z}})$ be the congruence subgroup encoding ℓ-isogenies, defined as in ğ2.6. Then $\mathcal{A}_g(\ell)$ is the quotient stack $[\mathcal{A}_{g,\ell}/\Gamma']$, where Γ' denotes the image of $\Gamma^0(\ell)$ in $\operatorname{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$. It is smooth over $\mathbb{Z}[1/\ell]$. The maps $\mathcal{A}_{g,\ell} \to \mathcal{A}_g(\ell)$ and $\mathcal{A}_g(\ell) \to \mathcal{A}_g$ are finite, étale, and representable [DR73, §IV.2 and §IV.3]. We can extend the coarse space $\mathbf{A}_g(\ell)$ to $\mathbb{Z}$ by normalization, as we did for $\mathbf{A}_{g,n}$.

One can also define Siegel modular forms algebraically on $\mathcal{A}_g$. 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 $(\wedge^g \mathsf{H})^{\otimes k}$. 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

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

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 ğ2.1. The canonical line bundle $\wedge^g \mathsf{H}$ is ample, so modular forms give local coordinates on $\mathbf{A}_g$.

In the case $g=2$, the structure of the coarse moduli space $\mathbf{A}_2$ has been worked out explicitly [Igu60; Igu79]. In particular, the modular forms $\psi_4, \psi_6, \chi_{10}, \chi_{12}$ from Theorem 2.1 are defined over $\mathbb{Z}$. The Jacobian locus $\mathbf{M}_2$ consisting of Jacobians of hyperelliptic curves is the open subscheme of $\mathbf{A}_2$ defined by $\chi_{10} \neq 0$. 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 define a birational map, and more precisely an isomorphism from $\mathbf{U} = \{\psi_4\chi_{10} \neq 0\} \subset \mathbf{M}_2$ to $\{j_3 \neq 0\} \subset \mathbb{A}^3$.

4.2. **The deformation map.** Consider the map

$$\begin{aligned} \mathit{\Phi}_\ell = (\mathit{\Phi}_{\ell,1}, \mathit{\Phi}_{\ell,2})\colon \mathcal{A}_g(\ell) &\to \mathcal{A}_g \times \mathcal{A}_g \\ A &\mapsto (A, A/K). \end{aligned}$$

It induces a map at the level of coarse moduli spaces, denoted by

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

We now study the relations between $\mathit{\Phi}_\ell$, $\mathbf{\Phi}_\ell$ and modular equations in detail in order to give precise conditions that guarantee the genericity of an isogeny in the sense of Definition 3.16 over any field k. An overview is as follows:

(1) At the level of stacks over $\mathbb{Z}[1/\ell]$, $\mathit{\Phi}_{\ell,1}$ and $\mathit{\Phi}_{\ell,2}$ are always finite étale, so there exists a deformation map $d\mathit{\Phi}_{\ell,2} \circ d\mathit{\Phi}_{\ell,1}^{-1}$ attached to every ℓ-isogeny φ.
(2) At points where $\mathit{\Phi}_{\ell,1}$ and $\mathit{\Phi}_{\ell,2}$ are *stabilizer-preserving*, we can compute this deformation map directly at the level of the coarse space $\mathbf{A}_g(\ell)$.
(3) If further the domain and codomain of φ have *generic automorphisms*, then we can compute the deformation map as $d\mathbf{\Phi}_{\ell,2} \circ d\mathbf{\Phi}_{\ell,1}^{-1}$.
(4) Under the assumptions of (3), the deformation map can be computed from a suitable normalization of the Siegel modular equations. In particular, if φ corresponds to a normal point in the image of $\mathbf{\Phi}_\ell$, then φ is generic.

Item (1) concretely means that the deformation map can always be computed after adding sufficient structure to rigidify the stacks involved, a costly procedure in general. The additional assumptions listed make the computations more and more tractable, at the expense of introducing new exceptions.

We begin with definitions, assuming all our stacks to be separated Deligne–Mumford stacks. We denote by $I_{\mathscr{X}}$ the inertia stack of a stack $\mathscr{X}$. If x is a point of $\mathscr{X}$, we denote by I_x the fiber of $I_{\mathscr{X}}$ at x, in other words the finite group of automorphisms of x. We say that a point x of $\mathcal{A}_g$ has *generic automorphisms* if $I_x = \mu_2$, or equivalently if the abelian variety A corresponding to x satisfies $\mathrm{Aut}(A) = \{\pm 1\}$. Points with generic automorphisms form an open substack of $\mathcal{A}_g$.

Let $f\colon \mathscr{X} \to \mathscr{Y}$ be a morphism of stacks. Then f is representable if and only if the map $I_{\mathscr{X}} \to \mathscr{X} \times_{\mathscr{Y}} I_{\mathscr{Y}}$ induced by f is a monomorphism [Stacks18, Tag 04YY]. We then say that f is *stabilizer-preserving* at x if the monomorphism on inertia $I_x \to I_{f(x)}$ induced by f is an isomorphism.

The following proposition accounts for step (1) of the overview, and characterizes points where the maps $\mathit{\Phi}_{\ell,i}$ are stabilizer-preserving.

Proposition 4.1. *Let ℓ be a prime.*

(1) The maps $\mathit{\Phi}_{\ell,1}$ and $\mathit{\Phi}_{\ell,2}$ are finite, étale and representable over $\mathbb{Z}[1/\ell]$.

(2) *Let k be a field of characteristic distinct from ℓ. 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 dual 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. Let x be a point of $\mathcal{A}_g(\ell)$ corresponding to a pair (A, K) in the moduli interpretation. The automorphisms of x in $\mathcal{A}_g(\ell)$ are exactly the automorphisms of A stabilizing K. In particular $\Phi_{\ell,1}$ is representable, and it is stabilizer-preserving at x if and only if all automorphisms of A stabilize K. The map $\Phi_{\ell,1}$ is finite étale by construction of $\mathcal{A}_g(\ell)$.

Any automorphism of (A, K), descends to $A' = A/K$, so $\Phi_{\ell,2}$ is representable as well. An automorphism of A' comes from an automorphism of (A, K) if and only if it stabilizes K', hence the condition for $\Phi_{\ell,2}$ to be stabilizer-preserving. We finally prove that $\Phi_{\ell,2}$ is finite étale. 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 $\mathbb{Z}[1/\ell]$. 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

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

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

The next proposition accounts for step (2) in the overview. From now on, if x is a point of $\mathcal{A}_g(\ell)$ or $\mathcal{A}_g$, we denote by $\mathbf{x}$ its reduction to the coarse moduli space.

Proposition 4.2. *Let $i = 1$ or 2. Let x be a k-point of $\mathcal{A}_g(\ell)$, and assume that $\Phi_{\ell,i}$ is stabilizer-preserving at x. Then $\mathbf{\Phi}_{\ell,i}$ is strongly étale at $\mathbf{x}$, in other words we have étale-locally around $\mathbf{x}$*

$$\mathcal{A}_g(\ell) = \mathbf{A}_g(\ell) \underset{\mathbf{A}_g}{\times} \mathcal{A}_g.$$

The point $\mathbf{x}$ is smooth in $\mathbf{A}_g(\ell)$ if and only if $\mathbf{\Phi}_{\ell,i}(\mathbf{x})$ is smooth in $\mathbf{A}_g$.

Proof. By Proposition 4.1, $\Phi_{\ell,i}$ is finite étale. The étaleness of $\mathbf{\Phi}_{\ell,i}$ at a stabilizer-preserving point then comes from Luna's fundamental lemma: see e.g. [Ryd13, Prop. 6.5 and Thm. 6.10]. Strong étaleness comes from the cartesian diagram in [Ryd13, Thm. 6.10], and directly implies the last statement in the proposition. ☐

Under the assumptions of Proposition 4.2, if $\Phi_{\ell,1}(x)$ 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 by the same reasoning as [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 $H^2(\operatorname{Spec} k, \operatorname{Aut}(x))$. But this obstruction vanishes since $\Phi_{\ell,1}(x)$ is represented by A/k, and the automorphism groups of x and $\Phi_{\ell,1}(x)$ are equal.

Remark 4.3. Concretely, Proposition 4.2 could be used in computations as follows. Let x be a k-point of $\mathcal{A}_g(\ell)$ where both $\Phi_{\ell,1}$ and $\Phi_{\ell,2}$ are stabilizer-preserving, and let $\mathbf{x}$ be its image in $\mathbf{A}_g(\ell)$. For $i \in \{1, 2\}$, let $\mathbf{y}_i = \mathbf{\Phi}_{\ell,i}(\mathbf{x})$, and let y_i be a lift of $\mathbf{y}_i$ to $\mathcal{A}_g$. Let $G = I_x$ be the common automorphism group of these objects. Finally, suppose that $\mathbf{x}$ is smooth in $\mathbf{A}_g(\ell)$ (equivalently, $\mathbf{y}_1$ or $\mathbf{y}_2$ is smooth in $\mathbf{A}_g$). By strong étaleness, the maps

$$d\mathbf{\Phi}_{\ell,i} : T_{\mathbf{x}}(\mathbf{A}_g(\ell)) \to T_{\mathbf{y}_i}(\mathbf{A}_g)$$

for $i \in \{1,2\}$ are isomorphisms.

Let B_1 be the completed local ring of $\mathcal{A}_g$ at y_1. By [DR73, §I.8.2.1], the completed local ring of $\mathbf{A}_g$ at $\mathbf{y}_1$ is B_1^G. Therefore, given $m = g(g+1)/2$ uniformizers $u_1, \ldots, u_m$ of $\mathcal{A}_g$ at y_1, we obtain $g(g+1)/2$ uniformizers of $\mathbf{A}_g$ at $\mathbf{y}_1$ as G-invariant polynomials in $u_1, \ldots, u_m$. Assume that such uniformizers of $\mathbf{A}_g$ have been computed at both $\mathbf{y}_1$ and $\mathbf{y}_2$. Then we can recover the deformation map at the level of stacks from the maps $d\mathbf{\Phi}_{\ell,i}$ up to an action of non-generic elements of G, i.e. up to choosing other 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-invariant uniformizers on $\mathbf{A}_g$. A key factor in this choice is the degree of the field extension we have to consider in order to rigidify the stack. For instance, if A is an abelian surface and k is a finite field, we can give A a full level 2 structure over an extension of degree at most 6; over a number field, this could take an extension of degree up to 720.

Under the additional assumption of generic automorphisms (3), computing the deformation map becomes considerably easier.

Proposition 4.4. *Let x be a k-point of $\mathcal{A}_g(\ell)$, and assume that both $\Phi_{\ell,1}(x)$ and $\Phi_{\ell,2}(x)$ have generic automorphisms. Then:*

(1) Both $\Phi_{\ell,1}$ and $\Phi_{\ell,2}$ are stabilizer-preserving at x.
(2) Both $\mathbf{\Phi}_{\ell,1}(\mathbf{x})$ and $\mathbf{\Phi}_{\ell,2}(\mathbf{x})$ are smooth points of $\mathbf{A}_g$, and the map $\mathcal{A}_g \to \mathbf{A}_g$ is étale at these points.
(3) The point $\mathbf{x}$ is smooth in $\mathbf{A}_g(\ell)$, and the map $\mathcal{A}_g(\ell) \to \mathbf{A}_g(\ell)$ is étale at $\mathbf{x}$.
(4) We have a commutative diagram

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

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

Proof. Item (1) follows from the definitions. For (2), let $y = \Phi_{\ell,1}(x)$. Since y has generic automorphisms, the map $[\mathcal{A}_g/\mu_2] \to \mathbf{A}_g$ is an isomorphism étale-locally around $\mathbf{y}$, by general facts on the étale-local structure of stacks [AV02, Lem. 2.2.3], [Ols06, Thm. 2.12]. The conclusion follows since $\mathcal{A}_g \to [\mathcal{A}_g/\mu_2]$ is étale. Item (3) similarly follows from the fact that $\mathcal{A}_g(\ell) \to \mathbf{A}_g(\ell)$ is an isomorphism étale-locally around $\mathbf{x}$. Finally, (2) and (3) imply (4). □

In the setting of Proposition 4.4, performing a change of uniformizers as sketched in Remark 4.3 is no longer necessary.

We finally proceed to step (4) in the overview, and investigate the relations between the coarse map $\mathbf{\Phi}_\ell$ and modular equations. The map $\mathbf{\Phi}_\ell$ is not injective, but reasoning as in [DR73, §VI.6] shows that it induces a birational isomorphism to its image. The open subscheme of $\mathbf{A}_g(\ell)$ where $\mathbf{\Phi}_\ell$ is an embedding is dense in every fiber of characteristic $p \nmid \ell$. We denote by Ψ_0 the schematic image of $\mathbf{\Phi}_\ell$, and denote by $p_1, p_2 \colon \Psi_0 \to \mathbf{A}_g$ the two projections. When $g = 2$, the modular equations $\Psi_{\ell,i}$ from ğ2.6 are equations for the image of $\Psi_0 \cap (\mathbf{U} \times \mathbf{U})$ in $\mathbb{A}^3 \times \mathbb{A}^3$ via the Igusa invariants j_1, j_2, j_3.

Proposition 4.5. *The scheme $\mathbf{A}_g(\ell)$ is the normalization of Ψ_0. Thus, if $\mathbf{x}_0$ is a point of Ψ_0, then $\mathbf{\Phi}_\ell \colon \mathbf{A}_g(\ell) \to \Psi_0$ induces a local isomorphism around $\mathbf{x}_0$ if and only if $\mathbf{x}_0$ is normal in Ψ_0.*

Proof. The map $\mathbf{A}_g(\ell) \to \Psi_0$ is separated and quasi-finite, and is birational by the above discussion. The scheme $\mathbf{A}_g(\ell)$ is normal because $\mathcal{A}_g(\ell)$ is normal, as seen from the description of its completed local rings [DR73, §I.8.2.1]. We deduce that $\mathbf{A}_g(\ell)$ is the normalization of Ψ_0 by Zariski's main theorem [Gro64, Cor. IV.8.12.11]. □

Combining Propositions 4.4 and 4.5, we obtain the following conclusion.

Corollary 4.6. *Let x be a k-point of $\mathcal{A}_g(\ell)$ corresponding to an ℓ-isogeny φ, and let $\mathbf{x}_0 = \mathbf{\Phi}_\ell(\mathbf{x})$. Assume that both $\Phi_{\ell,1}(x)$ and $\Phi_{\ell,2}(x)$ have generic automorphisms and that Ψ_0 is normal at $\mathbf{x}_0$. Then the deformation map $\mathscr{D}(\varphi)$ can be computed as $dp_2(\mathbf{x}_0) \circ dp_1(\mathbf{x}_0)^{-1}$. If further $\mathbf{x}_0 \in \mathbf{U} \times \mathbf{U}$, then $\mathscr{D}(\varphi)$ can be computed from the derivatives of the Siegel modular equations at the point $\mathbf{x}_0$ seen in $\mathbb{A}^3 \times \mathbb{A}^3$.*

Remark 4.7. We have the following characterization of non-normal points on Ψ_0, generalizing the remark of [Sch95, p. 248]. Let k be a field of characteristic $p > 0$, and let $\mathbf{x}_0$ be a k-point of Ψ_0. We remark that $\Psi_0 \otimes k$ is reduced (because the generic automorphisms over k are $\{\pm 1\}$ hence the generic points are smooth), so satisfies Serre's conditions S_1 and R_0 [Stacks18, Tag 031R]. Normality is equivalent to Serre's conditions S_2 and R_1 [Stacks18, Tag 031S]. Let ξ be a point specializing to x_0 and of codimension 1 (resp. 2). If ξ is of characteristic p, it is of codimension 0 (resp. 1) in $\Psi_0 \otimes k$, hence satisfies Serre's conditions. So $\mathbf{x}_0$ is normal in $\Psi_0 \otimes k$ if and only if every lift ξ of $\mathbf{x}_0$ of characteristic 0 is normal.

Now assume that $\Phi_{\ell,1}$ is stabilizer-preserving at $x \in \mathcal{A}_g(\ell)$, let $\mathbf{x}_0 = \mathbf{\Phi}_\ell(\mathbf{x})$ and assume that $\mathbf{\Phi}_{\ell,1}(\mathbf{x}) \in \mathbf{A}_g$ is smooth. Then by Propositions 4.2 and 4.5, $\mathbf{x}_0$ is smooth in Ψ_0 if and only if p_1 is étale at $\mathbf{x}_0$, if and only if $\mathbf{x}_0$ is normal in Ψ_0. Hence, by the above discussion, $\mathbf{x}_0$ is singular if and only if it is the reduction of a singular point in characteristic 0.

4.3. **The Kodaira–Spencer isomorphism.** Let $A \to S$ be a proper abelian scheme, and assume for simplicity that S is smooth over $\mathbb{Z}[1/2]$. Its associated *Kodaira–Spencer map* was first introduced in [KS58]; we refer to [FC90, §III.9] and [And17, §1.3] for more details. This map takes the form

$$\kappa \colon T_S \to \operatorname{Sym}^2 \operatorname{Lie}_S(A) = \operatorname{Hom}_{\mathrm{Sym}}\big(\operatorname{Lie}_S(A)^\vee, \operatorname{Lie}_S(A^\vee)\big),$$

where T_S denotes the tangent bundle on S. 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]. In particular, if x is a k-point of $\mathcal{A}_g$ represented by a p.p. abelian variety A/k, we have a canonical isomorphism $T_x(\mathcal{A}_g) \simeq \operatorname{Sym}^2 T_0(A)$.

As a consequence, if j is a modular invariant (i.e. a rational map $\mathcal{A}_g \to \mathbb{A}^1$), then via the Kodaira–Spencer isomorphism, its differential dj naturally becomes a Siegel modular function of weight Sym^2 in the sense of ğ4.1.

Over $\mathbb{C}$, the Kodaira–Spencer isomorphism can be described explicitly.

Proposition 4.8. *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* $\kappa\colon T_{\mathcal{A}_g} \to \mathrm{Sym}^2 \mathrm{Lie}_S \mathscr{X}_g$ *by* $\mathbb{H}_g \to \mathcal{A}_g^{\mathrm{an}}$ *is an isomorphism* $T_{\mathbb{H}_g} \simeq \mathrm{Sym}^2 V$ *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 all $1 \leq j,k \leq g$*, where* δ_{jk} *is the Kronecker symbol.*

Proof. The pullback of the Kodaira–Spencer map is an isomorphism by [And17, §2.2]. Its expression can be obtained 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 Riemann theta function θ as a section, and its deformation along τ is given by the heat equation [CvdG00, p. 9]:

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

From Proposition 4.8, we recover that the derivatives of 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 DJ defined in §3.4 are correctly normalized.

The Kodaira–Spencer isomorphism allows us to define deformation matrices of ℓ-isogenies in an algebraic context, and Proposition 3.17 remains valid.

Definition 4.9. Let k be a field of characteristic not 2 or ℓ, let $\varphi\colon A \to A'$ be an ℓ-isogeny representing a k-point of $\mathcal{A}_g(\ell)$, and fix bases of $T_0(A)$ and $T_0(A')$ 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 $T_x(\mathcal{A}_g)$ and $T_{x'}(\mathcal{A}_g)$ over k, where x, x' are the k-points of $\mathcal{A}_g$ corresponding to A and A'. 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 $\mathscr{D}(\varphi)$ when the above choice of bases is understood.

Proposition 4.10. *Let* φ *be as in Definition 4.9, and let* $d\varphi$ *and* $\mathscr{D}(\varphi)$ *be its tangent and deformation matrices in a choice of bases of* $T_0(A)$ *and* $T_0(A')$*. Then*

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

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

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

over $\mathbb{Z}[1/2\ell]$. All the line bundles involved 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 $\mathbb{C}^g$. In this case, the deformation map at φ is given by $\tau \to \tau/\ell$, so the result follows from the description of the Kodaira–Spencer map over $\mathbb{C}$ in Proposition 4.8. $\square$

4.4. **Modular forms and covariants.** In §4.3, we showed that the differentials of modular invariants are algebraic Siegel modular functions of weight Sym^2. In the case of the Igusa invariants when $g = 2$ over $\mathbb{C}$, Theorem 3.10 identifies these modular functions with explicit covariants of genus 2 curve equations. We now prove an algebraic analogue of this statement. As a consequence, all the computations of Section 3 remain valid over every field of characteristic not 2 or ℓ.

Note that covariants make sense over every ring R, replacing $\mathbb{C}$ by R in Definition 3.4. In order to relate them with algebraic Siegel modular forms, we consider 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 τ_g is $\pi_* \Omega^1 \mathscr{C}_g / \mathscr{M}_g$, and both vector bundles carry compatible actions of GL_g.

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 $U \subset X$ be the open locus of binary forms with nonzero discriminant. Then $U \to \mathscr{M}_2$ is naturally identified with the Hodge frame bundle on $\mathscr{M}_2$, by sending the binary form W to the curve $y^2 = W(x, 1)$ with the basis of differential forms $(x\,dx/y, dx/y)$ [CFvdG17, §4]. In other words, U is the moduli space of genus 2 hyperelliptic curves $\pi \colon C \to S$ endowed with a rigidification $\mathcal{O}_S^{\oplus 2} \simeq \pi_* \Omega^1_{C/S}$. Therefore, over $\mathbb{Z}[1/2]$, every Siegel modular form of weight ρ pulls back to a fractional covariant of weight ρ.

Write $\mathrm{Cov}(f)$ for the covariant attached to a Siegel modular function f, and denote by C the canonical covariant of weight $\det^{-2} \mathrm{Sym}^6$, i.e. the binary sextic form itself. We now show that Proposition 3.8 remains true in the algebraic setting.

Proposition 4.11. *The equality* $\mathrm{Cov}(\chi_{10})\, C = \mathrm{Cov}(\chi_{6,8})$ *holds over* $\mathbb{Z}[1/2]$.

Proof. The covariants $\mathrm{Cov}(\chi_{10})$ and C have integer coefficients, so they are defined over $\mathbb{Z}[1/2]$. Since the Hodge bundle is without torsion, it is enough to check equality over $\mathbb{C}$, which is the content of Proposition 3.8. □

As a consequence of Proposition 4.11, the identification of the derivatives of the Igusa invariants as explicit covariants (Theorem 3.10) still holds over $\mathbb{Z}[1/2]$.

Remark 4.12. In fact, one can show as in Theorem 3.5, by considering suitable compactifications, that a Siegel modular form pulls back to a polynomial covariant over every 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 2. This suggests another, entirely algebraic proof of Proposition 4.11. By dimension considerations, we have $\mathrm{Cov}(\chi_{10})\, C = \lambda\, \mathrm{Cov}(\chi_{6,8})$ for some $\lambda \in \mathbb{Q}^\times$. The covariant $\mathrm{Cov}(\chi_{10})\, C$ is defined over $\mathbb{Z}$ and primitive; therefore, if we can show that the Fourier coefficients of $\chi_{6,8}$ are globally coprime integers, we will have $\lambda = \pm 1$. An algebraic way to obtain $\lambda = 1$ could be to study degenerations from hyperelliptic curves to elliptic curves using [Liu93, Thm. 1.II].

Remark 4.13. Let k be a field of characteristic different from 2 and 3, and let A be a p.p. abelian surface over k such that $\mathrm{Aut}(A) = \{\pm 1\}$ and $j_3(A) \neq 0$. Let E be a genus 2 curve equation for A. Then as a consequence of Theorem 3.10 over $\mathbb{Z}[1/2]$, we obtain an explicit Kodaira–Spencer isomorphism at A: it is equivalent to give

(1) A deformation $\widetilde{E}$ of E over $k[\epsilon]/(\epsilon^2)$,
(2) The Igusa invariants of $\mathrm{Jac}(\mathcal{C}_{\widetilde{E}})$ in $k[\epsilon]/(\epsilon^2)$,
(3) A vector $\alpha w_1^2 + \beta w_1 w_2 + \gamma w_2^2 \in \mathrm{Sym}^2 \Omega^1(\mathcal{C}_E)$, where $(w_1, w_2) = \omega_E$ is the canonical basis of differential forms on $\mathcal{C}_E$.

Switching between representations can be done in $O(1)$ operations in k.

4.5. **Hilbert–Blumenthal stacks.** There exists a similar algebraic interpretation of the results of Section 3 for isogenies of Hilbert type in every dimension. This reformulation is based on *Hilbert–Blumenthal stacks*, which classify abelian schemes with a real multiplication structure [Rap78; Cha90]. We will simply outline the main results, as the proof methods are similar to the Siegel case.

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* $\mathbb{Z}_K$ if it is endowed with a morphism $\iota\colon \mathbb{Z}_K \to \operatorname{End}(A)$ such that $\operatorname{Lie}(A)$ is locally free of rank 1 as a $\mathbb{Z}_K \otimes \mathcal{O}_S$-module. The stack $\mathscr{H}_g$ of p.p. abelian schemes with real multiplication by $\mathbb{Z}_K$ 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 yields the *Hilbert embedding* $\mathscr{H}_g \to \mathcal{A}_g$, which is an $\operatorname{Aut}(K)$-gerbe over its image, the *Humbert stack*. The map $\mathscr{H}_g \to \mathcal{A}_g$ is finite [Gro64, EGA IV.15.5.9], [DR73, Lem 1.19], and we described its analytification in Section 2.

If β is a totally positive prime of $\mathbb{Z}_K$, we can also construct the stack $\mathscr{H}_g(\beta)$ of abelian schemes with real multiplication endowed with the kernel of a β-isogeny over $\mathbb{Z}[1/N_{K/\mathbb{Q}}(\beta)]$. We are interested in the map

$$\begin{aligned} \Phi_\beta = (\Phi_{\beta,1}, \Phi_{\beta,2})\colon \mathscr{H}_g(\beta) &\to \mathscr{H}_g \times \mathscr{H}_g \\ A &\mapsto (A, A/K). \end{aligned}$$

As above, we use bold characters to denote the associated coarse maps and spaces. We then have the following analogue of Proposition 4.4.

Proposition 4.14. *Let k be a field of characteristic not dividing $N_{K/\mathbb{Q}}(\beta)$. Let x be a k-point of $\mathscr{H}_g(\beta)$, and assume that both $\Phi_{\beta,1}(x)$ and $\Phi_{\beta,2}(x)$ have generic automorphisms. Then x maps to a smooth point of $\mathbf{H}_g(\beta)$, both $\Phi_{\beta,1}(x)$ and $\Phi_{\beta,2}(x)$ map to smooth points of $\mathbf{H}_g$, 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.

We deduce the following sufficient conditions to ensure the genericity of an isogeny as in ğ3.5. Let $\Psi_\beta \subset \mathbf{H}_g \times \mathbf{H}_g$ be the image of $\mathbf{\Phi}_\beta$, and let $\Psi_{\beta,\overline{\beta}} \subset \mathbf{A}_g \times \mathbf{A}_g$ denote the image of Ψ_β under the Hilbert embedding.

Corollary 4.15. *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 further that (x_1, x_2) does not lie in the image of $\Phi_{\overline{\beta}}$, in other words the corresponding abelian varieties are β-isogenous but not $\overline{\beta}$-isogenous, and that (x_1, x_2) maps to a normal point of Ψ_β. Let $\mathbf{y}$ the image of $\mathbf{x}$ by the forgetful morphism $\mathbf{H}_g \times \mathbf{H}_g \to \mathbf{A}_g \times \mathbf{A}_g$, and assume finally that $\mathbf{y}$ lies in $\mathbf{U} \times \mathbf{U}$. Then the β-isogeny corresponding to x is generic in the sense of ğ3.5.*

To obtain an algebraic interpretation of Proposition 3.20, we invoke the Hilbert analogue of the Kodaira–Spencer isomorphism [Rap78, Prop. 1.6 and Prop. 1.9]. If

$A \to S$ is an abelian scheme corresponding to a point x of $\mathscr{H}_g$, this isomorphism is

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

Thus, on Hilbert–Blumenthal stacks, the deformation map is represented by an element of $\mathbb{Z}_K \otimes \mathcal{O}_S$ rather than a matrix in $\mathcal{O}_S$. By [Rap78, § 1.5], the Kodaira–Spencer isomorphisms at A in the Hilbert and Siegel case fit in a commutative diagram with the forgetful maps:

$$\begin{tikzcd} T_x(\mathscr{H}_g) \arrow[r] \arrow[d] & T_x(\mathcal{A}_g) \arrow[d] \\ \mathrm{Hom}_{\mathbb{Z}_K \otimes \mathcal{O}_S}(\mathrm{Lie}(A)^\vee, \mathrm{Lie}(A^\vee)) \arrow[r] & \mathrm{Hom}_{\mathrm{Sym}}(\mathrm{Lie}_S(A)^\vee, \mathrm{Lie}_S(A^\vee)). \end{tikzcd}$$

In view of Proposition 4.8 and the analytic description of the forgetful map in ğ2.4 (easily generalized to every dimension g), the Kodaira–Spencer isomorphism in the Hilbert case takes the following form over $\mathbb{C}$.

Proposition 4.16. *The pullback of the Kodaira–Spencer isomorphism under the analytic cover $\mathbb{H}_1^g \to \mathscr{H}_g{}^{an}$ satisfies for every $1 \le j \le g$:*

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

This result gives an algebraic interpretation for the presence of the matrix T in Proposition 3.20: in genus 2, the part of $T_x(\mathcal{A}_2)$ coming from the Hilbert space is the span of $dz_1 \otimes dz_1$ and $dz_2 \otimes dz_2$. We deduce from Proposition 4.16 a relation between the tangent and deformation matrices in the Hilbert case.

Proposition 4.17. *Let $\varphi\colon A \to A'$ be a β-isogeny between abelian schemes with real multiplication over a base $S \to \mathbb{Z}[1/N_{K/\mathbb{Q}}(\beta)]$. Denote by $d\varphi$ and $\mathscr{D}(\varphi)$ its associated tangent and deformation maps, seen as elements of $\mathbb{Z}_K \otimes \mathcal{O}_S$-modules. Then under the Kodaira–Spencer isomorphism, we have $(d\varphi)^2 = \beta\mathscr{D}(\varphi)$.*

The last remaining step to prove that the computations of ğ3.5 remain valid over every field is to give an algebraic interpretation of the notion of (potentially) Hilbert-normalized bases and the method to construct them in Algorithm 3.23.

Let k be a field. Provided that $\operatorname{char} k \nmid \Delta$, and up to taking an étale extension of k, we may assume that k splits $\mathbb{Z}_K$, and fix a trivialization $\mathbb{Z}_K \otimes k \simeq k^g$. 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 a Hilbert-normalized basis of $T_0(A)$ is simply a basis of $\mathrm{Lie}(A)$ as a k-vector space on which $\mathbb{Z}_K$ acts diagonally. 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

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

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 $g = 2$, this ensures that the basis $(w_1, \dots, w_g)$ is potentially Hilbert-normalized.

5. Computing the isogeny from its tangent map

Assume that we are given the tangent map $d\varphi$ of an isogeny $\varphi\colon A \to A'$ between Jacobians of genus 2 curves defined over a field k, computed for instance from derivatives of modular equations as in Section 3. We now describe how to compute φ as a rational map by solving a differential system with Newton iterations.

This approach is not new: [Elk98] introduces a differential equation to compute isogenies in genus 1, and [BMS+08] solves it with Newton iterations. These ideas were extended to genus 2 in [CE15, ğ6.2] and [CMS+19, ğ5.2]. (Note that $d\varphi$ is obtained there in totally different ways, respectively using the kernel of φ as input and via a numerical approach whose complexity is hard to control.) We will indicate the relevant differences between these references and the differential system we set up. Mainly, Newton iterations allow us to reach a quasi-linear complexity in ℓ instead of (at best) quasi-quadratic using an iterative method.

5.1. **General strategy.** In general, the task of computing φ 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 of the coordinates (a_i).

One method to determine φ from $d\varphi$ is to work with formal groups. Let $x_1, \ldots, x_g$ be local uniformizers at 0_A. Knowing $d\varphi$ allows us to write a differential system satisfied by the functions $\varphi^* a'_j$, and we can attempt to solve it with a multivariate Newton algorithm. Upon success, 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 a multivariate rational reconstruction algorithm to obtain φ as a rational map, assuming that the power series precision is large enough compared to the degrees of the functions $\varphi^* a'_j$ in the variables (a_i). For the whole method to work, φ must be completely determined by its tangent map. This will be the case when $\operatorname{char} k$ is large with respect to the degree of φ. In practice, Newton iterations fail to reach sufficiently high power series precision if $\operatorname{char} k$ is too small, hence the bound $8\ell + 1$ in Theorem 1.1.

In genus 2 and away from characteristic 2, nice simplifications occur. Let E and F be genus 2 curve equations, let $A = \mathrm{Jac}(\mathcal{C}_E)$ and $A' = \mathrm{Jac}(\mathcal{C}_F)$, and assume that we are given the matrix of $d\varphi$ in the bases of $T_0(A)$ and $T_0(A')$ that are dual to ω_E and ω_F respectively (see ğ3.1). Then φ is determined by the composition

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

where P is any point on $\mathcal{C}_E$, the symbol $\mathcal{C}_F^{2,\mathrm{sym}}$ denotes the symmetric square of the curve $\mathcal{C}_F$, and m is the rational map given by

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

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 $\mathcal{C}_E$ around P and perform the Newton iterations and rational reconstruction over the univariate power series ring $k[[z]]$.

We explain how to solve the resulting differential system in ğ5.2. One difficulty is that the differential system we obtain is singular, so we need to use the geometry of the curves to find the first few terms in the series before switching to Newton iterations. In ğ5.3, 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 ğ5.1, and assume that the characteristic of k is not 2. Write the curve equations $\mathcal{C}_E$, $\mathcal{C}_F$ and the tangent matrix as

$$\mathcal{C}_E\colon v^2 = E(u), \quad \mathcal{C}_E\colon y^2 = F(x), \quad d\varphi = \begin{pmatrix} m_{1,1} & m_{1,2} \\ m_{2,1} & m_{2,2} \end{pmatrix}.$$

We assume that φ is separable, so $d\varphi$ is invertible. Let $P \in \mathcal{C}_E(k)$ be a base point on $\mathcal{C}_E$ (enlarging k if necessary). We denote by φ_P the associated map $\mathcal{C}_E \to \mathcal{C}_F^{2,\mathrm{sym}}$. Since $\varphi_P(P)$ is zero in $\mathrm{Jac}(\mathcal{C}_F)$, we have

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

for some $Q \in \mathcal{C}_F$, where i denotes the hyperelliptic involution. Below, we will choose P such a way that Q is not a Weierstrass point on $\mathcal{C}_F$. If z is a local uniformizer of $\mathcal{C}_E$ at P, and R is a finite extension of $k[[z]]$, we define a *local lift of φ_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

$$\begin{tikzcd} \operatorname{Spec} R \arrow[rr, "{(x_1,y_1),(x_2,y_2)}"] \arrow[d] & & \mathcal{C}_F \times \mathcal{C}_F \arrow[d] \\ \operatorname{Spec} k[[z]] \arrow[r] & \mathcal{C}_E \arrow[r, "\varphi_P"] & \mathcal{C}_F^{2,\mathrm{sym}}. \end{tikzcd}$$

Assume that Q is not a Weierstrass point on $\mathcal{C}_F$. Since the unordered pair $\{Q, i(Q)\}$ is defined over k, Q is defined over a quadratic extension k' of k. The map $\mathcal{C}_F \times \mathcal{C}_F \to \mathcal{C}_F^{2,\mathrm{sym}}$ is étale at $(Q, i(Q))$, and thus induces an isomorphism of completed local rings. Therefore, a local lift of φ_P exists over $k'[[z]]$.

The basis ω_F of $\Omega^1(\mathrm{Jac}(\mathcal{C}_F))$ corresponds to the pair of differential forms

$$\Big(\frac{x_1\,dx_1}{y_1} + \frac{x_2\,dx_2}{y_2}, \frac{dx_1}{y_1} + \frac{dx_2}{y_2}\Big)$$

on $\mathcal{C}_F^{2,\mathrm{sym}}$. Thus, every local lift (x_1, x_2, y_1, y_2) satisfies the differential system

$$(S) \qquad \begin{cases} \dfrac{x_1}{y_1}\dfrac{dx_1}{dz} + \dfrac{x_2}{y_2}\dfrac{dx_2}{dz} &=& (m_{1,1}u + m_{1,2})\dfrac{1}{v}\dfrac{du}{dz} \\ \dfrac{1}{y_1}\dfrac{dx_1}{dz} + \dfrac{1}{y_2}\dfrac{dx_2}{dz} &=& (m_{2,1}u + m_{2,2})\dfrac{1}{v}\dfrac{du}{dz} \\ \quad y_1^2 = F(x_1) \\ \quad y_2^2 = F(x_2), \end{cases}$$

where we consider the coordinates u, v on $\mathcal{C}$ as elements of $k[[z]]$, and d/dz denotes differentiation with respect to z. In the remainder of this section, we focus on solving this system up to a given precision, starting with the determination of Q.

Remark 5.1. In [CE15], a differential system is used to compute a local lift of φ_P at a base point other than P. In our context, it is unclear how one would initialize such a system, as it would require knowing the image of φ at a non-zero point of $\mathrm{Jac}(\mathcal{C}_E)$. In contrast, [CMS+19, ğ5] (specialized to the genus 2 case) also uses the zero point as a base point. However, they consider a birational map $\mathcal{C}_F^{2,\mathrm{sym}} \to \mathrm{Jac}(\mathcal{C}_F)$ coming from a degree 2 divisor $2P_0$ where P_0 is not a Weierstrass point (whereas we take the canonical divisor, in other words P_0 is a Weierstrass point). This removes the question of determining Q, but in exchange one has to work with Puiseux series.

Proposition 5.2. *The point Q is uniquely determined by the following property: if ω_P (resp. ω'_Q) is a nonzero differential form on $\mathcal{C}_E$ (resp. $\mathcal{C}_F$) vanishing at P (resp. Q), then there exists $\lambda \in k^\times$ such that*

$$\varphi^* \omega'_Q = \lambda\, \omega_P.$$

Proof. First, assume that Q is not a Weierstrass point, so that a local lift $\widetilde{\varphi}_P$ exists over $k'[[z]]$, where k' is a quadratic extension of k. The tangent space of $\mathcal{C}_F \times \mathcal{C}_F$ at $(Q, i(Q))$ decomposes as

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

where the last map is given by the hyperelliptic involution on the second term. Now consider the tangent vector $d\widetilde{\varphi}_P/dz$ at $z = 0$, and write it as $(v + w, w)$ for some $v, w \in T_Q(\mathcal{C}_F)$. Then $v \neq 0$: indeed the whole direction (w, w) is contracted to zero in the Jacobian, so if v were zero, every differential form on the Jacobian would be pulled back to zero via φ_P, contradicting the separability of φ. 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, as claimed.

If Q is a Weierstrass point, we can still find a local lift (x_1, y_1, x_2, y_2) of φ_P with coefficients in $k'[[\sqrt{z}]]$, where k'/k is a quadratic extension [Stacks18, Tag 09E8]. After a change of variables, we may assume that P and Q are not at infinity. Write $P = (u_0, v_0)$ and $Q = (x_0, 0)$. The equality in the proposition can be rewritten as

$$x_0 = \frac{m_{1,1}u_0 + m_{1,2}}{m_{2,1}u_0 + m_{2,2}}. \tag{5.1}$$

To show this, we use the system (S). Write

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

Then the relation $y^2 = F(x)$ in (S) 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 $dx/y = 2dy/F'(x)$ (where F' is the derivative of F), we have

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

Inspection of the $(\sqrt{z})^{-1}$ term gives $v_1 = -v_2$. Write $e = F'(x_0)$. Then the constant terms 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, so $m_{2,1}u_0 + m_{2,2}$ is nonzero, and quotienting the two lines gives the result. $\square$

Using Proposition 5.2, specifically (5.1), we choose a base point P such that Q is not Weierstrass. Then a local lift $\widetilde{\varphi}_P = (x_1, x_2, y_1, y_2)$ of φ_P exists over $k'[[z]]$, where k' is quadratic over k, and knowing $Q = (x_0, y_0)$ specifies its constant term.

The next step is to compute the power series x_1, x_2, y_1, y_2 up to $O(z^2)$. Write

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

Using the curve equations, we can compute y_1 and y_2 up to $O(z^2)$ in terms of v_1 and 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

$$v_1 + v_2 = \frac{y_0}{x_0}(m_{1,1}u_0 + m_{2,1})d_0 = y_0(m_{2,1}u_0 + m_{2,2})d_0. \tag{5.2}$$

Combining the two lines of (S), 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

$$v_1^2 + v_2^2 = y_0 r_1. \tag{5.3}$$

Equalities (5.2) and (5.3) 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.

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

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

where x_1^0 is the polynomial of degree at most $n-1$ that has been computed. The series δx_i and δy_i start at the term z^n. Linearizing (S), we obtain the following.

Proposition 5.3. *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 are 2×2 matrices with coefficients in $k'[[z]]$ and have explicit expressions in terms of x_1^0, x_2^0, y_1^0, y_2^0, u, v, E and F. 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 $e = F'(x_0)$, the constant term of N is

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

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] and is related to our choice of base point at 0_A, is that the matrix M is not invertible in $k'[[z]]$. We can nonetheless adapt the divide-and-conquer strategy from [BCG+17, ğ13.2].

Lemma 5.4. *The determinant* $\det M(z) = \dfrac{x_1^0 - x_2^0}{y_1^0 y_2^0}$ *has valuation one in* z*.*

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, and φ_P would pull back every differential form on $\mathcal{C}_F$ to zero, a contradiction. □

By Lemma 5.4, we can find $I \in \mathcal{M}_2\big(k'[[z]]\big)$ such that $IM = \begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix}$.

Lemma 5.5. *Let* $\kappa \geq 1$*, and assume that* $\operatorname{char} k > \kappa + 1$*. Let* $A = IN$*. Then the matrix* $A + \kappa$ *has an invertible constant term.*

Proof. By Lemma 5.4, the leading term of $\det(M)$ is λz for some nonzero $\lambda \in k'$. Using Proposition 5.3, we see that the constant term of $\det(A+\kappa)$ is $\lambda^2\kappa(\kappa+1)$. □

Proposition 5.6. *Let* $1 \leq \nu \leq 2n-1$*, and assume that* $\operatorname{char} k = 0$ *or* $\operatorname{char} k > \nu$*. 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

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

We show that θ can be computed from this kind of equation up to $O(z^\nu)$ using a divide-and-conquer strategy. If $\nu > 1$, write $\theta = \theta_1 + z^{\nu_1}\theta_2$ where $\nu_1 = \lfloor \nu/2 \rfloor$. Then

$$z\frac{d\theta_1}{dz} + (A+\kappa)\theta_1 = B + O(z^{\nu_1})$$

for some other series B. By induction, we recover θ_1 up to $O(z^{\nu_1})$. Then, we have

$$z\frac{d\theta_2}{dz} + (A+\kappa+\nu_1)\theta_2 = C + O(z^{\nu-\nu_1})$$

where C has an expression in terms of θ_1. This is enough to recover θ_2 up to $O(z^{\nu-\nu_1})$, so we can recover θ up to $O(z^\nu)$. 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 $2, \ldots, \nu - 1$ when computing the solution of (S) up to precision $O(z^\nu)$. By Lemma 5.5, the constant term of $A + \kappa$ is invertible. This concludes the induction. The complexity estimate follows from standard lemmas in computer algebra [BCG+17, Lem. 1.12]. □

As a consequence of Proposition 5.6, we can indeed solve (S) in quasi-linear time.

Proposition 5.7. *Let* $\nu \geq 1$*, and let* k *be a field such that* $\operatorname{char} k = 0$ *or* $\operatorname{char} k > \nu$*. Let* E *and* F *be genus* 2 *curve equations over* k *such that there exists an isogeny* $\varphi : \operatorname{Jac}(\mathcal{C}_E) \to \operatorname{Jac}(\mathcal{C}_F)$*, and assume that we are given the matrix* $d\varphi$ *in the bases of* $T_0(\operatorname{Jac}(\mathcal{C}_E))$ *and* $T_0(\operatorname{Jac}(\mathcal{C}_F))$ *associated with this choice of equations. Let* $P \in \mathcal{C}_E(k)$ *be a base point such that* $\varphi_P(P) = \{Q, i(Q)\}$ *for some non-Weierstrass point* Q *on* $\mathcal{C}_F$*. Let* k' *be the field of definition of* Q*, and let* z *be a uniformizer of* $\mathcal{C}_E$ *at* P*. Then one can compute the local lift* $\widetilde{\varphi}_P$ *as power series in* $k'[[z]]$ *up to precision* $O(z^\nu)$ *using* $\widetilde{O}(\nu)$ *operations in* k'*.*

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 a finite precision. For this, we need upper bounds on the degrees of these rational fractions.

The degrees of s, p, q, r as morphisms from $\mathcal{C}_E$ to $\mathbb{P}^1$ can be computed as intersection numbers of divisors on $\mathrm{Jac}(\mathcal{C}_F)$, namely $\varphi_P(\mathcal{C}_E)$ and the polar divisors of s, p, q and r. They are already known in the case of an ℓ-isogeny.

Proposition 5.8 ([CE15, ğ6.1])**.** *Let $\varphi\colon \mathrm{Jac}(\mathcal{C}_E) \to \mathrm{Jac}(\mathcal{C}_F)$ be an ℓ-isogeny, and let $P \in \mathcal{C}_E(k)$. 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 are 4ℓ, 4ℓ, 12ℓ, and 8ℓ respectively.*

Now assume that $\mathrm{Jac}(\mathcal{C}_E)$ and $\mathrm{Jac}(\mathcal{C}_F)$ have real multiplication by $\mathbb{Z}_K$ given by embeddings ι_E, ι_F, and that $\varphi\colon \big(\mathrm{Jac}(\mathcal{C}_E), \iota_E\big) \to \big(\mathrm{Jac}(\mathcal{C}_F), \iota_F\big)$ is a β-isogeny. Denote the theta divisors on $\mathrm{Jac}(\mathcal{C}_E)$ and $\mathrm{Jac}(\mathcal{C}_F)$ by Θ_E and Θ_F respectively, and denote by $\eta_P\colon \mathcal{C}_E \to \mathrm{Jac}(\mathcal{C}_E)$ the map $Q \mapsto [Q - P]$. Then $\eta_P(\mathcal{C}_E)$ is algebraically equivalent to Θ_E.

Lemma 5.9. *The polar divisors of s, p, q, r as rational functions on $\mathrm{Jac}(\mathcal{C}_F)$ are algebraically equivalent to $2\Theta_F$, $2\Theta_F$, $6\Theta_F$ and $4\Theta_F$ respectively.*

Proof. See [CE15, ğ6.1]. For instance, $s = x_1 + x_2$ has a pole of order 1 along each of the two divisors $\big\{(\infty_\pm, Q)\colon Q \in \mathcal{C}_F\big\}$, where $\infty_\pm$ are the two points at infinity on $\mathcal{C}_F$, assuming that we choose a degree 6 hyperelliptic model for $\mathcal{C}_F$. Each of these divisors is algebraically equivalent to Θ_F. The proof for p, q, and r is similar. □

By Theorem 2.4, if (A, ι) is a p.p. abelian surface with real multiplication by $\mathbb{Z}_K$, then we have an injective map $\mathbb{Z}_K \to \mathrm{NS}(A)$ given by $\alpha \mapsto \mathcal{L}_A(\iota(\alpha))$.

Lemma 5.10. *Let φ be a β-isogeny as above. Then the divisor $\varphi_P(\mathcal{C}_E)$ is algebraically equivalent to the divisor corresponding to the line bundle $\mathcal{L}_{\mathrm{Jac}(\mathcal{C}_F)}(\iota_F(\overline{\beta}))$.*

Proof. Since $\mathrm{Jac}(\mathcal{C}_F)$ is a smooth surface, the divisor $\varphi_P(\mathcal{C}_E)$ corresponds to a line bundle on $\mathrm{Jac}(\mathcal{C}_F)$. By Theorem 2.4, this line bundle is algebraically equivalent to $\mathcal{L}_{\mathrm{Jac}(\mathcal{C}_F)}(\iota_F(\alpha))$ for some $\alpha \in \mathrm{End}^\dagger(\mathrm{Jac}(\mathcal{C}_F))$. Consider $\varphi^*\big(\varphi_P(\mathcal{C}_E)\big)$ as a divisor on $\mathrm{Jac}(\mathcal{C}_E)$. By definition, we have

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

Therefore, up to algebraic equivalence,

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

By Definition 2.5, the pullback $\varphi^*\Theta_F$ corresponds to the line bundle $\mathcal{L}_{\mathrm{Jac}(\mathcal{C}_E)}(\iota_E(\beta))$ up to algebraic equivalence. Therefore, for every $\gamma \in \mathbb{Z}_K$,

$$\varphi^*\mathcal{L}_{\mathrm{Jac}(\mathcal{C}_F)}(\iota_F(\gamma)) = \mathcal{L}_{\mathrm{Jac}(\mathcal{C}_E)}(\iota_E(\gamma\beta)).$$

By Theorem 2.4 applied on $\mathrm{Jac}(\mathcal{C}_E)$, we have $\alpha\beta = N_{K/\mathbb{Q}}(\beta)$, so $\alpha = \overline{\beta}$. □

The next step is to compute the intersection number of Θ_F and the divisor corresponding to $\mathcal{L}_{\mathrm{Jac}(\mathcal{C}_F)}(\iota_F(\alpha))$ on $\mathrm{Jac}(\mathcal{C}_F)$, for every $\alpha \in \mathbb{Z}_K$.

Proposition 5.11. *Let (A, ι) be a p.p. abelian surface with real multiplication by $\mathbb{Z}_K$, and let Θ be its theta divisor. Then for all $\alpha \in \mathbb{Z}_K$, we have*

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

Proof. By [Kan19, Rem. 16], the quadratic form

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

on $\mathrm{NS}(A)$ corresponds via Theorem 2.4 to the quadratic form on $\mathbb{Z}_K$ given by

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

Thus, for every $\alpha = a + b\sqrt{\Delta} \in \mathbb{Z}_K$, we have

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

On the other hand, the Riemann–Roch theorem [Mil86a, Thm. 13.3] gives

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

Proposition 5.12. *Let φ be a β-isogeny as above, and let (s,p,q,r) be the rational representation of φ at P. Then the degrees of s, p, q, and r as morphisms from $\mathcal{C}_F$ to $\mathbb{P}^1$ are $2\,\mathrm{Tr}_{K/\mathbb{Q}}(\beta)$, $2\,\mathrm{Tr}_{K/\mathbb{Q}}(\beta)$, $6\,\mathrm{Tr}_{K/\mathbb{Q}}(\beta)$ and $4\,\mathrm{Tr}_{K/\mathbb{Q}}(\beta)$ respectively.*

Proof. The degrees of s,p,q and r can be computed as the intersection of the polar divisors from Lemma 5.9 and the divisor $\varphi_P(\mathcal{C}_E)$. By Lemma 5.10, the line bundle associated with $\varphi_P(\mathcal{C}_E)$, up to algebraic equivalence, is $\mathcal{L}_{\mathrm{Jac}(\mathcal{C}_F)}(\iota_F(\overline{\beta}))$. Its intersection number with Θ_F is nonnegative, hence by Proposition 5.11, we have

$$\big(\varphi_P(\mathcal{C}_E) \cdot \Theta_F\big) = \mathrm{Tr}_{K/\mathbb{Q}}(\overline{\beta}) = \mathrm{Tr}_{K/\mathbb{Q}}(\beta). \qquad \square$$

In order to reformulate Propositions 5.8 and 5.12 in terms of concrete degrees of rational fractions, we use the following lemma.

Lemma 5.13. *Let $s\colon \mathcal{C}_E \to \mathbb{P}^1$ be a morphism of degree d.*

1. *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 $d/2$.*
2. *In general, let X, Y be the rational fractions such that*

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

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

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

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

The degrees of these morphisms are bounded by $2d$ and $2d-6$ respectively. $\square$

We can thus summarize the rational reconstruction step as follows.

Proposition 5.14. *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 $\nu = 8\ell + 1$ in the Siegel case, and $\nu = 4\,\mathrm{Tr}_{K/\mathbb{Q}}(\beta) + 1$ in the Hilbert case. Then, given $\widetilde{\varphi}_P$ and $\widetilde{\varphi}_{i(P)}$ to 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 $\mathcal{C}_F$.

First, assume that P is a Weierstrass point of $\mathcal{C}_E$. Then s and p are invariant under the hyperelliptic involution. Therefore, we have to recover rational fractions in u of degree $d \leq 2\ell$ (resp. $d \leq \mathrm{Tr}_{K/\mathbb{Q}}(\beta)$). This can be done in quasi-linear time from their power series expansion to precision $O(u^{2d+1})$ [BCG+17, ğ7.1]. Since u has valuation 2 in z, it suffices to compute $\widetilde{\varphi}_P$ to precision $O(z^{4d+1})$.

Second, assume that P is not a Weierstrass point of $\mathcal{C}_E$. Then the series defining $s(u,-v)$ and $p(u,-v)$ are given by $\widetilde{\varphi}_{i(P)}$. It is enough to compute rational fractions of degree $d \leq 4\ell$ (resp. $d \leq 2\operatorname{Tr}_{K/\mathbb{Q}}(\beta)$) 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 $O(z^{2d+1})$. $\square$

6. Summary of the algorithm

Now let us summarize the isogeny algorithm and prove Theorem 1.1. We also state an analogous result in the case of β-isogenies (Theorem 6.3).

Let k be a field, and let A, A' be two p.p. abelian surfaces A, A' over k. We specify them by giving their Igusa invaraints j and j', as well as a genus 2 curve equation E such that $\operatorname{Jac}(\mathcal{C}_E) = A$ to resolve twisting ambiguities. In the Siegel case, we assume that A and A' are ℓ-isogenous over k for some prime ℓ. In the Hilbert case, we assume that A and A' have real multiplication by $\mathbb{Z}_K$ for some real quadratic field K and are β-isogenous for some totally positive prime $\beta \in \mathbb{Z}_K$. We then compute the isogeny $\varphi : A \to A'$ as follows.

Algorithm 6.1.

1. Construct a genus 2 curve equation F over k such that $A' = \operatorname{Jac}(\mathcal{C}_F)$ over $\overline{k}$ using Mestre's algorithm [Mes91]. In the Hilbert case, use Algorithm 3.23 to ensure that E and F are potentially Hilbert-normalized.
2. Compute at most 4 candidates for the tangent matrix $d\varphi$ of φ using Proposition 3.17 or 3.20. Run the rest of the algorithm on each candidate.
3. Make a change of basis to ensure that E, F and $d\varphi$ are defined over k (but not necessarily Hilbert-normalized.)
4. Choose a suitable base point P on $\mathcal{C}_E$ using Proposition 5.2 and compute the power series $\widetilde{\varphi}_P$ and $\widetilde{\varphi}_{i(P)}$ to precision $O(z^{8\ell+1})$ or $O(z^{4\operatorname{Tr}_{K/\mathbb{Q}}(\beta)+1})$ respectively, following Proposition 5.7.
5. Try to recover the rational representation of φ at P using Proposition 5.14. Output the result if rational fractions of the correct degrees are found.

Theorem 6.2. *Let ℓ be a prime, and let k be a field such that $\operatorname{char} k = 0$ or $\operatorname{char} k > 8\ell+1$. Let $\mathbf{U} \subset \mathbf{A}_2(k)$ be the open set consisting of p.p. abelian surfaces A such that $\operatorname{Aut}(A) \simeq \{\pm 1\}$ and $j_3(A) \neq 0$. Let $A, A' \in \mathbf{U}$, let j, j' be their Igusa invariants, and let E be a genus 2 curve equation over k such that $A = \operatorname{Jac}(\mathcal{C}_E)$. 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 Siegel modular equations $\Psi_{\ell,i}$ for $1 \leq i \leq 3$ is normal at (j, j'). Then, given j, j' and E as well as the derivatives of the Siegel modular equations of level ℓ at (j, j'), Algorithm 6.1 succeeds and returns*

1. *a genus 2 curve equation F over k such that $A' = \operatorname{Jac}(\mathcal{C}_F)$,*
2. *a point $P \in \mathcal{C}_E(k')$ where k'/k is a quadratic extension,*
3. *the rational representation $(s, p, q, r) \in k'(u, v)^4$ at the base point P of an ℓ-isogeny $\varphi\colon \operatorname{Jac}(\mathcal{C}_E) \to \operatorname{Jac}(\mathcal{C}_F)$ defined over k.*

This algorithm costs $\widetilde{O}(\ell)$ elementary operations and $O(1)$ square roots in k'.

Proof. Mestre's algorithm returns a curve equation F defined over k, and costs $O(1)$ operations in k and $O(1)$ square roots. Under our hypotheses, φ is generic by Proposition 4.4, so Proposition 3.17 allows us to recover $\operatorname{Sym}^2(d\varphi)$ using $O(1)$

operations in k, so we recover $d\varphi$ up to sign using $O(1)$ square roots and elementary operations. We can twist F in a unique way so that $d\varphi$ is defined over k. Then we must have $A = \mathrm{Jac}(\mathcal{C}_F)$ over k. Given our hypothesis on $\operatorname{char} k$, we can compute the local lifts and perform the rational reconstruction in $\widetilde{O}(\ell)$ operations in k'. □

In the Hilbert case, Theorem 6.2 has the following analogue.

Theorem 6.3. *Let K be a real quadratic field and $\beta \in \mathbb{Z}_K$ a totally positive prime. Let k be a field such that $\operatorname{char} k = 0$ or $\operatorname{char} k > 4\,\mathrm{Tr}_{K/\mathbb{Q}}(\beta) + 1$. Let $A, A' \in \mathbf{U}$ be p.p. abelian surfaces over k with real multiplication by $\mathbb{Z}_K$, let j, j' be their Igusa invariants, and let E be a curve equation over k such that $A = \mathrm{Jac}(\mathcal{C}_E)$. Assume that A and A' are β-isogenous but not $\overline{\beta}$-isogenous, and that the subvariety of $\mathbb{A}^3 \times \mathbb{A}^3$ cut out by the Hilbert modular equations of level β and the Humbert equation is normal at (j, j'). Then, given j, j', E, and the derivatives of the Hilbert modular equations of level β at (j, j'), Algorithm 6.1 succeeds and returns*

(1) a genus 2 curve equation F over k such that $A' = \mathrm{Jac}(\mathcal{C}_F)$,
(2) a point $P \in \mathcal{C}_E(k')$ where k'/k is a quadratic extension,
(3) at most 4 quadruples $(s, p, q, r) \in k'(u, v)^4$, one of which is the rational representation at the base point P of a β-isogeny $\varphi\colon \mathrm{Jac}(\mathcal{C}_E) \to \mathrm{Jac}(\mathcal{C}_F)$ defined over k.

This algorithm costs $\widetilde{O}\big(\mathrm{Tr}_{K/\mathbb{Q}}(\beta)\big) + O_K(1)$ elementary operations and $O(1)$ square roots in k'. The implied constants, except in $O_K(1)$, are independent of K.

Proof. By Corollary 4.15, the isogeny $\varphi : A \to A'$ is generic, and defined over k. Using Algorithm 3.23, we obtain potentially Hilbert-normalized curves equations E' and F' defined over a common quadratic extension of k; this costs $O_K(1)$ elementary operations and $O(1)$ square roots in k. We obtain four candidates for $\pm d\varphi$. For each candidate, we now make a change of variables to E and the (not necessarily Hilbert-normalized) curve equation F output by Mestre's algorithm, so that both $\mathcal{C}_E$ and $\mathcal{C}_F$ are defined over k, and twist $\mathcal{C}_F$ so that $d\varphi$ is also defined over k. We then have $A' = \mathrm{Jac}(\mathcal{C}_F)$, and we continue as in the Siegel case. For the correct value of $d\varphi$, rational reconstruction will succeed and output fractions of the correct degrees. □

Remark 6.4. In the Hilbert case, we expect that the algorithm returns only one answer for the rational representation of φ at P, as the incorrect candidates for $d\varphi$ should lead to garbage in Step (5) of the algorithm. Note that testing for correctness of the output might be more expensive than the isogeny algorithm itself.

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

In this final section, we present a variant of our isogeny algorithm in the case of p.p. abelian varieties with real multiplication by $\mathbb{Z}_K$ where $K = \mathbb{Q}(\sqrt{5})$. We work over $\mathbb{C}$, but the methods of ğ4 show that the computations remain valid over a general base. The Humbert surface attached to K is rational: its function field can be generated by only two elements called the Gundlach invariants. Having only two coordinates reduces the size of modular equations, allowing us to illustrate our algorithm with an example of a cyclic isogeny of degree 11 over a finite field.

7.1. **Hilbert modular forms for $K = \mathbb{Q}(\sqrt{5})$.** We keep the notation used to describe the Hilbert embedding in ğ2.4. Hilbert modular forms have Fourier expansions in terms of

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

We use this notation and the term *w-expansions* to avoid any confusion with q-expansions of Siegel modular forms. Apart from the constant term, a term in $w_1^a w_2^b$ can appear with a nonzero coefficient only 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 $\mathbb{C}[w_2, w_2^{-1}][[w_1]]$ modulo an ideal of the form (w_1^ν).

Theorem 7.1 ([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*

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

Following [MR20], we define the *Gundlach invariants* for $K = \mathbb{Q}(\sqrt{5})$ as

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

Recall that we denote by σ the involution $(t_1, t_2) \mapsto (t_2, t_1)$ of $\mathbf{H}_2(\mathbb{C})$. The Gundlach invariants define a birational map $\mathbf{H}_2(\mathbb{C})/\sigma \to \mathbb{C}^2$.

By Proposition 2.3, 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 the Igusa invariants.

Proposition 7.2 ([LY11, Prop. 4.5])**.** *In the case $K = \mathbb{Q}(\sqrt{5})$, we have*

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

Let $\beta \in \mathbb{Z}_K$ be a totally positive prime. We define the *Hilbert modular equations of level β* in terms of Gundlach invariants to be the irreducible polynomials $\Psi_{\beta,1}, \Psi_{\beta,2} \in \mathbb{Q}[G_1, G_2, G_1', G_2']$ with the following properties:

- $\Psi_{\beta,1} \in \mathbb{Q}[G_1, G_2, G_1']$ is the (non-monic) minimal polynomial of the meromorphic function $g_1(t/\beta)$ over the field $\mathbb{C}\bigl(g_1(t), g_2(t)\bigr)$,

- We have $\deg_{G_2'} \Psi_{\beta,2} = 1$ and an equality of meromorphic functions
$$g_2(t/\beta) = \Psi_{\beta,2}\big(g_1(t), g_2(t), g_1(t/\beta)\big).$$

These modular equations have been computed in full up to $N_{K/\mathbb{Q}}(\beta) = 41$ [Mil16].

7.2. **Hilbert-normalized curve equations.** We give another method to reconstruct such equations using the pullback of the modular form $\chi_{6,8}$ as a Hilbert modular form. We continue to use the notation of ğ2.4.

Proposition 7.3. *Define the functions $b_i(t)$ for $0 \leq i \leq 6$ on $\mathbb{H}_1^2$ by*
$$\det{}^8 \operatorname{Sym}^6(R)\, \chi_{6,8}\big(H(t)\big) = \sum_{i=0}^{6} b_i(t)\, x^i.$$
Then b_2 and b_4 are identically zero, and we have
$$\begin{aligned} b_3^2 &= 4F_{10}F_6^2, \\ b_1b_5 &= \frac{36}{25}F_{10}F_6^2 - \frac{4}{5}F_{10}^2G_2, \\ b_0b_6 &= \frac{-4}{25}F_{10}F_6^2 + \frac{1}{5}F_{10}^2G_2, \\ b_3\big(b_0^2b_5^3 + b_1^3b_6^2\big) &= 123F_{10}^3F_6 - \frac{32}{25}F_{10}^2F_6^2G_2^2 + \frac{288}{125}F_{10}F_6^4G_2 - \frac{3456}{3125}F_6^6. \end{aligned}$$

Proof. By Proposition 2.3, each coefficient b_i is a Hilbert modular form for K of weight $(8+i, 14-i)$, and σ exchanges b_i and b_{6-i}. From the q-expansion for $\chi_{6,8}$, we compute the w-expansions of the b_i's, and use linear algebra to identify symmetric combinations of the b_i's of even weight in terms of the generators G_2, F_6, F_{10}. We find that $b_2b_4 = 0$, and thus both b_2 and b_4 must be identically zero. □

By construction, for each $t \in \mathbb{H}_1^2$, the genus 2 curve equation $\sum_{i=0}^{6} b_i(t)x^i$ is potentially Hilbert-normalized. Thus, we obtain an alternative to Algorithm 3.23 for the construction of a potentially Hilbert-normalized curve equation given a tuple of Igusa invariants (j_1, j_2, j_3) that does not use the Humbert equation.

Algorithm 7.4.

(1) Compute the Gundlach invariants (g_1, g_2) mapping to (j_1, j_2, j_3) via H with Proposition 7.2, and choose values for G_2, F_6, F_{10} giving these invariants.
(2) Compute b_3^2, b_1b_5, etc. using Proposition 7.3.
(3) Recover values for the coefficients as follows. Choose a square root for b_3. Choose a arbitrary 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 of Algorithm 7.4 is defined over a quadratic extension of k.

7.3. **Computing the tangent matrix.** Using Gundlach invariants instead of Igusa invariants, we can compute the tangent matrix of a β-isogeny without any reference to the Hilbert embedding into the Siegel threefold. To formulate this result, we develop a notion of covariant attached to a Hilbert modular form that one can evaluate on a Hilbert-normalized curve equation, as announced in ğ3.5.

First, if (A, ι) is a p.p. abelian surface with real multiplication by $\mathbb{Z}_K$, if ω is a Hilbert-normalized basis of $\Omega^1(A)$, and if f is a Hilbert modular form of weight (k_1, k_2), then the quantity $f(A, \iota, \omega)$ makes sense. To define it, choose $t \in \mathbb{H}_1^2$ and an isomorphism $\eta : (A, \iota) \to (A_K(t), \iota_K(t))$. Then the matrix of η^* in the bases $\omega_K(t)$ and ω is a diagonal matrix $\mathrm{Diag}(r_1, r_2)$, and we set

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

This allows us to define the "covariant" $\mathrm{Cov}_K(f)$ as the rule which, to genus 2 curve equation E that is Hilbert-normalized for a real multiplication embedding ι on $\mathrm{Jac}(\mathcal{C}_E)$, associates $f(\mathrm{Jac}(\mathcal{C}_E), \iota, \omega_E)$.

Next, we note that if f is a Hilbert modular function of weight 0, its partial derivatives

$$\frac{1}{\pi i}\frac{\partial f}{\partial t_1} \quad \text{and} \quad \frac{1}{\pi i}\frac{\partial f}{\partial t_2},$$

where (t_1, t_2) are the coordinates on $\mathbb{H}_1^2$, are Hilbert modular functions of weight $(2, 0)$ and $(0, 2)$ respectively. This is easily seen by differentiating the equation $f(\gamma t) = f(t)$, for all $\gamma \in \Gamma_K$, with respect to t. As a consequence, the function

$$DG(t) := \Big(\frac{1}{\pi i}\frac{\partial g_k}{\partial t_l}\Big)_{1 \le k,l \le 2}$$

is a "matrix-valued" Hilbert modular function; its weight is the representation ρ of $\mathrm{GL}_1(\mathbb{C}) \times \mathrm{GL}_1(\mathbb{C})$ on $\mathrm{Mat}_{2\times 2}(\mathbb{C})$ given by

$$\rho(r_1, r_2) : M \mapsto M \,\mathrm{Diag}(r_1^2, r_2^2).$$

We will formulate the computation of the tangent matrix $d\varphi$ in terms of the associated covariant $\mathrm{Cov}_K(DG)$. This raises the question of how to evaluate this covariant on a given potentially Hilbert-normalized curve equation. Fortunately, we can directly relate this to our study of $\mathrm{Cov}(DJ)$ on the Siegel threefold. Let $M(g_1, g_2)$ be the 3×2 matrix obtained by differentiating Proposition 7.2, so that

$$DH^*J(t) := \Big(\frac{1}{\pi i}\frac{\partial H^* j_k}{\partial t_l}\Big)_{1 \le k \le 3,\, 1 \le l \le 2} = M(g_1(t), g_2(t)) \cdot DG(t).$$

Proposition 7.5. *Let E be a potentially Hilbert-normalized genus 2 curve equation, and let (g_1, g_2) be the Gundlach invariants of $\mathrm{Jac}(\mathcal{C}_E)$. Then we have*

$$\mathrm{Cov}(DJ)(E) \cdot T = M(g_1, g_2) \cdot \mathrm{Cov}_K(DG)(E).$$

Proof. Equip $\mathrm{Jac}(\mathcal{C}_E)$ with the real multiplication embedding for which E is Hilbert-normalized, and choose an isomorphism $\eta : \mathrm{Jac}(\mathcal{C}_E) \to A_K(t)$ for some $t \in \mathbb{H}_1^2$. Let $r \in \mathrm{GL}_2(\mathbb{C})$ be the matrix of η^* in the bases $\omega_K(t)$ and ω_E, and let $\tau = H(t)$. By the expression of the Hilbert embedding, the columns of $DH^*J(t)$ contain the derivatives of the Igusa invariants at τ in the directions

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

Therefore, we have

$$\begin{aligned} DH^*J(t) &= DJ(\tau) \cdot \mathrm{Sym}^2(R^t) \cdot T && \text{by Lemma 3.13} \\ &= \mathrm{Cov}(DJ)(E) \cdot \mathrm{Sym}^2(r^{-t}) \cdot T && \text{by Lemma 3.19} \\ &= \mathrm{Cov}(DJ)(E) \cdot T \cdot r^{-2} && \text{as } r \text{ is diagonal.} \end{aligned}$$

On the other hand,

$$DH^*J(t) = M(g_1, g_2) \cdot DG(t) = M(g_1, g_2) \cdot \mathrm{Cov}_K(DG)(E) \cdot r^{-2}. \qquad \square$$

Since the Igusa invariants define a birational map from $\mathbf{H}_2(\mathbb{C})/\sigma$ to the Humbert surface, the matrix $M(g_1, g_2)$ generically has rank 2. Thus we can combine Proposition 7.5 with the expression of DJ as a covariant to evaluate $\mathrm{Cov}_K(DG)(E)$.

Now we can formulate an alternative to Proposition 3.20 to compute the tangent matrix $d\varphi$. We define the 2×2 matrices

$$D\Psi_{\beta,L} \coloneqq \left(\frac{\partial \Psi_{\beta,n}}{\partial G_k}\right)_{1\leq n,k\leq 2} \quad \text{and} \quad D\Psi_{\beta,R} \coloneqq \left(\frac{\partial \Psi_{\beta,n}}{\partial G'_k}\right)_{1\leq n,k\leq 2}.$$

Proposition 7.6. *Let $\varphi : A \to A'$ be a β-isogeny between p.p. abelian surfaces with real multiplication by $\mathbb{Z}_K$. Let g (resp. g') denote the Gundlach invariants of A (resp. A'), and let E (resp. F) be a Hilbert-normalized curve equations for A (resp. A'). Assume that (A, A') is generic in the sense that the matrices $D\Psi_{\beta,L}(g, g')$, $D\Psi_{\beta,R}(g, g')$, $\mathrm{Cov}_K(DG)(E)$ and $\mathrm{Cov}_K(DG)(F)$ are invertible. Then the only β-isogenies from A to A' are $\pm\varphi$, and we have*

$$(d\varphi)^2 = -\,\mathrm{Diag}(\beta, \overline{\beta})\cdot \mathrm{Cov}(DG)(F)^{-1}\cdot D\Psi_{\beta,R}(g, g')^{-1}\cdot D\Psi_{\beta,L}(g, g')\cdot \mathrm{Cov}_K(DG)(E).$$

Proof. Left to the reader: one can follow the proof of Proposition 3.17. □

Using the formalism of ğ4, one can prove that (A, A') is generic if A and A' have only $\mathbb{Z}_K^\times$ as automorphisms, have $g_1 \neq 0$, and if the modular equations in terms of Gundlach invariants cut out a normal subvariety of $\mathbb{A}^2 \times \mathbb{A}^2$ at (g, g').

7.4. **An example of a 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, such that $\beta = 26213$.

Consider the Gundlach invariants

$$(g_1, g_2) = \big(23, 56260\big), \quad (g'_1, g'_2) = \big(8, 36073\big).$$

Algorithm 7.4 provides the Hilbert-normalized curve equations

$$\mathcal{C}_E \colon v^2 = E(u) = 13425u^6 + 34724u^5 + 102u^3 + 54150u + 11111,$$
$$\mathcal{C}_F \colon y^2 = F(x) = 47601x^6 + 35850x^5 + 40476x^3 + 24699x + 40502.$$

The derivatives of the Gundlach invariants at these points are given by

$$\mathrm{Cov}_K(DG)(E) = \begin{pmatrix} 43658 & 17394 \\ 16028 & 26656 \end{pmatrix}, \quad \mathrm{Cov}_K(DG)(F) = \begin{pmatrix} 15131 & 739 \\ 50692 & 49952 \end{pmatrix}.$$

Computing derivatives of the modular equations as in Proposition 3.20, we find that the isogeny is compatible with the real multiplication embeddings for which E and F 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:

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

where $\alpha^2+\alpha+2=0$. We see that for these choices of curve equations, the isogeny φ is only defined over a quadratic extension of k; we could take a quadratic twist of $\mathcal{C}_F$ to find a tangent matrix over k instead.

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

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

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. We solve the differential system up to precision $O(z^{29})$. It turns out that the correct tangent matrix is $d\varphi_{\overline{\beta},+}$ as the other series do not come from rational fractions of degrees prescribed by Proposition 5.12. We obtain in particular

$$s(u) = \frac{50255u^6 + 40618u^5 + 17196u^4 + 9527u^3 + 22804u^2 + 49419u + 11726}{u^6 + 40883u^5 + 22913u^4 + 41828u^3 + 18069u^2 + 14612u + 7238},$$

$$p(u) = \frac{35444u^6 + 9569u^5 + 52568u^4 + 3347u^3 + 9325u^2 + 32206u + 7231}{u^6 + 40883u^5 + 22913u^4 + 41828u^3 + 18069u^2 + 14612u + 7238}.$$

References

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

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

[BGL+16] S. Ballentine, A. Guillevic, E. Lorenzo García, C. Martindale, M. Massierer, B. Smith, and J. Top. "Isogenies for point counting on genus two hyperelliptic curves with maximal real multiplication". *Algebraic Geometry for Coding Theory and Cryptography*. Vol. 9. Los Angeles: Springer, 2016, pp. 63–94.

[BL04] C. Birkenhake and H. Lange. "Complex Abelian Varieties". 2nd ed. Springer, 2004.

[Bol87] O. Bolza. "Darstellung der rationalen ganzen Invarianten der Binärform sechsten Grades durch die Nullwerthe der zugehörigen θ-Functionen". *Math. Ann.* 30.4 (1887), pp. 478–495.

[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". *Math. Comp.* 77.263 (2008), pp. 1755–1778.

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

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

[Cha90] C.-L. Chai. "Arithmetic minimal compactification of the Hilbert–Blumenthal moduli spaces". *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". *Surveys in Differential Geometry*. Vol. 7. 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". *Math. Ann.* 369.3-4 (2017), pp. 1649–1669.

[CR15] R. Cosset and D. Robert. "Computing (ℓ, ℓ)-isogenies in polynomial time on Jacobians of genus 2 curves". *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". *Math. Comp.* 88.317 (2019), pp. 1303–1339.

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

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

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

[DJR+22] A. Dudeanu, D. Jetchev, D. Robert, and M. Vuille. "Cyclic isogenies for abelian varieties with real multiplication". *Moscow Math. J.* 22.4 (2022), pp. 613–655.

[Eid21] E. Eid. "Fast computation of hyperelliptic curve isogenies in odd characteristic". *ISSAC '21Proceedings of the 2021 International Symposium on Symbolic and Algebraic Computation*. ACM, 2021, pp. 131–138.

[Elk98] N. D. Elkies. "Elliptic and modular curves over finite fields and related computational issues". *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". *Math. Comp.* 78.267 (2009), pp. 1809–1824.

[ET14] A. Enge and E. Thomé. *CMH: Computation of genus 2 class polynomials*. 2014. URL: `https://gitlab.inria.fr/cmh/cmh/`.

[FC90] G. Faltings and C.-L. Chai. "Degeneration of Abelian Varieties". Springer, 1990.

[FH91] W. Fulton and J. Harris. "Representation Theory. A First Course". Springer-Verlag, 1991.

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

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

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

[Gru10] D. Gruenewald. "Computing Humbert surfaces and applications". *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". *Comment. Math. Univ. St. Pauli* 61.1 (2012), pp. 51–75.

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

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

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

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

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

[Kie22a] J. Kieffer. *Counting points on abelian surfaces over finite fields with Elkies's method*. 2022. URL: https://arxiv.org/abs/2203.02009.

[Kie22b] J. Kieffer. "Degree and height estimates for modular equations on PEL Shimura varieties". *J. London Math. Soc. (2)* 105.2 (2022), pp. 1314–1361.

[Kie22c] J. Kieffer. *Evaluating modular equations for abelian surfaces*. 2022. URL: https://arxiv.org/abs/2010.10094.

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

[LT16] H. Labrande and E. Thomé. "Computing theta functions in quasi-linear time in genus 2 and above". *Algorithmic Number Theory Symposium XII, LMS J. Comp. Math.* 19 (2016), pp. 163–177.

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

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

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

[LR22] D. Lubicz and D. Robert. "Fast change of level and applications to isogenies". *Res. Number Theory* 9.1 (2022), p. 7.

[Mar20] C. Martindale. "Hilbert modular polynomials". *J. Number Theory* 213 (2020), pp. 464–498.

[Mes91] J.-F. Mestre. "Construction de courbes de genre 2 à partir de leurs modules". *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". *LMS J. Comp. Math.* 18 (2015), pp. 603–632.

[Mil16] E. Milio. *Database of modular polynomials of Hilbert and Siegel*. 2016. URL: https://members.loria.fr/EMilio/modular-polynomials.

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

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

[Mil86b] J. S. Milne. "Jacobian varieties". *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". *Math. Comp.* 88.316 (2019), pp. 847–888.

[Mum70] D. Mumford. "Abelian Varieties". Oxford University Press, 1970.

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

[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.

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

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

[PARI19] The PARI group. "Pari/GP version 2.11.0". 2019.

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

[Ryd13] D. Rydh. "Existence and properties of geometric quotients". *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". *Math. Comp.* 44.170 (1985), pp. 483–494.

[Sch95] R. Schoof. "Counting points on elliptic curves over finite fields". *J. Théor. Nombres Bordeaux* 7.1 (1995), pp. 219–254.

[Stacks18] The Stacks project authors. "The Stacks Project". 2018.

[Str14] M. Streng. "Computing Igusa class polynomials". *Math. Comp.* 83 (2014), pp. 275–309.

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

[Tho70] J. Thomae. "Beitrag zur Bestimmung von $\vartheta(0, 0, \dots 0)$ durch die Klassenmoduln algebraischer Functionen". *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". *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". *Math. Comp.* 69.232 (2000), pp. 1685–1697.

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

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