Degree and height estimates for modular equations on PEL Shimura varieties

Jean Kieffer

DEGREE AND HEIGHT ESTIMATES FOR MODULAR EQUATIONS ON PEL SHIMURA VARIETIES

JEAN KIEFFER

Abstract. We define modular equations in the setting of PEL Shimura varieties as equations describing Hecke correspondences, and prove upper bounds on their degrees and heights. This extends known results about elliptic modular polynomials, and implies complexity bounds for number-theoretic algorithms using these modular equations. In particular, we obtain tight degree bounds for modular equations of Siegel and Hilbert type for abelian surfaces.

1. Introduction

Modular equations encode the presence of isogenies between polarized abelian varieties. An example is given by the elliptic modular polynomial Φ_ℓ, where ℓ is a prime: this bivariate polynomial vanishes on the j-invariants of ℓ-isogenous elliptic curves [9, §11.C], and can be used to detect and compute such isogenies [11]. Elliptic modular polynomials are used for instance in the SEA algorithm to count points on elliptic curves over finite fields [32], and in multi-modular methods to compute class polynomials of imaginary quadratic fields [34]; being able to compute isogenies also has applications in cryptography. Analogues of Φ_ℓ for principally polarized abelian surfaces, called Siegel and Hilbert modular equationss in dimension 2, have recently been defined and computed [24, 25, 21], and are of similar interest.

In the first part of this paper, we define modular equations in the general setting of PEL Shimura varieties of finite level; these varieties are moduli spaces for abelian varieties with polarization, endomorphisms, and level structure, hence the name. Choose connected components $\mathcal{S}$ and $\mathcal{T}$ of such a Shimura variety of dimension $n \geq 1$; they have a canonical model over a certain number field L. Choose coordinates on $\mathcal{S}$ and $\mathcal{T}$ that are defined over L. Let H_δ be an absolutely irreducible Hecke correspondence defined by an adelic element δ of the underlying reductive group, and let $d(\delta)$ be the degree of H_δ. In the modular interpretation, H_δ parametrizes isogenies of a certain degree $l(\delta)$ between abelian varieties with PEL structure. Then the *modular equations of level* δ are a family of $n+1$ univariate polynomials $(\Psi_{\delta,m})_{1\leq m\leq n+1}$ with coefficients in the function field $L(\mathcal{S})$ of $\mathcal{S}$, of degree at most $d(\delta)$, describing H_δ on $\mathcal{S}\times\mathcal{T}$. This definition includes all the examples of modular polynomials cited above, and provides a unified context to study them.

For each $1 \leq m \leq n+1$, the coefficients of $\Psi_{\delta,m}$ can be seen as multivariate rational fractions with coefficients in L. From an algorithmic point of view, two quantities are of interest: first, the total degree of these fractions; and second, their height, which measures the size of their coefficients. For instance, if $\mathcal{F} \in \mathbb{Q}(Y_1,\dots,Y_n)$, write $\mathcal{F} = P/Q$ where $P, Q \in \mathbb{Z}[Y_1,\dots,Y_n]$ are coprime; then the

height $h(\mathcal{F})$ of $\mathcal{F}$ is defined as the maximum of $\log|c|$, where c runs through the nonzero coefficients of P and Q.

Our main result gives upper bounds on the degrees and heights of the coefficients of modular equations on a given PEL Shimura variety in terms of $d(\delta)$ and $l(\delta)$. This provides complexity bounds for algorithms involving these modular equations.

Theorem 1.1. *Let $\mathcal{S}$ and $\mathcal{T}$ be connected components of a simple PEL Shimura variety of type (A) or (C) of finite level and dimension $n \geq 1$, with underlying reductive group G. Let L be the field of definition of $\mathcal{S}$ and $\mathcal{T}$, and choose coordinates on $\mathcal{S}$ and $\mathcal{T}$ that are defined over L. Then there exist constants C_1 and C_2 such that the following holds. Let H_δ be an absolutely irreducible Hecke correspondence on $\mathcal{S}\times\mathcal{T}$ defined by an adelic element δ of G; let $d(\delta)$ be the degree of H_δ, and let $l(\delta)$ be the degree of the isogenies described by H_δ in the modular interpretation. Let $\mathcal{F}$ be a multivariate rational fraction over L occuring as a coefficient of one of the modular equations $\Psi_{\delta,m}$ for $1 \leq m \leq n+1$. Then*

1. *The total degree of $\mathcal{F}$ is bounded above by $C_1\, d(\delta)$.*
2. *The height of $\mathcal{F}$ is bounded above by $C_2\, d(\delta)\max\{1, \log l(\delta)\}$.*

This result generalizes known bounds on the size of the elliptic modular polynomial Φ_ℓ, which has degree $\ell+1$ in both variables. We have $h(\Phi_\ell) \sim 6\ell\log\ell$ as ℓ tends to infinity [8], and explicit bounds can be given [4]. Since $d(\delta) = \ell+1$ and $l(\delta) = \ell$ in this case, Theorem 1.1 seems optimal up to the value of the constants.

In the case of Siegel and Hilbert modular equations in dimension 2, this result is new, and we can provide explicit values for the constants C_1 and C_2. In particular, the degree bounds that we obtain match exactly with experimental data.

The strategy to prove part 1 of Theorem 1.1 is to exhibit a particular modular form that behaves as the denominator of $\Psi_{\delta,m}$, and to control its weight; then, we show that rewriting quotients of modular forms in terms of the chosen coordinates transforms bounded weights into bounded degrees. The proof of part 2 is inspired by previous works on Φ_ℓ [31]. We prove height bounds on *evaluations* of modular equations at certain points using well-known results on the Faltings height of isogenous abelian varieties [12]. Then we use a general tight relation between the height of a rational fraction over a number field and the height of its evaluations at sufficiently many points, proved by the author in a separate paper [18].

This paper is organized as follows. In Section 2, we recall the necessary background on PEL Shimura varieties. In Section 3, we define the modular equations associated with a choice of PEL setting and absolutely irreducible Hecke correspondence, and explain how we recover the Siegel and Hilbert modular equations in dimension 2 as special cases. Sections 4 and 5 are devoted to the proof of the degree and height bounds respectively.

2. Background on PEL Shimura varieties

Our presentation is based on Milne's expository notes [27], which serve as a general reference for this section. These notes are themselves based on Deligne's reformulation of Shimura's works [10]. We use the following notation: if G is a connected reductive algebraic group over $\mathbb{Q}$, then

- G^{der} is the derived group of G,
- Z is the center of G,

- $G^{\mathrm{ad}} = G/Z$ is the adjoint group of G,
- $T = G/G^{\mathrm{der}}$ is the largest abelian quotient of G,
- $\nu\colon G \to T$ is the natural quotient map,
- $G^{\mathrm{ad}}(\mathbb{R})_+$ is the connected component of 1 in $G^{\mathrm{ad}}(\mathbb{R})$ for the real topology,
- $G(\mathbb{R})_+$ is the preimage of $G^{\mathrm{ad}}(\mathbb{R})_+$ in $G(\mathbb{R})$, and finally
- $G(\mathbb{Q})_+ = G(\mathbb{Q}) \cap G(\mathbb{R})_+$.

We write $\mathbb{A}_f$ for the ring of finite adeles of $\mathbb{Q}$.

PEL data. Let $(B, *)$ be a finite-dimensional simple $\mathbb{Q}$-algebra with positive involution. The center F of B is a number field; let $F_0 \subset F$ be the subfield of invariants under $*$. For simplicity, we make the technical assumption that B is either of type (A) or (C) [27, Prop. 8.3]: this means that for every embedding θ of F_0 in an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$, the algebra with positive involution $(B \otimes_{F_0,\theta} \overline{\mathbb{Q}}, *)$ is isomorphic to a product of factors of the form, respectively,

(A) $M_n(\overline{\mathbb{Q}}) \times M_n(\overline{\mathbb{Q}})$ with $(a, b)^* = (b^t, a^t)$, or
(C) $M_n(\overline{\mathbb{Q}})$ with $a^* = a^t$.

Let (V, ψ) be a faithful symplectic $(B, *)$-module. This means that V is a finite-dimensional $\mathbb{Q}$-vector space equipped with a faithful B-module structure and a nondegenerate alternating $\mathbb{Q}$-bilinear form ψ such that for all $b \in B$ and for all $u, v \in V$,

$$\psi(b^* u, v) = \psi(u, bv).$$

Let $\mathrm{GL}_B(V)$ denote the group of automorphisms of V respecting the action of B, and let G be its reduced algebraic subgroup defined by

$$G(\mathbb{Q}) = \big\{ g \in \mathrm{GL}_B(V) \mid \psi(gx, gy) = \psi(\mu(g)x, y) \text{ for some } \mu(g) \in F_0^\times \big\}.$$

The group G is connected and reductive, and its derived group is $G^{\mathrm{der}} = \ker(\mu) \cap \ker(\det)$ [27, Prop. 8.7]. We warn the reader that our G is denoted by G_1 in [27, §8 of the 2017 version]. In Milne's terminology, our G will define a Shimura variety (so that the results of [27, §5] apply), but not strictly speaking a PEL Shimura variety. This choice of reductive group will allow us to consider more Hecke correspondences later on.

Let x be a complex structure on $V(\mathbb{R})$, meaning an endomorphism of $V(\mathbb{R})$ such that $x^2 = -1$. We say that x is *positive for* ψ if it commutes with the action of B and if the bilinear form $(u, v) \mapsto \psi\big(u, x(v)\big)$ on $V(\mathbb{R})$ is symmetric and positive definite. In particular, $x \in G(\mathbb{R})$ and $\mu(x) = 1$. Such a complex structure x_0 exists [27, Prop. 8.14]. Define X_+ to be the orbit of x_0 under the action of $G(\mathbb{R})_+$ by conjugation; the space X_+ is a hermitian symmetric domain [27, Cor. 5.8]. We call the tupe $(B, *, V, \psi, G, X_+)$ a *simple PEL Shimura datum of type (A) or (C)*, or simply a *PEL datum*. To simplify notations, we abbreviate PEL data as pairs (G, X_+), the underlying data (V, ψ) and $(B, *)$ being implicit.

PEL Shimura varieties. Let (G, X_+) be a PEL datum as above, let K be a compact open subgroup of $G(\mathbb{A}_f)$, and let K_∞ be the stabilizer of x_0 in $G(\mathbb{R})_+$. The *PEL Shimura variety* associated with (G, X_+) of level K is the double quotient

$$\begin{aligned} \mathrm{Sh}_K(G, X_+)(\mathbb{C}) &= G(\mathbb{Q})_+ \backslash (X_+ \times G(\mathbb{A}_f))/K \\ &= G(\mathbb{Q})_+ \backslash (G(\mathbb{R})_+ \times G(\mathbb{A}_f))/K_\infty \times K. \end{aligned} \tag{1}$$

Actually, this quotient will be the set of $\mathbb{C}$-points of the Shimura variety, hence the notation. In the first line of (1), the group $G(\mathbb{Q})_+$ acts on both X_+ and $G(\mathbb{A}_f)$ by conjugation and left multiplication respectively, and K acts on $G(\mathbb{A}_f)$ by right multiplication. When the context is clear, we omit (G, X_+) from the notation. The set $\mathrm{Sh}_K(\mathbb{C})$ is given the quotient topology obtained from the real topology on $G(\mathbb{R})_+$ and the adelic topology on $G(\mathbb{A}_f)$.

In order to describe $\mathrm{Sh}_K(\mathbb{C})$ more explicitly, we study its connected components. The projection to the second factor induces a map with connected fibers from $\mathrm{Sh}_K(\mathbb{C})$ to the double quotient $G(\mathbb{Q})_+\backslash G(\mathbb{A}_f)/K$, which is finite [27, Lem. 5.12]. Let $\mathcal{C}$ be a set of representatives in $G(\mathbb{A}_f)$ for this double quotient. The connected component $\mathcal{S}_c$ of $\mathrm{Sh}_K(\mathbb{C})$ indexed by $c \in \mathcal{C}$ can be identified with $\Gamma_c\backslash X_+$, where $\Gamma_c = G(\mathbb{Q})_+ \cap cKc^{-1}$ is an arithmetic subgroup of $\mathrm{Aut}(X_+)$ [27, Lem. 5.13]. Thus, the Shimura variety $\mathrm{Sh}_K(\mathbb{C})$ has a natural structure of a complex analytic space, and is an algebraic variety by the theorem of Baily and Borel [27, Thm. 3.12].

Since G^{der} is simply connected, by [27, Thm. 5.17 and Lem. 5.20] (the assumption that K is sufficiently small is not actually needed there), the map ν induces an isomorphism

$$G(\mathbb{Q})_+\backslash G(\mathbb{A}_f)/K \simeq \nu(G(\mathbb{Q})_+)\backslash T(\mathbb{A}_f)/\nu(K).$$

Therefore the set of connected components of $\mathrm{Sh}_K(\mathbb{C})$ is a finite abelian group. Moreover, each connected component is itself a Shimura variety with underlying group G^{der} [27, Rem. 5.23].

A fundamental theorem states that $\mathrm{Sh}_K(G, X_+)$ exists as an algebraic variety defined over the *reflex field* $E(G, X_+)$, which is a number field contained in $\mathbb{C}$, depending only on the PEL datum [27, §12-14]. The field of definition of the individual connected components of $\mathrm{Sh}_K(\mathbb{C})$ depends on K, and is a finite abelian extension of $E(G, X_+)$.

2.2. **The modular interpretation.** Our motivation in constructing PEL Shimura varieties is to obtain moduli spaces of complex abelian varieties with polarization, endomorphism, and level structures. This *modular interpretation* of PEL Shimura varieties is usually formulated in terms of isogeny classes of abelian varieties [27, Thm. 8.17]. In order to obtain a modular interpretation in terms of *isomorphism* classes of abelian varieties in the spirit of [6, §2.6.2], we fix

- a PEL datum (G, X_+),
- a lattice $\Lambda_0 \subset V$,
- a compact open subgroup $K \subset G(\mathbb{A}_f)$ which stabilizes the lattice $\widehat{\Lambda}_0 = \Lambda_0 \otimes \widehat{\mathbb{Z}} \subset V(\mathbb{A}_f)$, and
- a set $\mathcal{C} \subset G(\mathbb{A}_f)$ of representatives for the finite double quotient $G(\mathbb{Q})_+\backslash G(\mathbb{A}_f)/K$.

By definition, a lattice in V is a subgroup of $V(\mathbb{Q})$ generated by a $\mathbb{Q}$-basis of V, hence a free $\mathbb{Z}$-module of rank $\dim V$. If p is a prime number, then a lattice in $V(\mathbb{Q}_p)$ is a subgroup of the form $\bigoplus_{i\in I} \mathbb{Z}_p e_i$ where $(e_i)_{i\in I}$ is a $\mathbb{Q}_p$-basis of $V(\mathbb{Q}_p)$. Finally, a lattice in $V(\mathbb{A}_f)$ is a product of lattices in $V(\mathbb{Q}_p)$ for each p that are equal to $V(\mathbb{Z}_p)$ for all p but finitely many. Recall that the local-global principle for lattices holds: the map $\Lambda \mapsto \widehat{\Lambda} = \Lambda \otimes \widehat{\mathbb{Z}}$ is a bijection between lattices in V and lattices in $V(\mathbb{A}_f)$, and its inverse is intersection with $V(\mathbb{Q})$. The assumption that K stabilizes $\widehat{\Lambda}_0$ does not imply a loss of generality, because every compact open subgroup of $G(\mathbb{A}_f)$ stabilizes some lattice in $V(\mathbb{A}_f)$.

To complete the setup, let $\mathcal{O}$ be the largest order in B stabilizing Λ_0. We keep the notation of §2.1: for every $c \in \mathcal{C}$, we write $\Gamma_c = G(\mathbb{Q})_+ \cap cKc^{-1}$, and we denote by $\mathcal{S}_c = \Gamma_c \backslash X_+$ the connected component of $\mathrm{Sh}_K(\mathbb{C})$ associated with c.

We define a *polarized lattice* to be a pair (Λ, ϕ) where Λ is a free $\mathbb{Z}$-module of finite rank and $\phi\colon \Lambda \times \Lambda \to \mathbb{Z}$ is a nondegenerate alternating form. Given a polarized lattice (Λ, ϕ), we can extend ϕ to the $\mathbb{Q}$-vector space $\Lambda \otimes \mathbb{Q}$, and we define

$$\Lambda^\perp = \{v \in \Lambda \otimes \mathbb{Q} \mid \forall w \in \Lambda,\ \phi(v, w) \in \mathbb{Z}\}.$$

Then $\Lambda^\perp/\Lambda$ is a finite abelian group called the *polarization type* of (Λ, ϕ). We say that ϕ is a *principal polarization* on Λ if $\Lambda^\perp = \Lambda$.

A modular interpretation in terms of lattices. Using the data above, we define a standard polarized lattice for every connected component of $\mathrm{Sh}_K(\mathbb{C})$ as follows.

Definition 2.1. For each $c \in \mathcal{C}$, we define

$$\widehat{\Lambda}_c = c(\widehat{\Lambda}_0) \quad \text{and} \quad \Lambda_c = \widehat{\Lambda}_c \cap V(\mathbb{Q}).$$

The action of c, or any other element of $G(\mathbb{A}_f)$, on adelic lattices is easily defined locally at each prime. Since c respects the action of B on $V(\mathbb{A}_f)$, the order $\mathcal{O}$ is again the stabilizer of $\widehat{\Lambda}_c$, and thus of Λ_c. Let $\lambda_c \in \mathbb{Q}_+^\times$ be such that the nondegenerate alternating form $\psi_c = \lambda_c \psi$ satisfies $\psi_c(\Lambda_c \times \Lambda_c) = \mathbb{Z}$. We call (Λ_c, ψ_c) with its structure of $\mathcal{O}$-module the *standard polarized lattice* associated with (Λ_0, c).

Choose $c \in \mathcal{C}$, and let (Λ_c, ψ_c) be the standard polarized lattice associated with (Λ_0, c). We consider tuples $(\Lambda, x, \iota, \phi, \eta K)$ where

- Λ is a free $\mathbb{Z}$-module of rank $\dim V$,
- $x \in \mathrm{End}(\Lambda \otimes \mathbb{R})$ is a complex structure on $\Lambda \otimes \mathbb{R}$,
- ι is an embedding $\mathcal{O} \hookrightarrow \mathrm{End}_{\mathbb{Z}}(\Lambda)$,
- $\phi\colon \Lambda \times \Lambda \to \mathbb{Z}$ is a nondegenerate alternating $\mathbb{Z}$-bilinear form on Λ,
- ηK is a K-orbit of $\widehat{\mathbb{Z}}$-linear isomorphisms of $\mathcal{O}$-modules $\widehat{\Lambda}_0 \to \Lambda \otimes \widehat{\mathbb{Z}}$,

satisfying the following condition of compatibility with (Λ_c, ψ_c):

($\star$) There exists an isomorphism of $\mathcal{O}$-modules $a\colon \Lambda \to \Lambda_c$, carrying ηK to cK and x to an element of X_+, such that

$$\exists \zeta \in \mu(\Gamma_c),\ \forall u, v \in \Lambda,\ \phi(u, v) = \psi_c\big(\zeta a(u), a(v)\big).$$

For short, we will call such a tuple a *lattice with PEL structure defined by* (Λ_0, c), or simply a *lattice with PEL structure* when the dependency on (Λ_0, c) is understood.

An *isomorphism* between two lattices with PEL structure $(\Lambda, x, \iota, \phi, \eta K)$ and $(\Lambda', x', \iota', \phi', \eta' K)$ is an isomorphism of $\mathcal{O}$-modules $f\colon \Lambda \to \Lambda'$ that sends x to x', sends ηK to $\eta' K$, and such that $\phi(u, v) = \phi'\big(\zeta f(u), f(v)\big)$ for some $\zeta \in \mu(\Gamma_c)$.

For every lattice with PEL structure $(\Lambda, x, \iota, \phi, \eta K)$, the compatibility condition ($\star$) implies in particular that the complex structure x is positive for ϕ, the adjunction involution defined by ϕ coincides with $*$ on B, the action of B on $\Lambda \otimes \mathbb{Q}$ leaves the complex structure x invariant, and the polarized lattices (Λ, ϕ) and (Λ_c, ψ_c) have the same polarization type.

Proposition 2.2. *Let $c \in \mathcal{C}$, and let $\mathcal{Z}_c$ be the set of isomorphism classes of lattices with PEL structure defined by (Λ_0, c). Then the map*

$$\begin{array}{ccc} \mathcal{Z}_c & \longrightarrow & \mathcal{S}_c \\ (\Lambda, x, \iota, \phi, \eta K) & \longmapsto & [axa^{-1},\, c] \quad \text{where } a \text{ is as in } (\star) \end{array}$$

is well-defined and bijective. The inverse map is

$$[x, c] \mapsto (\Lambda_c, x, \iota, \psi_c, cK).$$

where ι is the natural action of $\mathcal{O}$ on Λ_c.

Proof. The proof is direct and omitted; the details are similar to [27, Prop. 6.3]. □

A modular interpretation in terms of isomorphism classes of abelian varieties. Giving an abelian variety A over $\mathbb{C}$ is the same as giving the lattice $\Lambda = H_1(A, \mathbb{Z})$ and a complex structure on the universal covering $\Lambda \otimes \mathbb{R}$ of A. Under this identification, endomorphisms of A correspond to endomorphisms of Λ that respect the complex structure. Moreover, giving a polarization on A is the same as giving a nondegenerate alternating form $\phi\colon \Lambda \times \Lambda \to \mathbb{Z}$ such that the bilinear form $(u, v) \mapsto \phi(u, iv)$ is symmetric and positive definite. The *polarization type* of A is the polarization type of (Λ, ϕ).

Recall that for every prime number p, the Tate module $T_p(A)$ is defined as the projective limit of the torsion subgroups $A[p^n]$ as n tends to infinity:

$$T_p(A) = \varprojlim A[p^n] = \varprojlim \Lambda/p^n\Lambda = \Lambda \otimes \mathbb{Z}_p.$$

Therefore $\Lambda \otimes \widehat{\mathbb{Z}}$ is canonically isomorphic to the global Tate module $\widehat{T}(A)$ of A, defined as

$$\widehat{T}(A) = \prod_{p \text{ prime}} T_p(A).$$

Fix $c \in \mathcal{C}$, and let (Λ_c, ψ_c) be the standard polarized lattice associated with (Λ_0, c). We define a *complex abelian variety with PEL structure defined by* (Λ_0, c) to be a tuple $(A, \phi, \iota, \eta K)$ where

- (A, ϕ) is a complex polarized abelian variety of dimension $\dim V$,
- ι is an embedding $\mathcal{O} \hookrightarrow \mathrm{End}(A)$,
- ηK is a K-orbit of $\widehat{\mathbb{Z}}$-linear isomorphisms of $\mathcal{O}$-modules $\widehat{\Lambda}_0 \to \widehat{T}(A)$,

satisfying the following condition of compatibility with (Λ_c, ψ_c):

($\star\star$) There exists an isomorphism of $\mathcal{O}$-modules $a\colon H_1(A, \mathbb{Z}) \to \Lambda_c$, carrying ϕ to ψ_c, carrying ηK to cK, and such that the complex structure induced by a on $V(\mathbb{R})$ belongs to X_+.

If $(A, \phi, \iota, \eta K)$ is a complex abelian variety with PEL structure defined by (Λ_0, c), then condition ($\star\star$) implies that A and (Λ_c, ψ_c) have the same polarization type, and that the Rosati involution on $\mathrm{End}(A) \otimes \mathbb{Q}$ (which is adjuction with respect to ϕ) restricts to $*$ on B.

An *isomorphism* between complex abelian varieties with PEL structure $(A, \phi, \iota, \eta K)$ and $(A', \phi', \iota', \eta' K)$ is an isomorphism of complex polarized abelian varieties $f\colon (A, \phi) \to (A,' \phi')$ respecting the action of $\mathcal{O}$ and sending ηK to $\eta' K$.

The difference with the setting of Proposition 2.2 is that isomorphisms of complex abelian varieties with PEL structure must respect the polarizations exactly, rather

than up to an element of $\mu(\Gamma_c)$. In general, $\mu(\Gamma_c) \neq \{1\}$, but there is the following workaround. If $\varepsilon \in F^\times$ lies in the center of B, then multiplication by ε defines an element in the center of $G(\mathbb{Q})$. Therefore it makes sense to define

$$\mathcal{E}_K = \{\varepsilon \in F^\times \mid \varepsilon \in K\} = \{\varepsilon \in F^\times \mid \varepsilon \in \Gamma_c\}, \quad \text{for every } c \in G(\mathbb{A}_f).$$

Proposition 2.3. *Let $c \in \mathcal{C}$, and let (Λ_c, ψ_c) be the standard polarized lattice associated with (Λ_0, c). If $\mu(\mathcal{E}_K) = \mu(\Gamma_c)$, then the map*

$$[x, c] \longmapsto \big(V(\mathbb{R})/\Lambda_c, \psi_c, \iota, cK\big),$$

where $V(\mathbb{R})$ is seen as a complex vector space via x, and ι is the action of $\mathcal{O}$ on $V(\mathbb{R})/\Lambda_c$ induced by the action of B on $V(\mathbb{R})$, is a bijection between $\mathcal{S}_c$ and the set of isomorphism classes of complex abelian varieties with PEL structure defined by (Λ_0, c).

Proof. When defining $\mathcal{Z}_c$ as in Proposition 2.2, we can impose $\zeta = 1$ in condition $(\star)$ and strengthen the notion of isomorphism between lattices with PEL structure to respect the polarizations exactly. Indeed, multiplying the isomorphism a by $\varepsilon \in \mathcal{E}_K$ leaves everything invariant except the alternating form, which is multiplied by $\mu(\varepsilon)$. The result follows then from the equivalence of categories between lattices and complex abelian varieties outlined above. □

Remark 2.4. The group $\mu(\mathcal{E}_K)$ always has finite index in $\mu(\Gamma_c)$. Indeed, if $\mathbb{Z}_{F_0}^\times$ denotes the unit group of F_0, then

$$\mu(\mathcal{E}_K) \subset \mu(\Gamma_c) \subset \mathbb{Z}_{F_0}^\times$$

and $\mu(\mathcal{E}_K)$ contains a subgroup of finite index in $\mathbb{Z}_{F_0}^\times$, namely all the squares of elements in $\mathbb{Z}_{F_0}^\times \cap K$. By [7, Thm. 1], there exists a compact open subgroup M of $\mu(K)$ such that $\mathbb{Z}_{F_0}^\times \cap M = \mu(\mathcal{E}_K)$. Define $K' = K \cap \mu^{-1}(M)$. Then $\mathcal{E}_{K'} = \mathcal{E}_K$, and for every $c \in G(\mathbb{A}_f)$, we have

$$G(\mathbb{Q})_+ \cap cK'c^{-1} = \{\gamma \in \Gamma_c \mid \mu(\gamma) \in \mu(\mathcal{E}_K)\}.$$

Therefore the hypothesis of Proposition 2.3 will be satisfied for the smaller level subgroup K'.

When considering the classical modular curves as Shimura varieties associated with the reductive group $G = \mathrm{GL}_2$ acting on $V = \mathbb{Q}^2$, we can take $\Lambda_0 = \mathbb{Z}^2$ and $\psi = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Then Proposition 2.3 applies, and we let the reader check that we recover the usual modular interpretation of modular curves in terms of complex elliptic curves with level structure.

2.3. **Modular forms on PEL Shimura varieties.** Our definition of modular equations will involve choices of coordinates on connected components of PEL Shimura varieties. These coordinates, also called modular functions, are obtained as quotients of modular forms. This section briefly presents modular forms on PEL Shimura varieties without going into technical details.

Let (G, X_+) be a PEL datum, and let $K_\infty \subset G(\mathbb{R})_+$ be the stabilizer of a fixed complex structure $x_0 \in X_+$. Attached to this data is a certain canonical character of K_∞ [1, §1.8], denoted by $\rho\colon K_\infty \to \mathbb{C}^\times$. Let K be a compact open subgroup of $G(\mathbb{A}_f)$. A *modular form* of weight $w \in \mathbb{Z}$ on $\mathrm{Sh}_K(G, X_+)(\mathbb{C})$ is a function

$$f\colon G(\mathbb{Q})_+ \backslash \big(G(\mathbb{R})_+ \times G(\mathbb{A}_f)\big)/K \to \mathbb{C}$$

that satisfies suitable growth and holomorphy conditions [26, Prop. 3.2], and such that

$$\forall x \in G(\mathbb{R})_+,\ \forall g \in G(\mathbb{A}_f),\ \forall k_\infty \in K_\infty,\ f([xk_\infty, g]) = \rho(k_\infty)^w f([x,g]).$$

The weight of f is denoted by $\mathrm{wt}(f)$. We also say that f is *of level* K.

Let $\mathcal{S}$ be a connected component of $\mathrm{Sh}_K(\mathbb{C})$, or a union of these, and let L be its field of definition. A *modular form of weight* w *on* $\mathcal{S}$ is the restriction of a modular form of weight w on $\mathrm{Sh}_K(\mathbb{C})$ to the preimage of $\mathcal{S}$ in $G(\mathbb{Q})_+\backslash\big(G(\mathbb{R}_+)\times G(\mathbb{A}_f)\big)/K$ by the natural projection. There is a canonical notion of modular forms on $\mathcal{S}$ being defined over L [26, Chap. III]. A *modular function* on $\mathcal{S}$ is the quotient of two modular forms of the same weight, the denominator being nonzero on each connected component of $\mathcal{S}$.

The following result is well known; since we did not find a precise reference in the literature, we present a short proof.

Theorem 2.5. *Let $\mathcal{S}$ be a connected component of the Shimura variety $\mathrm{Sh}_K(\mathbb{C})$, and let L be its field of definition. Then the graded L-algebra of modular forms on $\mathcal{S}$ defined over L is finitely generated, and there exists a weight $w \geq 1$ such that modular forms of weight w defined over L realize a projective embedding of $\mathcal{S}$. Every element of the function field $L(\mathcal{S})$ is a quotient of two modular forms of the same weight defined over L.*

Proof. Choose an element $c \in \mathcal{C} \subset G(\mathbb{A}_f)$ defining the connected component $\mathcal{S}$, so that $\mathcal{S} = \Gamma_c\backslash X_+$ where $\Gamma_c = G(\mathbb{Q})_+ \cap cKc^{-1}$. Assume first that the level subgroup K of $G(\mathbb{A}_f)$ is sufficiently small, so that Γ_c is torsion-free. Then, by the Baily–Borel theorem [1, Thm. 10.11], there exists an ample line bundle $\mathcal{M}_\mathbb{C}$ on $\mathcal{S}$ such that for every $w \geq 1$, the algebraic sections of $\mathcal{M}_\mathbb{C}^{\otimes w}$ are exactly the modular forms of weight w on $\mathcal{S}$.

In fact, $\mathcal{M}_\mathbb{C}$ is the inverse determinant of the tangent bundle on $\mathcal{S}$ [1, Prop. 7.3]. Since $\mathcal{S}$ has a model over L, there is a line bundle $\mathcal{M}$ on $\mathcal{S}$ defined over L such that $\mathcal{M} \otimes_L \mathbb{C} = \mathcal{M}_\mathbb{C}$. This is a particular case of a general result on the rationality of automorphic vector bundles [26, Chap. III, Thm. 4.3]. For every $w \geq 1$, the L-vector space modular forms of weight w on $\mathcal{S}$ defined over L is $H^0(\mathcal{S}, \mathcal{M}^{\otimes w})$. Since $\mathcal{M} \otimes_L \mathbb{C}$ is ample, $\mathcal{M}$ is ample too, and this implies the conclusions of the theorem.

In general, we can always find a level subgroup K' of finite index in K such that the arithmetic subgroups $G(\mathbb{Q})_+ \cap cK'c^{-1}$ for $c \in G(\mathbb{A}_f)$ are torsion free [27, Prop. 3.5], and we can assume that K' is normal in K. Let $\mathcal{S}'$ be a connected component of $\mathrm{Sh}_{K'}(\mathbb{C})$ lying over $\mathcal{S}$, and let L' be its field of definition. Then the conclusions of the theorem hold for $\mathcal{S}'$. We can identify the modular forms on $\mathcal{S}$ defined over L with the modular forms on $\mathcal{S}'$ defined over L' that are invariant under the action of a subgroup of K/K'. Therefore the conclusions of the theorem also hold for $\mathcal{S}$ by Noether's theorem [29] on invariants under finite groups. □

We can also consider modular forms that are symmetric under certain automorphisms of Sh_K. Let Σ be a finite group of automorphisms of V as a $\mathbb{Q}$-vector space that leaves the symplectic form ψ invariant, and also acts on B in such a way that

$$\forall u \in V,\ \forall b \in B,\ \forall \sigma \in \Sigma,\ \sigma(bu) = \sigma(b)\sigma(u).$$

This implies that the elements of Σ commute with the involution $*$, and hence leave F_0 stable. Under these assumptions, each $\sigma \in \Sigma$ induces an automorphism

of G defined over $\mathbb{Q}$, also denoted by σ. Assume further that these automorphisms leave $G(\mathbb{R})_+$, X_+, K, K_∞, ν and the character ρ invariant. Then Σ can be seen as a finite group of automorphisms of $\mathcal{S}$, and one can check as in [27, Thm. 13.6] that these automorphisms are defined over L. Then for every modular form f of weight w on $\mathcal{S}$ defined over L, and every $\sigma \in \Sigma$, the function

$$\sigma \cdot f \ : \ [x, g] \mapsto f([\sigma^{-1}(x), \sigma^{-1}(g)])$$

is a modular form of weight w on $\mathcal{S}$ defined over L. We say that f is *symmetric* under Σ if $\sigma \cdot f = f$ for every $\sigma \in \Sigma$.

Proposition 2.6. *Let Σ be a finite group of automorphisms of G as above. Then the graded L-algebra of symmetric modular forms on $\mathcal{S}$ defined over L is finitely generated, and every symmetric modular function on $\mathcal{S}$ defined over L is the quotient of two symmetric modular forms of the same weight defined over L.*

Proof. This results from Theorem 2.5 and another application of Noether's theorem. □

2.4. **Hecke correspondences.** We fix a PEL datum (G, X_+) as above, as well as a compact open subgroup $K \subset G(\mathbb{A}_f)$. Let $\delta \in G(\mathbb{A}_f)$, and let $K' = K \cap \delta K \delta^{-1}$. Consider the diagram

$$\begin{array}{ccc} \mathrm{Sh}_{K'}(\mathbb{C}) & \xrightarrow{R(\delta)} & \mathrm{Sh}_{\delta^{-1}K'\delta}(\mathbb{C}) \\ \downarrow{\scriptstyle p_1} & & \downarrow{\scriptstyle p_2} \\ \mathrm{Sh}_K(\mathbb{C}) & & \mathrm{Sh}_K(\mathbb{C}) \end{array} \tag{2}$$

where the map $R(\delta)$ is $[x, g] \mapsto [x, g\delta]$, and p_1 and p_2 are the natural projections. This diagram defines a correspondence H_δ in $\mathrm{Sh}_K \times \mathrm{Sh}_K$, called the *Hecke correspondence* of level δ, consisting of all pairs of the form $\big(p_1(x), p_2(R(\delta)x)\big)$ for $x \in \mathrm{Sh}_{K'}$. Hecke correspondences are algebraic: the diagram (2) is the analytification of a diagram existing at the level of algebraic varieties. Moreover, Hecke correspondences are defined over the reflex field [27, Thm. 13.6].

We define the *degree* of H_δ to be the index

$$d(\delta) = [K : K'] = [K : K \cap \delta K \delta^{-1}].$$

This index is finite as both K and K' are compact open subgroups of $G(\mathbb{A}_f)$, and is the degree of the map $\mathrm{Sh}_{K'} \to \mathrm{Sh}_K$. One can also consider H_δ as a map from Sh_K to its $d(\delta)$-th symmetric power, sending $z \in \mathrm{Sh}_K$ to the set $\{z' \in \mathrm{Sh}_K \mid (z, z') \in H_\delta\}$.

It is easy to see how H_δ behaves with respect to connected components: if z lies in the connected component indexed by $t \in T(\mathbb{A}_f)$, then its images lie in the connected component indexed by $t\,\nu(\delta)$.

We call the Hecke correspondence H_δ *absolutely irreducible* if for every connected component $\mathcal{S}$ of $\mathrm{Sh}_K(\mathbb{C})$ with field of definition L, the preimage of $\mathcal{S}$ in $\mathrm{Sh}_{K'}$ is absolutely irreducible as a variety defined over L (or equivalently, connected as a variety over $\mathbb{C}$). A sufficient condition for H_δ to be absolutely irreducible is that $\nu(K') = \nu(K)$.

Modular interpretation of Hecke correspondences. In the modular interpretation, Hecke correspondences describe isogenies of a certain type between polarized

abelian varieties. Let Λ_0, $\mathcal{C}$, and $\mathcal{O}$ be as in §2.2, and write

$$K = \bigsqcup_{i=1}^{d(\delta)} \kappa_i K',$$

where $\kappa_i \in G(\mathbb{A}_f)$ for each $1 \leq i \leq d(\delta)$. Let $c \in \mathcal{C}$, denote by $\mathcal{S}_c$ the connected component of $\mathrm{Sh}_K(\mathbb{C})$ indexed by c, and consider the lattice with PEL structure $(\Lambda_c, x, \iota, \psi_c, cK)$ associated with a point $[x, c] \in \mathcal{S}_c$ by Proposition 2.2.

In order to construct the lattices associated with $[x, c]$ via the Hecke correspondence H_δ, we partition the orbit cK into the K'-orbits $c\kappa_i K'$ for $1 \leq i \leq d(\delta)$. Each element $c\kappa_i\delta \in G(\mathbb{A}_f)$ is then a $\widehat{\mathbb{Z}}$-linear embedding of $\mathcal{O}$-modules $\widehat{\Lambda}_0 \hookrightarrow V(\mathbb{A}_f)$; it is well defined up to right multiplication by $\delta^{-1}K'\delta$, hence by K. Let $\Lambda_i \subset V(\mathbb{Q})$ be the lattice such that $\Lambda_i \otimes \widehat{\mathbb{Z}}$ is the image of this embedding. There is still a natural action of $\mathcal{O}$ on Λ_i. The decomposition $c\kappa_i\delta K = q_i c' K$, with $q_i \in G(\mathbb{Q})_+$ and $c' \in \mathcal{C}$, is well defined, and the element c' does not depend on i.

Proposition 2.7. *Let $\delta \in G(\mathbb{A}_f)$, let $z = [x, c] \in \mathcal{S}_c$, and construct Λ_i, q_i, c' as above. Then the image of z under the Hecke correspondence H_δ in the modular interpretation of Proposition 2.3 is given by the $d(\delta)$ isomorphism classes of tuples with representatives*

$$\Big(\Lambda_i, x, \frac{\lambda_{c'}}{\lambda_c}\psi_c\big(\mu(q_i^{-1})\cdot,\cdot\big), c\kappa_i\delta K\Big) \qquad \text{for} \quad 1 \leq i \leq d(\delta).$$

Proof. By construction, the images of $[x, c]$ via the Hecke correspondence are the points $[q_i^{-1}x, c']$ of $\mathrm{Sh}_K(\mathbb{C})$. The relation $c\kappa_i\delta K = q_i c' K$ shows that the map q_i^{-1} sends the lattice Λ_i to $\Lambda_{c'}$. This map also respects the action of $\mathcal{O}$, and sends the complex structure x to $q_i^{-1}x$. Finally, it sends the polarization $(u, v) \mapsto \psi_c(u, v)$ on Λ_i to $(u, v) \mapsto \psi_c\big(\mu(q_i)u, v\big)$ on $\Lambda_{c'}$. □

After multiplying δ by a unique suitable element in $\mathbb{Q}_+^\times$, which does not change H_δ, we can assume that $\delta(\widehat{\Lambda}_0) \subset \widehat{\Lambda}_0$ and $\delta(\widehat{\Lambda}_0) \not\subset p\widehat{\Lambda}_0$ for every prime p; we say that δ is *normalized* with respect to Λ_0. In this case, we define the *isogeny degree* of H_δ as the unique integer $l(\delta) \geq 1$ such that $l(\delta)^{-1}\det(\delta)$ is a unit in $\widehat{\mathbb{Z}}$. In other words,

$$l(\delta) = \#\big(\widehat{\Lambda}_0/\delta(\widehat{\Lambda}_0)\big).$$

For a general $\delta \in G(\mathbb{A}_f)$, we set $l(\delta) = l(\lambda\delta)$ where $\lambda \in \mathbb{Q}_+^\times$ is chosen such that $\lambda\delta$ is normalized with respect to Λ_0.

Corollary 2.8. *Let $\delta \in G(\mathbb{A}_f)$. Then, in the modular interpretation of Proposition 2.3, the Hecke correspondence H_δ sends an abelian variety A with PEL structure to $d(\delta)$ abelian varieties $A_1, \ldots, A_{d(\delta)}$ such that for every $1 \leq i \leq d(\delta)$, there exists an isogeny $A_i \to A$ of degree $l(\delta)$.*

Proof. We can assume that δ is normalized with respect to Λ_0. Then, in the result of Proposition 2.7, each lattice Λ_i for $1 \leq i \leq d(\delta)$ is a sublattice of Λ_c endowed with the same complex structure x. Moreover, for every $1 \leq i \leq d(\delta)$, we have $\Lambda_c/\Lambda_i \simeq \widehat{\Lambda}_0/\delta(\widehat{\Lambda}_0)$, so the index of each Λ_i in Λ_c is $l(\delta)$. □

A relation between degrees For later purposes, we state an inequality relating $d(\delta)$

and a power of $l(\delta)$. Since $K \subset G(\mathbb{A}_f)$ is open, there exists a smallest integer $N \geq 1$ such that

$$\big\{g \in G(\mathbb{A}_f) \cap \mathrm{GL}(\widehat{\Lambda}_0) \mid g = 1 \bmod N\widehat{\Lambda}_0\big\} \subset K,$$

that we call the *level* of K with respect to $\widehat{\Lambda}_0$.

Proposition 2.9. *There exists a constant C depending on K and Λ_0 such that for every $\delta \in G(\mathbb{A}_f)$, we have $d(\delta) \leq C\ l(\delta)^{(\dim V)^2}$. We can take $C = N^{(\dim V)^2}$, where N is the level of K with respect to $\widehat{\Lambda}_0$.*

Proof. We can assume that δ is normalized with respect to $\widehat{\Lambda}_0$. Then $K \cap \delta K \delta^{-1}$ contains all the elements $g \in G(\mathbb{A}_f) \cap \mathrm{GL}(\widehat{\Lambda}_0)$ that are the identity modulo $\widehat{\Lambda} = l(\delta)N\widehat{\Lambda}_0$. In other words we have a morphism $K \to \mathrm{GL}(\Lambda_0/N\,l(\delta)\Lambda_0)$ whose kernel is contained in $K \cap \delta K \delta^{-1}$. This yields the result since $\#\,\mathrm{GL}(\Lambda_0/N\,l(\delta)\Lambda_0) \leq (N\,l(\delta))^{(\dim V)^2}$. □

Remark 2.10. The upper bound on $d(\delta)$ given in Proposition 2.9 is far from optimal in many cases: for instance, if δ is normalized with respect to $\widehat{\Lambda}_0$, if $l(\delta)$ is prime to N, and if moreover δ normalizes the image of K in $\mathrm{GL}(\Lambda_0/N\Lambda_0)$, then $d(\delta) \leq l(\delta)^{(\dim V)^2}$. But in general, the level of K does enter into account. As an example, take $G = \mathrm{GL}_2$, $\delta = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, and

$$K = \Big\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\widehat{\mathbb{Z}}) \mid a = d = 1 \bmod N \text{ and } c = 0 \bmod N \Big\}.$$

Then $d(\delta) = N$ even though $l(\delta) = 1$. In the modular interpretation, the Hecke correspondence H_δ has the effect of forgetting the initial K-level structure entirely.

3. Modular equations on PEL Shimura varieties

This section presents a general definition of modular equations on PEL Shimura varieties, generalizing three examples mentioned in the introduction: the elliptic modular polynomials, and the modular equations of Siegel and Hilbert type for abelian surfaces (see §3.3 and §3.4).

3.1. The example of elliptic modular polynomials.

Elliptic modular polynomials are the simplest example of modular equations. They are usually defined in terms of classical modular forms [9, §11.C]. In order to motivate the general definition, we translate this definition in the adelic language.

The underlying PEL datum is obtained by taking $V = \mathbb{Q}^2$, $\psi = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, and $B = \mathbb{Q}$ with $*$ the trivial involution. Then $G = \mathrm{GL}_2$, and $G(\mathbb{Q})_+$ consists of all rational 2×2 matrices with positive determinant. We take $\Lambda_0 = \mathbb{Z}^2$ and $K = \mathrm{GL}_2(\widehat{\mathbb{Z}})$, so that $\mathrm{Sh}_K(\mathbb{C})$ has only one connected component $\mathcal{S}$ (indexed by the identity matrix) and the maximal order of B stabilizing Λ_0 is $\mathcal{O} = \mathbb{Z}$. If we take the complex structure $x_0 = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ as a base point, then X_+ is naturally identified with the Poincaré upper half plane $\mathbb{H}_1$, with x_0 corresponding to $i \in \mathbb{H}_1$. Then $\mathcal{S}$ is identified with the modular curve $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}_1$, and modular forms on $\mathcal{S}$ in the sense of §2.3 correspond exactly to modular forms of level $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}_1$ in the classical sense. The reflex field $E(G, X_+)$ is equal to $\mathbb{Q}$ in this case, and the j-invariant realizes an isomorphism between Sh_K and the affine line $\mathbb{A}^1_{\mathbb{Q}}$; in particular j generates the function field of $\mathcal{S}$ over $\mathbb{Q}$.

Let ℓ be a prime number. Then the function on $\mathbb{H}_1$ given by $\tau \mapsto j(\tau/\ell)$ is invariant under the following congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$:

$$\Gamma^0(\ell) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \mid b = 0 \bmod \ell \right\}.$$

Therefore, the coefficients of the polynomial

$$P_\ell(\tau) = \prod_{\gamma \in \Gamma^0(\ell)\backslash \mathrm{SL}_2(\mathbb{Z})} \Big(Y - j(\tfrac{1}{\ell}\gamma\tau)\Big), \quad \text{for } \tau \in \mathbb{H}_1$$

are modular functions of level $\mathrm{SL}_2(\mathbb{Z})$. The elliptic modular polynomial Φ_ℓ is the unique element of $\mathbb{C}(X)[Y]$ satisfying the relation $\Phi_\ell(j(\tau), Y) = P_\ell(\tau)$ for every $\tau \in \mathbb{H}_1$; actually $\Phi_\ell \in \mathbb{Z}[X, Y]$. In other words, we have a map

$$\Gamma^0(\ell)\backslash\mathbb{H}_1 \to \mathcal{S} \times \mathcal{S}, \quad \tau \mapsto (\tau, \tau/\ell), \tag{3}$$

and the product $\mathcal{S}\times\mathcal{S}$ is birational to $\mathbb{P}^1\times\mathbb{P}^1$ via (j, j). The modular curve $\Gamma^0(\ell)\backslash\mathbb{H}_1$ is birational to its image in $\mathbb{P}^1 \times \mathbb{P}^1$, and Φ_ℓ is an equation of this image.

Remark that for every $\tau \in \mathbb{H}_1$, we have

$$\tau/\ell = \delta^{-1}\tau, \quad \text{where} \quad \delta = \left(\begin{smallmatrix} \ell & 0 \\ 0 & 1 \end{smallmatrix}\right) \in G(\mathbb{Q})_+.$$

Therefore, if $\tau \in \mathbb{H}_1$ corresponds to a point $[x, I_2] \in \mathrm{Sh}_K(\mathbb{C})$, then τ/ℓ corresponds to the point $[x, \delta]$. Moreover $\Gamma^0(\ell) = \mathrm{SL}_2(\mathbb{Z}) \cap \big(\delta\,\mathrm{SL}_2(\mathbb{Z})\delta^{-1}\big)$. Therefore the map (3) is precisely the Hecke correspondence H_δ given in diagram (2).

The function $\tau \mapsto j(\tau/\ell)$ corresponds to the modular function

$$\begin{array}{rccc} j_\delta \ : & G(\mathbb{Q})_+\backslash\big(G(\mathbb{A}_f) \times G(\mathbb{R})_+\big) & \to & \mathbb{C} \\ & [x, g] & \mapsto & j([x, g\delta]), \end{array}$$

which is right-invariant under $\delta K \delta^{-1}$. Let K'' be a normal subgroup of finite index in K contained in $K' = K \cap \delta K \delta^{-1}$. We let K act (on the left) on the set of modular functions of level K'' as follows: if $k \in K$ and f is such a function, then we define

$$k \cdot f \ : \ [x, g] \mapsto f([x, gk]).$$

Since K' is contained in the stabilizer of j_δ, the coefficients of the polynomial

$$Q_\ell = \prod_{\gamma \in K/K'} \big(Y - \gamma \cdot j_\delta\big) \tag{4}$$

are modular functions of level K; the analogue of Q_ℓ in the classical world is exactly P_ℓ, as inversion induces a bijection between right cosets of $\Gamma^0(\ell)$ in $\mathrm{SL}_2(\mathbb{Z})$ and left cosets of K' in K. The general definition of modular equations involves analogues of the product (4) for other Hecke correspondences.

3.2. **General definition of modular equations.** Let (G, X_+) be a PEL datum, let K be a compact open subgroup of $G(\mathbb{A}_f)$, and let Σ be a finite group of automorphisms of G as in §2.3. Let n be the complex dimension of X_+; we assume that $n \geq 1$. Let $\mathcal{S}$, $\mathcal{T}$ be connected components of $\mathrm{Sh}_K(G, X_+)(\mathbb{C})$, and let L be their field of definition.

To complete the picture, we also need to choose coordinates on $\mathcal{S}$ and $\mathcal{T}$. Since the field $L(\mathcal{S})$ of modular functions on $\mathcal{S}$ has transcendence degree n over L, the field $L(\mathcal{S})^\Sigma$ of modular functions on $\mathcal{S}$ that are symmetric under Σ also has transcendence degree n over L. Choose a transcendence basis $(j_1, \ldots, j_n)$ of $L(\mathcal{S})^\Sigma$ over L, and another symmetric function j_{n+1} that generates the remaining finite

extension, whose degree is denoted by e. On $\mathcal{S}$, the function j_{n+1} satisfies a minimal relation of the form

(5)
$$E(j_1,\dots,j_{n+1})=0 \qquad \text{where} \quad E=\sum_{k=0}^{e} E_k(J_1,\dots,J_n)\,J_{n+1}^k \in L[J_1,\dots,J_{n+1}]$$

and E is irreducible. If $L(\mathcal{S})^\Sigma$ is purely transcendental over L (if $\Sigma=\{1\}$, this means that $\mathcal{S}$ is birational to $\mathbb{P}^n_L$), then we take $j_{n+1}=1$, ignore eq. (5), and work with n invariants only.

We proceed similarly to define coordinates on $\mathcal{T}$: no confusion will arise if we also denote them by $j_1,\dots,j_{n+1}$. We refer to all the data defined up to now as the *PEL setting*. Throughout the paper, our constants will depend on this data only.

Given a PEL setting as above, let $\delta\in G(\mathbb{A}_f)$ be an adelic element of G defining an absolutely irreducible Hecke correspondence H_δ that intersects $\mathcal{S}\times\mathcal{T}$ nontrivially. We want to define explicit polynomials with coefficients in $L(\mathcal{S})$, called the *modular equations of level* δ, describing H_δ in the product $\mathcal{S}\times\mathcal{T}$. To do this, we mimic the definition of elliptic modular polynomials in the language of PEL Shimura varities given in §3.1. As in §2.4, we write $K'=K\cap\delta K\delta^{-1}$.

Let K'' be a normal subgroup of finite index in K, contained in K', and stabilized by Σ. Let $\mathcal{S}''$ be the preimage of $\mathcal{S}$ in $\mathrm{Sh}_{K''}(\mathbb{C})$. There is a left action of $K\rtimes\Sigma$ on the space of modular functions on $\mathcal{S}''$, given by

$$(k,\sigma)\cdot f \;:\; [x,g]\mapsto \sigma\cdot f([x,gk]).$$

The modular functions that are invariant under $K'\rtimes\{1\}$ (resp. $K\rtimes\Sigma$) are exactly the rational functions on $H_\delta\cap(\mathcal{S}\times\mathcal{T})$ defined over $\mathbb{C}$ (resp. the rational functions on $\mathcal{S}$ defined over $\mathbb{C}$ and invariant under Σ). The modular functions

$$j_{i,\delta} \;:\; [x,g]\mapsto j_i([x,g\delta])$$

for $1\le i\le n+1$ are defined over L and generate the function field of $H_\delta\cap(\mathcal{S}\times\mathcal{T})$. We define the decreasing chain of subgroups

$$K\rtimes\Sigma=K_0\supset K_1\supset\cdots\supset K_{n+1}\supset K'$$

as follows: for each $1\le i\le n+1$, the subgroup K_i is the stabilizer of the functions $j_{1,\delta},\dots,j_{i,\delta}$. In §3.1, we had $K_0=K$ and $K_1=K'$.

Galois theory applied to the Galois covering $\mathcal{S}''\to\mathcal{S}$ tells us that for every $1\le i\le n+1$, the field $L(j_1,\dots,j_{n+1},j_{1,\delta},\dots,j_{i,\delta})$ is the function field of the preimage of $\mathcal{S}$ in the Shimura variety Sh_{K_i}, and consists of all modular functions on $\mathcal{S}''$ defined over L that are invariant under K_i. In other words, we have a tower of

function fields:

$$\begin{array}{c} L(j_1,\dots,j_{n+1},j_{1,\delta},\dots,j_{n+1,\delta}) = L(H_\delta \cap (\mathcal{S}\times\mathcal{T})) \\ \text{degree } d_{n+1} \Big| \\ \vdots \\ \text{degree } d_2 \Big| \\ L(j_1,\dots,j_{n+1},j_{1,\delta}) \\ \text{degree } d_1 \Big| \\ L(\mathcal{S})^\Sigma. \end{array}$$

where $d_i = [K_{i-1} : K_i]$ for $1 \leq i \leq n+1$. The modular equations of level δ are defining equations for the successive extensions in the tower.

Definition 3.1. The *modular equations* of level δ on $\mathcal{S}\times\mathcal{T}$ are the tuple $(\Psi_{\delta,1}, \Psi_{\delta,2}, \dots, \Psi_{\delta,n+1})$ defined as follows: for each $1 \leq m \leq n+1$, $\Psi_{\delta,m}$ is the multivariate polynomial in the m variables $Y_1,\dots,Y_m$ defined by

$$\Psi_{\delta,m} = \sum_{\gamma\in K_0/K_{m-1}} \left(\left(\prod_{i=1}^{m-1} \prod_{\gamma_i} \Big(Y_i - \gamma_i \cdot j_{i,\delta} \Big) \right) \prod_{\gamma_m \in K_{m-1}/K_m} \Big(Y_m - \gamma\gamma_m \cdot j_{m,\delta} \Big) \right)$$

where the middle product is over all $\gamma_i \in K_0/K_i$ such that $\gamma_i = \gamma$ modulo K_{i-1}, but $\gamma_i \neq \gamma$ modulo K_i. The expression for $\Psi_{\delta,m}$ makes sense, because multiplying γ on the right by an element in K_{m-1} only permutes the factors in the last product.

In the case of the Hecke correspondence considered in §3.1, the polynomial $\Psi_{\delta,1}$ is precisely Q_ℓ. The precise formula is inspired from preexisting definitions of modular equations for abelian surfaces [3, 24, 25, 21]. We will return to these examples in §3.3 and §3.4.

Let us give elementary properties of modular equations. First, we need a lemma.

Lemma 3.2. *Let $\gamma,\gamma' \in K_0$ and $1 \leq i \leq n+1$. Assume that the equality $\gamma \cdot j_{i,\delta} = \gamma' \cdot j_{i,\delta}$ holds on one connected component of $\mathcal{S}''$. Then it holds on all connected components of $\mathcal{S}''$.*

Proof. Write $\gamma = (k,\sigma)$ and $\gamma' = (k',\sigma')$ where $k,k' \in K$ and $\sigma,\sigma' \in \Sigma$. Let $c \in G(\mathbb{A}_f)$ be an adelic element of G defining the connected component $\mathcal{S}$ in $\mathrm{Sh}_K(\mathbb{C})$, so that $\mathcal{S} = \Gamma_c\backslash X_+$ with $\Gamma_c = G(\mathbb{Q})_+ \cap cKc^{-1}$. By assumption, there exists an element $g \in G(\mathbb{A}_f)$ such that $g = c$ in the double quotient space $G(\mathbb{Q})_+\backslash G(\mathbb{A}_f)/K$, and

$$\forall x \in X_+,\ j_{i,\delta}\big([\sigma^{-1}(x), \sigma^{-1}(gk)]\big) = j_{i,\delta}\big([\sigma'^{-1}(x), \sigma'^{-1}(gk')]\big). \tag{6}$$

Since H_δ is absolutely irreducible, we have $G(\mathbb{Q})_+\backslash G(\mathbb{A}_f)/K = G(\mathbb{Q})_+\backslash G(\mathbb{A}_f)/K'$. Using the description of connected components of a PEL Shimura variety in §2.1, and the fact that the action Σ leaves ν invariant, we find that there exist $\gamma_1,\gamma_2 \in G(\mathbb{Q})_+$ such that $gk = \gamma_1\sigma(c) \bmod \sigma(K')$ and $gk' = \gamma_2\sigma'(c) \bmod \sigma'(K')$. Then equation (6) is equivalent to the following:

$$\forall x \in X_+,\ j_{i,\delta}\big([x,c]\big) = j_{i,\delta}\big([\sigma'^{-1}(\gamma_2^{-1}\gamma_1\sigma(x)), c]\big). \tag{7}$$

Note that $\gamma_2^{-1}\gamma_1$ is well-defined and independent of g, up to multiplication on the left by an element of $G(\mathbb{Q})_+ \cap \sigma'(cK'c^{-1})$, and on the right by an element of $G(\mathbb{Q})_+ \cap \sigma(cK'c^{-1})$. Therefore equation (7) holds for every $g \in G(\mathbb{A}_f)$ such that $g = c$ in $G(\mathbb{Q})_+ \backslash G(\mathbb{A}_f)/K$. In other words, the equality $\gamma \cdot j_{i,\delta} = \gamma' \cdot j_{i,\delta}$ holds on every connected component of $\mathcal{S}''$. □

Proposition 3.3. *Let $1 \leq m \leq n+1$, and let $\gamma \in K_0/K_{m-1}$. Then, up to multiplication by an element in $L(j_1, \dots, j_{n+1}, \gamma \cdot j_{1,\delta}, \dots, \gamma \cdot j_{m-1,\delta})^\times$, we have*

$$\Psi_{\delta,m}(\gamma \cdot j_{1,\delta}, \dots, \gamma \cdot j_{m-1,\delta}, Y_m) = \prod_{\gamma_m \in K_{m-1}/K_m} \Big(Y_m - \gamma\gamma_m \cdot j_{m,\delta}\Big).$$

Proof. By Definition 3.1, the above equality holds true after multiplying the right hand side by

$$f = \prod_{i=1}^{m-1} \prod_{\substack{\gamma_i \in K_0/K_i \\ \gamma_i \neq \gamma \\ \gamma_i = \gamma \bmod K_{i-1}}} \Big(\gamma \cdot j_{i,\delta} - \gamma_i \cdot j_{i,\delta}\Big)$$

The function f a product of nonzero modular functions on $\mathcal{S}''$ defined over L. In order to show that $f \in L(j_1, \dots, j_{n+1}, \gamma \cdot j_{1,\delta}, \dots, \gamma \cdot j_{m-1,\delta})$, we check that f is invariant under the action of $\gamma K_{m-1}\gamma^{-1}$. By definition of the subgroups K_i, no factor of f is identically zero on $\mathcal{S}''$. Therefore f is invertible by Lemma 3.2. □

Let $1 \leq m \leq n+1$. Proposition 3.3 implies that up to scaling, the univariate polynomial $\Psi_{\delta,m}(j_{1,\delta}, \dots, j_{m-1,\delta}, Y_m)$ is the minimal polynomial of $j_{m,\delta}$ over the field $L(j_1, \dots, j_{n+1}, j_{1,\delta}, \dots, j_{m-1,\delta})$. In other words, when the multiplicative coefficient in Proposition 3.3 does not vanish, which is generically the case, $\Psi_{\delta,m}$ provides all the possible values for $j_{m,\delta}$ once $j_1, \dots, j_{n+1}$ and $j_{1,\delta}, \dots, j_{m-1,\delta}$ are known. In particular, modular equations vanish on H_δ as promised.

We could also define other modular equations $\Phi_{\delta,m}$ for which there is true equality in Proposition 3.3, as in the case of the classical modular polynomial Φ_l, but they have a more complicated expression. In practice, using the polynomials $\Psi_{\delta,m}$ is more convenient as they are typically smaller.

Proposition 3.4. *Let $1 \leq m \leq n+1$. The coefficients of $\Psi_{\delta,m}$ lie in $L(j_1, \dots, j_{n+1})$. The degree of $\Psi_{\delta,m}$ in Y_m is $[K_{m-1} : K_m]$, and for each $1 \leq i < m$, the degree of $\Psi_{\delta,m}$ in Y_i is at most $[K_{i-1} : K_i] - 1$.*

Proof. It is clear from Definition 3.1 that the action of K_0 leaves $\Psi_{\delta,m}$ invariant. Hence the coefficients of $\Psi_{\delta,m}$ are rational functions on $\mathcal{S}$ invariant under Σ and defined over L, so the first statement holds. The second part is obvious. □

In general, using a nontrivial Σ increases the degree of modular equations. This has a geometric interpretation: modular equations describe the Hecke correspondence H_δ and its conjugates under Σ simultaneously.

Let $J_1, \dots, J_{n+1}$ be indeterminates, and let $1 \leq m \leq n+1$. By the equation (5) satisfied by j_{n+1} on $\mathcal{S}$, there exists a unique element of the ring $L(J_1, \dots, J_n)[J_{n+1}, Y_1, \dots, Y_m]$ with degree at most $e-1$ in J_{n+1} which, when evaluated at $J_i = j_i$ for $1 \leq i \leq n+1$, yields $\Psi_{\delta,m}$. In the sequel, we also denote it by $\Psi_{\delta,m}$ for simplicity. Therefore the coefficients of $\Psi_{\delta,m}$ will be either functions on $\mathcal{S}$, i.e. as elements of $L(j_1, \dots, j_{n+1})$, or multivariate rational fractions in the indeterminates $J_1, \dots, J_{n+1}$ that are polynomial in J_{n+1} of degree at most $e-1$, depending on the context.

Remark 3.5. In several cases, the function $j_{1,\delta}$ already generates the whole extension of function fields, so that $K_1 = \cdots = K_{n+1} = K'$,

$$\Psi_{\delta,1} = \prod_{\gamma_1 \in K_0/K'} \big(Y_1 - \gamma_1 \cdot j_{1,\delta}\big),$$

and for every $2 \leq m \leq n+1$,

$$\Psi_{\delta,m} = \sum_{\gamma \in K_0/K'} \left(\left(\prod_{\gamma_1 \neq \gamma} \big(Y_1 - \gamma_1 \cdot j_{1,\delta}\big) \right) \big(Y_m - \gamma \cdot j_{m,\delta}\big) \right). \tag{8}$$

In this case, for each $2 \leq m \leq n+1$, we have $\Psi_{\delta,m}(j_{1,\delta}) = \partial_{Y_1}\Psi_{\delta,1}(j_{1,\delta})(Y_m - j_{m,\delta})$, where ∂_{Y_1} denotes derivative with respect to Y_1. Therefore $\Psi_{\delta,m}$ is just the expression of $j_{m,\delta}$ as an element of $L(\mathcal{S})^{\Sigma}[\, j_{1,\delta}]$ in a compact representation inspired from [14].

In this case, we often keep only the constant term in equation (8), and consider the modular equations $\Psi_{\delta,m}$ for $2 \leq m \leq n+1$ as elements of the ring $L(J_1, \ldots, J_n)[J_{n+1}, Y]$ with degree at most e in J_{n+1}, defined by

$$\Psi_{\delta,m}(j_1, \ldots, j_{n+1}) = \sum_{\gamma \in K_0/K'} \big(\gamma \cdot j_{m,\delta}\big) \prod_{\gamma_1 \neq \gamma} \big(Y - \gamma_1 \cdot j_{1,\delta}\big).$$

Then, we simply have $j_{m,\delta} = \Psi_{\delta,m}(j_{1,\delta})/\partial_{Y_1}\Psi_{\delta,1}(j_{1,\delta})$.

3.3. **Modular equations of Siegel type for abelian surfaces.** The Siegel modular varieties are prominent examples of PEL Shimura varieties. They are moduli spaces for complex abelian varieties of dimension g with a certain polarization and level structure. Another example is given by the Hilbert modular varieties, for which the PEL structure contains an additional real multiplication embedding. In this subsection and the next, we explain how these examples fit in the general setting of PEL Shimura varieties, and we show that modular equations of Siegel and Hilbert type in dimension 2 [24, 25] are special cases of modular equations as defined above.

Siegel moduli spaces. Let $g \geq 1$. The *Siegel modular variety* of dimension g [27, §6] is obtained by taking $B = \mathbb{Q}$, with trivial involution $*$, and taking the symplectic module (V, ψ) to be $V = \mathbb{Q}^{2g}$ with

$$\forall u, v \in V,\ \psi(u,v) = u^t \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix} v.$$

Then $G = \mathrm{GSp}_{2g}$. The $\mathbb{Q}$-algebra B is simple of type (C). We can choose X_+ to be the set of all complex structures on $V(\mathbb{R})$ that are positive for ψ [27, §6], and we have

$$G(\mathbb{R})_+ = \{g \in G(\mathbb{R}) \mid \mu(g) > 0\}.$$

The reflex field is $\mathbb{Q}$ [27, §14]. Generalizing the example of modular curves, we can identify X_+ with the Siegel upper half-space $\mathbb{H}_g$ endowed with the usual action of $\mathrm{GSp}_{2g}(\mathbb{R})_+$:

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot \tau = (a\tau + b)(c\tau + d)^{-1}$$

for every $\tau \in \mathbb{H}_g$ and $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G(\mathbb{R})_+$, where a, b, c, and d are $g \times g$ blocks.

Let $(e_1, \ldots, e_{2g})$ be the canonical basis of $V(\mathbb{Q})$. Choose positive integers $D_1 | \cdots | D_g$ such that $D_1 = 1$, and let $\Lambda_0 \subset V(\mathbb{Q})$ be the lattice generated by $e_1, \ldots, e_g, D_1 e_{g+1}, \ldots, D_g e_{2g}$.

Then the type of the polarization ψ on Λ_0 is a product of cyclic groups of order $D_1, \dots, D_g$; we also say that ψ is of type $(D_1, \dots, D_g)$. Let K be a compact open subgroup of $G(\mathbb{A}_f)$ that stabilizes $\Lambda_0 \otimes \widehat{\mathbb{Z}}$, and let $\mathcal{S}$ be the connected component of $\mathrm{Sh}_K(\mathbb{C})$ defined by the identity matrix in $G(\mathbb{A}_f)$. Then $\mathcal{S}$ is identified with the quotient $\Gamma \backslash \mathbb{H}_g$, where

$$\Gamma = \mathrm{GSp}_{2g}(\mathbb{Q})_+ \cap K = \mathrm{Sp}_{2g}(\mathbb{Q}) \cap K.$$

By Proposition 2.3, $\mathcal{S}$ is a moduli space for polarized abelian varieties with polarization type $(D_1, \dots, D_g)$ and level K structure such that $H_1(A, \mathbb{Z})$ is isomorphic to the standard polarized lattice to (Λ_0, ψ). This modular interpretation coincides with the classical one [2, §8.1]. Also, modular forms on $\mathcal{S}$ can be identified with Siegel modular forms in the classical sense, as we mentioned in §3.1 in the case $g = 1$.

Siegel modular equations. We now focus on the special case given by

$$g = 2,\ D_1 = D_2 = 1,\ \Lambda_0 = \mathbb{Z}^{2g},\ K = \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}}).$$

Then $\mathrm{Sh}_K(\mathbb{C})$ has only one connected component defined over $\mathbb{Q}$, and classifies principally polarized abelian surfaces over $\mathbb{C}$. Modular forms on Sh_K are identified with classical Siegel modular forms of level $\mathrm{Sp}_4(\mathbb{Z})$. As shown by Igusa [17], the graded $\mathbb{Q}$-algebra of these modular forms is generated by four elements of respective weights 4, 6, 10, and 12. These generators can be taken to be I_4, I'_6, I_{10}, and I_{12} in Streng's notation [33, p. 42]. The function field of Sh_K over $\mathbb{Q}$ is therefore generated by the three algebraically independent *Igusa invariants*:

$$j_1 = \frac{I_4 I'_6}{I_{10}}, \quad j_2 = \frac{I_4^2 I_{12}}{I_{10}^2}, \quad j_3 = \frac{I_4^5}{I_{10}^2}.$$

Let ℓ be a prime, and consider the Hecke correspondence of level

$$\delta = \begin{pmatrix} \ell I_2 & 0 \\ 0 & I_2 \end{pmatrix} \qquad \text{as a } 4 \times 4 \text{ matrix in } 2 \times 2 \text{ blocks.}$$

The group $K \cap \delta K \delta^{-1} \cap G(\mathbb{Q})_+$ is usually denoted by $\Gamma^0(\ell)$, and the degree of H_δ is

$$d(\delta) = \ell^3 + \ell^2 + \ell + 1.$$

The Hecke correspondence H_δ is absolutely irreducible, and describes all principally polarized abelian surfaces ℓ-isogeous to a given one; the degree of these isogenies is $l(\delta) = \ell^2$. In this case, the function $j_{1,\delta}$ generates the function field on the Hecke correspondence [3, Lem. 4.2], so that $d_1 = d(\delta)$ and $d_2 = d_3 = 1$, in the notation of §3.2. The modular equations from Definition 3.1 are called the Siegel modular equations of level ℓ in Igusa invariants. They have been computed for $\ell = 2$ and $\ell = 3$ [24].

Hilbert moduli spaces. Let F be a totally real number field of degree g over $\mathbb{Q}$, and let $B = F$ with trivial involution $*$. The $\mathbb{Q}$-algebra B is simple of type (C). Let $V = F^2$, which is a $\mathbb{Q}$-vector space of dimension $2g$, and define the symplectic form ψ on V as follows:

$$\forall a, b, c, d \in F,\ \psi\big((a, b), (c, d)\big) = \mathrm{Tr}_{F/\mathbb{Q}}(ad - bc).$$

Then (V, ψ) is a faithful symplectic $(B, *)$-module, where B acts on V by multiplication. The associated algebraic group is $G = \mathrm{GL}_2(F)$. The g real embeddings of F induce identifications

$$V(\mathbb{R}) = (\mathbb{R}^2)^g \quad \text{and} \quad G(\mathbb{R}) = \prod_{i=1}^{g} \mathrm{GL}_2(\mathbb{R}).$$

The subgroup $G(\mathbb{R})_+$ consists of matrices with totally positive determinant.

There is a particular complex structure $x_0 \in G(\mathbb{R})$ on $V(\mathbb{R})$ given by

$$x_0 = \left(\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix} \right) \right)_{1 \leq i \leq g}.$$

Let X_+ be the $G(\mathbb{R})_+$-conjugacy class of x_0. Then (G, X_+) is called a *Hilbert Shimura datum*. Its reflex field is $\mathbb{Q}$: see [35, §X.4] when $g = 2$, and [27, Ex. 12.4] in general. The domain X_+ can be identified with $\mathbb{H}_1^g$, where $\mathbb{H}_1$ is the complex upper half-plane, endowed with the action of $\mathrm{GL}_2(\mathbb{R})_+$ on each coordinate.

Let $\mathbb{Z}_F$ be the integer ring of F, and take $\Lambda_0 = \mathbb{Z}_F \oplus \mathbb{Z}_F^\vee$, where $\mathbb{Z}_F^\vee$ is the dual of $\mathbb{Z}_F$ with respect to the trace form. Then the stabilizer of Λ_0 in B is $\mathbb{Z}_F$, and ψ is principal on Λ_0. Let K be a compact open subgroup of $\mathrm{GL}(\Lambda_0 \otimes \widehat{\mathbb{Z}})$.

Remark 3.6. In the Hilbert setting, the group $\mu(\Gamma_c)$ is not equal to $\mu(\mathcal{E})$ in general. For instance, if $K = \mathrm{GL}(\Lambda_0 \otimes \widehat{\mathbb{Z}})$, and $c = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right)$, then

$$\Gamma_c = G(\mathbb{R})_+ \cap K = \{g \in \mathrm{GL}(\Lambda_0) \mid \det(g) \text{ is totally positive}\},$$

so $\mu(\Gamma_c)$ is the set of totally positive units in $\mathbb{Z}_F$. On the other hand, $\mu(\mathcal{E})$ is the set of all squares of units. For instance, if $g = 2$, then $\mu(\mathcal{E}) = \mu(\Gamma_c)$ if and only if the fundamental unit in $\mathbb{Z}_F$ has negative norm.

We now assume that K has been chosen in such a way that

$$G(\mathbb{Q})_+ \cap K = \left\{ g \in \mathrm{GL}(\Lambda_0) \mid \mu(g) \in \mathbb{Z}_F^{\times 2} \right\}. \tag{9}$$

The Shimura variety $\mathrm{Sh}_K(G, X_+)(\mathbb{C})$ has several connected components: the narrow class group of F is a quotient of $\pi_0(\mathrm{Sh}_K(\mathbb{C}))$ [35, Cor. I.7.3]. Let $\mathcal{S}$ be the connected component defined by the identity matrix in $G(\mathbb{A}_f)$. Then there is a natural isomorphism

$$\mathcal{S} = (G(\mathbb{Q})_+ \cap K) \backslash \mathbb{H}_1^g \simeq \mathrm{SL}(\mathbb{Z}_F \oplus \mathbb{Z}_F^\vee) \backslash \mathbb{H}_1^g.$$

By Proposition 2.3, the component $\mathcal{S}$ parametrizes principally polarized abelian varieties with real multiplication by $\mathbb{Z}_F$ and level K structure such that $H_1(A, \mathbb{Z})$ is isomorphic to the polarized lattice (Λ_0, ψ) with its additional data. The modular forms of weight w on $\mathcal{S}$ are identified with the classical Hilbert modular forms of weight $(w, w, \ldots, w)$ for F and level $\mathrm{SL}(\mathbb{Z}_F \oplus \mathbb{Z}_F^\vee)$ [13, §4].

In the special case $g = 2$, let $\Sigma = \{1, \sigma\}$, where σ is the involution of V coming from real conjugation in F. On $G(\mathbb{R})_+$, the involution σ acts as permutation of the two factors. Modular forms that are symmetric under Σ are symmetric Hilbert modular forms in dimension 2 in the usual sense [5, §1.3].

Hilbert modular equations. Let F be a real quadratic field, and assume moreover that the fundamental unit of F has negative norm; then $K = \mathrm{GL}(\Lambda_0 \otimes \widehat{\mathbb{Z}})$ satisfies (9). Let $\beta \in \mathbb{Z}_F$ be totally positive and prime, and let

$$\delta = \begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix} \in G(\mathbb{A}_f).$$

The Hecke correspondence H_δ is absolutely irreducible, has degree $d(\delta) = N_{F/\mathbb{Q}}(\beta)+1$, and parametrizes isogenies of degree $l(\delta) = N_{F/\mathbb{Q}}(\beta)$. One can check that H_δ intersects $\mathcal{S} \times \mathcal{S}$ nontrivially. Being able to consider this Hecke correspondence is the reason for our different choice of G in §2 compared to [27, §8].

As invariants on $\mathcal{S}$, one possibility is to use the pullback of Igusa invariants by the forgetful map to the Siegel threefold, i.e. the Siegel moduli space for $g = 2$ [20]. They are symmetric with respect to Σ, and the equation relating these three invariants is the equation of the associated *Humbert surface*, the image of the Hilbert surface $\mathcal{S}$ inside the Siegel threefold. In this case, the modular equations describe simultaneously β- and $\sigma(\beta)$-isogenies [25].

In special cases, the field of Σ-invariant modular functions can be generated by two elements called *Gundlach invariants*. This reduction of the number of variables is interesting in practice. For instance, if $F = \mathbb{Q}(\sqrt{5})$, then the graded $\mathbb{Q}$-algebra of symmetric Hilbert modular forms is free over three generators F_2, F_6, and F_{10} of respective weights 2, 6, and 10 [15]; therefore, $L(\mathcal{S})^\Sigma = \mathbb{Q}(g_1, g_2)$ where the Gundlach invariants g_1 and g_2 are defined by

$$g_1 = \frac{F_2^5}{F_{10}}, \quad g_2 = \frac{F_2^2 F_6}{F_{10}}.$$

Moreover, g_1 and g_2 are algebraically independent. The associated modular equations are called the Hilbert modular equations of level β in Gundlach invariants for $F = \mathbb{Q}(\sqrt{5})$, and have been computed up to $N_{F/\mathbb{Q}}(\beta) = 59$ [23]. They also describe both β- and $\sigma(\beta)$-isogenies.

4. Degree estimates for modular equations

We fix a PEL setting as in §3.2; in particular we make a choice of invariants $j_1, \dots, j_{n+1}$ on the Shimura components $\mathcal{S}$ and $\mathcal{T}$. Let $\delta \in G(\mathbb{A}_f)$, and assume that the Hecke correspondence H_δ intersects $\mathcal{S} \times \mathcal{T}$ nontrivially. In Definition 3.1, we defined the modular equations $\Psi_{\delta,1}, \dots, \Psi_{\delta,n+1}$; they are multivariate polynomials in the variables $Y_1, \dots, Y_{n+1}$ describing H_δ and its conjugates under Σ. Their coefficients are uniquely determined rational fractions in $L(J_1, \dots, J_n)[J_{n+1}]$ of degree at most e in J_{n+1}, where the integer e is defined as in equation (5). The goal of this section is to prove the upper bounds on the degree of the coefficients of the modular equations $\Psi_{\delta,m}$ given in the first part of Theorem 1.1. We also give explicit variants in the case of modular equations for abelian surfaces. As indicated in the introduction, the proof works by identifying a denominator of the modular equations, then by analyzing the degree of the rational fractions we obtain when rewriting a quotient of modular forms of bounded weights in terms of the invariants $j_1, \dots, j_{n+1}$.

4.1. The common denominator of $\Psi_{\delta,m}$.

We keep the notation used in §3.2: in particular

$$K' = K \cap \delta K \delta^{-1}, \quad K_0 = K \rtimes \Sigma,$$

and K'' is a normal subgroup of finite index in K, contained in K' and stabilized by Σ. The natural action of K_0 on modular functions of level K'' extends to an action on modular forms.

For each $1 \leq i \leq n+1$, fix a nonzero modular form χ_i invariant under Σ and defined over L such that $\chi_i j_i$ is again a modular form (i.e. has no poles); we say

that χ_i is a *denominator* of j_i. This is possible by Proposition 2.6. For each i, the function

$$\chi_{i,\delta} \ : \ [x,g] \mapsto \chi_i([x,g\delta])$$

is a modular form of weight $\mathrm{wt}(\chi_i)$ on the preimage of $\mathcal{S}$ in $\mathrm{Sh}_{K'}(\mathbb{C})$. We define the functions $g_{\delta,m}$ on $\mathcal{S}$ for $1 \leq m \leq n+1$ as follows:

$$g_{\delta,m} = \prod_{i=1}^{m} \prod_{\gamma \in K_0/K'} \gamma \cdot \chi_{i,\delta}.$$

Lemma 4.1. *For every $1 \leq m \leq n+1$, the function $g_{\delta,m}$ is a nonzero symmetric modular form on $\mathcal{S}$, and*

$$\mathrm{wt}(g_{\delta,m}) = (\#\Sigma)\, d(\delta) \sum_{i=1}^{m} \mathrm{wt}(\chi_i).$$

Proof. By construction, the function $g_{\delta,m}$ is a modular form of level K'' and weight $\sum_{i=1}^{m} \#(K_0/K')\ \mathrm{wt}(\chi_i)$. We have $\#(K_0/K') = (\#\Sigma)\, d(\delta)$. Each modular form $\gamma \cdot \chi_{i,\delta}$ is nonzero on every connected component of $\mathrm{Sh}_{K''}(\mathbb{C})$ above $\mathcal{S}$, hence $g_{\delta,m}$ is nonzero as well.

Acting by an element of K_0 permutes the factors in the product defining $g_{\delta,m}$, so $g_{\delta,m}$ is in fact a symmetric modular form on $\mathcal{S}$. □

Proposition 4.2. *For every $1 \leq m \leq n+1$, the coefficients of the multivariate polynomial $g_{\delta,m}\Psi_{\delta,m}$ are symmetric modular forms on $\mathcal{S}$.*

Proof. By Definition 3.1, the polynomial $\Psi_{\delta,m}$ is a sum of terms of the form

$$\left(\prod_{i=1}^{m-1} \prod_{\gamma_i} \Big(Y_i - \gamma_i \cdot j_{i,\delta} \Big) \right) \prod_{\gamma_m \in K_{m-1}/K_m} \Big(Y_m - \gamma\gamma_m \cdot j_{m,\delta} \Big)$$

where $\gamma \in K_0$ is fixed, and the middle product is over all $\gamma_i \in K_0/K_i$ such that $\gamma_i = \gamma$ modulo K_{i-1}, but $\gamma_i \neq \gamma$ modulo K_i. In this expression, all the cosets γ_i and $\gamma\gamma_m$ are simultaneously disjoint as subsets of K_0/K'. Each denominator is accounted for by some factor in the product defining $g_{\delta,m}$, so the coefficients of $g_{\delta,m}\Psi_{\delta,m}$ are modular forms. □

When the modular functions $j_1, \ldots, j_{n+1}$ have similar denominators, it is possible to make a better choice for $g_{\delta,m}$.

Proposition 4.3. *Assume that there exists a modular form χ on $\mathcal{S}$ such that for every i, we have $\chi_i = \chi^{\alpha_i}$ for some integer $\alpha_i \geq 0$. Let $1 \leq m \leq n+1$, and define*

$$g_{\delta,m} = \Big(\prod_{\gamma \in K_0} \gamma \cdot \chi_\delta \Big)^{\alpha}, \qquad \text{where } \alpha = \max_{1 \leq i \leq m} \alpha_i.$$

Then $g_{\delta,m}$ is a nonzero symmetric modular form on $\mathcal{S}$, and

$$\mathrm{wt}(g_{\delta,m}) = (\#\Sigma)\ d(\delta)\, \alpha\, \mathrm{wt}(\chi).$$

Moreover, the coefficients of $g_{\delta,m}\Psi_{\delta,m}$ are symmetric modular forms on $\mathcal{S}$.

The proof is similar to that of Proposition 4.2, and omitted.

4.2. **Writing quotients of modular forms in terms of invariants.** Let f/g be a quotient of symmetric modular forms of weight w on $\mathcal{S}$. We show that when we rewrite such a quotient in terms of the invariants $j_1, \dots, j_{n+1}$, the degree of the rational fractions we obtain is bounded linearly in w. To make the proportionality constant explicit, we define the *symmetric geometric complexity* of our invariants as follows.

Definition 4.4. Let f_k for $1 \le k \le r$ be nonzero generators over L for the graded ring of symmetric modular forms on $\mathcal{S}$, with respective weights w_k. For each $1 \le k \le r-1$, let $\beta_k \ge 1$ be the minimal integer such that

$$\beta_k w_k \in \mathbb{Z}w_{k+1} + \cdots + \mathbb{Z}w_r.$$

We can find nonzero modular forms $\lambda_k, \xi_k \in L[f_{k+1}, \dots, f_r]$ such that $\mathrm{wt}(\lambda_k) - \mathrm{wt}(\xi_k) = \beta_k w_k$. For every $1 \le k \le r-1$, the function $\xi_k f_k^{\beta_k}/\lambda_k$ is a quotient of two symmetric modular forms of the same weight on $\mathcal{S}$; hence there exist polynomials $P_k, Q_k \in L[J_1, \dots, J_{n+1}]$ such that

$$\frac{\xi_k f_k^{\beta_k}}{\lambda_k} = \frac{P_k(j_1, \dots, j_{n+1})}{Q_k(j_1, \dots, j_{n+1})}.$$

Denote the total degrees of P_k and Q_k by $\deg(P_k)$ and $\deg(Q_k)$ respectively. We define the *symmetric geometric complexity* of $j_1, \dots, j_{n+1}$ relative to the choice of $f_k, \lambda_k, \psi_k, P_k, Q_k$ to be the positive rational number given by, either

(1)
$$\left(1 + \max_{1 \le k \le r-1} \frac{\mathrm{wt}(\xi_k)}{\beta_k w_k}\right) \max_{1 \le k \le r-1} \frac{\deg(P_k)}{\beta_k w_k + \mathrm{wt}(\xi_k)},$$
if the following conditions are satisfied: for every $1 \le k \le r-1$, the modular forms λ_k and ξ_k are powers of f_r and f_{r-1} respectively (in particular $\xi_{r-1} = 1$), and $Q_k = 1$; or

(2)
$$\sum_{k=1}^{r-1} \left(\frac{1}{\beta_k w_k} \max\bigl\{\deg(P_k), \deg(Q_k)\bigr\} \prod_{l=1}^{k-1} \left(1 + \frac{\mathrm{wt}(\xi_l)}{\beta_l w_l}\right)\right),$$
otherwise.

Note that formula 1, when it applies, yields a smaller result than formula 2.

The *symmetric geometric complexity* of $j_1, \dots, j_{n+1}$, denoted by $\mathrm{SGC}(j_1, \dots, j_{n+1})$, is the infimum of this quantity over all possible choices of modular forms f_k, λ_k, ξ_k and polynomials P_k, Q_k.

Given Definition 4.4, explicit upper bounds on the geometric complexity are easy to obtain if a generating set of modular forms is known. Note that the symmetric geometric complexity is invariant under permutations of the invariants $j_1, \dots, j_{n+1}$, in contrast with their *geometric complexity* to be defined later, which takes into account the fact that j_{n+1} is considered differently in equation (5).

Proposition 4.5. *Let $w \ge 0$, let f, g be symmetric modular forms on $\mathcal{S}$ of weight w, and assume that g is nonzero. Then there exist polynomials $P, Q \in L[J_1, \dots, J_{n+1}]$ of total degree at most $\mathrm{SGC}(j_1, \dots, j_{n+1})w$ such that*

$$\frac{f}{g} = \frac{P(j_1, \dots, j_{n+1})}{Q(j_1, \dots, j_{n+1})}.$$

Moreover, Q can be chosen independently of f.

Proof. We keep the notation used in Definition 4.4, and make a choice of generators f_k for $1 \le k \le r$, modular forms λ_k, ξ_k for $1 \le k \le r-1$, and polynomials $P_k, Q_k \in L[J_1, \dots, J_{n+1}]$ for $1 \le k \le r-1$. Let C be symmetric geometric complexity of $j_1, \dots, j_{n+1}$ relative to this choice.

Let f, g be as in the proposition. Then f and g can be expressed as a sum of monomial terms of the form

$$c f_1^{\alpha_1} \cdots f_r^{\alpha_r} \qquad \text{with } c \in L \text{ and } \sum_{k=1}^{r} \alpha_k w_k = w.$$

We give algorithms to rewrite the fraction $P/Q = f/g$ (currently a rational fraction in terms of the modular forms f_k) as a fraction of invariants, and bound the total degree of the output.

Case 1 of Definition 4.4. We assume that λ_k and ξ_k are powers of f_r and f_{r-1} respectively for every $1 \le k \le r-1$. In this case, for each $1 \le k \le r-2$, the integer β_k can be seen as the order of w_k in the group $\mathbb{Z}/(\mathbb{Z}w_{r-1} + \mathbb{Z}w_r)$. We can write

$$w = \sum_{k=1}^{r-2} s_k w_k \pmod{\mathbb{Z}w_{r-1} + \mathbb{Z}w_r}$$

for some integers $0 \le s_k < \beta_k$, and this determines the integers s_k uniquely (if such a linear combination vanishes, considering the smallest nonzero s_k yields a contradiction). Then each monomial appearing in P and Q is divisible by $f_1^{s_1} \cdots f_{r-2}^{s_{r-2}}$. After simplifying by this common factor, we can assume that the common weight w of P and Q satisfies $w \in \mathbb{Z}w_{r-1} + \mathbb{Z}w_r$. Then, for each $1 \le k \le r-2$, the exponent of f_k in each monomial of P and Q is divisible by β_k. For convenience, write

$$a = \max_{1 \le k \le r-1} \frac{\operatorname{wt}(\xi_k)}{\beta_k w_k}.$$

In order to rewrite P/Q in terms of invariants, we proceed as follows.

(1) Multiply P and Q by $f_{r-1}^{\lfloor aw/\operatorname{wt}(f_{r-1})\rfloor}$.
(2) For each $1 \le k \le r-2$, replace each occurence of $f_k^{\beta_k}$ by $\lambda_k P_k/\xi_k$ in P and Q.
(3) Let $0 \le s_{r-1} < \beta_{r-1}$ be such that $w = s_{r-1}w_{r-1} \mod w_r$, and divide P and Q by $f_{r-1}^{s_{r-1}}$.
(4) Replace each occurence of $f_{r-1}^{\beta_{r-1}}$ by $\lambda_{r-1}P_{r-1}$ in P and Q.
(5) Finally, divide P and Q by $f_r^{(w - s_{r-1}w_{r-1})/w_r}$.

This algorithm runs independently on each monomial of P and Q. Let $M = c\prod_{k=1}^{r} f_k^{\alpha_k}$, with $c \in L$, be such a monomial after step 1. Let us show that the exponent of f_{r-1} in M remains nonnegative after step 2. In this step, we introduce a denominator given by

$$\prod_{k=1}^{r-2} \xi_k^{\alpha_k/\beta_k} = \prod_{k=1}^{r-2} f_{r-1}^{\frac{\operatorname{wt}(\xi_k)\alpha_k}{\operatorname{wt}(f_{r-1})\beta_k}}.$$

We have

$$\sum_{k=1}^{r-2} \frac{\mathrm{wt}(\xi_k)\alpha_k}{\mathrm{wt}(f_{r-1})\beta_k} \leq a \sum_{k=1}^{r-2} \frac{\alpha_k w_k}{\mathrm{wt}(f_{r-1})} \leq \frac{aw}{\mathrm{wt}(f_{r-1})},$$

hence

$$\sum_{k=1}^{r-2} \frac{\mathrm{wt}(\xi_k)\alpha_k}{\mathrm{wt}(f_{r-1})\beta_k} \leq \left\lfloor \frac{aw}{\mathrm{wt}(f_{r-1})} \right\rfloor \leq \alpha_{r-1} \qquad \text{by step 1}$$

because the left hand side is an integer. Therefore, at the end of step 2, M belongs to the polynomial ring $L[J_1, \ldots, J_{n+1}][f_{r-1}, f_r]$. Hence, we have $M \in L[J_1, \ldots, J_{n+1}][f_{r-1}^{\beta_{r-1}}, f_r]$ after step 3, and finally $M \in L[J_1, \ldots, J_{n+1}]$ after step 5.

It remains to bound the total degree of M after step 5. To do this, we consider the total weight of M in $f_1, \ldots, f_{r-1}$. For each $1 \leq k \leq r-1$, the modular form λ_k is a power of f_r; hence replacing $f_k^{\beta_k}$ by $\lambda_k P_k/\xi_k$ in steps 2 or 4 reduces this weight by $\beta_k w_k + \mathrm{wt}(\xi_k)$, and increases the total degree of M in $J_1, \ldots, J_{n+1}$ by at most $\deg(P_k)$. At the beginning of step 2, the total weight of M in $f_1, \ldots, f_{r-1}$ is at most $(1+a)w$. Therefore the total degree of M in $J_1, \ldots, J_{n+1}$ at the end of the algorithm is bounded above by

$$(1+a)w \max_{1 \leq k \leq r-1} \frac{\deg(P_k)}{\beta_k w_k + \deg(\xi_k)} = Cw.$$

Case 2 of Definition 4.4. In the general case, we perform replacements and simplifications in a sequential way.

We start by defining integers z_k, d_k for $0 \leq k \leq r-1$ and s_k, a_k for $1 \leq k \leq r-1$ by induction as follows:

- $z_0 = w$ and $d_0 = 0$;
- For each $1 \leq k \leq r$, the integer $0 \leq s_k < \beta_k$ is defined by the relation
$$z_{k-1} = s_k w_k \pmod{\mathbb{Z}w_{k+1} + \cdots + \mathbb{Z}w_r};$$
- $a_k = \left\lfloor \frac{z_{k-1}}{\beta_k w_k} \right\rfloor$ for each $1 \leq k \leq r-1$;
- $z_k = z_{k-1} - s_k w_k + a_k \,\mathrm{wt}(\xi_k)$ for each $1 \leq k \leq r-1$;
- $d_k = d_{k-1} + a_k \max\{\deg(P_k), \deg(Q_k)\}$ for each $1 \leq k \leq r-1$.

In order to rewrite P/Q in terms of invariants, we use the following algorithm. For $k = 1$ up to $k = r-1$, do:

(1) Divide P and Q by $f_k^{s_k}$;
(2) Replace each occurence of $f_k^{\beta_k}$ by $\dfrac{\lambda_k P_k}{\xi_k Q_k}$ in P and Q;
(3) Multiply P and Q by $\xi_k^{a_k} Q_k^{a_k}$.

Finally, simplify the remaining occurences of f_r. We prove the following statement (H_k) by induction for every $1 \leq k \leq r$:

(H_k) At the beginning of the k-th loop, P and Q are elements of the ring $L[J_1, \ldots, J_{n+1}][f_k, \ldots, f_r]$ of weight z_{k-1}, with total degree at most d_{k-1} in $J_1, \ldots, J_{n+1}$, such that

$$\frac{f}{g} = \frac{P(j_1, \ldots, j_{n+1})}{Q(j_1, \ldots, j_{n+1})}.$$

The statement (H_1) is true by definition of z_0 and d_0; assume that (H_k) is true for some $k \geq 1$. Then we see, in order, that during the k-th loop:

- $z_{k-1} \in \sum_{i=k}^{r} \mathbb{Z} w_i$, so s_k is well defined.
- In each monomial of P and Q, the exponent of f_k is of the form $a\beta_k + s_k$ for some integer $a \leq a_k$. Therefore step 1 is an exact division, and after step 2 there are no more occurences of f_k in P or Q.
- After step 3, P and Q are elements of $L[J_1, \ldots, J_{n+1}][f_{k+1}, \ldots, f_r]$ of weight

$$z_{k-1} - s_k w_k + a_k \operatorname{wt}(\xi_k) = z_k.$$

It remains to show that the degree of P, Q in $J_1, \ldots, J_{n+1}$ is bounded by d_k after step 3. This comes from the following observation: during the k-th loop, we only multiply the polynomials in $J_1, \ldots, J_{n+1}$ already present by $P_k^b Q_k^{a_k - b}$ for some $0 \leq b \leq a_k$. This proves our claim (H_k) for all $1 \leq k \leq r$.

At the end of the algorithm, all the occurences of f_r cancel out. Therefore we obtain polynomials P and Q of total degree at most d_{r-1} such that

$$\frac{f}{g} = \frac{P(j_1, \ldots, j_{n+1})}{Q(j_1, \ldots, j_{n+1})}.$$

By induction, we obtain

$$z_k \leq w \prod_{l=1}^{k} \left(1 + \frac{\operatorname{wt}(\xi_l)}{\beta_l w_l}\right)$$

and

$$d_{r-1} \leq \sum_{k=1}^{r-1} \left(\frac{w}{\beta_k w_k} \max\{\deg(P_k), \deg(Q_k)\} \prod_{l=1}^{k-1} \left(1 + \frac{\operatorname{wt}(\xi_l)}{\beta_l w_l}\right)\right) = Cw.$$

In both cases 1 and 2, the algorithm runs independently on the numerator and denominator, hence Q can be chosen independently of f. □

4.3. **Degree bounds in canonical form.** Recall that the modular function j_{n+1} satisfies eq. (5): we have $E(j_1, \ldots, j_{n+1}) = 0$ where

$$E = \sum_{k=0}^{e} E_k(J_1, \ldots, J_n)\, J_{n+1}^k \in L[J_1, \ldots, J_n, J_{n+1}]$$

has degree e in J_{n+1} and is irreducible. Let d_E denote the total degree of E in the variables $J_1, \ldots, J_n$. In this section, we work in the ring $L(J_1, \ldots, J_n)[J_{n+1}]$ modulo E. We say that a fraction $R \in L(J_1, \ldots, J_{n+1})$ is in *canonical form* if R is a polynomial in J_{n+1} of degree at most $e - 1$.

Proposition 4.6. *Let $d \geq 0$, let $P, Q \in L[J_1, \ldots, J_{n+1}]$ be polynomials of total degree at most d, and assume that $Q(j_1, \ldots, j_{n+1})$ is not identically zero. Let $R \in L(J_1, \ldots, J_n)[J_{n+1}]$ be the fraction in canonical form such that $P/Q = R \mod E$. Then the total degree of R in $J_1, \ldots, J_n$ is bounded above by $(e + 2d_E)d$.*

Proof. In this proof, degrees and coefficients are taken with respect to the variable J_{n+1} unless otherwise specified. First, we invert the denominator Q. Consider the resultant

$$Z = \operatorname{Res}_{J_{n+1}}(Q, E) \in L[J_1, \ldots, J_n],$$

which is nonzero by hypothesis. Let $U, V \in L[j_1, \dots, j_{n+1}]$ be the associated Bézout coefficients, so that

$$Z = UQ + VE.$$

The inverse of Q modulo E is U/Z, so we have $P/Q = UP/Z \mod E$.

It is well-known that Z (resp. Q) has a polynomial expression of degree e (resp. $e-1$) in the coefficients of Q, and degree $\deg(Q)$ in the coefficients of E. Since the total degree of Q is at most d, the total degrees of Z and UP in $J_1, \dots, J_n$ are bounded above by $d(e + d_E)$. The degree of UP in J_{n+1} is at most $d + e - 1$.

Now, we reduce UP/Z modulo E to obtain a numerator of degree at most $e - 1$ in J_{n+1}. We can decrease this degree by 1 by multiplying above and below by $E_e(J_1, \dots, J_n)$ and using the relation

$$E_e J_{n+1}^e = -\sum_{k=0}^{e-1} E_k J_{n+1}^k \qquad \mod E.$$

When doing so, the total degree in $J_1, \dots, J_n$ increases by at most d_E. This operation is done at most d times; therefore the result has total degree at most $(e+2d_E)d$ in $J_1, \dots, J_n$ and degree at most $e-1$ in J_{n+1}. □

Definition 4.7. We define the *geometric complexity* of the invariants $j_1, \dots, j_{n+1}$ to be

$$\mathrm{GC}(j_1, \dots, j_{n+1}) = (e + 2d_E)\,\mathrm{SGC}(j_1, \dots, j_{n+1}) + e - 1.$$

This quantity depends on the choice of j_{n+1} as a distinguished invariant.

Proposition 4.8. *Let $w \geq 0$, let f, g be symmetric modular forms on $\mathcal{S}$ of weight w, and assume that g is nonzero. Let $R \in L(J_1, \dots J_n)[J_{n+1}]$ be the rational fraction in canonical form such that*

$$\frac{f}{g} = R(j_1, \dots, j_{n+1}).$$

Then the total degree of R in $J_1, \dots, J_{n+1}$ is bounded above by $\mathrm{GC}(j_1, \dots, j_{n+1})w$.

Proof. Combine Propositions 4.5 and 4.6. □

We are ready to prove the first part of Theorem 1.1 on degree bounds for modular equations, with an explicit expression for the constant C_1.

Theorem 4.9. *Let H_δ be an absolutely irreducible Hecke correspondence on $\mathcal{S} \times \mathcal{T}$ defined by an adelic element δ of G, and let $d(\delta)$ be the degree of H_δ. For each $1 \leq i \leq n+1$, let χ_i be a denominator of j_i as in §4.1. Let $1 \leq m \leq n+1$. Finally, let*

$$C_1 = GC(j_1, \dots, j_{n+1})\,(\#\Sigma) \sum_{i=1}^{m} \mathrm{wt}(\chi_i).$$

Then there exists a polynomial $D_m \in L[J_1, \dots, J_n]$ of total degree at most $C_1\, d(\delta)$ such that $D_m \Psi_{\delta,m}$ is a polynomial in $J_1, \dots, J_{n+1}, Y_1, \dots, Y_m$ whose total degree in $J_1, \dots, J_{n+1}$ is also bounded above by $C_1\, d(\delta)$. In particular, if $\mathcal{F} \in L(J_1, \dots, J_n)[J_{n+1}]$ is a coefficient of $\Psi_{\delta,m}$, then the total degree of $\mathcal{F}$ is bounded above by $C_1\, d(\delta)$.

Proof. Let $g_{\delta,m}$ be the modular form on $\mathcal{S}$ defined in §4.1, and let $\mathcal{F}$ be a coefficient of $\Psi_{\delta,m}$. By Proposition 4.2, the modular function $\mathcal{F}(j_1, \dots, j_{n+1})$ is of the

form $f/g_{\delta,m}$, where f is a modular form on $\mathcal{S}$ of weight $\mathrm{wt}(g_{\delta,m})$. By Lemma 4.1, we have

$$\mathrm{wt}(g_{\delta,m}) = (\#\Sigma)\, d(\delta) \sum_{i=1}^{m} \mathrm{wt}(\chi_i),$$

so the degree bound on $\mathcal{F}$ follows from Proposition 4.8. By Proposition 4.5, the denominator can be chosen independently of the coefficient of $\Psi_{\delta,m}$ we consider, hence the existence of a common denominator D_m of the correct total degree. □

4.4. **Explicit degree bounds in dimension 2.** Our methods provide new results about the degrees of the coefficients of modular equations of Siegel and Hilbert type for abelian surfaces, introduced in §3.3 and §3.4 respectively. In the Hilbert case, we restrict to the quadratic field $F = \mathbb{Q}(\sqrt{5})$, and consider modular equations in terms of Gundlach invariants.

In both cases, we can take $j_{n+1} = 1$ and $E = J_{n+1} - 1$ in the notation of §3.2. Then the notions of geometric complexity and symmetric geometric complexity coincide.

Lemma 4.10. *Let j_1, j_2, and j_3 denote the Igusa invariants on the Siegel threefold $\mathrm{Sp}_4(\mathbb{Z})\backslash\mathbb{H}_2$, as defined in §3.3. Then we have*

$$\mathrm{GC}(j_1, j_2, j_3, 1) \leq \frac{1}{6}.$$

Proof. Recall that the graded $\mathbb{Q}$-algebra of Siegel modular forms of level $\mathrm{Sp}_4(\mathbb{Z})$ is generated by

$$f_1 = I_6', \quad f_2 = I_{12}, \quad f_3 = I_4, \quad \text{and} \quad f_4 = I_{10}.$$

We are in case 1 of Definition 4.4, since

$$\frac{I_6' I_4}{I_{10}} = j_1, \quad \frac{I_{12} I_4^2}{I_{10}^2} = j_2, \quad \text{and} \quad \frac{I_4^5}{I_{10}^2} = j_3.$$

The definition gives

$$\mathrm{SGC}(j_1, j_2, j_3, 1) \leq \left(1 + \frac{2}{3}\right) \cdot \frac{1}{10} = \frac{1}{6}.$$

□

Proposition 4.11. *Let ℓ be a prime number, and let $\Psi_{\ell,m}$ for $1 \leq m \leq 3$ denote the Siegel modular equations of level ℓ in Igusa invariants. Let $\mathcal{F} \in \mathbb{Q}(J_1, J_2, J_3)$ be a coefficient of $\Psi_{\ell,1}$ (resp. $\Psi_{\ell,2}$ or $\Psi_{\ell,3}$). Then the total degree of $\mathcal{F}$ is bounded above by $5\, d(\ell)/3$ (resp. $10\, d(\ell)/3$), where $d(\ell) = \ell^3 + \ell^2 + \ell + 1$.*

Proof. The integer $d(\ell)$ is the degree of the Hecke correspondence. The denominators of j_1, j_2, and j_3 can be taken to be the modular forms I_{10}, I_{10}^2, and I_{10}^2. Let $g_{\ell,m}$ for $1 \leq m \leq 3$ be the common denominators of the modular equations $\Psi_{\ell,m}$ defined in Proposition 4.3, so that $g_{\ell,2} = g_{\ell,3} = g_{\ell,1}^2$ and $\mathrm{wt}(g_{\ell,1}) = 10\, d(\ell)$.

Then $\mathcal{F}(j_1, j_2, j_3)$ is the quotient of two modular forms of degree $10\, d(\ell)$ (resp. $20\, d(\ell)$) on $\mathcal{S}$, by Proposition 4.3. Therefore the result follows from Lemma 4.10 and Proposition 4.8. □

Lemma 4.12. *Let $F = \mathbb{Q}(\sqrt{5})$, and let g_1, g_2 denote the Gundlach invariants on the Hilbert surface $\mathrm{SL}(\mathbb{Z}_F \oplus \mathbb{Z}_F^\vee)\backslash\mathbb{H}_1^2$, as defined in §3.4. Then we have*

$$\mathrm{GC}(g_1, g_2, 1) \leq \frac{1}{6}.$$

Proof. Choose F_6, F_2, and F_{10} as generators of the graded $\mathbb{Q}$-algebra of Hilbert modular forms of level $\mathrm{SL}(\mathbb{Z}_F \oplus \mathbb{Z}_F^\vee)$. We have

$$\frac{F_6 F_2^2}{F_{10}} = g_2 \quad \text{and} \quad \frac{F_2^5}{F_{10}} = g_1.$$

Therefore we are in case 1 of Definition 4.4, and

$$\mathrm{GC}(g_1, g_2, 1) \leq \left(1 + \frac{2}{3}\right) \cdot \frac{1}{10} = \frac{1}{6}.$$

□

Proposition 4.13. *Let $F = \mathbb{Q}(\sqrt{5})$, let $\beta \in \mathbb{Z}_F$ be a totally positive prime, and let $\Psi_{\beta,m}$ for $m \in \{1, 2\}$ denote the Hilbert modular equations of level β in Gundlach invariants. Let $\mathcal{F} \in \mathbb{Q}(J_1, J_2)$ be a coefficient of $\Psi_{\beta,1}$ or $\Psi_{\beta,2}$. Then the total degree of $\mathcal{F}$ is bounded above by $10\, d(\beta)/3$, where $d(\beta) = N_{F/\mathbb{Q}}(\beta) + 1$.*

Proof. The integer $d(\beta)$ is the degree of the Hecke correspondence, and the automorphism group Σ used to define the Hilbert modular equations has order 2. We can take the modular F_{10} as denominator of both g_1 and g_2; the common denominators $g_{\beta,1} = g_{\beta,2}$ from Proposition 4.3 have weight $20\, d(\beta)$, so the result follows from Lemma 4.10 and Proposition 4.8. □

The degree bounds in Propositions 4.11 and 4.13 are both reached experimentally. In the Siegel case with $\ell = 2$, the maximum degree is 25; in the Hilbert case with $N_{F/\mathbb{Q}}(\beta) = 41$, the maximum degree is 140 [23].

5. Height estimates for modular equations

Another important information when manipulating modular equations, besides their degrees, is the size of their coefficients. More precisely, we use the notion of *heights* of elements, polynomials and rational fractions over a number field. The goal of this section is to prove part 2 of Theorem 1.1, giving height bounds on coefficients of modular equations.

As mentioned in the introduction, the proof is inspired by existing works on elliptic modular polynomials [31]. First, we study the heights of modular equations evaluated at well-chosen points, using the fact that the underlying Hecke correspondence describes isogenous abelian varieties. Then we apply the main result of [18], which gives a tight relation between the height of a rational fraction and the heights of sufficiently many of its evaluations.

5.1. **Definition of heights.** Let us recall the well-known definitions. We use the following notation:

- L is a number field of degree d_L over $\mathbb{Q}$;
- $\mathcal{V}_L^0$ (resp. $\mathcal{V}_L^\infty$) is the set of all nonarchimedean (resp. archimedean) places of L; and
- $\mathcal{V}_L = \mathcal{V}_L^0 \sqcup \mathcal{V}_L^\infty$ is the set of all places of L.

For each place v of L,

- L_v (resp. $\mathbb{Q}_v$) denotes the completion of L (resp. $\mathbb{Q}$) at v,
- $d_v = [L_v : \mathbb{Q}_v]$ denotes the local extension degree of $L/\mathbb{Q}$ at v, and
- $|\cdot|_v$ denotes the normalized absolute value associated with v.

We normalize the nonarchimedean absolute values of L in the following way: for each $v \in \mathcal{V}_L^0$, if $p \in \mathcal{P}_{\mathbb{Q}}$ is the prime below v, then $|p|_v = 1/p$.

The (absolute logarithmic Weil) *height* of projective tuples, affine tuples, elements, polynomials and rational fractions over L is defined as follows.

Definition 5.1. Let $n \geq 1$, and let $y_0, \dots, y_n \in L$.

(1) The *projective height* of $(y_0 : \cdots : y_n) \in \mathbb{P}_L^n$ is

$$h(y_0 : \cdots : y_n) = \sum_{v \in \mathcal{V}_L} \frac{d_v}{d_L} \log\big(\max_{0 \leq i \leq n} |y_i|_v\big).$$

(2) The *affine height* of $(y_1, \dots, y_n) \in L^n$ is the projective height of $(1 : y_1 : \cdots : y_n)$:

$$h(y_1, \dots, y_n) = \sum_{v \in \mathcal{V}_L} \frac{d_v}{d_L} \log\big(\max\{1, \max_{1 \leq i \leq n} |y_i|_v\}\big).$$

In particular, for every $y \in L$, we have

$$h(y) = \sum_{v \in \mathcal{V}_L} \frac{d_v}{d_L} \log\big(\max\{1, |y|_v\}\big).$$

(3) Let $P \in L[Y_1, \dots, Y_n]$ be a multivariate polynomial over L, and write

$$P = \sum_{k=(k_1,\dots,k_n) \in \mathbb{N}^n} c_k Y_1^{k_1} \cdots Y_n^{k_n}.$$

Let $v \in \mathcal{V}_L$. We write

$$|P|_v = \max_{k \in \mathbb{N}^n} |c_k|_v$$

and

$$h(P) = \sum_{v \in \mathcal{V}_L} \frac{d_v}{d_L} \log\big(\max\{1, |P|_v\}\big).$$

In other words, $h(P)$ is the height of the affine tuple formed by all the coefficients of P.

(4) Let $\mathcal{F} \in L(Y_1, \dots, Y_n)$ be a multivariate rational fraction over L, and choose coprime polynomials $P, Q \in L[Y_1, \dots, Y_n]$ such that $\mathcal{F} = P/Q$. Then we define $h(\mathcal{F})$ as the height of the projective tuple formed by all the coefficients of P and Q.

Here are a few elementary properties of heights.

(1) Projective heights are well defined, by the product formula [16, Lem. B.2.1(a)]. Therefore the height of a fraction is also well defined.

(2) Heights are independent of the ambient number field [16, Lem. B.2.1(c)], by another application of the product formula. In particular we note that

$$\sum_{v \in \mathcal{V}_L^\infty} \frac{d_v}{d_L} = 1.$$

(3) If $L = \mathbb{Q}$, then Definition 5.1 coincides with the naive one given in the introduction.

Informally, the height of an element $y \in L$ measures the amount of information needed to represent y.

5.2. **Heights, evaluations and roots.** In this section, we state relations between

(1) The height of a univariate polynomial over L and the height of its roots;
(2) The height of a multivariate polynomial or multivariate rational fraction over L with the heights of its values at special points.

Several of the statements are easy consequences of the formulæ from Definition 5.1, while others are more intricate and are proved by the author in a separate paper [18].

Let us start with the evaluation of polynomials; the following proposition is a slight generalization of [16, Prop. B.7.1].

Proposition 5.2. *Let $d \geq 0$, let $P \in L[Y_1, \dots, Y_n]$ be a polynomial of total degree at most d, let $1 \leq m \leq n$, and let $y_1, \dots, y_m \in L$. Write $Q = P(y_1, \dots, y_m, Y_{m+1}, \dots, Y_n)$. Then*

$$h(Q) \leq h(P) + m \log(d+1) + d\, h(y_1, \dots, y_n).$$

More generally, if $\mathcal{I}_1 \sqcup \cdots \sqcup \mathcal{I}_r$ is a partition of $[\![1, m]\!]$, and if $d_k \geq 0$ denotes an upper bound on the total degree of P in the variables Y_i for $i \in \mathcal{I}_k$, then

$$h(Q) \leq h(P) + \sum_{k=1}^{r} (\#\mathcal{I}_k) \log(d_k + 1) + \sum_{k=1}^{r} d_k\, h\big((y_i)_{i \in \mathcal{I}_k}\big).$$

Proof. It is enough to prove the second statement. If $v \in \mathcal{V}_L^0$, we have

$$\big|P(y_1, \dots, y_m, Y_{m+1}, \dots, Y_n)\big|_v \leq |P|_v \prod_{k=1}^{r} \Big(\max\big\{1, \max_{i \in \mathcal{I}_k} |y_i|_v\big\}\Big)^{d_k}.$$

If $v \in \mathcal{V}_L^\infty$, the same estimate holds after multiplying the right hand side by the number of possible monomials in $Y_1, \dots, Y_m$, which is

$$\prod_{k=1}^{r} (d_k + 1)^{\#\mathcal{I}_k}.$$

Taking logarithms and summing gives the result. □

As a consequence, we can bound the height of a monic polynomial by the height of its roots.

Proposition 5.3. *Let $Q \in L[Y]$ be monic of degree d, and let $\alpha_1, \dots, \alpha_d$ be its roots in the algebraic closure of L. Then*

$$h(Q) \leq \sum_{i=1}^{d} h(\alpha_k) + d \log 2.$$

Proof. Apply Proposition 5.2 on the multivariate polynomial

$$P = \prod_{k=1}^{d} (Y_{d+1} - Y_k)$$

with $m = d$, $y_k = \alpha_k$, and $\mathcal{I}_k = \{k\}$. Since the coefficients of P all belong to $\{-1, 0, 1\}$, we have $h(P) = 0$. □

Conversely, the height of a univariate polynomial over L controls the height of its roots.

Proposition 5.4. *Let $P \in L[Y] \backslash \{0\}$, and let α be a root of P. Then*

$$h(\alpha) \leq h(P) + \log(2).$$

Proof. We reproduce the proof given in a lecture by F. Pazuki. We can assume that P is monic. Let $v \in \mathcal{V}_L$. We want to show that $|\alpha|_v \leq |P|_v$ if $v \in \mathcal{V}_L^0$, and $|\alpha|_v \leq 2|P|_v$ if $v \in \mathcal{V}_L^\infty$. Since P is monic, we always have $|P|_v \geq 1$. Write $P = X^n + \sum_{k=0}^{n-1} c_k Y^k$, for some $n \geq 1$.

If $v \in \mathcal{V}_L^0$, we can assume that $|\alpha|_v \geq 1$. Then

$$|\alpha|_v = \left|\sum_{i=0}^{n-1} c_k \alpha^k\right|_v \leq |P|_v |\alpha|_v^{n-1},$$

so $|\alpha|_v \leq |P|_v$.

If $v \in \mathcal{V}_L^\infty$, we can assume that $|\alpha|_v \geq 2$. Then, by the triangle inequality, we obtain

$$|\alpha|_v \leq |P|_v |\alpha_v|^{n-1} \left(1 + \frac{1}{|\alpha|_v} + \cdots + \frac{1}{|\alpha|_v^{n-1}}\right) \leq 2|\alpha|_v^{n-1}|P|_v,$$

so $|\alpha|_v \leq 2|P|_v$. Taking logarithms and summing over all places of L yields the result. □

We now turn to the more difficult questions of giving upper bounds on the height of a polynomial or rational fraction from its values at special points. Our choice is to consider (almost) consecutive integers.

Proposition 5.5 (([18, Prop. 1.1])). *Let $[\![A, B]\!]$ be an interval in $\mathbb{Z}$. Write $D = B - A$ and $M = \max\{|A|, |B|\}$. Let $d \geq 1$, let $P \in L[Y]$ be a univariate polynomial of degree at most d, let $N \geq d+1$, and let $y_1, \ldots, y_N$ be distinct elements of $[\![A, B]\!]$. Let $H \geq 0$, and assume that $h(P(y_i)) \leq H$ for every $1 \leq i \leq N$. Then we have*

$$h(P) \leq \frac{N}{N-d} H + D \log(D) + d \log(2M) + \log(d+1).$$

Note that the bound on $h(P)$ is of the order of dH when $N = d + 1$, as suggested by the Lagrange interpolation formula. On the other hand, if we take for instance $N = 2d$, then the bound on $h(P)$ is roughly in $O(H)$. This remark will be crucial in §5.6, when we consider the evaluation of multivariate polynomials in each variable successively.

Proposition 5.6 (([18, Prop. 1.2])). *Let $[\![A, B]\!]$ be an interval in $\mathbb{Z}$. Write $D = B - A$ and $M = \max\{|A|, |B|\}$. Let $d \geq 1$, and let $\mathcal{F} \in L(Y)$ be a univariate rational fraction of degree at most d. Let S be a subset of $[\![A, B]\!]$ containing no poles of $\mathcal{F}$, let $\eta \geq 1$, and let $H \geq \max\{4, \log(2M)\}$. Assume that*

(1) $h(\mathcal{F}(y)) \leq H$ for every $y \in S$.
(2) S contains at least D/η elements.
(3) $D \geq \max\{\eta d^3 H, 4\eta d d_L\}$.

Then we have

$$h(F) \leq H + C_L \eta d \log(\eta d H) + d \log(2M) + \log(d+1),$$

where C_L is a constant depending only on L. We can take $C_{\mathbb{Q}} = 960$.

The bound on $h(\mathcal{F})$ given in Proposition 5.6 is roughly in $O(H)$ as well, but the number of evaluation points that we have to consider is bounded from below in terms of H.

5.3. **Heights of abelian varieties.** We fix a PEL setting as in §3.2, and keep the notation used there. We also write $\mathcal{S} = \Gamma\backslash X_+$, where Γ is a subgroup of $G(\mathbb{Q})_+$.

Different types of heights can be defined for an abelian variety A over $\overline{\mathbb{Q}}$. The *Faltings height* $h_F(A)$ is defined in [12, §3] in terms of Arakelov degrees of metrized line bundles on A. If A is given a principal polarization $\mathcal{L}$, and $r \geq 2$ is an even integer, we can also define the *Theta height of level* r of $(A, \mathcal{L})$, denoted by $h_{\Theta,r}(A, \mathcal{L})$, as the projective height of level r theta constants of $(A, \mathcal{L})$ [30, Def. 2.6]. Finally, if A is an abelian variety with PEL structure over $\overline{\mathbb{Q}}$ given by a point $z \in \mathcal{S}$ where $j_1, \dots, j_{n+1}$ are well defined, we can define the *j-height* of A as

$$h_j(A) = h\big(j_1(A), \dots, j_{n+1}(A)\big).$$

We also write $\overline{h}_F(A) = \max\{1, h_F(A)\}$ and define $\overline{h}$, $\overline{h}_{\Theta,r}$, and $\overline{h}_j$ similarly.

The goal of this section is to relate the j-heights of isogenous abelian varieties, under mild conditions related to the geometry of the moduli space. Such a relation is known for instance in the case of elliptic curves, taking the usual j-invariant as coordinate [31, Thm. 1.1]. To this end, we relate the j-height with the Faltings height, since the latter behaves well with respect to isogenies. Theta heights are an intermediate step between concrete values of invariants and the Faltings height. More precisely, we use the two following results.

Proposition 5.7. *Let A, A' be abelian varieties over $\overline{\mathbb{Q}}$, and assume that an isogeny $\varphi\colon A \to A'$ exists. Then*

$$\big|h_F(A) - h_F(A')\big| \leq \frac{1}{2}\log(\deg\varphi).$$

Proof. This is a consequence of [12, Lem. 5]. □

Theorem 5.8 (([30, Cor. 1.3])). *For every $g \geq 1$, and every even $r \geq 2$, there exists a constant $C(g, r)$ such that the following holds. Let $(A, \mathcal{L})$ be a principally polarized abelian variety of dimension g defined over $\overline{\mathbb{Q}}$. Then*

$$\Big|\overline{h}_{\Theta,r}(A, \mathcal{L}) - \frac{1}{2}\,\overline{h}_F(A)\Big| \leq C(g, r)\log\big(\min\{\overline{h}_F(A), \overline{h}_{\Theta,r}(A, \mathcal{L})\} + 2\big).$$

We can take

$$C(g, r) = 1000 r^{2g}\log^5(r^{2g}).$$

5.4. **Relating the j-height and the Faltings height.** Using Theorem 5.8, we can prove that the j-height and the Faltings height of a generic abelian variety with PEL structure are related.

Proposition 5.9. *There exists a nonzero polynomial $P \in L[Y_1, \dots Y_{n+1}]$ and a positive constant C such that the following holds: if A is the abelian variety with PEL structure associated with a point $z \in \mathcal{S}$ where $j_1, \dots, j_{n+1}$ are well defined and $P(j_1, \dots, j_{n+1}) \neq 0$, and if A is defined over $\overline{\mathbb{Q}}$, then*

$$\frac{1}{C}\,\overline{h}_F(A) \leq \overline{h}_j(A) \leq C\,\overline{h}_F(A).$$

Proof. By [27, Thm. 5.17], we can write $\mathcal{S} = \Gamma'\backslash X_+$ where Γ' is a congruence subgroup of G^{der}. Since $G^{\mathrm{der}} \subset \ker(\det)$, it embeds into $\mathrm{GSp}_{2g}(\mathbb{Q})$, where $2g = \dim_{\mathbb{Q}} V$. Therefore, by [27, Thm. 5.16], we can find a congruence subgroup Γ'' of G^{der} and an even integer $r \geq 4$ such that $\Gamma''\backslash X_+$ embeds in the moduli space $\mathcal{A}_{\Theta,r}$

of principally polarized abelian varieties of dimension g with level r Theta structure. We have a diagram

$$\begin{array}{ccccc} & & \widetilde{\mathcal{S}} = \widetilde{\Gamma}\backslash X_+ & & \\ & \swarrow^{p'} & & \searrow^{p''} & \\ \mathcal{S} = \Gamma'\backslash X_+ & & & & \mathcal{S}'' = \Gamma''\backslash X_+ \xhookrightarrow{\iota} \mathcal{A}_{\Theta,r} \end{array} \tag{10}$$

where $\widetilde{\Gamma} = \Gamma' \cap \Gamma''$. The maps p' and p'' are finite coverings. All the varieties and maps in this diagram are defined over $\overline{\mathbb{Q}}$.

The modular interpretation of diagram (10) is the following. Let (Λ, ψ) be the standard polarized lattice associated with the connected component $\mathcal{S}$, as in Proposition 2.2. We can find a sublattice $\Lambda'' \subset \Lambda$, and $\lambda \in \mathbb{Q}^\times$ such that $(\Lambda'', \lambda\psi)$ is principally polarized. A point $z \in \mathcal{S}$ defines a complex structure x on $\Lambda \otimes \mathbb{R} = V(\mathbb{R})$, up to action of Γ. Lifting z to $\widetilde{z} \in \widetilde{\mathcal{S}}$ corresponds to considering x up to action of $\widetilde{\Gamma}$ only, and this group leaves Λ'' and its level r Theta structure stable. Then the image of $\widetilde{z}$ in $\mathcal{A}_{\Theta,r}$ is then given by $(\Lambda'', x, \lambda\psi)$.

In particular, if $\widetilde{z} \in \widetilde{\mathcal{S}}$, and if A and A'' are the abelian varieties corresponding to the points $p'(\widetilde{z}) \in \mathcal{S}$ and $\iota \circ p''(\widetilde{z}) \in \mathcal{A}_{\Theta,r}$ respectively, then A and A'' are linked by an isogeny of degree $d = \#(\Lambda/\Lambda'')$. Hence, by Proposition 5.7 and Theorem 5.8, we have

$$\begin{aligned} \left|\overline{h}_F(A) - 2\,\overline{h}_{\Theta,r}(A'')\right| &\leq \frac{\log(d)}{2} + C(g,r)\log\left(\min\{\overline{h}_F(A), \overline{h}_{\Theta,r}(A'')\} + 2 + \frac{\log(d)}{2}\right) \\ &\leq C_F \min\{\overline{h}_F(A), \overline{h}_{\Theta,r}(A'')\} \end{aligned}$$

with $C_F = (2 + \log(d))C(g,r)$. Therefore

$$\overline{h}_F(A) \leq (2 + C_F)\,\overline{h}_{\Theta,r}(A''), \qquad \overline{h}_{\Theta,r}(A'') \leq \frac{1 + C_F}{2}\,\overline{h}_F(A). \tag{11}$$

Now we relate the Theta height and the j-height using relation between modular functions; the genericity hypothesis encoded in the polynomial P appears in this step. Denote by $\theta_0, \ldots, \theta_k$ the Theta constants of level r. They define a projective embedding of $\mathcal{A}_{\Theta,r}$, therefore the pullbacks of $\theta_1/\theta_0, \ldots, \theta_k/\theta_0$ generate the function field of $\mathcal{S}''$. By definition, $j_1, \ldots, j_{n+1}$ are coordinates on $\mathcal{S}$. To ease notation, we identify all these functions with their pullbacks to $\widetilde{\mathcal{S}}$.

By the primitive element theorem, there exists a function f on $\widetilde{\mathcal{S}}$ such that both $(j_1, \ldots, j_{n+1}, f)$ and $(\theta_1/\theta_0, \ldots, \theta_k/\theta_0, f)$ are generating families for the function field of $\widetilde{\mathcal{S}}$ over $\overline{\mathbb{Q}}$. We choose polynomials

$$P_J \in \overline{\mathbb{Q}}[Y_1, \ldots, Y_{n+1}, X] \quad \text{and} \quad P_\Theta \in \overline{\mathbb{Q}}[Y_1, \ldots, Y_k, X]$$

such that $P_J(j_1, \ldots, j_{n+1}, X)$ and $P_\Theta(\theta_1/\theta_0, \ldots, \theta_k/\theta_0, X)$ are (non necessarily monic) minimal polynomials of f over the function fields of $\mathcal{S}$ and $\mathcal{S}''$ respectively. We also choose polynomials $N_{J,i}, D_{J,i} \in \overline{\mathbb{Q}}[Y_1, \ldots, Y_k, X]$ for each $1 \leq i \leq n+1$, and $N_{\Theta,i}, D_{\Theta,i} \in \overline{\mathbb{Q}}[Y_1, \ldots, Y_{n+1}, X]$ for each $1 \leq i \leq k$, such that the following equalities hold on $\widetilde{\mathcal{S}}$:

$$\begin{aligned} j_i &= \frac{N_{J,i}}{D_{J,i}}(\theta_1/\theta_0, \ldots, \theta_k/\theta_0, f) && \text{for each } 1 \leq i \leq n+1, \text{ and} \\ \theta_i/\theta_0 &= \frac{N_{\Theta,i}}{D_{\Theta,i}}(j_1, \ldots, j_{n+1}, f) && \text{for each } 1 \leq i \leq k. \end{aligned}$$

Let $\widetilde{F}$ be the smallest Zariski closed subset of $\widetilde{\mathcal{S}}$ such that outside $\widetilde{F}$, the following properties are all satisfied:

- all the functions f, j_i for $1 \leq i \leq n+1$ and θ_i/θ_0 for $1 \leq i \leq k$ are well defined;
- the polynomials $P_J(j_1, \dots, j_{n+1}, X)$ and $P_\Theta(\theta_1/\theta_0, \dots, \theta_k/\theta_0, X)$ do not vanish;
- the quantities $D_{J,i}(\theta_1/\theta_0, \dots, \theta_k/\theta_0, f)$ for $1 \leq i \leq k$ and $D_{\Theta,i}(j_1, \dots, j_{n+1}, f)$ for $1 \leq i \leq k$ do not vanish.

Then $\widetilde{F}$ has codimension 1 in $\widetilde{\mathcal{S}}$, hence $\mathcal{U} = \mathcal{S} \backslash p'(\widetilde{F})$ is open dense in $\mathcal{S}$. Let $P \in L[j_1, \dots, j_{n+1}]$ be a polynomial such that $\{P \neq 0\} \subset \mathcal{U}$.

Let $z \in \mathcal{S}$ be a point where $j_1, \dots, j_{n+1}$ are well defined, take values in $\overline{\mathbb{Q}}$, and satisfy $P(j_1, \dots, j_{n+1}) \neq 0$. We look at the diagram (10), from left to right. Lift z to a point $\widetilde{z} \in \widetilde{\mathcal{S}}$; by construction, $\widetilde{z} \notin \widetilde{F}$. By Propositions 5.2 and 5.4, we have

$$\overline{h}\big(j_1(\widetilde{z}), \dots, j_{n+1}(\widetilde{z}), f(\widetilde{z})\big) \leq C\, \overline{h}\big(j_1(z), \dots, j_{n+1}(z)\big) \tag{12}$$

with $C = h(P_J) + (n+1)\log(d_J + 1) + d_J + 1$, where d_J denotes the total degree of P_J in $Y_1 \dots, Y_{n+1}$. Writing $z'' = p''(\widetilde{z})$, we also have for every $1 \leq i \leq k$,

$$\overline{h}(\theta_i/\theta_0(\widetilde{z})) \leq C\, \overline{h}\big(j_1(\widetilde{z}), \dots, j_{n+1}(\widetilde{z}), f(\widetilde{z})\big) \tag{13}$$

with $C = h(N_{\Theta,i}) + h(D_{\Theta,i}) + (n+2)\big(\log(\deg(N_{\Theta,i}) + 1) + \log(\deg(D_{\Theta,i}) + 1)\big) + \deg(N_{\Theta,i}) + \deg(D_{\Theta,i})$, where deg denotes the total degree. Combining equations (12) and (13), we obtain

$$\overline{h}\Big(\frac{\theta_1}{\theta_0}(z''), \dots, \frac{\theta_k}{\theta_0}(z'')\Big) \leq C_\Theta\, \overline{h}\big(j_1(z), \dots, j_{n+1}(z)\big)$$

where C_Θ has an explicit expression in terms of the heigts and degrees of the polynomials P_J and $N_{\Theta,i}, D_{\Theta,i}$ for $1 \leq i \leq k$. Equivalently, in the notation above, we have

$$\overline{h}_{\Theta,r}(A'') \leq C_\Theta\, \overline{h}_j(A),$$

so by (11)

$$\overline{h}_F(A) \leq (2 + C_F) C_\Theta\, \overline{h}_j(A).$$

Going through the diagram from right to left gives the reverse inequality

$$\overline{h}_j(A) \leq \frac{(1 + C_F) C_J}{2}\, \overline{h}_F(A)$$

where C_J is defined in a similar way to C_Θ in terms of the polynomials P_Θ and $N_{J,i}, D_{J,i}$ for $1 \leq i \leq n+1$. □

Assume that the integers r and d, the modular function f, as well as the polynomials $P_J, P_\Theta, N_{J,i}, D_{J,i}, N_{\Theta,i}$, and $D_{\Theta,i}$ can be explicitly determined. Then both the polynomial P and the constant C in Proposition 5.9 can be determined explicitly as well. We will do this computation in a slightly different way in §5.7 in the case of Igusa invariants on the Siegel threefold.

From now on, we define $\mathcal{U}$ to be the Zariski open set in $\mathcal{S}$ where $j_1, \dots, j_{n+1}$ are well defined and $P(j_1, \dots, j_{n+1}) \neq 0$.

Corollary 5.10. *Let C be the constant from Proposition 5.9, let z and z' be points of $\mathcal{U}$ and let A and A' be the abelian varieties with PEL structure associated with z*

and z' respectively. Assume that A and A' are defined over $\overline{\mathbb{Q}}$, and are linked by an isogeny of degree d. Then

$$\overline{h}_j(A') \leq C^2(\overline{h}_j(A) + \log d).$$

Proof. Combine Propositions 5.7 and 5.9. □

Remark 5.11. We can presumably do better than Corollary 5.10. For instance, when studying j-invariants of isogenous elliptic curves, one can prove that $|h(j(E)) - h(j(E'))|$ is bounded by logarithmic terms [31, Thm. 1.1]. This is also the kind of bound provided by Theorem 5.8. The rough estimate in Corollary 5.10 is sufficient for our purposes, but has the drawback that the constants we derive from it are very pessimistic.

5.5. **Heights of evaluated modular equations.** Let $\mathcal{U}$ (resp. $\mathcal{U}'$) be an open set of $\mathcal{S}$ (resp. $\mathcal{T}$) where a relation between the j-height and the Faltings height holds, as in Proposition 5.9. Define $\mathcal{U}_\delta \subset \mathcal{S}$ to be the Zariski open set of all points $[x, g] \in \mathcal{S}$ such that $[x, g] \in \mathcal{U}$, and moreover the images of $[x, g]$ under the (symmetrized) Hecke correspondence H_δ all lie in $\mathcal{U}'$: in other words $[\sigma(x), \sigma(gk\delta)] \in \mathcal{U}'$ for every $(k, \sigma) \in K_0/K_{n+1}$, in the notation of §3.2. Finally, we define $\mathcal{V}_\delta \subset L^n$ to be the Zariski open set of all points $(j_1, \dots, j_n)$ where the equation (5) given by $E(j_1, \dots, j_n, J_{n+1})$ has e distinct roots and the following property holds: if j_{n+1} is a root of (5), then $(j_1, \dots, j_{n+1})$ are the invariants of some point $z \in \mathcal{U}_\delta$. In particular, the modular equations $\Psi_{\delta,m}$ do not have poles on $\mathcal{V}_\delta$.

Lemma 5.12. *There exist a positive constant C independent of δ, and a nonzero polynomial $P_\delta \in L[J_1, \dots, J_n]$ of total degree at most $C\, d(\delta)$ such that $\{P_\delta(j_1, \dots, j_n) \neq 0\} \subset \mathcal{V}_\delta$.*

Proof. Let $E \in L[J_1, \dots, J_{n+1}]$ be the polynomial defined in §3.2, of degree e in J_{n+1}, so that the equation satisfied by j_{n+1} on $\mathcal{S}$ takes the form $E(j_1, \dots, j_{n+1}) = 0$.

Let R be the the resultant of E and its derivative with respect to J_{n+1}. If R does not vanish at $(j_1, \dots, j_n) \in L^n$, then the polynomial $E(j_1, \dots, j_n, J_{n+1}) \in L[J_{n+1}]$ has e distinct roots.

Similarly, there is a polynomial $Q \in L[J_1, \dots, J_{n+1}]$ such that every tuple $(j_1, \dots, j_{n+1})$ satisfying (5) and such that $Q(j_1, \dots, j_{n+1}) \neq 0$ lies in the image of $\mathcal{S}$. Let R' be the resultant of Q and E with respect to J_{n+1}. If R' does not vanish at $(j_1, \dots, j_n)$, then for every root j_{n+1} of $E(j_1, \dots, j_n, J_{n+1})$, the tuple $(j_1, \dots, j_{n+1})$ lies in the image of $\mathcal{S}$.

Let λ, λ' be symmetric modular forms on $\mathcal{S}$ and $\mathcal{T}$ respectively, defined over L, such that $\{\lambda \neq 0\} \subset \mathcal{U}$ and $\{\lambda' \neq 0\} \subset \mathcal{U}'$. These modular forms can be chosen independently of δ. As in §4.1, we construct the modular form

$$\lambda^\delta = \lambda \prod_{\gamma \in K_0/K'} \gamma \cdot \lambda'_\delta$$

where λ'_δ is the modular form $[x, g] \mapsto \lambda'([x, g\delta])$ of level K'. The modular form λ^δ is defined over L and has weight

$$\mathrm{wt}(\lambda^\delta) = \mathrm{wt}(\lambda) + (\#\Sigma)\, d(\delta)\, \mathrm{wt}(\lambda').$$

Modular forms realize a projective embedding of $\mathcal{S}$ by Theorem 2.5; therefore, possibly after increasing the weight by a constant independent of δ, we can find a

symmetric modular form ξ defined over L such that $\mathrm{wt}(\lambda^\delta) = \mathrm{wt}(\xi)$ and the divisors of λ^δ and ξ have no common codimension 1 components. By Proposition 4.8, if we write

$$\frac{\lambda^\delta}{\xi} = \sum_{k=0}^{e-1} R_k(j_1, \dots, j_n) j_{n+1}^k \qquad \text{where } R_k \in L(J_1, \dots, J_n),$$

then $\deg R_k \le \mathrm{GC}(j_1, \dots, j_{n+1}) \,\mathrm{wt}(\lambda^\delta)$ for every $0 \le k \le e-1$. Taking the resultant of $\sum R_k J_{n+1}^k$ and E with respect to J_{n+1} yields a rational fraction $R'' \in L(J_1, \dots, J_n)$ of total degree at most

$$(e-1)d_E + e \max_{0 \le k \le e-1} \deg(R_k),$$

where d_E denotes the total degree of E in $j_1, \dots, j_n$. If R', R'' are well defined and do not vanish at $(j_1, \dots, j_n)$, then for every root j_{n+1} of (5), the tuple $(j_1, \dots, j_{n+1})$ comes from a point $z \in \mathcal{U}_\delta$.

We take P_δ to be the product of R, R', and the numerator of R''. The polynomials R and R' are independent of δ, and the degree of R'' is bounded above linearly in $d(\delta)$. □

If upper bounds on the degree of equations defining $\mathcal{U}$ and $\mathcal{U}'$ are explicitly known, together with the polynomials E and Q, then the proof of Lemma 5.12 allows us to determine a valid constant C explicitly.

Proposition 5.13. *There exists a constant C, independent of δ, such that the following holds. Let $(j_1, \dots, j_n) \in \mathcal{V}_\delta$, and let $1 \le m \le n+1$. Then*

$$h\big(\Psi_{\delta,m}(j_1, \dots, j_n)\big) \le C\, d(\delta)\big(\overline{h}(j_1, \dots, j_n) + \log l(\delta)\big).$$

Proof. Let $\mathcal{J}$ be the set of roots of equation (5) at $(j_1, \dots, j_n)$, and let $j_{n+1} \in \mathcal{J}$. Let $[x, g]$ be a point of $\mathcal{S}$ describing an abelian variety A with PEL structure whose invariants are $(j_1, \dots, j_{n+1})$. For every $\sigma \in \Sigma$, denote by A_σ the abelian variety with PEL structure associated with the point $[\sigma(x), \sigma(g)]$. Then for every $\gamma = (\sigma, k) \in K_0/K_m$, the point $[\sigma(x), \sigma(gk\delta)]$ describes an abelian variety A_γ which is related to A_σ by an isogeny of degree $l(\sigma(\delta)) = l(\delta)$, by Corollary 2.8. Therefore, by Corollary 5.10, we have

$$\overline{h}\big(\gamma \cdot j_{1,\delta}([x, g]), \dots, \gamma \cdot j_{n+1,\delta}([x, g])\big) \le C(\overline{h}\big(j_1, \dots, j_{n+1}) + \log l(\delta)\big).$$

where the constant $C > 0$ is independent on δ. By Definition 3.1, the polynomial $\Psi_{\delta,m}(j_1, \dots, j_n, j_{n+1}) \in L[Y_1, \dots, Y_m]$ is the evaluation of a certain multivariate polynomial at the values $\gamma \cdot j_{i,\delta}([x, g])$, for $1 \le i \le m$ and $\gamma \in K_0/K_i$, each appearing with degree 1. The number of such values is

$$d_1 + d_1 d_2 + \cdots + d_1 \cdots d_m \le m\,(\#\Sigma)\, d(\delta).$$

Therefore, by Proposition 5.2, we have

$$\begin{aligned} h\big(\Psi_{\delta,m}(j_1, \dots, j_{n+1})\big) &\le m\,(\#\Sigma)\, d(\delta) \log(2) + m\,(\#\Sigma)\, d(\delta)\, C\big(\overline{h}(j_1, \dots, j_{n+1}) + \log l(\delta)\big) \\ &\le C'\, d(\delta)\big(\overline{h}(j_1, \dots, j_{n+1}) + \log l(\delta)\big). \end{aligned}$$

where C and C' denote explicit constants independent of δ. In order to obtain $\Psi_{\delta,m}(j_1, \dots, j_n)$, we interpolate a polynomial of degree $e-1$ in j_{n+1} where $\mathcal{J}$ is the set of interpolation points. By Propositions 5.2 and 5.4, we have

$$h(j_{n+1}) \le C\, \overline{h}(j_1, \dots, j_n) \qquad \text{for every } j_{n+1} \in \mathcal{J},$$

where C is a constant independent on δ. The result follows by applying Proposition 5.5 with $N = d + 1$. □

The proof of Proposition 5.13 provides an explicit value of C if the constant from Corollary 5.10 is known.

5.6. **Heights of coefficients of modular equations.** We are ready to prove upper bounds on the heights of modular equations (the second part of Theorem 1.1) using Proposition 5.13 and the results on heights of fractions given in §5.2. From now on, we add subscripts to constants: for instance $C_{5.9}$ denotes a constant *larger than* 1 such that Proposition 5.9 holds with this value of C. Moreover, we denote by $C_{\log}$ a constant independent of δ such that $\log d(\delta) \leq C_{\log} \max\{1, \log l(\delta)\}$. By Proposition 2.9, we can take $C_{\log} = (\dim V)^2 + \log(C_{2.9})$, where V denotes the $\mathbb{Q}$-vector space defining the PEL datum.

Definition 5.14. We call an (n, N_1, N_2)-*evaluation tree* a rooted tree of depth n, arity N_1 at depths $0, \dots, n-2$, and arity N_2 at depth $n-1$, such that every vertex but the root is labeled by an element of $\mathbb{Z}$ and the sons of every vertex are distinct.

Let T be an (n, N_1, N_2)-evaluation tree, and let $1 \leq k \leq n$. The k-th *evaluation set* $\mathcal{I}_k(T)$ of T is the set of points $(y_1, \dots, y_k) \in \mathbb{Z}^k$ such that y_1 is a son of the root, and y_{i+1} is a son of y_i for every $1 \leq i \leq k-1$. We say that T is *bounded by* M if the absolute value of every vertex is bounded above by M. We say that T has *amplitude* (D_1, D_2) if for every vertex y of depth $0 \leq r \leq n-2$ (resp. depth $n-1$) in T, the sons of y lie in an integer interval of amplitude at most D_1 (resp. D_2); by definition, the amplitude of $[\![A, B]\!]$ is $B - A$.

Let T be an (n, N_1, N_2)-evaluation tree, let $a = (a_1, \dots, a_n) \in \mathbb{Z}^n$, and let $M \geq 1$ be an integer. Let $\mathcal{F}$ be a coefficient of $\Psi_{\delta,m}$ for some $1 \leq m \leq n+1$, seen as a polynomial in the variables $J_{n+1}, Y_1, \dots, Y_m$; hence $\mathcal{F} \in L(J_1, \dots, J_n)$. Write $\mathcal{F} = P/Q$ in irreducible form, and let $d = \deg(\mathcal{F})$; assume that $d \geq 1$. We say that T, a and M are *valid evaluation data for* $\mathcal{F}$ if the following conditions are satisfied:

(1) T and a are bounded by M
(2) We have $M \geq 2B \log^2(B+1)$, where
$$B = 4C_{4.9}^3 C_{5.13}\, d(\delta)^4 \max\{1, \log l(\delta)\}.$$
(3) $N_1 = 2d$ and $N_2 \geq M$.
(4) T has amplitude $(4d, 2M)$.
(5) For every $(y_1, \dots, y_n) \in \mathcal{I}_n(T)$, the point
$$(j_1, \dots, j_n) = (y_1 y_n + a_1, \dots, y_{n-1} y_n + a_{n-1}, y_n + a_n)$$
belongs to $\mathcal{V}_\delta$.
(6) For every $(y_1, \dots, y_{n-1}) \in \mathcal{I}_{n-1}(T)$, the two polynomials P and Q evaluated at the tuple $(y_1 Y + a_1, \dots, y_{n-1} Y + a_{n-1}, Y + a_n)$ are coprime in $L[Y]$.
(7) $Q(a_1, \dots, a_n) \neq 0$.

Lemma 5.15. *There exists a constant C, independent of δ, such that the following holds. Let $\mathcal{F}$ be a coefficient of $\Psi_{\delta,m}$ of degree $d \geq 1$. Then there exist valid evaluation data (T, a, M) for $\mathcal{F}$ such that*

$$C\, d(\delta)^4 \max\{1, \log^3(l(\delta))\} \leq M < C\, d(\delta)^4 \max\{1, \log^3(l(\delta))\} + 1 \tag{14}$$

and $M \geq 4d[L:\mathbb{Q}]$. *We can take*

$$C = \max\{C_1, C_2, C_3\}$$

where

$$C_1 = 24C_{4.9}^3 C_{5.13}\big(4C_{\log} + \log(24C_{4.9}^3 C_{5.13}) + 1\big),$$
$$C_2 = 14C_{4.9}^2 + 5C_{5.12}, \quad \textit{and} \quad C_3 = 4C_{4.9}[L:\mathbb{Q}].$$

Proof. Let M be as in (14). Condition 1 in Definition 5.14 holds because $C \geq C_1$.

We start by constructing the vector a. Note that $M \geq 2d+1$. Since Q is nonzero, and has degree at most d in Y_1, we can find $a_1 \in \mathbb{Z}$ such that $|a_1| \leq M$ and the polynomial $Q(a_1, Y_2, \ldots, Y_n)$ is nonzero. Iterating, we find a vector $a = (a_1, \ldots, a_n)$ bounded by M such that $Q(a_1, \ldots, a_n) \neq 0$.

We now build the evaluation tree T down from the root. Let P_δ be an equation for the complement of $\mathcal{V}_\delta$ as in Lemma 5.12, and define

$$R_\delta = P_\delta(Y_1Y_n + a_1, \ldots, Y_{n-1}Y_n + a_{n-1}, Y_n + a_n)$$

which is a nonzero polynomial of degree at most $2C_{5.12}\, d(\delta)$. Let R be the resultant with respect to Y_n of the two polynomials

$$P(Y_1Y_n + a_1, \ldots, Y_{n-1}Y_n + a_{n-1}, Y_n + a_n)$$

and

$$Q(Y_1Y_n + a_1, \ldots, Y_{n-1}Y_n + a_{n-1}, Y_n + a_n).$$

The polynomial R is nonzero and has total degree at most $4d^2$.

We want to choose $2d$ values of y_1, lying in an interval with amplitude at most $4d$, such that neither R_δ nor R vanishes when evaluated at $Y_1 = y_1$; this nonvanishing condition excludes at most $4d^2 + 2C_{5.12}\, d(\delta)$ possible values of y_1. At least one of the integer intervals of the form $[\![5kd, (5k+4)d]\!]$ for $0 \leq k \leq 2d + C_{5.12}\, d(\delta)/d$ contains at least $2d$ valid choices of y_1. Then $|y_1|$ is always bounded above by $5(2d^2 + C_{5.12}\, d(\delta)) + 4d \leq M$, because $C \geq C_2$.

We iterate this procedure to construct T up to depth $n-1$ with the right arity, bound and amplitude, such that the evaluations of the polynomials R_δ and R are nonzero at every point $(y_1, \ldots, y_{n-1}) \in \mathcal{I}_{n-1}(T)$.

We conclude by constructing n-th level of T. Let $(y_1, \ldots, y_{n-1}) \in \mathcal{I}_{n-1}(T)$. Then, as before, at most $4d^2 + 2C_{5.12}\, d(\delta) \leq M$ values for y_n are forbidden as they make either R_δ or R vanish. This leaves at least M available values for y_n in $[\![-M, M]\!]$.

For every $(y_1, \ldots, y_n) \in \mathcal{I}_n(T)$, the nonvanishing of the polynomials R_δ and R at $(y_1, \ldots, y_n)$ guarantees conditions 5 and 6 of Definition 5.14 respectively. Finally, the inequality $C \geq C_3$ ensures that $M \geq 4d[L:\mathbb{Q}]$. □

Theorem 5.16. *Let H_δ be an absolutely irreducible Hecke correspondence on $\mathcal{S} \times \mathcal{T}$ defined by an element $\delta \in G(\mathbb{A}_f)$, and let $d(\delta)$ be the degree of H_δ. Let $\mathcal{F} \in L(J_1, \ldots, J_n)$ be a coefficient of one of the modular equations $\Psi_{\delta,m}$ for $1 \leq m \leq n+1$. Then the height of $\mathcal{F}$ is bounded above by $C\, d(\delta)$, where C is a constant independent of δ; more precisely we can take*

$$C = 2^{n-1}\big(2C_{5.13}(1 + C'') + 2C_{5.6}C_{4.9}\big(\log(4C_{4.9}C_{5.13}) + 2C_{\log} + 1 + C''\big) + 4C_{4.9}(\log(C_{4.9}) + C_{\log}) + 2C_{4.9}(\log(2) + C'') + 2\log(2C_{4.9}) + 2\big),$$

where $C'' = 3 + \log(2C_{5.15}) + 4C_{\log}$.

Proof. By Lemma 5.15, there exist valid evaluation data (T, a, M) for $\mathcal{F}$ such that the inequality $M \le C_{5.15}\, d(\delta)^4 \max\{1, \log^3 l(\delta)\} + 1$ holds. After scaling P and Q by an element of $L^\times$, we can assume that $Q(a_1, \dots, a_n) = 1$.

Let $(y_1, \dots, y_{n-1}) \in \mathcal{I}_{n-1}(T)$, and write

$$\widetilde{\mathcal{F}}(Y) = \mathcal{F}(y_1 Y + a_1, \dots y_{n-1} Y + a_{n-1}, Y + a_n).$$

For every son y_n of y_{n-1} in T, we have

$$h\big(y_1 y_n + a_1, \dots, y_{n-1} y_n + a_n\big) \le \log\big((M+1)M\big) \le 2\log(M+1).$$

Therefore, by Proposition 5.13,

$$\begin{aligned} h(\widetilde{\mathcal{F}}(y_n)) &\le C_{5.13}\, d(\delta)\big(2\log(M+1) + \log l(\delta)\big) \\ &\le 2C_{5.13}\, d(\delta)\big(\log(M+1) + \max\{1, \log l(\delta)\}\big). \end{aligned}$$

Denote this last quantity by H. We have $H \ge 4$ and $H \ge \log(2M)$. Moreover, in the notation of Definition 5.14, the inequality $M \ge 2B\log^2(B+1)$ ensures that

$$\frac{M}{\log(M+1)} \ge B \ge d^3\big(4C_{5.13}\, d(\delta) \max\{1, \log l(\delta)\}\big).$$

Therefore $M \ge d^3 H$.

We are in position to apply Proposition 5.6 for the univariate rational fraction $\widetilde{F}$ on the interval $[\![-M, M]\!]$, with $\eta = 2$, using the sons of $(y_1, \dots, y_{n-1})$ in T as evaluation points. We obtain

$$\begin{aligned} h(\widetilde{\mathcal{F}}) &\le H + 2C_{5.6} d \log(2dH) + d\log(2M) + \log(d+1) \\ &\le C'\, d(\delta) \max\{1, \log l(\delta)\}, \end{aligned}$$

where C' is a constant independent of δ. In order to obtain an explicit expression for C', we note that

$$\log(M+1) \le C'' \max\{1, \log l(\delta)\}$$

where C'' is defined as in the statement of the theorem. We check that we can take

$$\begin{aligned} C' = {} & 2C_{5.13}(1 + C'') + 2C_{5.6}C_{4.9}\big(\log(4C_{4.9}C_{5.13}) + 2C_{\log} + 1 + C''\big) \\ & + C_{4.9}(\log(2) + C'') + \log(2C_{4.9}) + 1. \end{aligned}$$

In the second part of the proof, we relate the height of $\widetilde{\mathcal{F}}$ with the height of $\mathcal{F}$. The quotient

$$\frac{P(y_1 Y + a_1, \dots, y_{n-1} Y + a_{n-1}, Y + a_n)}{Q(y_1 Y + a_1, \dots, y_{n-1} Y + a_{n-1}, Y + a_n)}$$

is a way to write $\widetilde{\mathcal{F}}$ in irreducible form in $L(Y)$, and has a coefficient equal to 1. Therefore $h(\widetilde{\mathcal{F}})$ is the affine height of the coefficients appearing in the quotient. Hence

$$h\big(P(y_1 Y_n + a_1, \dots, y_{n-1} Y_n + a_{n-1}, Y_n + a_n)\big) \le C'\, d(\delta) \max\{1, \log l(\delta)\}$$

for every $(y_1, \dots, y_{n-1}) \in \mathcal{I}_{n-1}(P)$, and the same inequality holds for Q. Since $N_1 = 2d$, we can interpolate successively the variables $y_{n-1}, \dots, y_1$, using Proposition 5.5

with $2d$ evaluation points at each vertex of the tree T. Finally we obtain

$$\begin{aligned} h(\mathcal{F}) &\leq 2^{n-1}\big(C'\, d(\delta)\max\{1,\log l(\delta)\} + 4d\log(4d) + d\log(2M) + \log(d+1)\big) \\ &\leq 2^{n-1}\big(C' + 4C_{4.9}(\log(C_{4.9}) + C_{\log}) + C_{4.9}(\log(2) + C'') \\ &\qquad + \log(2C_{4.9}) + 1\big)\, d(\delta)\max\{1,\log l(\delta)\}. \end{aligned}$$

□

5.7. **Explicit height bounds in dimension 2.** In this final section, we derive explicit height bounds for modular equations of Siegel type for abelian surfaces. Our first aim is to provide an explicit value for the constant in Corollary 5.10, using Theta constants of level 4 as an intermediate step. To relate Theta heights and j-heights in this setting, we use Mestre's algorithm and Thomae's formulæ instead of writing out polynomials $N_{J,i}, D_{J,i}, N_{\Theta,i}$, and $D_{\Theta,i}$ as in the proof of Proposition 5.9.

Proposition 5.17. *Let A be a principally polarized abelian surface defined over $\overline{\mathbb{Q}}$ where j_1, j_2, j_3 are well defined, and assume that $j_3(A) \neq 0$. Then we have*

$$h_j(A) \leq 40\, h_{\Theta,4}(A) + 12 \quad \textit{and} \quad h_{\Theta,4}(A) \leq 200\, h_j(A) + 1000.$$

Proof. Recall the expression of Igusa invariants in terms of the Siegel modular forms I_4, I_6', I_{10}, and I_{12}:

$$j_1 = \frac{I_4 I_6'}{I_{10}}, \quad j_2 = \frac{I_4^2 I_{12}}{I_{10}^2}, \quad \text{and} \quad j_3 = \frac{I_4^5}{I_{10}^2}. \tag{15}$$

These modular forms have a polynomial expression in terms of theta constants of level 4: see for instance [33, §II.7.1]. The total degrees of the polynomials giving I_4, I_6', I_{10} and I_{12} are $8, 12, 20$ and 24 respectively; they contain respectively $10, 60, 1$ and 15 monomials, and their height is zero. Up to scaling, we may assume that the first theta constant θ_0 takes the value 1. Then, by Proposition 5.2, we have

$$h(I_4^5,\, I_4 I_6' I_{10},\, I_4^2 I_{12},\, I_{10}^2) \leq 5\log(10) + 40\, h_{\Theta,4}(A),$$

hence the first inequality

$$h_j(A) \leq 40\, h_{\Theta,4}(A) + 12.$$

For the second inequality, we follow Mestre's algorithm [22]. Starting from $j_1(A), j_2(A)$ and $j_3(A)$, Mestre's algorithm constructs a hyperelliptic curve $y^2 = f(x)$ whose Jacobian is isomorphic to A over $\overline{\mathbb{Q}}$. Choosing $I_{10} = 1$ in equation (15), we see that $j_1(A), j_2(A)$ and $j_3(A)$ are realized by values of I_2, I_4, I_6', and I_{10} in $\overline{\mathbb{Q}}$ such that

$$h(I_2, I_4, I_6', I_{10}) \leq h_j(A).$$

The roots of f are the intersection points of a conic and a cubic in $\mathbb{P}^2$ whose equations are given explicitly in terms of I_2, I_4, I_6, and I_{10}. In order to obtain the equation $\sum_{i,j=1}^3 c_{ij} z_i z_j = 0$ of the conic, we start from Mestre's equation $\sum_{i,j=1}^3 A_{ij} x_i x_j = 0$ and substitute the expressions of A, B, C, and D in terms of I_2, I_4, I_6', and I_{10}. Then we multiply by $2^{11}3^{13}5^{14}$ and make the substitutions

$$z_1 = 202500 x_1, \quad z_2 = 225 x_2, \quad z_3 = x_3.$$

Then, each coefficient c_{ij} has an expression as a multivariate polynomial in I_2, I_4, and I_6' (recall that $I_{10} = 1$) of total degree at most 7; its coefficients are integers whose absolute values are bounded by $324 \cdot 10^6$. By Proposition 5.2, we have

$$h\big((c_{ij})_{1\leq i,j\leq 3}\big) \leq 7(h_j(A) + \log(3)) + 19.6 + 3\log(8) \leq 7h_j(A) + 33.6.$$

If we restrict to c_{11}, c_{12}, and c_{22}, then we obtain a smaller upper bound, since the total degree and the height of coefficients are at most 5 and 18.3 respectively. Similarly, the cubic equation, denoted by $\sum_{1\leq i\leq j\leq k\leq 3} c_{ijk} z_i z_j z_k = 0$, has total degree at most 11 in I_2, I_4, and I_6', and has integer coefficients whose heights are at most 33.5.

In order to find the hyperelliptic curve equation f, we parametrize the conic. Let us show that it contains a point P_0 defined over $\overline{\mathbb{Q}}$ such that $h(P_0) \leq 5h_j(A) + 29.9$. We can assume that $c_{11} \neq 0$; otherwise we take $P_0 = (1 : 0 : 0)$. Let α be a root of the monic polynomial

$$\alpha^2 + \frac{c_{12}}{c_{11}}\alpha + \frac{c_{22}}{c_{11}} = 0.$$

The point $P_0 = (\alpha : 1 : 0)$ belongs to the conic, and by Proposition 5.4,

$$\begin{aligned} h(P_0) = h(\alpha) &\leq h(c_{11}, c_{12}, c_{22}) + \log(2) \\ &\leq 5(h_j(A) + \log(3)) + 18.3 + 3\log(6) + \log(2) \\ &\leq 5h_j(A) + 29.9. \end{aligned}$$

We parametrize the conic using P_0 as a base point; for simplicity, we continue to assume that $c_{11} \neq 0$. For $(u : v) \in \mathbb{P}^1(\overline{\mathbb{Q}})$, the point $(z_1 : z_2 : z_3)$ defined by

$$\begin{aligned} z_1 &= \alpha(c_{11}u^2 + c_{13}uv + c_{33}v^2) - u((2c_{11}\alpha + c_{12})u + (c_{13}\alpha + c_{23})v), \\ z_2 &= c_{11}u^2 + c_{13}uv + c_{33}v^2, \quad \text{and} \\ z_3 &= -v((2c_{11}\alpha + c_{12})u + (c_{13}\alpha + c_{23})v) \end{aligned}$$

runs through the conic. Substituting these expressions in the cubic equation gives the curve equation f. The polynomials we obtain have total degrees at most 29 in I_2, I_4, and I_6'; they have degree at most 3 in α; and their coefficients are integers whose heights are bounded above by 86.9. Therefore, by Proposition 5.2 (separating I_2, I_4, I_6' from α), we have

$$\begin{aligned} h(f) &\leq 29(h_j(A) + \log(3)) + 86.9 + 3(5h_j(A) + 29.9) + 3\log(30) + \log(4) \\ &\leq 44h_j(A) + 220.1. \end{aligned}$$

Making f monic does not change its height.

Thomae's formulæ [28, IIIa.8.1] give an expression of the Theta constants of level 4 of A in terms of roots of f: if θ is one of these Theta constants, then θ^4 is a product of 18 differences of roots of f (up to a common multiplicative factor). Therefore, by Proposition 5.4, we obtain

$$h_{\Theta,4}(A, L) \leq \tfrac{1}{4} \cdot 18(h(f) + \log(4)) \leq 198h_j(A) + 997.$$

□

As a consequence, we obtain an explicit analogue of Corollary 5.10 in the case of isogenies between principally polarized abelian surfaces.

Proposition 5.18. *Let A and A' be principally polarized abelian surfaces over $\overline{\mathbb{Q}}$ where j_1, j_2, j_3 are well defined, and assume that $j_3(A)j_3(A') \neq 0$. Let $d \geq 1$ be an integer. If A and A' are linked by an isogeny of degree d, then we have*

$$\overline{h}_j(A') \leq 8000\,\overline{h}_j(A) + 1.08 \cdot 10^{11} \log(\overline{h}_j(A)) + 1.67 \cdot 10^{12} + 20 \log d.$$

Proof. By Theorem 5.8 and Proposition 5.7 and 5.17 (noting that $C(2,4) \leq 1.35 \cdot 10^9$), we have

$$\begin{aligned}
\overline{h}_{\Theta,4}(A) &\leq 200\,\overline{h}_j(A) + 1000,\\
\tfrac{1}{2}\,\overline{h}_F(A) &\leq \overline{h}_{\Theta,4}(A) + C(2,4)\log(\overline{h}_{\Theta,4}(A) + 2)\\
&\leq 200\,\overline{h}_j(A) + C(2,4)\log(1202) + C(2,4)\log(\overline{h}_j(A)),\\
\tfrac{1}{2}\,\overline{h}_F(A') &\leq \tfrac{1}{2}\,\overline{h}_F(A) + \tfrac{1}{4}\log \ell,\\
\overline{h}_{\Theta,4}(A') &\leq \tfrac{1}{2}\,\overline{h}_F(A') + C(2,4)\log(\overline{h}_F(A') + 2)\\
&\leq 200\,\overline{h}_j(A) + C(2,4)\log(1202) + 2C(2,4)\log(\overline{h}_j(A)) + \tfrac{1}{4}\log \ell\\
&\quad + C(2,4)\log\big(402 + 2C(2,4)\log(1202) + C(2,4) + \tfrac{1}{2}\log \ell\big),\\
&\leq 200\,\overline{h}_j(A) + 2C(2,4)\log(\overline{h}_j(A)) + 4.17 \cdot 10^{10} + \tfrac{1}{2}\log \ell, \quad \text{and}\\
\overline{h}_j(A') &\leq 40\,\overline{h}_{\Theta,4}(A) + 12\\
&\leq 8000\,\overline{h}_j(A) + 80C(2,4)\log \overline{h}_j(A) + 1.67 \cdot 10^{12} + 20\log \ell.
\end{aligned}$$

□

In Lemma 5.12, we take $\lambda = I_4$ and $\lambda' = I_4 I_{10}$. We have

$$\mathrm{wt}(\lambda^\delta) = 14\,d(\delta) + 4,$$

which is greater than 16, the minimum weight for which Siegel modular forms define a projective embedding of $\mathcal{S}$. Hence ξ can be chosen to be a modular form of weight $\mathrm{wt}(\lambda^\delta)$. The fraction R'' has degree at most $\frac{7}{3}(d(\delta)+1)$ by Lemma 4.10; this is also an upper bound on $\deg(P_\delta)$.

We also mimic the proof of Proposition 5.13 in the Siegel case. Let $[x, g]$ be a point of $\mathcal{S}$ with Igusa invariants $(j_1, j_2, j_3) \in \mathcal{V}_\delta$. For each $1 \leq m \leq 3$, by Remark 3.5, the polynomial $\Psi_{\delta,m}(j_1, j_2, j_3)$ is the evaluation of a multivariate polynomial in $2\,d(\delta)$ variables. Moreover, the Hecke correspondence describes isogenies of degree ℓ^2. By Proposition 5.18, we have

(16)
$$h\big(\Psi_{\delta,m}(j_1,j_2,j_3)\big) \leq 2\,d(\delta)\big(8000\,\overline{h}(j_1,j_2,j_3) + 1.08\cdot 10^{11}\log(\overline{h}_j(A)) + 1.67\cdot 10^{12} + 40\log \ell\big).$$

Therefore, we can take

$$C_{5.13} = 3.35 \cdot 10^{12}.$$

Moreover, we have $d(\delta) = \ell^3 + \ell^2 + \ell + 1$ and $l(\delta) = \ell^2$. Hence we can take

$$C_{\log} = \frac{3}{2} + \log(2) \leq 2.2.$$

We also take

$$\begin{aligned}
C_{5.6} &= 960 && \text{because } L = \mathbb{Q},\\
C_{4.9} &= \frac{10}{3} && \text{by Proposition 4.11, and}\\
C_{5.12} &= 15 && \text{since } d(\delta) \geq 15.
\end{aligned}$$

In Lemma 5.15, we can take

$$C_{5.15} = 1.36 \cdot 10^{17}$$

and in Theorem 5.16, we can take

$$C_{5.16} = 1.42 \cdot 10^{15}.$$

Since $d(\delta) \leq 2\ell^3$ and $\max\{1, \log \ell(\delta)\} \leq 2\log(\ell)$, we obtain the following result.

Theorem 5.19. *Let $\ell \geq 1$ be a prime number, and let $\mathcal{F} \in \mathbb{Q}(J_1, J_2, J_3)$ be a coefficient of one of the Siegel modular equations of level ℓ in Igusa invariants. Then we have*

$$h(\mathcal{F}) \leq 5.68 \cdot 10^{15} \ell^3 \log(\ell).$$

In order to obtain tighter height bounds on Siegel modular equations, we could repeat the computations of §5.6 using an expression of the form (16) for the height of evaluated modular equations, instead of the simpler formula used in Proposition 5.13. However we cannot hope to obtain a constant in Theorem 5.19 that is much smaller than $C(2,4) \simeq 1.35 \cdot 10^9$ using our methods. Experimentally, we observe that the tighter inequalities $h(\mathcal{F}) \leq 48.7\, \ell^3 \log(\ell)$ and $h(\mathcal{F}) \leq 43.6\, \ell^3 \log(\ell)$ hold for $\ell = 2$ and $\ell = 3$ respectively.

We could also give an analogue of Theorem 5.19 in the case of modular equations of Hilbert type for $\mathbb{Q}(\sqrt{5})$ in Gundlach invariants. To replace Proposition 5.17, we would use the relations between Gundlach and Igusa invariants (see for instance [25, §2.3]) and the explicit curve equation given by [19, Prop. A.4]. We leave the precise calculations for future work.

Acknowledgements. The author thanks Fabien Pazuki and his Ph.D. advisors, Damien Robert and Aurel Page, for answering the author's questions. The author also thanks the anonymous referees for helpful comments. Finally, acknowledgments are due to Aurel Page for his careful proofreading of an earlier version of the paper.

References

[1] W. L. Baily, Jr. and A. Borel. Compactification of arithmetic quotients of bounded symmetric domains. *Ann. of Math. (2)*, 84:442–528, 1966.
[2] C. Birkenhake and H. Lange. *Complex abelian varieties*. Springer, second edition, 2004.
[3] R. Bröker and K. Lauter. Modular polynomials for genus 2. *LMS J. Comp. Math.*, 12:326–339, 2009.
[4] R. Bröker and A. V. Sutherland. An explicit height bound for the classical modular polynomial. *Ramanujan J.*, 22(3):293–313, 2010.
[5] J. H. Bruinier. Hilbert modular forms and their applications. In *The 1-2-3 of modular forms*, Universitext, pages 105–179. Springer, 2008.
[6] H. Carayol. Sur la mauvaise réduction des courbes de Shimura. *Compositio Math.*, 59(2):151–230, 1986.
[7] C. Chevalley. Deux théorèmes d'arithmétique. *J. Math. Soc. Japan*, 3(1):36–44, 1951.
[8] P. Cohen. On the coefficients of the transformation polynomials for the elliptic modular function. *Math. Proc. Cambridge Philos. Soc.*, 95(3):389–402, 1984.
[9] D. A. Cox. *Primes of the form $x^2 + ny^2$*. John Wiley & Sons, second edition, 2013.
[10] P. Deligne. Travaux de Shimura, 1970.
[11] N. D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational perspectives on number theory (Chicago, 1995)*, volume 7, pages 21–76. Amer. Math. Soc., 1998.
[12] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörper. *Invent. Math.*, 73(3):349–366, 1983.

[13] E. Freitag. *Hilbert modular forms*. Springer-Verlag, 1990.
[14] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng. The 2-adic CM method for genus 2 curves with application to cryptography. In *Advances in Cryptology – Asiacrypt 2006*, pages 114–129, Shanghai, 2006. Springer.
[15] K.-B. Gundlach. Die Bestimmung der Funktionen zur Hilbertschen Modulgruppe des Zahlkörpers $\mathbb{Q}(\sqrt{5})$. *Math. Ann.*, 152:226–256, 1963.
[16] M. Hindry and J. H. Silverman. *Diophantine geometry*. Springer, 2000.
[17] J.-I. Igusa. On Siegel modular forms of genus two. *Amer. J. Math.*, 84:175–200, 1962.
[18] J. Kieffer. Upper bounds on the heights of polynomials and rational fractions from their values. 2020.
[19] J. Kieffer, A. Page, and D. Robert. Computing isogenies from modular equations in genus two. 2019.
[20] K. Lauter and T. Yang. Computing genus 2 curves from invariants on the Hilbert moduli space. *J. Number Theory*, 131(5):936–958, 2011.
[21] C. Martindale. Hilbert modular polynomials. *J. Number Theory*, 213:464–498, 2020.
[22] J.-F. Mestre. Construction de courbes de genre 2 à partir de leurs modules. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, page 313–334. Birkhäuser, 1991.
[23] E. Milio. Database of modular polynomials. https://members.loria.fr/EMilio/modular-polynomials.
[24] E. Milio. A quasi-linear time algorithm for computing modular polynomials in dimension 2. *LMS J. Comput. Math.*, 18:603–632, 2015.
[25] E. Milio and D. Robert. Modular polynomials on Hilbert surfaces. *J. Number Theory*, 216:403–459, 2020.
[26] J. S. Milne. Canonical models of (mixed) Shimura varieties and automorphic vector bundles. In *Automorphic forms, Shimura varieties, and L-functions (Ann Arbor, 1988)*, volume 1, page 283–414. Academic Press, 1990.
[27] J. S. Milne. Introduction to Shimura varieties. In *Harmonic analysis, the trace formula, and Shimura varieties*, pages 265–378. Amer. Math. Soc., 2005.
[28] D. Mumford. *Tata lectures on theta. II*. Birkhäuser, 1984.
[29] E. Noether. Der Endlichkeitssatz der Invarianten endlicher Gruppen. *Math. Ann.*, 77(1):89–92, 1915.
[30] F. Pazuki. Theta height and Faltings height. *Bull. Soc. Math. France*, 140(1):19–49, 2012.
[31] F. Pazuki. Modular invariants and isogenies. *Int. J. Number Theory*, 15(3):569–584, 2019.
[32] R. Schoof. Counting points on elliptic curves over finite fields. *J. Théorie Nr. Bordx.*, 7(1):219–254, 1995.
[33] M. Streng. *Complex multiplication of abelian surfaces*. PhD thesis, Universiteit Leiden, 2010.
[34] A. V. Sutherland. Computing Hilbert class polynomials with the Chinese remainder theorem. *Math. Comp.*, 80(273):501–538, 2011.
[35] G. van der Geer. *Hilbert modular surfaces*. Springer, 1988.