HAL open science

Degree and height estimates for modular equations on PEL Shimura varieties

Jean Kieffer

To cite this version:

Jean Kieffer. Degree and height estimates for modular equations on PEL Shimura varieties. 2020. hal-02436057v2

HAL Id: hal-02436057

https://hal.science/hal-02436057v2

Preprint submitted on 6 Mar 2020 (v2), last revised 16 Aug 2021 (v4)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Degree and height estimates for modular equations on PEL Shimura varieties

Jean Kieffer

Université de Bordeaux
jean.kieffer@math.u-bordeaux.fr

Abstract

We define modular equations in the setting of PEL Shimura varieties as equations describing Hecke correspondences, and prove degree and height bounds for them. This extends known results about classical modular polynomials. In particular, we obtain tight degree bounds for modular equations of Siegel and Hilbert type for abelian surfaces. One step consists in proving tight bounds on the heights of rational fractions over number fields in terms of the heights of their evaluations; the results we obtain are of independent interest.

1 Introduction

Modular equations encode the presence of isogenies between polarized abelian varieties. The classical modular polynomial Φ_ℓ is an example: 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. Analogues of Φ_ℓ for principally polarized abelian surfaces, called Siegel and Hilbert modular polynomials in dimension 2, have recently been defined and computed [18, 19, 15].

In 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. Let H_δ be a Hecke correspondence of degree $d(\delta)$ on such a Shimura variety. In the modular interpretation, H_δ parametrizes isogenies of a certain degree $\ell(\delta)$. Given connected components $\mathcal{S}$, $\mathcal{S}'$ of the Shimura variety and a choice of invariants on them, we define modular equations $\Psi_{\delta,m}$ as a set of polynomials describing H_δ on $\mathcal{S} \times \mathcal{S}'$. The coefficients of $\Psi_{\delta,m}$ are rational fractions defined over a number field, and we prove that their degrees and heights are governed by $d(\delta)$ and $\ell(\delta)$.

Theorem 1.1. *Let $\mathcal{S}$, $\mathcal{S}'$ be connected components of a simple PEL Shimura variety of type (A) or (C) of finite level, and choose invariants on them. Then there exists explicit constants C_1, C_2 depending on this setting such that the following holds. Let H_δ be a Hecke correspondence of degree $d(\delta)$ describing isogenies of degree $\ell(\delta)$ between abelian varieties with PEL structure, and assume that $H(\delta)$ intersects $\mathcal{S} \times \mathcal{S}'$ nontrivially. Let $\mathcal{F}$ be a rational fraction occurring as a coefficient of one of the modular equations $\Psi_{\delta,m}$. Then*

1. *The total degree of $\mathcal{F}$ is bounded by $C_1\, d(\delta)$. The same estimate holds if we require all the fractions $\mathcal{F}$ to share a common denominator.*
2. *The height of $\mathcal{F}$ is bounded by $C_2\, d(\delta) \log \ell(\delta)$.*

This result generalizes known bounds about the size of the classical modular polynomial Φ_ℓ, which has coefficients in $\mathbb{Z}$, is symmetric, and has degree $\ell+1$ in both variables. The height $h(\Phi_\ell)$ is then the maximum value of $\log|c|$, where c ranges over the coefficients of Φ_ℓ. We have $h(\Phi_\ell) \sim 6\ell\log(\ell)$ as ℓ grows [8], and explicit bounds can be given [5]. In particular Theorem 1.1 seems optimal up to the value of the constants. For abelian surfaces, even degree bounds for modular equations were unknown, and the degree bounds we obtain match exactly with experimental data.

From the algorithmic point of view, Theorem 1.1 provides complexity bounds for algorithms involving modular equations. For instance, classical modular polynomials are used for instance in the SEA algorithm to count points on elliptic curves [26], and in multi-modular methods to compute class polynomials of imaginary quadratic fields [28]; being able to compute isogenies also has applications in elliptic curve cryptography. General modular equations are of similar interest.

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 invariants transforms bounded weight into bounded degree. The proof of part 2 is inspired by previous works on Φ_ℓ [24]. We prove height bounds on *evaluations* of modular equations at certain points using well-known results on the Faltings height of isogenous abelian surfaces. To obtain bounds on *coefficients* of modular equations, we need to bound the height of a rational fraction from the heights of its values at certain points. Since the bounds obtained from a direct analysis of the interpolation algorithm are inefficient in our setting, it is crucial to use more evaluation points than the required number for the interpolation problem to have a unique solution. We prove the following result in this direction.

Theorem 1.2. *Let L be a number field of degree d_L. Then there exists an explicit constant C_3, depending only on L, such that the following holds. Let $[\![A,B]\!]$ be an interval in $\mathbb{Z}$; write $D = B - A$ and $M = \max\{|A|,|B|\}$. Let $\mathcal{F} \in L(Y)$ be a rational fraction of degree at most $d \geq 1$. Let $S \subset [\![A,B]\!]$ containing at least $2D/3$ elements and no poles of $\mathcal{F}$. Let $H \geq \max\{3, \log(2M)\}$, and assume that*

(i) $h(\mathcal{F}(y)) \leq H$ *for every* $y \in S$.

(ii) $D > \max\{d^4 H \log(dH), 6d\, d_L\}$.

Then we have

$$h(\mathcal{F}) \leq 3H + C_3 \log(dH) + 3d\log(2M).$$

In contrast, the height bound obtained from the interpolation algorithm is of the order of d^2H. Theorem 1.2 seems new even in the simpler case $L = \mathbb{Q}$ and is of independent interest.

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. Section 4 is devoted to the proof of the degree bounds. Then we recall basic facts about heights, and prove

Theorem 1.2, in Section 5. We finish the proof of height bounds for modular equations in Section 6.

Notation. Throughout the paper, the symbol C stands for an explicit constant depending only on the PEL setting. Its value may change from one line to the next unless we label it explicitly as C_1, etc.

Acknowledgements. The author thanks Fabien Pazuki and his Ph.D. advisors, Damien Robert and Aurel Page, for helpful discussions and answering the author's questions. The author also thanks Aurel Page for his careful proofreading of the paper.

2 Background on PEL Shimura varieties

Our presentation is inspired by Milne's [21], which serves 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,
- $\nu : G \to T$ 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 $\mathbb{Q}$.

2.1 Simple PEL Shimura varieties of type (A) or (C)

Let $(B, *)$ be a simple $\mathbb{Q}$-algebra with positive involution. The center F of B is a number field; let F_0 be the subfield of invariants under $*$. For simplicity, we make the technical assumption that B is of type (A) or (C) [21, Prop. 8.3].

Let (V, ψ) be a faithful symplectic $(B, *)$-module. This means that V is a faithful B-module equipped with an 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 algebraic subgroup defined by

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

We warn the reader that our G is denoted G_1 in [21, §8], and that consequently the definition of a PEL Shimura variety used here differs slightly from Milne's. The group G is connected and reductive, and by [21, Prop. 8.7], its derived group is $G^{\mathrm{der}} = \ker(\mu) \cap \ker(\det)$.

Let x be a *complex structure* on $V(\mathbb{R})$, meaning an endomorphism of $V(\mathbb{R})$ such that $x \circ x = -1$. We say that x is *positive* for ψ if it commutes with the action of B and the form $(u, v) \mapsto \psi\big(u, x(v)\big)$ is symmetric and positive definite. Such a complex structure x_0 exists [21, 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 [21, Cor. 5.8]. We call the pair (G, X_+) a *simple PEL Shimura datum of type (A) or (C)*, or simply a *PEL datum*.

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 coset

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

In the first description, $G(\mathbb{Q})_+$ 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 projection to the second factor induces a map with connected fibers from $\mathrm{Sh}_K(\mathbb{C})$ to the double coset $G(\mathbb{Q})_+ \backslash G(\mathbb{A}_f)/K$, which is finite [21, Lem. 5.12]. Let $\mathcal{C}$ be a set of representatives in $G(\mathbb{A}_f)$ for this double coset. 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 $\mathrm{Aut}(X_+)$ [21, Lem. 5.13]. Thus, the Shimura variety has a natural structure of a complex analytic space, and is an algebraic variety by the theorem of Baily and Borel [21, Thm. 3.12].

Since G^{der} is simply connected, by [21, Thm. 5.17 and Lem. 5.20], 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} [21, Rem. 5.23].

In fact, $\mathrm{Sh}_K(G, X_+)$ exists as an algebraic variety defined over the *reflex field*, which is a number field depending only on G and X_+ [21, §12-14]. In general, the field of definition of an individual connected component of $\mathrm{Sh}_K(\mathbb{C})$ may be larger.

2.2 The modular interpretation

The Shimura variety $\mathrm{Sh}_K(G, X_+)(\mathbb{C})$ has a modular interpretation in terms of *isogeny* classes of abelian varieties with PEL structure [21, Thm. 8.17]. After choosing lattices in V, we can rephrase it in terms of *isomorphism* classes of

such varieties, in a flavor similar to [6, §2.6.2]. This second description is closer to the applications we have in mind.

A *lattice* in a topological abelian group is a cocompact and discrete subgroup. Recall that the map $\Lambda \mapsto \widehat{\Lambda} = \Lambda \otimes \widehat{\mathbb{Z}}$ is a bijection between lattices in V and lattices in $V(\mathbb{A}_f)$; its inverse is intersection with $V(\mathbb{Q})$.

Let $\widehat{\Lambda}_0$ be a lattice in $V(\mathbb{A}_f)$ that is stabilized by K, and let $\Lambda_0 = \widehat{\Lambda}_0 \cap V(\mathbb{Q})$. Let $\mathcal{O}$ be the largest order in B stabilizing Λ_0. We construct a standard polarized lattice for each connected component as follows. For $c \in \mathcal{C}$, write

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

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. Choose $\lambda_c \in \mathbb{Q}_+^\times$ such that $\psi_c = \lambda_c \psi$ takes integer values on $\Lambda_c \times \Lambda_c$. Define

$$\Lambda_c^\perp = \{v \in V(\mathbb{Q}) \mid \forall w \in \Lambda_c,\ \psi_c(v,w) \in \mathbb{Z}\}.$$

Then $\Lambda_c^\perp$ is a lattice in V containing Λ_c. We call the finite group $\mathcal{T}_c = \Lambda_c^\perp / \Lambda_c$ the *polarization type* of (Λ_c, ψ_c).

We first formulate a modular interpretation using lattices. Let $\mathcal{Z}_c$ be the set of isomorphism classes of 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 $\mathcal{O} \hookrightarrow \mathrm{End}_{\mathbb{Z}}(\Lambda)$,
- $\phi : \Lambda \times \Lambda \to \mathbb{Z}$ 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: $(\star)$ there exists an isomorphism of $\mathcal{O}$-modules $a : \Lambda \to \Lambda_c$, carrying ηK to cK and x to an element of X_+, such that

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

Isomorphisms between tuples are isomorphisms of $\mathcal{O}$-modules $f : \Lambda \to \Lambda'$ that send x to x', send ηK to $\eta' K$, and such that $\phi(u,v) = \phi'\big(\zeta f(u), f(v)\big)$ for some $\zeta \in \mu(\Gamma_c)$.

In particular, for every $(\Lambda, x, \iota, \phi, \eta K) \in \mathcal{Z}_c$, the complex structure x is positive for ϕ, the Rosati 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 type of the polarization ϕ on Λ is $\mathcal{T}_c$.

Theorem 2.1. *Let $c \in \mathcal{C}$, let $\mathcal{S}_c = \Gamma_c \backslash X_+$ be the associated connected component of $\mathrm{Sh}_K(G, X_+)(\mathbb{C})$, and define $\mathcal{Z}_c$ as above. Then the map*

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

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 [21, Prop. 6.3]. □

We want to rephrase Theorem 2.1 using the language 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. Giving a polarization on A is the same as giving an alternating nondegenerate bilinear form ϕ taking integral values on Λ such that $(u, v) \mapsto \phi(u, iv)$ is symmetric and positive definite. Then, endomorphisms of A correspond to endomorphisms of Λ that respect the complex structure, and $\Lambda \otimes \widehat{\mathbb{Z}}$ is canonically isomorphic to the global Tate module

$$\widehat{T}(A) = \prod_{\ell \text{ prime}} T_\ell(A).$$

When $c \in \mathcal{C}$ is fixed, we define a *complex abelian variety with PEL structure* to be a tuple $(A, \phi, \iota, \eta K)$ where

- (A, ϕ) is a complex polarized abelian variety with polarization type $\mathcal{T}_c$,
- ι is an embedding $\mathcal{O} \hookrightarrow \mathrm{End}(A)$ such that the Rosati involution on B is $*$,
- 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: $(\star)$ there exists an isomorphism of $\mathcal{O}$-modules $a : H_1(A, \mathbb{Z}) \to \Lambda_c$, carrying ϕ to ψ_c, carrying ηK to cK, and such that the induced complex structure on $V(\mathbb{R})$ belongs to X_+.

The difference with the setting of Theorem 2.1 is that isomorphisms of polarized abelian varieties should respect the polarizations *exactly*, rather than up to an element of $\mu(\Gamma_c)$. In general, $\mu(\Gamma_c)$ is not trivial, but there is the following workaround. If $\varepsilon \in F^\times$, then multiplication by ε defines an element in the center of $G(\mathbb{Q})$, so it makes sense to define

$$\mathcal{E} = \{\varepsilon \in F^\times \mid \varepsilon \in K\} = \{\varepsilon \in F^\times \mid \varepsilon \in \Gamma_c\}.$$

Theorem 2.2. *Let $c \in \mathcal{C}$, and assume that $\mu(\mathcal{E}) = \mu(\Gamma_c)$. Then the map*

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

where $V(\mathbb{R})$ is seen as a complex vector space via x, and ι is the action of $\mathcal{O}$ 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.

Proof. When defining $\mathcal{Z}_c$, we can impose $\zeta = 1$ in condition $(\star)$ and strengthen the notion of isomorphism between tuples to respect the polarizations exactly: indeed, multiplying a by some $\varepsilon \in \mathcal{E}$ leaves everything invariant except the alternating form, which gets multiplied by $\mu(\varepsilon)$. The result follows then from Theorem 2.1. □

Remark 2.3. In any case, $\mu(\mathcal{E})$ has finite index in $\mu(\Gamma_c)$: indeed, if $\mathbb{Z}_{F_0}^\times$ denotes the unit group of F_0, we have

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

and $\mathcal{E}$ contains a subgroup of finite index in $\mathbb{Z}_{F_0}^\times$. By [7, Th. 1], there exists a compact open subgroup M of $\mu(K)$ such that $\mathbb{Z}_{F_0}^\times \cap M = \mu(\mathcal{E})$. Define $K' = K \cap \mu^{-1}(M)$, and denote by Γ'_c the associated arithmetic subgroups. Then $\mathcal{E}$ remains the same for K', and for $c \in G(\mathbb{A}_f)$ we have

$$\Gamma'_c = \{\gamma \in \Gamma_c \mid \mu(\gamma) \in \mu(\mathcal{E})\}.$$

Thus raising the level allows us to reach the situation of Theorem 2.2, at the cost of adding connected components.

2.3 Modular forms on PEL Shimura varieties

A *modular form* of weight $w \in \mathbb{Z}$ on $\mathrm{Sh}_K(G, X_+)(\mathbb{C})$ is a function

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

that satisfies suitable growth and holomorphy conditions [20, Prop. 3.2], and such that

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

Here $\rho : K_\infty \to \mathbb{C}^\times$ is a certain canonical character of K_∞. The weight of f is denoted by $\mathrm{wt}(f)$. We also say that f is *of level* K.

From a geometric point of view, there is a line bundle $\mathcal{M}$ on $\mathrm{Sh}_K(\mathbb{C})$ such that modular forms of weight w are the holomorphic sections of $\mathcal{M}^{\otimes w}$ that are again holomorphic when extended to the Baily-Borel compactification of $\mathrm{Sh}_K(\mathbb{C})$. In fact, $\mathcal{M}$ is the inverse determinant of the tangent bundle on Sh_K [1, Prop. 7.3].

Let $\mathcal{S}$ be a connected component of $\mathrm{Sh}_K(\mathbb{C})$, and L its field of definition. A modular form of weight w on $\mathcal{S}$ is simply the restriction to $\mathcal{S}$ of a weight w modular form on $\mathrm{Sh}_K(\mathbb{C})$. Modular forms on $\mathcal{S}$ generate a graded ring. The following result is well known; since we did not find a precise reference in the literature, we present a short proof.

Theorem 2.4. *The graded ring of modular forms on $\mathcal{S}$ is generated by finitely many elements defined over L, and modular forms of sufficiently high weight realize a projective embedding of $\mathcal{S}$. Every meromorphic function on $\mathcal{S}$ is a quotient of two modular forms of the same weight.*

Proof. As shown by Baily and Borel [1, Thm. 10.11], modular forms of sufficiently high weight give a projective embedding of $\mathcal{S}$ which is a priori defined over $\mathbb{C}$. In other words, the line bundle $\mathcal{M}$ is ample on $\mathcal{S}$. It can be defined over L, and remains ample as a line bundle on the variety $\mathcal{S}$ over L. Therefore the graded L-algebra

$$\bigoplus_{w \geq 0} H^0(\mathcal{S}, \mathcal{M}^{\otimes w})$$

is finitely generated, and consists of modular forms defined over L. They also give a projective embedding provided the weight is high enough. The second part of the statement is an easy consequence of the first. $\square$

We can also consider modular forms that are symmetric under certain automorphisms of Sh_K. Let Σ be a finite group of automorphisms of G that leaves $G(\mathbb{Q})_+$, K, K_∞, ν and the character ρ invariant. Then for every modular form f of weight w on $\mathcal{S}$, and every $\sigma \in \Sigma$, the function

$$f^\sigma \ : \ [x, g] \mapsto f([\sigma(x), \sigma(g)])$$

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

Proposition 2.5. *Let Σ be a finite group of automorphism of G as above. Then symmetric modular forms generate a graded ring that is also finitely generated over L, and every symmetric modular function is the quotient of two symmetric modular forms of sufficiently high weight.*

Proof. This is a consequence of Theorem 2.4 and Noether's theorem [22] on invariants under finite groups. $\square$

2.4 Hecke correspondences

Let $\delta \in G(\mathbb{A}_f)$, and let $K' = K \cap \delta K \delta^{-1}$. Consider the diagram

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

where the map $R(\delta)$ is $[x, g] \mapsto [x, g\delta]$. 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, and are defined over the reflex field [21, Thm. 13.6].

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

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

It is finite as both K and K' are compact open in $G(\mathbb{A}_f)$, and is the degree of the map $p_1 \ : \ H_\delta \to \mathrm{Sh}_K$. We 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 $t\,\nu(\delta)$.

In the modular interpretation, Hecke correspondences describe isogenous abelian varieties such that the isogeny is of a certain type. Let us describe the

construction. After multiplying δ by a suitable element in $\mathbb{Q}^\times$, which does not change H_δ, we can assume that $\delta(\widehat{\Lambda}_0) \subset \widehat{\Lambda}_0$. Write

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

Let $c \in \mathcal{C}$, 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 Theorem 2.1.

Partition the orbit cK into K'-orbits $c\kappa_i K'$. Each $c\kappa_i\delta$ is then a $\widehat{\mathbb{Z}}$-linear embedding of $\mathcal{O}$-modules $\widehat{\Lambda}_0 \hookrightarrow \widehat{\Lambda}_c$; it is well defined up to right multiplication by $\delta^{-1}K'\delta$, hence by K. Let $\Lambda_i \subset \Lambda_c$ 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 2.6. *Let $\delta \in G(\mathbb{A}_f)$. Let $c \in \mathcal{C}$ and let $\mathcal{S}_c$ be the associated connected component of $\mathrm{Sh}_K(\mathbb{C})$. Let $z = [x, c] \in \mathcal{S}_c$, and construct Λ_i, q_i, c' as above. Then the image of z by the Hecke correspondence H_δ is given by the $d(\delta)$ isomorphism classes of tuples with representatives*

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

Proof. 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 $\Lambda_{c'}$. □

We define the *isogeny degree* of H_δ as

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

Corollary 2.7. *Let $\delta \in G(\mathbb{A}_f)$. Then, in the modular interpretation of Theorem 2.2, 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 i, there exists an isogeny $A \to A_i$ of degree $\ell(\delta)$.*

Proof. By Proposition 2.6, the Hecke correspondence consists in taking $d(\delta)$ suitable sublattices $\Lambda_i \subset \Lambda_c$, and then descending the polarization to recover something isomorphic to the standard lattice $\Lambda_{c'}$. Since the complex structure remains the same, and $\Lambda_c/\Lambda_i \simeq \widehat{\Lambda}_0/\delta(\widehat{\Lambda}_0)$, the result follows. □

For later purposes, we state a relation between $d(\delta)$ and $\ell(\delta)$.

Lemma 2.8. *We have $d(\delta) \le C\,\ell(\delta)^C$.*

Proof. Since K is open, we can find an integer $N \geq 1$ such that

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

Then $K \cap \delta K \delta^{-1}$ contains those elements $g \in G(\mathbb{A}_f) \cap \mathrm{GL}(\widehat{\Lambda}_0)$ that are the identity modulo $\widehat{\Lambda} = N\widehat{\Lambda}_0 \cap N\delta(\widehat{\Lambda}_0)$. This $\widehat{\Lambda}$ belongs to the set $\mathcal{Y}$ of sublattices of index $N^{\dim V}\ell(\delta)$ in $\widehat{\Lambda}_0$. We have $\#\mathcal{Y} \leq C\,\ell(\delta)^C$. The group K acts on $\mathcal{Y}$, and $K \cap \delta K \delta^{-1}$ contains the stabilizer of $\widehat{\Lambda}$; the claim follows. □

3 Modular equations on PEL Shimura varieties

3.1 The PEL setting

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 $n \neq 0$. Let $\mathcal{S}$, $\mathcal{S}'$ be connected components of $\mathrm{Sh}_K(G, X_+)(\mathbb{C})$, and let L be a number field over which $\mathcal{S}$ and $\mathcal{S}'$ are defined.

To complete the picture, we also need to choose *invariants*, which are coordinates on $\mathcal{S}$, $\mathcal{S}'$ given by modular functions. Since the field $L(\mathcal{S})$ of functions on $\mathcal{S}$ has transcendence degree n, the field $L(\mathcal{S})^\Sigma$ of functions on $\mathcal{S}$ that are symmetric under Σ also has transcendence degree n. Choose a transcendence basis $(j_1, \ldots, j_n)$ of $L(\mathcal{S})^\Sigma$, and another symmetric function j_{n+1} that generates the remaining finite extension. On $\mathcal{S}$, the function j_{n+1} satisfies a minimal relation of the form

$$j_{n+1}^e + \sum_{k=0}^{e-1} E_k(j_1, \ldots, j_n)\, j_{n+1}^k = 0. \tag{E}$$

We proceed similarly to define a basis of functions on $\mathcal{S}'$: no confusion will arise if we also denote them by $j_1, \ldots, j_{n+1}$. We refer to all the data defined up to now as the *PEL setting*. Throughout the paper, the symbol C refers to a constant that depends on this data only.

3.2 Definition of modular equations

Let $\delta \in G(\mathbb{A}_f)$ defining a Hecke correspondence H_δ that intersects $\mathcal{S} \times \mathcal{S}'$ nontrivially. We want to define explicit polynomials, called *modular equations* of level δ, describing H_δ in the product $\mathcal{S} \times \mathcal{S}'$.

The ring of meromorphic functions on H_δ, denoted by $L(H_\delta)$, is a finite extension of degree $(\#\Sigma)\, d(\delta)$ of $L(\mathcal{S})^\Sigma$. We can identify it with the ring of modular functions of trivial weight on $\widetilde{\mathcal{S}} \subset \mathrm{Sh}_{K'}(\mathbb{C})$, where $K' = K \cap \delta K \delta^{-1}$ and $\widetilde{\mathcal{S}}$ is the preimage of $\mathcal{S}$ in $\mathrm{Sh}_{K'}(\mathbb{C})$. Let

$$K'' = \bigcap_{\sigma \in \Sigma} \sigma(K') = K \cap \bigcap_{\sigma \in \Sigma} \sigma(\delta) K \sigma(\delta)^{-1}.$$

There is a right action of $K \rtimes \Sigma$ on modular forms for K'', given by

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

For $\gamma \in K \rtimes \Sigma$, we write this action as $f \mapsto f^{\gamma}$. The modular forms invariant under $K' \times \{1\}$ (resp. $K \rtimes \Sigma$) are exactly the elements of $L(H_\delta)$ (resp. $L(\mathcal{S})^{\Sigma}$). The functions

$$j_{k,\delta} \ : \ [x, g] \mapsto j_k([x, g\delta])$$

for $1 \leq k \leq n+1$ belong to $L(H_\delta)$. We define the chain of subgroups

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

where K_m is the subgroup that leaves $j_{1,\delta}, \ldots, j_{m,\delta}$ invariant, and we write $d_i = [K_{i-1} : K_i]$.

Definition 3.1. The *modular equations* of level δ on $\mathcal{S} \times \mathcal{S}'$ are the tuple $(\Psi_{\delta,1}, \Psi_{\delta,2}, \ldots, \Psi_{\delta,n+1})$ defined as follows: for each $1 \leq m \leq n+1$, set

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

where the middle product is over all $\gamma_i \in K_0/K_i$ such that $\gamma_i = \gamma \bmod K_{i-1}$, but $\gamma_i \neq \gamma \bmod K_i$.

Therefore, $\Psi_{\delta,m}$ is a multivariate polynomial in the m variables $Y_1, \ldots, Y_m$. 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.

Lemma 3.2. *The coefficients of $\Psi_{\delta,m}$ lie in $L(j_1, \ldots, j_{n+1})$. The degree of $\Psi_{\delta,m}$ in Y_m is d_m, and its degree in Y_i for $i < m$ is at most $d_i - 1$.*

Proof. It is clear from the formula that the action of K_0 leaves $\Psi_{\delta,m}$ invariant. Hence the coefficients of $\Psi_{\delta,m}$ are elements of $L(\mathcal{S})^{\Sigma}$, and this field is generated by $j_1, \ldots, j_{n+1}$ over L. The second statement is obvious from the formula. □

Using the equation (E) satisfied by j_{n+1} on $\mathcal{S}$, there is a unique way to write $\Psi_{\delta,m}$ as an element of the ring $L(j_1, \ldots, j_n)[j_{n+1}, Y_1 \ldots, Y_m]$ with degree at most $e-1$ in j_{n+1}. We call this expression the *canonical form* of $\Psi_{\delta,m}$, and we can consider its coefficients to be rational fractions in n variables $J_1, \ldots, J_n$.

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

$$\Psi_{\delta,m}(j_{1,\delta}^{\gamma}, \ldots, j_{m-1,\delta}^{\gamma}, Y_m) = \prod_{\gamma_m \in K_{m-1}/K_m} \left(Y_m - j_m^{\gamma\gamma_m} \right).$$

Proof. This is straightforward from Definition 3.1. □

Proposition 3.3 has two consequences. First, modular equations vanish on H_δ, as promised; and second, provided the multiplicative coefficient does not vanish, which is generically the case, $\Psi_{\delta,m}$ provides all the possible values for $j_{m,\delta}$ once $j_1, \ldots, j_{n+1}$ and $j_{1,\delta}, \ldots, j_{m-1,\delta}$ are known. We can also define other modular equations $\Phi_{\delta,m}$ for which there is true equality in Proposition 3.3, but they have a more complicated expression. In practice, using the $\Psi_{\delta,m}$ is more convenient as they are typically smaller.

Remark 3.4. There is a geometric picture behind the definition of $\Psi_{\delta,m}$. For simplicity, assume that H_δ is irreducible. Then $L(H_\delta)$ is a field, and is generated by the $j_{i,\delta}$ for $1 \leq i \leq n+1$. We have a tower of function fields:

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

Proposition 3.3 implies that up to scaling, $\Psi_{\delta,m}(j_{1,\delta}, \ldots, j_{m-1,\delta}, Y_m)$ is the minimal polynomial of $j_{m,\delta}$ over $L(j_1, \ldots, j_{n+1}, j_{1,\delta}, \ldots, j_{m-1,\delta})$. Therefore it is a defining equation for the m-th floor of the tower above.

If $j_{1,\delta}$ is a generator of the whole field extension $L(H_\delta)/L(\mathcal{S})^\Sigma$, then for every $2 \leq m \leq n+1$, we have $d_m = 1$ and the polynomial $\Psi_{\delta,m}$ is just the expression of $j_{m,\delta}$ in terms of $j_1, \ldots, j_{n+1}$, and $j_{1,\delta}$.

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

3.3 Modular equations of Siegel type for abelian surfaces

The Siegel modular varieties are prominent examples of PEL Shimura varieties. They classify abelian varieties of dimension g with a certain polarization and level structure. Another example is given by the Hilbert modular varieties, which do the same with 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. In particular, we show that modular equations of Siegel and Hilbert type in dimension 2 [18, 19] are special cases of modular equations as defined above.

Let $g \geq 1$. The *Siegel modular variety* of dimension g is obtained by taking $B = \mathbb{Q}$, with trivial $*$, 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 $G = \mathrm{GSp}_{2g}(\mathbb{Q})$. 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, and we have

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

The reflex field is $\mathbb{Q}$ [21, §14]. In fact, X_+ can be identified with the Siegel upper half-space $\mathcal{H}_g$ endowed with the classical action of $\mathrm{GSp}_{2g}(\mathbb{Q})$.

Choose positive integers $D_1|\cdots|D_g$, and let Λ_0 be the lattice generated by the vectors $e_1, \ldots, e_g, D_1 e_{g+1}, \ldots, D_g e_{2g}$. Then the polarization ψ has type $(D_1, \ldots, D_g)$ on Λ_0. Let K be a compact open subgroup of $G(\mathbb{A}_f)$ that stabilizes $\Lambda_0 \otimes \widehat{\mathbb{Z}}$, and let $\mathcal{S}_1$ denote the connected component of $\mathrm{Sh}_K(\mathbb{C})$ above $1 \in G(\mathbb{A}_f)$. This component is identified with $\Gamma \backslash \mathcal{H}_g$, where

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

By Theorem 2.2, $\mathcal{S}_1$ is a moduli space for polarized abelian varieties with polarization type $(D_1, \ldots, D_g)$ and level K structure such that $H_1(A, \mathbb{Z})$ is isomorphic to Λ_0 with its additional data. This modular interpretation coincides with the classical one [3, §8.1]. Also, modular forms on $\mathcal{S}_1$ are Siegel modular forms in the classical sense.

Taking $g = 1$ and $D_1 = 1$, we find the classical modular curves, which are quotients of the upper half plane $\mathcal{H}_1$ by congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$.

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, and classifies principally polarized abelian surfaces. Modular forms on Sh_K are Siegel modular forms of level $\Gamma(1) = \mathrm{Sp}_4(\mathbb{Z})$. As shown by Igusa [14], the graded ring of modular forms is generated by four elements of respective weights 4, 6, 10, 12. These can be taken to be I_4, I_6', I_{10}, I_{12} in Streng's notation [27, p. 42]. The function field of Sh_K is generated by three algebraically independent *Igusa–Streng 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

$$\delta = \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} \qquad \text{as a } 4 \times 4 \text{ matrix in } 2 \times 2 \text{ blocks.}$$

Then the group $K \cap \delta K \delta^{-1} \cap G(\mathbb{Q})_+$ is the usual group $\Gamma_0(\ell)$, and the degree of H_δ is

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

The Hecke correspondence describes all principally polarized abelian surfaces ℓ-isogeous to a given one; the degree of these isogenies is $\ell(\delta) = \ell^2$. In this case, the function $j_{1,\delta}$ generates the function field on the Hecke correspondence, 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 the usual modular equations of Siegel type and level ℓ. They have been computed for $\ell = 2$ and $\ell = 3$ [18].

3.4 Modular equations of Hilbert type for abelian surfaces

Let F be a totally real number field of degree g over $\mathbb{Q}$, and let $B = F$ with trivial $*$. 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 by

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

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 an identification

$$G(\mathbb{R}) = \prod_{i=1}^{g} \mathrm{GL}_2(\mathbb{R}).$$

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

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

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 [29, §X.4] when $g = 2$, and [21, Ex. 12.4] in general. The domain X_+ can be identified with $\mathcal{H}_1^g$, where $\mathcal{H}_1$ 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 $\mathbb{Z}_F$. Let K be a compact open subgroup of $\mathrm{GL}(\Lambda_0 \otimes \mathbb{A}_f)$.

Remark 3.5. In this setting, $\mu(\Gamma_c)$ is not equal to $\mu(\mathcal{E})$ in general. For instance, if $K = \mathrm{GL}(\Lambda_0 \otimes \mathbb{A}_f)$, and $c = 1$ is the trivial class, 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 such that

$$G(\mathbb{Q})_+ \cap K = \big\{g \in \mathrm{GL}_2(\mathbb{Z}_F \oplus \mathbb{Z}_F^\vee) \mid \mu(g) \in \mathbb{Z}_F^{\times 2}\big\}.$$

The Shimura variety $\mathrm{Sh}_K(G, X_+)(\mathbb{C})$ has several connected components: the narrow class group of F appears in $\pi_0(\mathrm{Sh}_K(\mathbb{C}))$ [29, Cor. I.7.3]. Let $\mathcal{S}_1$ be the connected component associated with $c = 1$. Then there is a natural isomorphism

$$\mathcal{S}_1 = (G(\mathbb{Q})_+ \cap K)\backslash\mathcal{H}_1^g \simeq \mathrm{SL}_2(\mathbb{Z}_F \oplus \mathbb{Z}_F^\vee)\backslash\mathcal{H}_1^g.$$

By Theorem 2.2, the component $\mathcal{S}_1$ parametrizes polarized abelian varieties with real multiplication by $\mathbb{Z}_F$ and level K structure such that $H_1(A, \mathbb{Z})$ is isomorphic to Λ_0 with its additional data. Modular forms of weight w on $\mathcal{S}_1$ are classical Hilbert modular forms of weight (w, w) and level $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z}_F \oplus \mathbb{Z}_F^\vee)$.

Now consider the special case $g = 2$, and let $\Sigma = \{1, \sigma\}$, where σ is the involution of G 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.

Let $\mathfrak{b}$ be a prime ideal of $\mathbb{Z}_F$, and define

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

The Hecke correspondence of level δ has degree $d(\delta) = N_{F/\mathbb{Q}}(\mathfrak{b}) + 1$, and parametrizes isogenies of degree $\ell(\delta) = N_{F/\mathbb{Q}}(\mathfrak{b})$. One can check that H_δ intersects $\mathcal{S}_1 \times \mathcal{S}_1$ nontrivially if and only if $\mathfrak{b}$ is trivial in the narrow class group of F, i.e. $\mathfrak{b} = (\beta)$ is principal and generated by a totally positive element.

Now assume that $\beta \in \mathbb{Z}_F$ is totally positive and prime, and let

$$\delta = \begin{pmatrix} 1 & 0 \\ 0 & \beta \end{pmatrix}.$$

One possibility is to use, as invariants on $\mathcal{S}_1$, the pullback of Igusa invariants by the forgetful map to the Siegel threefold. They are symmetric with respect to Σ, and the equation relating these three invariants is the equation of the associated Humbert surface. In this case, the modular equations describe simultaneously β- and $\sigma(\beta)$-isogenies [19].

In special cases, the field of Σ-invariant functions can be generated by two elements called *Gundlach invariants*. This reduction of the number of variables is interesting in practice. For instance, if $F = \mathbb{Q}(\sqrt{5})$, the graded ring of symmetric Hilbert modular forms is free over three generators F_2, F_6, F_{10} of respective weights 2, 6, and 10 [12]; therefore, $K(\mathcal{S}_1)^\Sigma = \mathbb{Q}(g_1, g_2)$ with

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

and g_1, g_2 are algebraically independent. The associated modular equations have been computed up to $N_{F/\mathbb{Q}}(\beta) = 59$ [17]. They also describe both β- and $\sigma(\beta)$-isogenies.

4 Degree estimates for modular equations

We fix a PEL setting as in §3.1. Let $\delta \in G(\mathbb{A}_f)$ such that $\delta(\widehat{\Lambda}_0) \subset \widehat{\Lambda}_0$, and such that the Hecke correspondence H_δ intersects $\mathcal{S} \times \mathcal{S}'$ nontrivially. In §3.2, we defined the modular equations $\Psi_{\delta,1}, \ldots, \Psi_{\delta,n+1}$; they are multivariate polynomials in $Y_1, \ldots, Y_{n+1}$ describing H_δ and its conjugates under Σ. When we write these modular equations in canonical form, the coefficients of $\Psi_{\delta,m}$ are uniquely determined rational fractions in $L(J_1, \ldots, J_n)$. The goal of this section is to prove the degree estimates about them given in Theorem 1.1, and their explicit variants for abelian surfaces. Recall that the symbol C (or C_1, etc.) denotes a constant that depends only on the setting.

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

For each $1 \leq i \leq n+1$, fix a modular form χ_i invariant under Σ such that $\chi_i j_i$ is holomorphic. This is possible by Proposition 2.5. Recall the notation

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

used in §3.2. For every i, the function

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

is a modular form of level K' and weight $\mathrm{wt}(\chi_i)$ on $\mathcal{S}$. There is a natural action of K_0 on modular forms of level K', and we define $g_{\delta,m}$ for $1 \leq m \leq n+1$ as

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

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. Acting by an element of $K \rtimes \Sigma$ only permutes the factors in the product defining $g_{\delta,m}$, so $g_{\delta,m}$ is invariant under the action of K and Σ. Moreover $g_{\delta,m}$ is a modular form of level K' of weight $\sum_{i=1}^{m} \#(K_0/K')\ \mathrm{wt}(\chi_i)$, and is nonzero because each $\chi_{i,\delta}^{\gamma}$ is. Since $\#(K_0/K') = (\#\Sigma)\, d(\delta)$, the result follows. □

Lemma 4.2. *For every $1 \leq m \leq n+1$, the multivariate polynomial $g_{\delta,m}\Psi_{\delta,m}$ has holomorphic coefficients.*

Proof. This is immediate from the formula in Definition 3.1. □

In other words, the function $g_{\delta,m}$ is a common denominator for the coefficients of $\Psi_{\delta,m}$.

When the invariants have similar denominators, it is possible to make a better choice for $g_{\delta,m}$. The proof is easy and omitted.

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

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

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 multivariate polynomial $g_{\delta,m}\Psi_{\delta,m}$ has holomorphic coefficients.

4.2 The rewriting procedure

By §4.1, each coefficient of $\Psi_{\delta,m}$ can be expressed as the quotient of two holomorphic modular forms of the same bounded weight w. We show that when we rewrite such a quotient in terms of the chosen invariants, the degree of the rational fractions we obtain is bounded linearly in w.

Proposition 4.4. *Let f, g be symmetric modular forms on $\mathcal{S}$ of weight w, and assume that g is nonzero. Then there exists polynomials P, $Q \in L[J_1, \dots, J_{n+1}]$ with total degree at most $C_4\, w$ 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. Let f_k for $1 \le k \le r$ be nonzero generators over L for the graded ring of symmetric modular forms, with respective weights w_k. For each $1 \le k \le r-1$, let $\beta_k \ge 1$ be the minimal integer such that

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

Then we can find nonzero modular forms λ_k, $\xi_k \in L[f_{k+1}, \dots, f_r]$ such that $\mathrm{wt}(\lambda_k) - \mathrm{wt}(\xi_k) = \beta_k w_k$. The modular function $\xi_k f_k^{\beta_k}/\lambda_k$ is symmetric under Σ, so we can find P_k, $Q_k \in L[J_1, \dots, J_{n+1}]$ such that

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

We claim that the conclusion of the proposition holds with

$$C_4 = \sum_{k=1}^{r-1} \left(\frac{1}{\beta_k w_k} \max\{\deg(P_k), \deg(Q_k)\} \prod_{l=1}^{k-1} \left(1 + \frac{\mathrm{wt}(\xi_l)}{\beta_l w_l} \right) \right).$$

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

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

In order to rewrite the fraction $P/Q = f/g$ (currently expressed as a rational fraction of the modular forms f_k) as a fraction of invariants, we proceed as follows. Set $z_0 = w$ and $d_0 = 0$. For $k = 1$ up to $r-1$, do:

- (s_k) Set $s_k \in \mathbb{N}$ to be minimal such that $z_{k-1} - s_k w_k \in \langle w_{k+1} \dots, w_r \rangle$.
- (a_k) Set $a_k = \left\lfloor \dfrac{z_{k-1}}{\beta_k w_k} \right\rfloor$.
- (S_k) Divide P and Q by $f_k^{s_k}$.
- (R_k) Replace each occurence of $f_k^{\beta_k}$ by $\dfrac{\lambda_k P_k}{\xi_k Q_k}$ in P and Q.
- (M_k) Multiply P and Q by $\xi_k^{a_k} Q_k^{a_k}$.
- (z_k) Set $z_k = z_{k-1} - s_k w_k + a_k \operatorname{wt}(\xi_k)$.
- (d_k) Set $d_k = d_{k-1} + a_k \max\{\deg(P_k), \deg(Q_k)\}$.

Finally, in step (S_r), simplify the remaining occurences of f_r. We prove the following statement $(\star)_k$ by induction for every $1 \le k \le r$:

Before step (s_k), P and Q are elements of the ring $L[J_1, \dots, J_{n+1}][f_k, \dots, f_r]$ of weight z_{k-1}, with total degree at most d_{k-1} in $J_1, \dots, J_{n+1}$, such that

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

The statement $(\star)_0$ is true by definition of z_0 and d_0; assume that $(\star)_k$ is true. Then we see, in order, that

- z_{k-1} must belong to $\langle w_k, \dots, w_r \rangle$, so s_k is well defined.
- In each monomial of P and Q, the exponent of f_k must be $a\beta_k + s_k$ for some integer $a \le a_k$. Therefore step (S_k) is an exact division, and after step (R_k) there are no more occurences of f_k in P or Q.
- After step (M_k), P and Q are elements of $L[J_1, \dots, J_{n+1}][f_{k+1}, \dots, f_r]$ of weight
$$z_{k-1} - s_k w_k + a_k \operatorname{wt}(\xi_k) = z_k.$$

None of those steps changed the fact that $(P/Q)(j_1, \dots, j_{n+1})$ equals f/g.

It remains to show that the degree of P, Q in $J_1, \dots, J_{n+1}$ is bounded by d_k after step (M_k). This comes from the observation that in steps (R_k)–(M_k), we only multiply polynomials in $J_1, \dots, J_{n+1}$ already present by $P_k^b Q_k^{a_k - b}$ for some $0 \le b \le a_k$, and rearranging terms afterwards cannot increase the total degree. This proves $(\star)_k$ for all $1 \le k \le r$.

Similarly, after step (S_r), all the occurences of f_r disappear. Therefore, at the end of this rewriting procedure, we obtain polynomials P, Q with total degree at most d_{r-1} such that

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

By induction, we obtain

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

and

$$d_{r-1} \le \sum_{k=1}^{r-1} \left(\frac{w}{\beta_k w_k} \max\{\deg(P_k), \deg(Q_k)\} \prod_{l=1}^{k-1} \left(1 + \frac{\mathrm{wt}(H_l)}{\beta_l w_l}\right)\right) = C_4\, w.$$

The algorithm runs independently on the numerator and the denominator, so the polynomial Q is independent of f. □

4.3 Degree bounds for the canonical form

Proposition 4.5. *Let P, $Q \in L[J_1, \ldots, J_{n+1}]$ with total degree at most d, and assume that $Q(j_1, \ldots, j_{n+1})$ is not identically zero. Write the fraction P/Q in canonical form using equation (E):*

$$\frac{P(j_1, \ldots, j_{n+1})}{Q(j_1, \ldots, j_{n+1})} = \sum_{k=0}^{e-1} R_k(j_1, \ldots, j_n)\, j_{n+1}^k.$$

Then $\deg R_k \le C_5\, d$ *for every* $0 \le k \le e-1$.

Proof. We work in the ring $L(J_1, \ldots, J_n)[J_{n+1}]$ modulo the equation (E), which we write as $E = 0$. In the proof, degrees and coefficients are taken with respect to the variable J_{n+1} unless otherwise specified. First, we invert the denominator Q. Let

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

Using the generic expression of resultants, we can find Bézout coefficients U, $V \in L[j_1, \ldots, j_{n+1}]$ such that

$$R = UQ + VE.$$

The inverse of Q modulo E is U/R, so we have

$$\frac{P(j_1, \ldots, j_{n+1})}{Q(j_1, \ldots, j_{n+1})} = \frac{U(j_1, \ldots, j_{n+1}) P(j_1, \ldots, j_{n+1})}{R(j_1, \ldots, j_n)}.$$

The resultant R has a polynomial expression of degree $e = \deg(E)$ in the coefficients of Q, and $\deg(Q)$ in the coefficients of E. The same is true for every coefficient of U, with e replaced by $e-1$. Since the total degree of Q is at most d, and E is part of the setting, the total degrees of U and R in $J_1, \ldots, J_{n+1}$ are bounded by some Cd; the same is true for the numerator UP.

Now, we reduce UP modulo E in order to obtain a polynomial of degree at most $e-1$ in J_{n+1}. We can decrease the degree by 1 using relation (E):

$$j_{n+1}^e = -\sum_{k=0}^{e-1} E_k(j_1, \ldots, j_n)\, j_{n+1}^k.$$

When doing so, the increase in total degree is bounded by C. Hence, after the euclidean division, total degrees remains bounded by Cd. $\square$

We are now ready to prove part 1 of Theorem 1.1.

Theorem 4.6. *Let $\mathcal{F}$ be a rational fraction occurring as a coefficient of one of the modular equations $\Psi_{\delta,m}$ in canonical form. Then the total degree of $\mathcal{F}$ is bounded by $C_1\, d(\delta)$. The same estimate holds if we require all the $\mathcal{F}$'s to share a common denominator.*

Proof. By Lemmas 4.1 and 4.2, each coefficient appearing in one of the $\Psi_{\delta,m}$ is of the form $f/g_{\delta,n+1}$, where f is holomorphic. By Lemmas 3.2 and 4.1, both f and $g_{\delta,n+1}$ are symmetric modular forms of weight

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

By Proposition 4.4, we can write

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

with $\deg(P), \deg(Q) \leq C_4\, w$, and Q is independent of f. By Proposition 4.5, the degrees of coefficients of $\Psi_{\delta,m}$ in canonical form are bounded by $C_4 C_5\, w$; note that the denominator is still independent of f. The theorem follows with

$$C_1 = C_4\, C_5\, (\#\Sigma) \sum_{i=1}^{n+1} \mathrm{wt}(\chi_i). \qquad \square$$

4.4 Explicit degree bounds in dimension 2

Even in the case of abelian surfaces, our methods provide new results about the degrees occuring in modular equations. We detail this in the Siegel case with Igusa invariants (§3.3), when ℓ is a prime, and in the Hilbert case with $F = \mathbb{Q}(\sqrt{5})$ and Gundlach invariants (§3.4), when $\beta \in F$ is a totally positive prime. The modular equations are denoted $\Psi_{\ell,1}$, $\Psi_{\ell,2}$, $\Psi_{\ell,3}$ and $\Psi_{\beta,1}$, $\Psi_{\beta,2}$ respectively.

Lemma 4.7. *In the dimension 2 Siegel case with Igusa–Streng invariants, we can take $C_4 = 1/6$.*

Proof. We follow the notation used in the proof of Proposition 4.4. Generators for the ring of modular forms are, $f_1 = I_6'$, $f_2 = I_{12}$, $f_3 = I_4$ and $f_4 = I_{10}$. We have $\beta_1 = \beta_2 = 1$, $\beta_3 = 5$, and the rewriting relations are

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

These relations are especially simple, and we can give a different rewriting algorithm for a quotient of modular forms of weight w, as follows. First, multiply by $I_4^{\lfloor 2w/3 \rfloor}$ above and below, and second, rewrite sequentially

$$I_4 I_6' \to I_{10} j_1, \quad I_{12} I_4^2 \to I_{10}^2 j_2, \quad I_4^5 \to I_{10}^2 j_3$$

This removes all the occurences of I_6' and I_{12} without introducing new denominators. The remaining occurences of I_4 and I_{10} must simplify.

Since I_{10} is never used on the left of a rewriting law, we can as well ignore it when computing the weight of a monomial. Then, the greatest ratio (degree in j_1, j_2, j_3)/(weight) is given by $I_4 I_6 \to I_{10} j_1$, with a ratio of $1/10$. Therefore we can take

$$C_4 = \left(1 + \frac{2}{3}\right) \cdot \frac{1}{10} = \frac{1}{6}. \qquad \square$$

Lemma 4.8. *In the dimension 2 Hilbert case with $F = \mathbb{Q}(\sqrt{5})$ and Gundlach invariants, we can take $C_4 = 1/6$.*

Proof. The proof is almost the same as in the Siegel case. The rewriting algorithm for a quotient of symmetric modular forms of weight w is as follows: first multiply numerator and denominator by $F_2^{\lfloor 2w/3 \rfloor}$, then rewrite sequentially

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

This introduces no new denominators, and the remaining occurrences of F_2 and F_{10} must simplify. Ignoring F_{10}, the first relation has the highest degree/weight ratio, which is $1/10$. Therefore we can take $C_4 = 1/6$ as above. $\square$

Remark 4.9. The proof of Proposition 4.4 would give $C_4 = 4/9$ and $C_4 = 1/3$ respectively. Informally, the reason why such an improvement is possible is that the numerator λ_i is always a power of f_r, and $Q_i = 1$. It seems tedious to write a general formula for C_4 that gives the right values here.

Proposition 4.10. *The coefficients of $\Psi_{\ell,1}$ (resp. $\Psi_{\ell,2}$, $\Psi_{\ell,3}$) have total degrees bounded by $5d(\ell)/3$ (resp. $10d(\ell)/3$), where $d(\ell) = \ell^3 + \ell^2 + \ell + 1$.*

Proof. The quantity $d(\ell)$ is the degree of the Hecke correspondence. We are in the situation of Proposition 4.3, so we can choose common denominators $g_{\ell,1}$, $g_{\ell,2}$, $g_{\ell,3}$ with

$$\mathrm{wt}(g_{\ell,1}) = 10d(\ell), \quad \mathrm{wt}(g_{\ell,2}) = \mathrm{wt}(g_{\ell,3}) = 20d(\ell)$$

and in fact $g_{\ell,2} = g_{\ell,3} = (g_{\ell,1})^2$. There is no relation between invariants in this case. By Lemma 4.7, the degree of the rational fractions in $\Psi_{\ell,m}$ is bounded by $\mathrm{wt}(g_{\ell,m})/6$ for $1 \le m \le 3$, and the result follows. $\square$

Proposition 4.11. *The coefficients of $\Psi_{\beta,1}$ and $\Psi_{\beta,2}$ have total degrees bounded by $10d(\beta)/3$, where $d(\beta) = N_{F/\mathbb{Q}}(\beta) + 1$.*

Proof. The quantity $d(\beta)$ is the degree of the Hecke correspondence, and the group Σ has order 2. We are also in the situation of Proposition 4.3: we can choose common denominators $g_{\beta_1} = g_{\beta_2}$ of weight $20d(\beta)$. As above, there is no relation between invariants, so the result follows from Lemma 4.8. □

The degree bounds in Propositions 4.10 and 4.11 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 [17].

5 Heights of fractions from their values

An important information when manipulating modular equations, besides the degree, is the size of all the coefficients that occur. The precise notion to use is that of *heights* of elements, polynomials and rational fractions over a number field L. In this section, we recall the definition of heights and give key results relating the height of a fraction with the height of its values. The symbol C (and C_1, etc.) stands for a constant that depends only on L.

5.1 Definition of heights

Let L be a number field of degree d_L over $\mathbb{Q}$. Write $\mathcal{V}_0$ (resp. $\mathcal{V}_\infty$) for the set of all nonarchimedean (resp. archimedean) places of L, and write $\mathcal{V} = \mathcal{V}_0 \sqcup \mathcal{V}_\infty$. Let $\mathcal{P}$ (resp. $\mathcal{P}_L$) be the set of primes in $\mathbb{Z}$ (resp. prime ideals in $\mathbb{Z}_L$). For each place v of L, write $d_v = [L_v : \mathbb{Q}_v]$, where subscripts denote completion. Denote by $|\cdot|_v$ the normalized absolute value associated with v: when $v \in \mathcal{V}_0$, and $p \in \mathcal{P}$ is the prime below v, we have $|p|_v = 1/p$. We denote the norm of ideals by N.

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

Definition 5.1.

1. For a projective tuple $(a_0 : \cdots : a_n) \in \mathbb{P}^n_L$, we write

$$h(a_0 : \ldots : a_n) = \sum_{v \in \mathcal{V}} \frac{d_v}{d_L} \log\big(\max_{0 \le i \le n} |a_i|_v\big).$$

2. For an affine tuple $(a_1, \ldots, a_n) \in L^n$, we write

$$h(a_1, \ldots, a_n) = h(1 : a_1 : \cdots : a_n) = \sum_{v \in \mathcal{V}} \frac{d_v}{d_L} \log\big(\max\{1, \max_{1 \le i \le n} |a_i|_v\}\big).$$

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

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

3. Let P be a multivariate polynomial over L, and write
$$P = \sum_{k=(k_1,\dots,k_n)} c_k Y_1^{k_1} \cdots Y_n^{k_n}.$$
Let $v \in \mathcal{V}$. We write
$$|P|_v = \max_k |c_k|_v$$
and
$$h(P) = \sum_{v\in\mathcal{V}} \frac{d_v}{d_L} \log\bigl(\max\{1, |P|_v\}\bigr).$$
In other words, $h(P)$ is the height of the affine tuple formed by all the coefficients of P. When $\mathfrak{p} \in \mathcal{P}_L$, we also write
$$v_{\mathfrak{p}}(P) = \min_k v_{\mathfrak{p}}(c_k).$$

4. Let $\mathcal{F} \in L(Y_1, \dots, Y_n)$, and choose coprime polynomials P, Q over L such that $\mathcal{F} = P/Q$. Then we define $h(\mathcal{F})$ as the height of the *projective* tuple formed by all its coefficients: if (c_k) denotes the collection of all the coefficients of P and Q, then
$$h(\mathcal{F}) = \sum_{v\in\mathcal{V}} \frac{d_v}{d_L} \log\bigl(\max_k |c_k|_v\bigr).$$

Heights are well defined and do not depend on the ambient field. In particular, the height of a fraction does not depend on the particular numerator or denominator chosen. When working with heights, we use without further mention the fact that
$$\sum_{v\in\mathcal{V}_\infty} \frac{d_v}{d_L} = 1.$$

Heights satisfy the *Northcott property*: for every bound $H \in \mathbb{R}$, the number of projective tuples $(a_0 : \cdots : a_n) \in \mathbb{P}^n_L$ such that $h(a_0 : \cdots : a_n) \le H$ is finite [13, §B.2]. Informally, the height of an element $y \in L$ (or a polynomial, etc.) is a good measure of how much information is needed to represent y. For instance, if $y = p/q \in \mathbb{Q}$ is in irreducible form, then $h(y) = \log\bigl(\max\{|p|, |q|\}\bigr)$.

Assume that L admits a fundamental unit ε. Then, by the Northcott property, $h(\varepsilon^n)$ tends to infinity as n grows. In general, multiplying integers by units changes the height. This causes problems in some of the proofs below, so we introduce a modified height as follows.

Definition 5.2. Let $y \in \mathbb{Z}_L$ be nonzero. Then we define
$$\widetilde{h}(y) = \frac{1}{d_L} \log\bigl(|N_{L/\mathbb{Q}}(y)|\bigr) = \sum_{v\in\mathcal{V}_\infty} \frac{d_v}{d_L} \log |y|_v.$$
More generally, if $P \in \mathbb{Z}_L[Y_1, \dots, Y_n]$ is nonzero, we define
$$\widetilde{h}(P) = \sum_{v\in\mathcal{V}_\infty} \frac{d_v}{d_L} \log |P|_v.$$

This modified height $\widetilde{h}$ for integers is invariant under multiplication by units. It does *not* satisfy the Northcott property in general. Still, there is a close relation between $\widetilde{h}$ and the classical height h.

Proposition 5.3. *Let $P \in \mathbb{Z}_L[Y_1, \dots, Y_n]$ be nonzero. Then we have*

$$0 \leq \widetilde{h}(P) \leq h(P).$$

Equality holds on the right if and only if $|P|_v \geq 1$ for every $v \in \mathcal{V}_\infty$.

Proof. If $c \in \mathbb{Z}_L$ is a nonzero coefficient of P, then

$$\widetilde{h}(P) \geq \widetilde{h}(c) = \frac{1}{d_L} \log\bigl(|N_{L/\mathbb{Q}}(c)|\bigr) \geq 0$$

because $N_{L/\mathbb{Q}}(c) \in \mathbb{Z}\backslash\{0\}$, so $|N_{L/\mathbb{Q}}(c)| \geq 1$. The rest is obvious. □

Proposition 5.4. *Let $P \in \mathbb{Z}_L[Y_1, \dots, Y_n]$ be nonzero. Then there is a unit $\varepsilon \in \mathbb{Z}_L^\times$ such that*

$$h(\varepsilon P) \leq \max\bigl\{C_6,\, \widetilde{h}(P)\bigr\}.$$

Proof. Let $m = \#\mathcal{V}_\infty$. In $\mathbb{R}^m$, we define the hyperplane H_s for $s \in \mathbb{R}$ by

$$H_s = \bigl\{(t_1, \dots, t_m) \in \mathbb{R}^m \mid t_1 + \cdots + t_m = s\bigr\},$$

and the convex cone Δ_s by

$$\Delta_s = \bigl\{(t_1, \dots, t_m) \in \mathbb{R}^m \mid \forall i,\ t_i \geq s\bigr\}.$$

The image of $\mathbb{Z}_L^\times$ by the logarithmic embedding

$$\mathrm{Log} = \Bigl(\frac{d_v}{d_L} \log|\cdot|_v\Bigr)_{v \in \mathcal{V}_\infty}$$

is a full rank lattice Λ in H_0; let V be a fundamental cell of Λ.

Then for every $s \geq C_7$, the convex set $H_s \cap \Delta_0$ contains a translate of V, hence

$$H_s = \Lambda + (H_s \cap \Delta_0).$$

Translating in the direction $(1, \dots, 1)$, we also have the following property: for every $s \geq 0$,

$$H_s = \Lambda + (H_s \cap \Delta_{-C_7/m}).$$

Let $P \in \mathbb{Z}_L[Y_1, \dots, Y_n]\backslash\{0\}$, and consider the point

$$\mathrm{Log}(P) = \Bigl(\frac{d_v}{d_L} \log|P|_v\Bigr)_{v \in \mathcal{V}_\infty} \in \mathbb{R}^m.$$

The sum of its coordinates is $s_P = \widetilde{h}(P)$. If $s_P \geq C_7$, then there is a unit $\varepsilon \in \mathbb{Z}_L^\times$ such that $\mathrm{Log}(P) + \mathrm{Log}(\varepsilon)$ belongs to Δ_0. Then $|\varepsilon P|_v \geq 1$ for every $v \in \mathcal{V}_\infty$, so

$$h(\varepsilon P) = \widetilde{h}(\varepsilon P) = \widetilde{h}(P)$$

by Proposition 5.3. On the other hand, if $0 \le s_P < C_7$, then we can still find a unit ε such that

$$d_v \log |\varepsilon P|_v \ge -\frac{C_7}{m}$$

for all $v \in \mathcal{V}_\infty$. Then

$$h(\varepsilon P) = \sum_{v \in \mathcal{V}_\infty} \frac{d_v}{d_L} \log \max\{1, |\varepsilon P|_v\} \le \log \widetilde{h}(\varepsilon P) + \sum_{v \in \mathcal{V}_\infty} \frac{C_7}{m} \le 2C_7.$$

This proves the claim with $C_6 = 2C_7$. □

Corollary 5.5. *Every principal ideal $\mathfrak{a}$ of $\mathbb{Z}_L$ has a generator $a \in \mathbb{Z}_L$ such that*

$$h(a) \le \max\{C_6, \frac{1}{d_L} \log N(\mathfrak{a})\}.$$

Proof. Apply Proposition 5.4 with $n = 0$ and P an arbitrary generator of $\mathfrak{a}$. □

5.2 Minimal forms of fractions

When $L = \mathbb{Q}$, every fraction $\mathcal{F}$ can be written as a quotient P/Q, where P and Q are integer polynomials that are coprime over $\mathbb{Z}$ and have height at most $h(\mathcal{F})$: choose P, Q such that the gcd of all their coefficients is 1. When $\mathbb{Z}_L$ is not a PID, this is not possible in general, but there is the following substitute.

Definition 5.6. Let $\mathcal{F} \in L(Y_1, \dots, Y_n)$. Then among all the possible ways to write $\mathcal{F} = P/Q$ with $P, Q \in \mathbb{Z}_L[Y_1, \dots, Y_n]$ where P, Q are coprime over L, there is one such that $h(Q)$ is minimal, by the Northcott property. We call it a *minimal form* of $\mathcal{F}$.

By Proposition 5.4, if $\mathcal{F}$ has a minimal form P/Q such that $h(Q) \ge C_6$, then $\widetilde{h}(Q) = h(Q)$.

Lemma 5.7. *Let $\mathcal{F} \in L(Y_1, \dots, Y_n)$ with minimal form P/Q, and let $\lambda \in L^\times$ such that λP, $\lambda Q \in \mathbb{Z}_L[Y]$. If $h(Q) \ge C_6$, then $|N_{L/\mathbb{Q}}(\lambda)| \ge 1$.*

Proof. By minimality, $h(\lambda Q) \ge h(Q) \ge C_6$, so after multiplying λ by a unit, we can assume that $\widetilde{h}(\lambda Q) = h(\lambda Q)$. This does not change $|N_{L/\mathbb{Q}}(\lambda)|$. Then

$$\widetilde{h}(\lambda) + \widetilde{h}(Q) = \widetilde{h}(\lambda Q) = h(\lambda Q) \ge h(Q) = \widetilde{h}(Q).$$

Therefore $\log |N_{L/\mathbb{Q}}(\lambda)| = \widetilde{h}(\lambda) \ge 0$. □

If P/Q is a minimal form of $\mathcal{F}$, then P, Q are almost coprime over $\mathbb{Z}_L$.

Proposition 5.8. *There is an ideal $\mathfrak{r}$ of $\mathbb{Z}_L$, depending only on L, such that the following holds. Let $\mathcal{F} \in L(Y_1, \dots, Y_n)$ with minimal form P/Q, and let $\mathfrak{a}$ be an ideal of $\mathbb{Z}_L$ dividing all the coefficients of P and Q. Then $\mathfrak{a}$ divides $\mathfrak{r}$.*

Proof. Let $\mathfrak{C}$ be a set of ideals in $\mathbb{Z}_L$ that are representatives for the class group of L, and define $C_8 = \max_{\mathfrak{c}\in\mathfrak{C}} N(\mathfrak{s})$. Take $\mathcal{F} \in L(Y)$ with minimal form P/Q, and let $\mathfrak{a}$ be an ideal of $\mathbb{Z}_L$ dividing all the coefficients of P and Q.

First, assume that $\widetilde{h}(Q) \le C_6$, and let q be a nonzero coefficient of Q. Then $\log|N_{L/\mathbb{Q}}(q)| \le d_L C_6$. Since $\mathfrak{a}$ divides q, we have $N(\mathfrak{a}) \le e^{d_L C_6}$.

Second, assume that $\widetilde{h}(Q) \ge C_6$. Let $\mathfrak{c} \in \mathfrak{C}$ belonging to the class of $\mathfrak{a}$, and let $\lambda \in L^\times$ be a generator of $\mathfrak{a}^{-1}\mathfrak{c}$. Since λP and λQ have integer coefficients, by Lemma 5.7, we have $|N_{L/\mathbb{Q}}(\lambda)| \ge 1$. Therefore $N(\mathfrak{a}) \le N(\mathfrak{c}) \le C_8$.

We can take $\mathfrak{r}$ to be the least common multiple of all ideals of $\mathbb{Z}_L$ of norm at most $\max\{e^{d_L C_6}, C_8\}$. □

If $P \in \mathbb{Q}[Y_1, \dots, Y_n]$, then we can find a minimal denominator $a \in \mathbb{Z}$ such that aP has coefficients in $\mathbb{Z}$ and $\max\{h(a), h(aP)\} \le h(P)$. The analogous statement in number fields is as follows.

Proposition 5.9. *For every $P \in L[Y_1, \dots, Y_n]$, there is an element $a \in \mathbb{Z}_L$ such that $aP \in \mathbb{Z}_L[Y_1, \dots, Y_n]$ and $\max\{h(a), h(aP)\} \le h(P) + C_9$.*

Proof. Let $\mathfrak{C}$ be a set of ideals in $\mathbb{Z}_L$ that are representatives for the class group of L, and let $P \in L[Y_1, \dots, Y_n]$, which we may assume nonzero. Let

$$\mathfrak{a} = \prod_{\mathfrak{p}\in\mathcal{V}_0} \mathfrak{p}^{\max\{0, -v_{\mathfrak{p}}(P)\}}$$

be the denominator ideal of P. Then

$$\log N(\mathfrak{a}) = \sum_{\mathfrak{p}\in\mathcal{V}_0} \log\max\{1, N(\mathfrak{p})^{-v_{\mathfrak{p}}(P)}\} = \sum_{\mathfrak{p}\in\mathcal{V}_0} d_{\mathfrak{p}} \log\max\{1, |P|_{\mathfrak{p}}\} \le d_L h(P).$$

Let $\mathfrak{c} \in \mathfrak{C}$ such that $\mathfrak{c}\mathfrak{a}$ is principal. By Corollary 5.5, we can find a generator a of $\mathfrak{c}\mathfrak{a}$ such that

$$h(a) \le \max\bigl\{C_6, \frac{1}{d_L}\log N(\mathfrak{c}\mathfrak{a})\bigr\} \le h(P) + C_9,$$

with

$$C_9 = \max\bigl\{C_6, \frac{1}{d_L}\max_{\mathfrak{c}\in\mathfrak{C}} \log N(\mathfrak{c})\bigr\}.$$

Then aP has integer coefficients, and we also have

$$\begin{aligned}
h(aP) &= \sum_{v\in\mathcal{V}_\infty} \frac{d_v}{d_L} \log\max\{1, |aP|_v\} \\
&\le \sum_{v\in\mathcal{V}_\infty} \frac{d_v}{d_L}\bigl(\log\max\{1, |P|_v\} + \log\max\{1, |a|_v\}\bigr) \\
&= h(P) + h(a) - \sum_{v\in\mathcal{V}_0} \frac{d_v}{d_L} \log\max\{1, |P|_v\} \\
&= h(P) + h(a) - \frac{1}{d_L}\log N(\mathfrak{a}) \\
&\le h(P) + C_9.
\end{aligned}$$

□

5.3 Evaluation and roots

The following proposition is a slight generalization of [13, Prop. B.7.1].

Proposition 5.10. *Let $P \in L[Y_1, \dots, Y_n]$ with total degree d, let $1 \le m \le n$, and let $y_1, \dots, y_m \in L$. Write $Q = P(y_1, \dots, y_m, Y_{m+1}, \dots, Y_n)$. Then*

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

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

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

Proof. It is enough to prove the second statement. If $v \in \mathcal{V}_0$, we have

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

If $v \in \mathcal{V}_\infty$, the same estimate holds after multiplying 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. □

We can use this result to bound the height of a monic polynomial by the height of its roots.

Proposition 5.11. *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*

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

Proof. Apply Proposition 5.10 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 polynomial controls the height of its roots.

Proposition 5.12. *Let $P \in L[Y]$ be monic, and let α be a root of P. Then*

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

Proof. This is a consequence of [2, Prop. 3.5]. □

5.4 Heights of polynomials from their values

The idea is to control the height of a polynomial P in terms of heights of evaluations of P at special points. We take these to be integers in an interval $[\![A, B]\!] \subset \mathbb{Z}$. Our basic tool is the Lagrange interpolation formula. In the rest of this section, we use the notation

$$D = B - A \quad \text{and} \quad M = \max\{|A|, |B|\}.$$

Lemma 5.13. *Let $y_1, \ldots, y_{d+1} \in [\![A, B]\!]$ be distinct, and write*

$$\frac{\prod_{k \neq i}(Y - y_k)}{\prod_{k \neq i}(y_i - y_k)} = \frac{1}{D!} Q_i(Y)$$

for every $1 \leq i \leq d+1$. Then $Q_i \in \mathbb{Z}[Y]$, and $|Q_i| \leq D!\,(2M)^d$.

Proof. Since the denominator $\prod_{k \neq i}(y_i - y_k)$ divides $D!$, we have

$$Q_i = N_i \prod_{k \neq i}(Y - y_i)$$

for some $N_i \in \mathbb{Z}$ dividing $D!$. Hence $Q_i \in \mathbb{Z}[Y]$. Moreover, if c is the coefficient of Y^{d-k} in Q_i, then

$$|c| \leq |N_i| \binom{d}{k} M^k \leq D!\, 2^d M^d. \qquad \square$$

Lemma 5.14. *Let $P \in L[Y]$ of degree $d \geq 1$, and $y_1, \ldots, y_{d+1}$ distinct values in $[\![A, B]\!]$. Assume that $h(P(y_i)) \leq H$ for every i. Then we have*

$$h(P) \leq (d+1)H + D\log(D) + d\log(2M) + \log(d+1).$$

Proof. Write the Lagrange interpolation formula:

$$P = \frac{1}{D!} \sum_{i=1}^{d+1} P(y_i)\, Q_i(Y)$$

in the notation of Lemma 5.13. If $v \in \mathcal{V}_0$, then

$$\begin{aligned} \max\{1, |P|_v\} &\leq \left|\frac{1}{D!}\right|_v \max\{1, |P(y_1)|_v, \ldots, |P(y_{d+1})|_v\} \\ &\leq \left|\frac{1}{D!}\right|_v \prod_{i=1}^{n+1} \max\{1, |P(y_i)|_v\}. \end{aligned}$$

If $v \in \mathcal{V}_\infty$, then by Lemma 5.13,

$$\max\{1, |P|_v\} \leq \sum_{i=1}^{d+1} |P(y_i)|_v\, 2^d M^d \leq (d+1) 2^d M^d \prod_{i=1}^{d+1} \max\{1, |P(y_i)|_v\}.$$

Since $h(1/D!) = h(D!) \leq D\log(D)$, taking logarithms and summing gives the result. $\square$

The bound on $h(P)$ in Lemma 5.14 is roughly dH, not H. This causes trouble when one wants to apply this result in a context of successive interpolations. However, we can get a better bound on $h(P)$ provided that a height bound is established on *more* than $d+1$ values of P.

Lemma 5.15. *Let $P \in L[Y]$ of degree d, and let $v \in \mathcal{V}_0$ (resp. $v \in \mathcal{V}_\infty$). Then the number of elements $y \in [\![A, B]\!]$ satisfying*

$$|P(y)|_v < |D!\,P|_v \quad \Big(\textit{resp. } |P(y)|_v < \frac{|P|_v}{(2M)^d(d+1)}\Big)$$

is at most d.

Proof. We argue by contradiction. Let $(y_i)_{1\le i\le d+1}$ be distinct elements of $[\![A, B]\!]$ satisfying the given inequality. If $v \in \mathcal{V}_0$, then the Lagrange interpolation formula and Lemma 5.13 give

$$|D!\,P|_v \le \max_i |P(y_i)|_v < |D!\,P|_v$$

which is a contradiction. If $v \in \mathcal{V}_\infty$, the contradiction is

$$|P|_v \le (2M)^d \sum_{i=1}^{d+1} |P(y_i)|_v < |P|_v. \qquad \square$$

Proposition 5.16. *Let $[\![A, B]\!] \subset \mathbb{Z}$. Write $D = B - A$ and $M = \max\{|A|, |B|\}$. Let $P \in L[Y]$ be a polynomial of degree $d \ge 1$, and let $y_1, \dots, y_{2d}$ be distinct elements of $[\![A, B]\!]$. Assume that $h(P(y_i)) \le H$ for every i. Then we have*

$$h(P) \le 2H + D\log D + d\log(2M) + \log(d+1).$$

Proof. If $v \in \mathcal{V}_0$, by Lemma 5.15, we have $|P(y_i)|_v \ge |D!\,P|_v$ for at least d values of i. Therefore

$$\prod_{i=1}^{2d} \max\{1, |P(y_i)|_v\} \ge |D!\,P|_v^d,$$

so

$$\log\max\{1, |P|_v\} \le \log\left|\frac{1}{D!}\right|_v + \frac{1}{d}\sum_{i=1}^{2d} \log\max\{1, |P(y_i)|_v\}.$$

If $v \in \mathcal{V}_\infty$, then at least d of the $P(y_i)$ satisfy $|P(y_i)|_v \ge |P|_v/(2M)^d(d+1)$, so

$$\prod_{i=1}^{2d} \max\{1, |P(y_i)|_v\} \ge \frac{|P|_v^d}{\big((2M)^d(d+1)\big)^d}$$

and

$$\log\max\{1, |P|_v\} \le d\log(2M) + \log(d+1) + \frac{1}{d}\sum_{i=1}^{2d} \log\max\{1, |P(y_i)|_v\}.$$

Since $h(1/D!) \le D\log D$, summing all the contributions yields the result. $\square$

5.5 Height of fractions from their values: preliminaries

We now turn to the problem of estimating the height of *rational fractions* in terms of the height of their values at certain points. Our first goal is to give a height bound using the minimal number of interpolation points; then, we make preparations for Theorem 1.2.

Lemma 5.17. *Let $P, Q \in \mathbb{Z}_L[Y]$ of degrees d_P and d_Q respectively, and let $0 \le k \le \min\{d_P, d_Q\} - 1$. Let R be the k-th subresultant of P and U, V the associated Bézout coefficients. Write $s = d_P + d_Q$. Then we have*

$$\begin{aligned} h(R) &\le (d_Q - k)h(P) + (d_P - k)h(Q) + \frac{s-2k}{2}\log(s-2k), \\ h(U) &\le (d_Q - k - 1)h(P) + (d_P - k)h(Q) + \frac{s-2k-1}{2}\log(s-2k-1), \\ h(V) &\le (d_Q - k)h(P) + (d_P - k - 1)h(Q) + \frac{s-2k-1}{2}\log(s-2k-1). \end{aligned}$$

Recall that R, U, V are polynomials over $\mathbb{Z}_L$ such that $UP + VQ = R$ and

$$\deg R \le k, \quad \deg U \le d_Q - k - 1, \quad \deg V \le d_P - k - 1.$$

Proof. Let r be a coefficient of R. Then r has an expression as a determinant of size $d_P + d_Q - 2k$; its entries in the first $d_Q - k$ columns are coefficients of P, and its entries in the last $d_P - k$ columns are coefficients of Q. Let $v \in \mathcal{V}_\infty$. By Hadamard's lemma, we can bound $|r|_v$ by the product of L^2-norms of the columns. Hence

$$|r|_v \le \big(\sqrt{d_P + d_Q - 2k}\ |P|_v\big)^{d_Q - k}\big(\sqrt{d_P + d_Q - 2k}\ |Q|_v\big)^{d_P - k}.$$

This gives the desired height bound on R.

The proof is the same for U (resp. V): the coefficients are determinants of size $d_P + d_Q - 2k - 1$, with one column less coming from P (resp. Q). □

Proposition 5.18. *Let $[\![A, B]\!] \subset \mathbb{Z}$. Write $D = B - A$ and $M = \max\{|A|, |B|\}$. Let $\mathcal{F} \in L(Y)$ of degree $d \ge 1$. Let d_P, d_Q be the degrees of its numerator and denominator respectively, and let $s = d_P + d_Q$. Let $y_1, \dots, y_{s+1}$ be distinct elements of $[\![A, B]\!]$ that are not poles of $\mathcal{F}$, and assume that $h(\mathcal{F}(y_i)) \le H$ for every i. Then we can write $\mathcal{F} = P/Q$ with $P, Q \in \mathbb{Z}_L[Y]$ such that $\deg P = d_P$, $\deg Q = d_Q$, and*

$$\begin{aligned} \max\{h(P), h(Q)\} \le{}& (d+1)(2d+1)H + (d+1)D\log(D) + (4d^2 + 3d)\log(2M) \\ &+ (2d+2)\log(2d+1) + (d+1)C_9. \end{aligned}$$

Proof. We follow the interpolation algorithm [4, §7.1]. Let $T \in L[Y]$ be the polynomial of degree at most s interpolating the points $(y_i, \mathcal{F}(y_i))$. According to Lemma 5.14, we have

$$h(T) \le (s+1)H + D\log(D) + s\log(2M) + \log(s+1). \qquad (\star)$$

By Proposition 5.9, we can find a denominator $a \in \mathbb{Z}_L$ such that $T' = aT$ is an element of $\mathbb{Z}_L[Y]$ and $\max\{h(a),\, h(T')\} \leq h(T) + C_9$. Define

$$Z = \prod_{i=1}^{s+1} (Y - y_i) \in \mathbb{Z}[Y].$$

The coefficients of Z are bounded in absolute value by $(2M)^{s+1}$, so we have $h(Z) \leq (s+1)\log(2M)$. Let P' be the d_P-th subresultant of T' and Z, and let

$$Q'T' + VZ = P'$$

be the associated Bézout equality. By Lemma 5.17, we have

$$\begin{aligned} h(P') &\leq (d+1)h(T') + d(s+1)\log(2M) + \frac{2d+1}{2}\log(2d+1), \\ h(Q') &\leq d\,h(T') + (s+1)d\log(2M) + d\log(2d+1). \end{aligned}$$

We can take $P = P'$ and $Q = aQ'$: they have the right degrees and satisfy

$$\max\{h(P),\, h(Q)\} \leq (d+1)(h(T)+C_9) + (s+1)d\log(2M) + (d+1)\log(2d+1).$$

Using the previous bound ($\star$) on $h(T)$ and the bound $s \leq 2d$ ends the proof. □

The reader may wish to skip the following lemmas until their use in the proof of Theorem 1.2 becomes apparent.

Lemma 5.19. *Let $D = B - A$, let $S \subset [\![A, B]\!]$ containing at least $2D/3$ elements, and let $1 \leq k < D/3$. Then there is a subinterval of $[\![A, B]\!]$ of amplitude at most $3k$ containing at least $k+1$ elements of S.*

Proof. Assume the contrary. We can partition $[\![A, B]\!]$ in at most $(D/3k) + 1$ intervals of amplitude at most $3k$, so

$$\frac{2D}{3} \leq \#S \leq k\left(\frac{D}{3k} + 1\right) = \frac{D}{3} + k.$$

This is absurd because $k < D/3$. □

Lemma 5.20. *Let $R \geq 1$ be an integer. Then*

$$\sum_{p \in \mathcal{P},\, p \mid R} \frac{\log p}{p-1} \leq \max\{1, C_{10}\log\log R\}.$$

Proof. Let m be the number of prime factors in R, and (p_i) the sequence of prime numbers in increasing order. It is enough to prove the claim for the integer $R' = \prod_{i=1}^{m} p_i$, which has both a greater left hand side, since $\log(p)/(p-1)$ is a decreasing function of p, and a smaller right hand side, since $R' \leq R$. We can assume $m \geq 2$. Then

$$\sum_{i=1}^{m} \frac{\log(p_i)}{p_i - 1} \leq \sum_{i=1}^{m} \frac{\log(p_i)}{p_i} + \sum_{i=1}^{m} \frac{\log(p_i)}{p_i(p_i-1)} \leq \log(p_m) + 2 + C_{11}$$

by Mertens's first theorem [16], and because the second series converges. By [25], we have $p_m < m \log m + m \log\log m$ if $m \geq 6$; so the rough bound $p_m \leq m^2$ holds. The result follows since $m \leq \log(R')$. $\square$

Lemma 5.21. *Let $R \in \mathbb{Z}_L$ be nonzero. Then*

$$\sum_{\substack{\mathfrak{p} \in \mathcal{P}_L,\, \mathfrak{p} \mid R \\ \mathfrak{p} \mid p \in \mathcal{P}}} \frac{\log(N(\mathfrak{p}))}{p-1} \leq d_L \max\{1, C_{10} \log\log |N_{L/\mathbb{Q}}(R)|\}.$$

Proof.

$$\begin{aligned}\sum_{\mathfrak{p} \mid R} \frac{\log(N(\mathfrak{p}))}{p-1} &\leq \sum_{p \mid N_{L/\mathbb{Q}}(R)} \frac{\sum_{\mathfrak{p} \mid p} \log(N(\mathfrak{p}))}{p-1} \\ &= d_L \sum_{p \mid N_{L/\mathbb{Q}}(R)} \frac{\log(p)}{p-1} \leq d_L \max\{1, C_{10} \log\log |N_{L/\mathbb{Q}}(R)|\}\end{aligned}$$

by Lemma 5.20. $\square$

Lemma 5.22. *Let $\mathfrak{p} \in \mathcal{P}_L$ over $p \in \mathcal{P}$, and let $L_\mathfrak{p}$ be the $\mathfrak{p}$-adic completion of L. Let $Q \in L_\mathfrak{p}[Y]$ of degree d with integer coefficients, and assume that $v_\mathfrak{p}(Q) = 0$. Let $y_1, \ldots, y_n$ be distinct values in $[\![A, B]\!]$, and write $D = B - A$; assume that $D \geq 1$. Let $\beta \in \mathbb{N}$. Then*

$$\sum_{i=1}^{n} \min\{\beta, v_\mathfrak{p}(Q(y_i))\} \leq d \left(\beta + d_L \frac{\log(D)}{\log N(\mathfrak{p})} + \frac{D}{p-1} \right).$$

Proof. Let λ be the leading coefficient of Q, and let $\alpha_1, \ldots, \alpha_d$ be the roots of Q in an algebraic closure of $L_\mathfrak{p}$, where we extend $|\cdot|_\mathfrak{p}$ and $v_\mathfrak{p}$. Up to reindexation, we may assume that $|\alpha_j|_\mathfrak{p} \leq 1$ for $1 \leq j \leq t$, and $|\alpha_j|_\mathfrak{p} > 1$ for $t+1 \leq j \leq d$. For every i, we have

$$|Q(y_i)|_\mathfrak{p} = |\lambda|_\mathfrak{p} \prod_{i=1}^{d} |y_i - \alpha_j|_\mathfrak{p} = \left(|\lambda|_\mathfrak{p} \prod_{j=t+1}^{d} |\alpha_j|_\mathfrak{p} \right) \prod_{j=1}^{t} |y_i - \alpha_j|_\mathfrak{p}.$$

We must have

$$\left(|\lambda|_\mathfrak{p} \prod_{j=t+1}^{d} |\alpha_j|_\mathfrak{p} \right) \geq 1,$$

for otherwise all the coefficients of Q would be divisible by $\mathfrak{p}$. Therefore

$$v_\mathfrak{p}(Q(y_i)) \leq \sum_{j=1}^{t} v_\mathfrak{p}(y_i - \alpha_j).$$

Let $k \in \mathbb{N}$ such that $p^k \leq D < p^{k+1}$. Since the y_i are all distinct modulo $\mathfrak{p}^{k+1}$, there are at most $t \leq d$ values of i such that $v_\mathfrak{p}(y_i - \alpha_j) > k$ for

some j. For these i's, we bound $\min\{\beta, v_{\mathfrak{p}}(Q(y_i))\}$ by β. This accounts for the term $d\beta$ in the lemma.

For all other values of i (say $i \in I$), we have $v_{\mathfrak{p}}(y_i - \alpha_j) \leq k$, and thus

$$v_{\mathfrak{p}}(y_i - \alpha_j) = \int_0^k \mathbf{1}_{u \leq v_{\mathfrak{p}}(y_i - \alpha_j)} du.$$

Any two y_i that fall in the same $\mathfrak{p}$-adic disk $\{u \leq v_{\mathfrak{p}}(y - \alpha_j)\}$ must coincide modulo $p^{\lceil u \rceil}$. Therefore, for a given α_j, and a given $u \in]l, l+1]$, there are at most $\lceil D/p^{l+1} \rceil$ values of i for which y_i can belong to this disk. Therefore

$$\begin{aligned}
\sum_{i \in I} v_{\mathfrak{p}}(Q(y_i)) &\leq \sum_{i \in I} \sum_{j=1}^{t} v_{\mathfrak{p}}(y_i - \alpha_j) \\
&= \sum_{i \in I} \sum_{j=1}^{t} \sum_{l=0}^{k-1} \int_l^{l+1} \mathbf{1}_{u \leq v_{\mathfrak{p}}(y_i - \alpha_j)} du \\
&= \sum_{j=1}^{t} \sum_{l=0}^{k-1} \int_l^{l+1} \left(\sum_{i \in I} \mathbf{1}_{u \leq v_{\mathfrak{p}}(y_i - \alpha_j)} \right) du \\
&\leq t \sum_{l=0}^{k-1} \left\lceil \frac{D}{p^{l+1}} \right\rceil \leq t \sum_{l=0}^{k-1} \left(\frac{D}{p^{l+1}} + 1 \right) \leq tk + \frac{tD}{p-1}.
\end{aligned}$$

We have $t \leq d$, and

$$k \leq \log_p(D) \leq d_L \frac{\log(D)}{\log N(\mathfrak{p})}.$$

This accounts for the two remaining terms in the lemma. □

5.6 Heights of fractions from their values: main result

We are now ready to prove Theorem 1.2.

Theorem 5.23. *Let $[\![A, B]\!] \subset \mathbb{Z}$. Write $D = B - A$ and $M = \max\{|A|, |B|\}$. Let $\mathcal{F} \in L(Y)$ of degree at most $d \geq 1$. Let $S \subset [\![A, B]\!]$ containing at least $2D/3$ elements and no poles of $\mathcal{F}$. Let $H \geq \max\{3, \log(2M)\}$, and assume that*

(i) $h(\mathcal{F}(y)) \leq H$ for every $y \in S$.

(ii) $D > \max\{d^4 H \log(dH), 6d\, d_L\}$.

Then we have

$$h(\mathcal{F}) \leq 3H + C_3 \log(dH) + 3d \log(2M).$$

Proof. Let P/Q be a minimal form of $\mathcal{F}$, and let $R = \mathrm{Res}(P, Q)$. Let $y_1, \ldots, y_n$ be distinct elements of S. For $1 \leq i \leq n$, we define ideals $\mathfrak{s}_i$, $\mathfrak{n}_i$ and $\mathfrak{d}_i$ of $\mathbb{Z}_L$ as follows:

$$\mathfrak{s}_i = \gcd(P(y_i), Q(y_i)), \quad (P(y_i)) = \mathfrak{n}_i \mathfrak{s}_i, \quad (Q(y_i)) = \mathfrak{d}_i \mathfrak{s}_i.$$

Then we have $\mathfrak{s}_i \mid R$, and $(\mathcal{F}(y_i)) = \mathfrak{n}_i \mathfrak{d}_i^{-1}$. Since $\mathfrak{n}_i$ and $\mathfrak{d}_i$ are coprime, we have $\log N(\mathfrak{d}_i) \le d_L h(\mathcal{F}(y_i))$, so

$$\log |N_{L/\mathbb{Q}}(Q(y_i))| \le \log N(\mathfrak{s}_i) + d_L H.$$

The proof runs as follows.

1. Obtain a bound on the resultant R.
2. Show that the product of all $\mathfrak{s}_i$'s has bounded norm.
3. Show that $\mathfrak{s}_i$ is reasonably small at least for some values of i.
4. Take care of archimedean places, and obtain a bound on $h(Q)$.
5. Deduce a bound on $h(P)$ and conclude.

We can assume that $h(Q) \ge C_6$. Otherwise, we can go directly to step 5.

Step 1. By Lemma 5.19 with $k = 2d$, we can find a subinterval $[\![A', B']\!]$ of $[\![A, B]\!]$ with amplitude at most $6d$ containing $2d+1$ elements $y_1, \dots, y_{2d+1}$ of S. We use these y_i as interpolation points in Proposition 5.18: we can write $\mathcal{F} = P'/Q'$ where P', Q' have integer coefficients and satisfy

$$h(P'),\, h(Q') \le 6d^2 H + 22d^2 \log(6d) + 7d^2 \log(2M) + 2dC_9 \le C_{12}\, d^2 H.$$

To simplify the right hand side, we use the inequalities $1 \le d,\ 6d \le D-1 \le 2M$, $\log(2M) \le H$, and $1 \le H$. We can take $C_{12} = 2C_9 + 35$.

Lemma 5.17 allows us to bound the resultant of P' and Q':

$$h\big(\mathrm{Res}(P', Q')\big) \le d \log(2d) + dh(P') + dh(Q') \le C_{13}\, d^3 H$$

with $C_{13} = 2C_{12} + 1$. In order to relate this to R, we use Lemma 5.7: we have $P' = \lambda P$ and $Q' = \lambda Q$ for some $\lambda \in L^\times$ such that $N(\lambda) \ge 1$. Therefore

$$\log |N_{L/\mathbb{Q}}(R)| \le \log \big| N_{L/\mathbb{Q}}\big(\mathrm{Res}(P', Q')\big)\big| \le d_L h\big(\mathrm{Res}(P', Q')\big) \le C_{14}\, d^3 H$$

with $C_{14} = d_L C_{13}$.

Step 2. Let $\mathfrak{p} \in \mathcal{P}_L$ be a prime factor of R with valuation $\beta_\mathfrak{p}$, and let $p \in \mathbb{Z}$ be the prime below $\mathfrak{p}$. Let $\mathfrak{r}$ be the ideal from Proposition 5.8. We claim:

$$\sum_{i=1}^{n} v_\mathfrak{p}(\mathfrak{s}_i) \le n\, v_\mathfrak{p}(\mathfrak{r}) + d\left(\beta_\mathfrak{p} + d_L \frac{\log(D)}{\log N(\mathfrak{p})} + \frac{D}{p-1}\right). \qquad (\star)$$

We can work in the $\mathfrak{p}$-adic completion $L_\mathfrak{p}$. Let π be a uniformizer of $L_\mathfrak{p}$, and let $r = \min\{v_\mathfrak{p}(P), v_\mathfrak{p}(Q)\}$. Then π^r must divide $\mathfrak{r}$, so $r \le v_\mathfrak{p}(\mathfrak{r})$. Write $\widetilde{P} = P/\pi^r$, $\widetilde{Q} = Q/\pi^r$. Then one of $\widetilde{P}$ and $\widetilde{Q}$ is not divisible by π; by symmetry, assume that π does not divide $\widetilde{Q}$. Then

$$v_\mathfrak{p}(\mathfrak{s}_i) \le \min\big\{\beta_\mathfrak{p}, r + v_\mathfrak{p}(\widetilde{Q}(y_i))\big\} \le v_\mathfrak{p}(\mathfrak{r}) + \min\big\{\beta_\mathfrak{p}, v_\mathfrak{p}(\widetilde{Q}(y_i))\big\}$$

so the claim follows from Lemma 5.22.

Inequality ($\star$) bounds the $\mathfrak{p}$-adic valuation of the product of all $\mathfrak{s}_i$'s. Taking the product over all prime divisors of R, we obtain

$$\begin{aligned}\prod_{i=1}^{n} N(\mathfrak{s}_i) \leq\ & N(\mathfrak{r})^n |N_{L/\mathbb{Q}}(R)|^d \ \exp \sum_{\substack{\mathfrak{p}\in\mathcal{P}_L,\, \mathfrak{p}|R \\ \mathfrak{p}|p\in\mathcal{P}}} \left(d\, d_L \log(D) + D\frac{\log(N(\mathfrak{p}))}{p-1} \right) \\ \leq\ & N(\mathfrak{r})^n |N_{L/\mathbb{Q}}(R)|^d \ \exp\Big(d\, d_L \log(D) \log\big(|N_{L/\mathbb{Q}}(R)|\big) \\ & \qquad + D d_L \max\big\{1, C_{10} \log\log |N_{L/\mathbb{Q}}(R)|\big\}\Big).\end{aligned}$$

Indeed, there are at most $\log |N_{L/\mathbb{Q}}(R)|$ prime ideals dividing R, and Lemma 5.21 applies. Since $\log |N_{L/\mathbb{Q}}(R)| \leq C_{14}\, d^3 H$, we obtain

$$\begin{aligned}\log\left(\prod_{i=1}^{n} N(\mathfrak{s}_i)\right) &\leq n \log N(\mathfrak{r}) + C_{14}\, d^4 H \big(1 + d_L \log(D)\big) + C_{10}\, D d_L \log(C_{14}\, d^3 H) \\ &\leq C_{15} \left(d^4 H \log(D) + D \log(dH)\right)\end{aligned}$$

with $C_{15} = \max\big\{2d_L C_{14},\, \log(N(\mathfrak{r})) + C_{10}\, d_L \big(3 + \log(C_{14})\big)\big\}$.

Step 3. We can now put into play the assumptions our assumptions about D and S being sufficiently large. Since $D \geq d^4 H \log(dH) > \exp(1)$, and $t/\log(t)$ is increasing for $t > \exp(1)$, we have

$$\frac{D}{\log(D)} \geq \frac{d^4 H}{4 + \log\log(dH)/\log(dH)} \geq \frac{d^4 H}{5}.$$

Moreover

$$\#S - d\, d_L \geq \frac{2D}{3} - \frac{D}{6} = \frac{D}{2}.$$

Therefore

$$\log\left(\prod_{i=1}^{n} N(\mathfrak{s}_i)\right) \leq C_{15}(5D + D\log(dH)) \leq C_{16} \log(dH)(\#S - d\, d_L)$$

with $C_{16} = 12 C_{15}$. This shows that in every subset of $\#S - d\, d_L$ elements of S, at least one must satisfy $\log N(\mathfrak{s}_i) \leq C_{16} \log(dH)$. Hence we may assume that

$$\log N(\mathfrak{s}_i) \leq C_{16} \log(dH)$$

for every $1 \leq i \leq r = d\, d_L + 1$. This implies

$$\log\big|N_{L/\mathbb{Q}}\big(Q(y_i)\big)\big| \leq C_{16} \log(dH) + d_L H.$$

Step 4. Let $v \in \mathcal{V}_\infty$. By Lemma 5.15, the inequality

$$|Q(y_i)|_v < \frac{|Q|_v}{(2M)^d (d+1)}$$

can only be true for at most d values of i. Since $\#\mathcal{V}_\infty \le d_L$, we can find $y \in S$ among the $(y_i)_{1\le i\le r}$ such that

$$\forall v \in \mathcal{V}_\infty,\ |Q(y)|_v \ge \frac{|Q|_v}{(2M)^d(d+1)}.$$

Then

$$\begin{aligned} h(Q) &\le \widetilde{h}(Q) && \text{by Proposition 5.4, since } h(Q) \ge C_6 \\ &\le \frac{1}{d_L}\log\big|N_{L/\mathbb{Q}}\big(Q(y)\big)\big| + d\log(2M) + \log(d+1) \\ &\le H + \frac{C_{16}}{d_L}\log(dH) + d\log(2M) + \log(d+1), \end{aligned}$$

in other words

$$h(Q) \le H + C_{17}\log(dH) + d\log(2M)$$

with $C_{17} = 1 + C_{16}/d_L$.

Step 5. Since $\#S \ge d\,d_L + 1$, by Lemma 5.15, we can find $y \in S$ such that

$$\forall v \in V_\infty,\ |P|_v \le (2M)^d(d+1)|P(y)|_v.$$

Then

$$\begin{aligned} h(P) &\le h(P(y)) + d\log(2M) + \log(d+1) && \text{because } P \in \mathbb{Z}_L[Y] \\ &\le h(Q(y)) + H + d\log(2M) + \log(d+1) && \text{as } P(y) = Q(y)\mathcal{F}(y) \\ &\le h(Q) + H + 2d\log(2M) + 2\log(d+1) && \text{by Proposition 5.10.} \end{aligned}$$

The result follows with $C_3 = C_{17} + 2$ since $h(\mathcal{F}) \le h(P) + h(Q)$. □

Remark 5.24. The proof gives an explicit value for C_3: we have

$$\begin{aligned} C_{14} &= d_L(4C_9 + 71), \\ C_{15} &= \max\big\{2d_LC_{14},\ \log(N(\mathfrak{r})) + C_{10}\,d_L\big(3 + \log(C_{14})\big)\big\} \quad \text{with } \mathfrak{r} \text{ as in Prop. 5.8}, \\ C_3 &= 3 + C_{15}/d_L. \end{aligned}$$

It would be interesting to know whether we can obtain an efficient bound on $h(\mathcal{F})$ using only $O(d)$ evaluation points, as was the case for polynomials, instead of $\widetilde{O}(d^4H)$.

6 Height estimates for modular equations

In this final section, we prove part 2 of Theorem 1.1 about the height of coefficients in modular equations. We fix a PEL setting as in §3, and keep the notation used there. We write $\mathcal{S} = \Gamma\backslash X_+$.

6.1 Heights of abelian varieties

Different types of heights can be defined for an abelian variety A over L. The *Faltings height* $h_F(A)$ is defined in [11, §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 $h_{\Theta,r}(A, \mathcal{L})$, as the projective height of level r theta constants of $(A, \mathcal{L})$ [23, Def. 2.6]. Finally, if A is an abelian variety with PEL structure over L given by a point $z \in \mathcal{S}$ where $j_1, \ldots, j_{n+1}$ are well defined, we can define the *j-height* of A as

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

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

The Faltings height behaves well with respect to isogenies.

Proposition 6.1. *Let A, A' be abelian varieties over $\overline{\mathbb{Q}}$, and assume that an isogeny $\phi : A \to A'$ exists. Then*

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

Proof. This is a consequence of [11, Lem. 5]. □

Our goal here is to establish a relation between $h_j(A)$ and $h_F(A)$ when A is an abelian variety with PEL structure. Theta heights are an intermediate step between concrete values of invariants and the Faltings height.

Theorem 6.2 ([23, Cor. 1.3])**.** *For every integer $g \geq 1$, and even integer $r \geq 2$, there is 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*

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

Proposition 6.3. *There is a nonzero polynomial $P \in L[Y_1, \ldots Y_{n+1}]$ such that the following holds. If A is the abelian variety with PEL structure associated with a point $z \in \mathcal{S}$ where $j_1, \ldots, j_{n+1}$ are well defined and $P(j_1, \ldots, j_{n+1}) \neq 0$, then*

$$\frac{1}{C_{18}}\overline{h}_F(A) \leq \overline{h}_j(A) \leq C_{18}\,\overline{h}_F(A).$$

Proof. By [21, Thm. 5.17], there is a finite covering $\mathcal{S}'$ of $\mathcal{S}$ which is a connected Shimura variety for the derived group G^{der}. 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 the reductive group $\mathrm{GSp}_{2g}(\mathbb{Q})$, where $2g = \dim_{\mathbb{Q}} V$. Therefore, by [21, 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

$$\begin{tikzcd}
 & \widetilde{\mathcal{S}} = \widetilde{\Gamma}\backslash X_+ \arrow[dl, "p'"'] \arrow[dr, "p''"] & \\
\mathcal{S}' = \Gamma'\backslash X_+ \arrow[d, "p"] & & \mathcal{S}'' = \Gamma''\backslash X_+ \arrow[r, hook] & \mathcal{A}_{\Theta,r} \\
\mathcal{S} & &
\end{tikzcd}$$

where $\widetilde{\Gamma} = \Gamma' \cap \Gamma''$. The maps p, p', p'' are finite coverings, and all the maps in this diagram are algebraic.

The modular interpretation is as follows. Let (Λ, ψ) be the standard polarized lattice associated with the connected component $\mathcal{S}$, as in Theorem 2.1. 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 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 given by $(\Lambda'', x, \lambda\psi)$.

In particular, if $\widetilde{x} \in \widetilde{\mathcal{S}}$, and if A, A'' are the abelian varieties corresponding to $\widetilde{x}$ in $\mathcal{S}$ and $\mathcal{A}_{\Theta,r}$ respectively, then A and A'' are linked by an isogeny of degree $d = \#(\Lambda/\Lambda'')$. Hence, by Proposition 6.1 and Theorem 6.2,

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

Denote by $\theta_0, \ldots, \theta_k$ the Theta constants of level r. They define a projective embedding of $\mathcal{A}_{\Theta,r}$. Then 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 $\mathcal{S}$; let $f_1, \ldots, f_{n+1}$ be generators for the function field of $\widetilde{\mathcal{S}}$. Since p_2 and $p \circ p_1$ are finite coverings, the functions $j_1, \ldots, j_{n+1}$ have fractional expressions in terms of $f_1, \ldots, f_{n+1}$, and the same is true for the θ_i/θ_0 on $\mathcal{S}''$. These polynomial systems are generically of dimension 0, so they can be inverted using Gröbner bases. By the primitive element theorem, up to a change of coordinates on $\widetilde{\mathcal{S}}$, we can assume that these Gröbner bases are in echelon form. We define $\widetilde{F}$ to be the Zariski closed subset of codimension 1 in $\widetilde{\mathcal{S}}$ where at least one of the denominators vanishes among all the fractional expression considered, or where one of the f_i is not well defined. Then $U = \mathcal{S}\backslash p \circ p_1(\widetilde{F})$ is open dense in $\mathcal{S}$. Let $P \in L[j_1, \ldots, j_{n+1}]$ such that $\{P \neq 0\} \subset U$.

Let $z \in \mathcal{S}$ where $j_1, \ldots, j_{n+1}$ are well defined, and $P(j_1, \ldots, j_{n+1}) \neq 0$. We look at the diagram above, from left to right. Lift z to a point $\widetilde{z} \in \widetilde{\mathcal{S}}$; by construction, $\widetilde{z} \notin \widetilde{F}$. By repeated applications of Propositions 5.10 and 5.12, we have

$$\overline{h}\big(f_1(\widetilde{z}), \ldots, f_{n+1}(\widetilde{z})\big) \leq C\,\overline{h}\big(j_1(z), \ldots, j_{n+1}(z)\big).$$

Writing $z'' = p_2(\widetilde{z})$, we also have

$$\overline{h}\Big(\frac{\theta_1}{\theta_0}(z''), \ldots, \frac{\theta_k}{\theta_0}(z'')\Big) \leq C\,\overline{h}\big(f_1(\widetilde{z}), \ldots, f_{n+1}(\widetilde{z})\big).$$

This implies, in the notation above,

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

so by equation ($\star$)

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

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

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

Corollary 6.4. *Let A, A' be the abelian varieties with PEL structure associated with $z, z' \in U$. Assume that A and A' are related by an isogeny of degree ℓ. Then*

$$\overline{h}_j(A') \leq C_{19}(\overline{h}_j(A) + \log \ell).$$

Proof. Combine Propositions 6.1 and 6.3. We may take $C_{19} = C_{18}^2$. □

Remark 6.5. We can presumably do better than Corollary 6.4. 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 [24, Thm. 1.1]. This is also the kind of bound provided by Theorem 6.2. However, the estimate in Corollary 6.4 is sufficient for our purposes, so we do not pursue this question further. This problem should be solved before attempting to give meaningful explicit values for the constant C_2 in Theorem 1.1.

6.2 Heights of evaluated modular equations

We keep the notation used in §3.2. Fix a Hecke correspondence H_δ of degree $d(\delta)$, and consider the modular equations $\Psi_{\delta,m}$ of level δ between connected components $\mathcal{S}$, $\mathcal{S}'$ of $\mathrm{Sh}_K(G, X_+)(\mathbb{C})$. Written in canonical form, the $\Psi_{\delta,m}$ can be seen as elements of the ring $L(J_1, \ldots, J_n)[J_{n+1}, Y_1, \ldots, Y_m]$.

Let U (resp. U') be the open subset of $\mathcal{S}$ (resp. $\mathcal{S}'$) constructed as in §6.1. Define $U_\delta \subset \mathcal{S}$ to be the Zariski open set of all points $[x, g] \in \mathcal{S}$ such that $[x, g] \in U$, and $[x, g\delta\gamma] \in U'$ for every $\gamma \in K_0/K_{n+1}$. Finally, we define $V_\delta \subset L^n$ to be the Zariski open set of all points $(j_1, \ldots, j_n)$ where the equation (E) (cf §3.1) has e distinct roots and the following property holds: if j_{n+1} is a root of (E), then $(j_1, \ldots, j_{n+1})$ are the invariants of some $z \in U_\delta$. In particular, the denominators of modular equations do not vanish on V_δ.

Lemma 6.6. *There is a nonzero polynomial $P_\delta \in L[J_1, \ldots, J_n]$ of total degree at most $Cd(\delta)$ such that $\{P_\delta \neq 0\} \subset V_\delta$.*

Proof. Let R be the the resultant of (E) and its derivative with respect to j_{n+1}. It is a rational fraction in $j_1, \ldots, j_n$ of degree C. If R is well defined and does not vanish at $(j_1, \ldots, j_n)$, then the equation (E) has e distinct roots.

Similarly, there is a polynomial $Q \in L[J_1, \ldots, J_{n+1}]$ such that every tuple $(j_1, \ldots, j_{n+1})$ satisfying (E) and such that $Q(j_1, \ldots, j_{n+1}) \neq 0$ lies in the image

of $\mathcal{S}$. Taking the resultant with (E) with respect to j_{n+1}, we obtain a rational fraction $R'(j_1, \dots, j_n)$ of degree C. If R' is well defined and does not vanish at $j_1, \dots, j_n$, then for every root j_{n+1} of (E), the tuple $(j_1, \dots, j_{n+1})$ lies in the image of $\mathcal{S}$.

Since U and U' only depend on the setting, the conditions defining U_δ are equivalent to asking that a certain modular form λ on $\mathcal{S}$ of weight $Cd(\delta)$ does not vanish: this modular form is constructed as in §4.1. After increasing the weight by a constant, we can find a modular form ξ such that $\mathrm{wt}(\lambda) = \mathrm{wt}(\xi)$ and the divisors of λ and ξ have no common codimension 1 components. By Propositions 4.4 and 4.5, we can write

$$\frac{\lambda}{\xi} = \sum_{k=0}^{e-1} R_k(j_1, \dots, j_n) j_{n+1}^k$$

where the R_k are rational fractions such that $\deg R_k \leq Cd(\delta)$ for every k. Taking the resultant with (E) with respect to j_{n+1} yields a rational fraction $R''(j_1, \dots, j_n)$ of degree still bounded by $Cd(\delta)$. If R', R'' are well defined and do not vanish at $(j_1, \dots, j_n)$, then for every root j_{n+1} of (E), the tuple $(j_1, \dots, j_{n+1})$ comes from a point $z \in U_\delta$.

Therefore we can take P_δ to be the product of all numerators and denominators of R, R' and R''. □

Proposition 6.7. *Let $(j_1, \dots, j_n) \in V_\delta$, and let $1 \leq m \leq n+1$. Then*

$$h\big(\Psi_{\delta,m}(j_1, \dots, j_n)\big) \leq C_{20}\, d(\delta)\big(\overline{h}(j_1, \dots, j_n) + \log \ell(\delta)\big).$$

Proof. Let $\mathcal{J}$ be the set of roots of (E) at $(j_1, \dots, j_n)$, and let $j_{n+1} \in \mathcal{J}$. Let $[x, g]$ be the point of $\mathcal{S}$ describing an abelian variety A with PEL structure whose invariants are $(j_1, \dots, j_{n+1})$. Then for every $\gamma \in K_0/K_m$, the point $[x, g\gamma\delta]$ describes an abelian variety A_δ which is related to A by an isogeny of degree $\ell(\delta)$, by Corollary 2.7. Therefore, by Corollary 6.4, we have

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

We now take a closer look at the formula in Definition 3.1. We see that $\Psi_{\delta,m}$ is the evaluation of a multivariate polynomial in the variables $j_{i,\delta}^\gamma([x,g])$ for $1 \leq i \leq m$ and $\gamma \in K_0/K_i$. The number of variables is

$$d_1 + d_1 d_2 + \cdots + d_1 \cdots d_m \leq m\, d(\delta),$$

and each variable appears with degree 1. Therefore, by Proposition 5.10,

$$\begin{aligned} h\big(\Psi_{\delta,m}(j_1, \dots, j_{n+1})\big) &\leq m\, d(\delta) \log(2) + m\, d(\delta)\, C\big(\overline{h}(j_1, \dots, j_{n+1}) + \log \ell(\delta)\big) \\ &\leq Cd(\delta)\big(\overline{h}(j_1, \dots, j_{n+1}) + \log \ell(\delta)\big). \end{aligned}$$

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 5.10 and 5.12, we have

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

Therefore, bluntly using the Lagrange interpolation formula is sufficient. □

6.3 Heights of coefficients of modular equations

In this final subsection, we prove height bounds on modular equations using Proposition 6.7 and the results on heights of fractions from §5.

Definition 6.8. We call an (n, N_1, N_2)-*evaluation tree* a rooted tree with 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 every vertex is bounded by M in absolute value. 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).

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

1. T and a are bounded by some M such that
$$M > \max\{d^4 H \log(d^4 H), 6d\, d_L\},$$
where
$$H = \max\big\{3,\ \log(2M),\ C_{20}\, d(\delta)\big(\log(M(M+1)) + \log \ell(\delta)\big)\big\}.$$
2. $N_1 = 2d$ and $N_2 \geq 2M/3$.
3. T has amplitude $(4d, M)$.
4. 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 V_δ.
5. For every $(y_1, \dots, y_{n-1}) \in \mathcal{I}_{n-1}(T)$, the polynomials P and Q evaluated at $(y_1 Y + a_1, \dots, y_{n-1} Y + a_{n-1}, Y + a_n)$ are coprime in $L[Y]$.
6. $Q(a_1, \dots, a_n) \neq 0$.

Lemma 6.9. *Let $\mathcal{F}$ be a coefficient of $\Psi_{\delta,m}$ of degree $d \geq 1$. Then there exist valid evaluation data (T, a) for $\mathcal{F}$ with $M = C_{21}\big(d(\delta)^6 + \log^2 \ell(\delta)\big)$.*

Proof. According to Theorem 4.6, we have $d \leq C d(\delta)$. Provided that C_{21} is large enough, condition 1 in the definition above will be satisfied.

Since Q is a nonzero polynomial, 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 $a = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ 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 V_δ as in Lemma 6.6, and define

$$R_\delta = P_\delta(Y_1 Y_n + a_1, \ldots, Y_{n-1} Y_n + a_{n-1}, Y_n + a_n)$$

which is a nonzero polynomial of degree at most $Cd(\delta)$. Finally, denote

$$R = \mathrm{Res}(P, Q)(Y_1 Y_n + a_1, \ldots, Y_{n-1} Y_n + a_{n-1}, Y_n + a_n)$$

which is nonzero and has degree at most $2d^2$. Therefore we can find $2d$ values for y_1, bounded by $Cd(\delta)^2$, and lying in an interval with amplitude at most $4d$, such that neither R_δ nor R vanishes when evaluated at $Y_1 = y_1$. We iterate this to construct T up to depth $n-1$ with the right arity, bound and amplitude, such that the evaluations of R_δ and R are nonzero at every $(y_1, \ldots, y_{n-1}) \in \mathcal{I}_{n-1}(T)$.

Let $(y_1, \ldots, y_{n-1}) \in \mathcal{I}_{n-1}(T)$. Then, as before, at most $Cd(\delta)^2$ values for y_n are forbidden as they make either R_δ or R vanish. Therefore it is easy to see that we can complete the tree, perhaps at the cost of increasing C_{21}. Nonvanishing of R_δ and R guarantees conditions 4 and 5 respectively. □

We are now ready to prove part 1 of Theorem 1.1.

Theorem 6.10. *Let $\mathcal{F}(j_1, \ldots, j_n)$ be a coefficient of some $\Psi_{\delta,m}$ in canonical form. Then $h(\mathcal{F}) \leq Cd(\delta) \log \ell(\delta)$.*

Proof. By Lemma 6.9, we can find valid evaluation data (T, a) for $\mathcal{F}$ bounded by $M = C\big(d(\delta)^6 + \log^2 \ell(\delta)\big)$. After scaling P and Q, we can assume that in fact $Q(a_1, \ldots, a_n) = 1$. Let $(y_1, \ldots, y_{n-1}) \in \mathcal{I}_{n-1}(T)$, and write

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

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

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

Therefore by Proposition 6.7

$$h(\widetilde{\mathcal{F}}(y_n)) \leq C_{20}\, d(\delta)\big(\log((M+1)M) + \log \ell(\delta)\big) = H.$$

By construction, the hypotheses of Theorem 1.2 are fulfilled, so

$$\begin{aligned} h(\widetilde{\mathcal{F}}) &\leq 3H + C \log(dH) + 3d \log(2M) \\ &\leq Cd(\delta) \log \ell(\delta) \qquad \text{by Lemma 2.8.} \end{aligned}$$

Moreover, the quotient

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

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

$$h\big(P(y_1Y_n + a_1, \ldots, y_{n-1}Y_n + a_{n-1}, Y_n + a_n)\big) \leq Cd(\delta)\log \ell(\delta)$$

for every $(y_1, \ldots, y_{n-1}) \in \mathcal{I}_{n-1}(P)$, and the same is true for Q. Since $N_1 \geq 2d$, we can now interpolate successively the variables $y_{n-1}, \ldots, y_1$, using Proposition 5.16 at each vertex of the tree T. Finally we obtain

$$h(\mathcal{F}) \leq Cd(\delta)\log \ell(\delta)$$

as claimed. □

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] A. Beshenov. Heights: Lectures by Fabien Pazuki. Available at https://www.math.u-bordeaux.fr/~abesheno/heights.pdf.

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

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

[5] R. Bröker and A. V. Sutherland. An explicit height bound for the classical modular polynomial. *Ramanujan J.*, 22(3):293–313, 2010.

[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] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörper. *Invent. Math.*, 73(3):349–366, 1983.

[12] K.-B. Gundlach. Die Bestimmung der Funktionen zur Hilbertschen Modulgruppe des Zahlkörpers $\mathbb{Q}(\sqrt{5})$. *Math. Ann.*, 152:226–256, 1963.

[13] M. Hindry and J. H. Silverman. *Diophantine Geometry*. Springer-Verlag, New York, 2000.

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

[15] C. Martindale. Hilbert modular polynomials. Preprint, 2019.

[16] F. Mertens. Ein Beitrag zur analytischen Zahlentheorie. *J. Reine Angew. Math.*, 78:46–62, 1874.

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

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

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

[20] J. S. Milne. Canonical models of (mixed) Shimura varieties and automorphic vector bundles. In *Automorphic forms, Shimura varieties, and L-functions, Vol. I (Ann Arbor, 1988)*, volume 10 of *Perspect. Math.*, page 283–414. Academic Press, Boston, 1990.

[21] J. S. Milne. Introduction to Shimura varieties. In *Harmonic Analysis, the Trace Formula, and Shimura Varieties*, volume 4 of *Clay Math. Proc.*, pages 265–378. Amer. Math. Soc., Providence, 2005.

[22] E. Noether. Der Endlichkeitssatz der Invarianten endlicher Gruppen. *Math. Ann.*, 77(1):89–92, 1915.

[23] F. Pazuki. Theta height and Faltings height. *Bull. Soc. Math. France*, 140(1):19–49, 2012.

[24] F. Pazuki. Modular invariants and isogenies. *Int. J. Number Theory*, 15(3):569–584, 2019.

[25] B. Rosser. Explicit bounds for some functions of prime numbers. *Am. J. Math.*, 63(1):211–232, 1941.

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

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

[28] A. V. Sutherland. Computing Hilbert class polynomials with the Chinese remainder theorem. *Math. Comp.*, 80(273):501–538, 2011.

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