Hilbert Modular Polynomials

Chloe Martindale

Hilbert Modular Polynomials

Chloe Martindale

Department of Mathematics and Computer Science,

Technische Universiteit Eindhoven,

P.O. Box 513, 5600 MB Eindhoven, The Netherlands

chloemartindale@gmail.com

Abstract

We present an algorithm to compute a higher dimensional analogue of modular polynomials. This higher dimensional analogue, the 'set of Hilbert modular polynomials', concerns cyclic isogenies of principally polarised abelian varieties with maximal real multiplication by a fixed totally real number field K_0. We give a proof that this algorithm is correct, and provide practical improvements and an implementation for the 2-dimensional case with $K_0 = \mathbb{Q}(\sqrt{5})$. We also explain applications of this algorithm to point counting, walking on isogeny graphs, and computing class polynomials.
Keywords: Hilbert modular polynomials, cyclic isogenies, abelian varieties, genus two, maximal real multiplication.

Acknowledgements. The author would like to thank her PhD supervisor, Marco Streng, for suggesting this research topic and for invaluable input and guidance. Sections 1-6 of this article also appear as Chapter 2 and relevant parts of Chapter 1 of the PhD thesis of the author [Mar18], which was completed at Universiteit Leiden and Université de Bordeaux with the support of funding from the ALGANT-doc programme. This work was also partly supported by the Netherlands Organisation for Scientific Research (NWO) under CHIST-ERA USEIT (grant number 651.002.004).

1 Introduction

The modular polynomial for elliptic curves of prime level p is an irreducible polynomial $\Phi_p(X, Y) \in \mathbb{Z}[X, Y]$ which, for every pair of p-isogenous elliptic curves E and E', satisfies

$$\Phi_p(j(E), j(E')) = 0,$$

where $j(E)$ is the j-invariant of the elliptic curve E. Examples of these modular polynomials can be found for example on Sutherland's website [Sut18]. One of the reasons that modular polynomials interest us is that given the j-invariant of an elliptic curve E over a field k, we can find

the j-invariants of all those elliptic curves that are p-isogenous to it by computing the roots of $\Phi_p(j(E), Y) \in k[Y]$. In this article, we describe an analogue of the modular polynomial for principally polarised abelian varieties of dimension g with real multiplication, which we call a *set of Hilbert modular polynomials*. This is a Hilbert modular function analogue of Dupont's work with Siegel modular functions in [Dup06]. The advantage of working in the Hilbert setting is that the coefficients and degrees of the polynomials are much more manageable than in the Siegel setting, making it possible to compute modular polynomials for higher prime levels than previously. Furthermore, Algorithm 5.8, which is implemented in MAGMA, computes these polynomials. This article gives a proof that the output of the algorithm is correct.

The modular polynomial for elliptic curves of level p parametrises p-isogenies of elliptic curves (for p prime) and is defined using the j-invariant. To generalise the modular polynomial to a Hilbert modular setting, we first fix a totally real number field K_0 of degree g over $\mathbb{Q}$, and we write $\mathcal{O}_{K_0}$ for its maximal order. We then need to replace j by an 'isomorphism invariant' for objects $(\mathrm{A}, \xi, \iota) \in \mathbf{POrd}_{\mathbb{C},K_0}$, the category of principally polarised complex abelian g-folds (A, ξ) with an appropriate embedding $\iota : \mathcal{O}_{K_0} \hookrightarrow \mathrm{End}(\mathrm{A})$ (see Definition 2.1 for the formal definition). Let $\overline{V}$ be the Hilbert modular variety for $\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^{\vee})$, as in Definition 2.13, where $\mathcal{O}_{K_0}^{\vee}$ is the trace dual of $\mathcal{O}_{K_0}$. We denote by $\mathcal{M}_{K_0}(\mathbb{Z})$ the ring of Hilbert modular forms with coefficients in $\mathbb{Z}$ (c.f. Definition 2.11), and we write $\mathbb{Q}(\mathcal{M}_{K_0}(\mathbb{Z}))$ for the field of quotients of modular forms in $\mathcal{M}_{K_0}(\mathbb{Z})$ of equal weight. We will see in Section 3 that for some $d \in \mathbb{Z}$, there exist d Hilbert modular functions

$$J_1, \ldots, J_d \in \mathbb{Q}(\mathcal{M}_{K_0}(\mathbb{Z})),$$

such that the function field of $\overline{V}$ is $\mathbb{C}(J_1, \ldots, J_d)$, and for such $J_1, \ldots, J_d$, there exists a Zariski-open affine subvariety U of $\overline{V}$ such that the rational map

$$(J_1, \ldots, J_d) : U \dashrightarrow \mathbb{A}^d_{\mathbb{C}}$$

is an injective morphism.

Definition 1.1. A d-tuple of $\mathbb{Q}$-linearly independant, non-constant Hilbert modular functions $(J_1, \ldots, J_d) \in \mathbb{Q}(\mathcal{M}_{K_0}(\mathbb{Z}))^{\times d}$ such that

$$\mathbb{C}(\overline{V}) = \mathbb{C}(J_1, \ldots, J_d)$$

is a choice of *RM isomorphism invariants* for K_0.

Remark 1.2. Fixing U as above, if $(\mathrm{A}, \xi, \iota) \in \mathbf{POrd}_{\mathbb{C},K_0}$ corresponds as in Lemma 2.4 to a point in U, then the d-tuple

$$(J_1, \ldots, J_d)(\mathrm{A}, \xi, \iota)$$

determines (A, ξ, ι) up to isomorphism. That is, on U, RM isomorphism invariants are isomorphism invariants in the intuitive sense.

Modular polynomials for elliptic curves of level p correspond to p-isogenies of elliptic curves. Hilbert modular polynomials have a level μ, where μ is a totally positive prime element of $\mathcal{O}_{K_0}$, and this corresponds

to 'μ-isogenies' between elements of $\mathbf{POrd}_{\mathbb{C},K_0}$. These isogenies respect the polarisation and the real multiplication; for the formal definition see Definition 2.2.

Definition 1.3. For a totally positive prime element μ of $\mathcal{O}_{K_0}$, and for $\tau, \tau' \in K_0 \otimes \mathbb{H}$, we say that *there exists a μ-isogeny*

$$\tau \to \tau'$$

if there exists a μ-isogeny

$$(\mathrm{A}, \xi, \iota) \longrightarrow (\mathrm{A}', \xi', \iota',)$$

where the isomorphism classes of (A, ξ, ι) and $(\mathrm{A}', \xi', \iota') \in \mathbf{POrd}_{\mathbb{C},K_0}$ correspond as in Lemma 2.4 to the equivalence classes of τ and τ' in V respectively. (It is well-known that τ and τ' satisfy

$$H_1(\mathrm{A}(\mathbb{C}), \mathbb{Z}) = \tau\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^{\vee} \quad \text{and} \quad H_1(\mathrm{A}'(\mathbb{C}), \mathbb{Z}) = \tau'\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^{\vee}).$$

We can now state our main theorem:

Theorem 1.4. *For a totally real number field K_0 of degree g over $\mathbb{Q}$, and a totally positive prime element μ of $\mathcal{O}_{K_0}$, let $\overline{V}$ be the Hilbert modular variety for K_0 (as defined in Definition 2.13), and fix a choice of RM isomorphism invariant $(J_1, \ldots, J_d)$ for K_0 (as defined in Definition 1.1). Then Algorithm 5.8 outputs a polynomial*

$$G_\mu(X_1, \ldots, X_d, Y) \in \mathbb{Z}[X_1, \ldots, X_d, Y]$$

that has degree $\mathrm{Norm}_{K_0/\mathbb{Q}}(\mu) + 1$ in Y and such that $\Delta G_\mu(J_1, \ldots, J_d, Y)$ is not constant zero on V, and outputs polynomials

$$H_{\mu,i}(X_1, \ldots, X_d, Y, Z_i) \in \mathbb{Z}[X_1, \ldots, X_d, Y, Z_i]$$

that are linear in Z_i, where $i = 2, \ldots d$. Furthermore, for any choice of Zariski-open subvariety U of $\overline{V}$ such that the map

$$(J_1, \ldots, J_d) : U \to \mathbb{A}^d_{\mathbb{C}}$$

is injective, for all but finitely many

$$[\tau], [\tau'] \in (U \cap V) - \{x \in (U \cap V) : \Delta G_\mu(J_1(x), \ldots, J_d(x), Y) = 0\},$$

there exists a μ-isogeny

$$\tau \to \tau'$$

if and only if

$$G(J_1(\tau), \ldots, J_d(\tau), J_1(\tau')) = 0,$$

and for $i = 2, \ldots, d$,

$$H_{\mu,i}(J_1(\tau), \ldots, J_d(\tau), J_1(\tau'), J_i(\tau')) = 0.$$

Definition 1.5. For a totally positive prime element $\mu \in K_0$, we define a *set of Hilbert modular polynomials of level μ* to be a set of polynomials

$$\left\{ \begin{array}{c} G_\mu(X_1, \ldots, X_d, Y) \in \mathbb{Z}[X_1, \ldots, X_d, Y], \\ H_{\mu,i}(X_1, \ldots, X_d, Y, Z_i) \in \mathbb{Z}[X_1, \ldots, X_d, Y, Z_i] \end{array} \right\}_{i=2,\ldots,d}$$

such that $G_\mu(X_1, \ldots, X_d, Y)$ and $H_{\mu,i}(X_1, \ldots, X_d, Y, Z_i)$ satisfy the conclusions of Theorem 1.4.

Remark 1.6. Even though Theorem 1.4 is over $\mathbb{C}$, in practise we can use it also over finite fields (see Section 6).

2 Preliminaries

2.1 Maximal real multiplication

In this article, we will study principally polarised abelian varieties of dimension g defined over $\mathbb{C}$ that have *maximal real multiplication*, that is, the real part of the endomorphism ring is a maximal order in a totally real number field of degree g over $\mathbb{Q}$.

Definition 2.1. Let K_0 be a totally real number field of degree g over $\mathbb{Q}$ with ring of integers $\mathcal{O}_{K_0}$, and define $\mathbf{Ord}_{k,g}$ to be the category of ordinary abelian varieties over a field k of dimension g. We define the objects of the category $\mathbf{Ord}_{k,K_0}$ to be pairs (A, ι), where $\mathrm{A} \in \mathbf{Ord}_{k,g}$ and $\iota : \mathcal{O}_{K_0} \hookrightarrow \mathrm{End}(\mathrm{A})$ is an embedding. A morphism in $\mathbf{Ord}_{k,K_0}$ between two objects (A, ι) and (A', ι') is given by a morphism $f : \mathrm{A} \to \mathrm{A}'$ in $\mathbf{Ord}_{k,g}$ such that the diagram

$$\begin{array}{ccc} \mathrm{End}(\mathrm{A}) \otimes \mathbb{Q} & \xrightarrow{g \mapsto f \circ g \circ f^{-1}} & \mathrm{End}(\mathrm{A}') \otimes \mathbb{Q} \\ {\scriptstyle \iota}\uparrow & \nearrow_{\iota'} & \\ K_0 & & \end{array}$$

commutes. We define the objects of the category $\mathbf{POrd}_{k,K_0}$ to be triples (A, ξ, ι), where $(\mathrm{A}, \iota) \in \mathbf{Ord}_{k,K_0}$ and $\xi : \mathrm{A} \to \mathrm{A}^\vee$ is a principal polarisation of A, and the image of ι is stable under the Rosati involution. A morphism in $\mathbf{POrd}_{k,K_0}$ between two objects (A, ξ, ι) and $(\mathrm{A}', \xi', \iota') \in \mathbf{POrd}_{k,K_0}$ is an isomorphism

$$f : (\mathrm{A}, \iota) \longrightarrow (\mathrm{A}', \iota')$$

in $\mathbf{Ord}_{k,K_0}$ that makes the diagram

$$\begin{array}{ccc} \mathrm{A} & \xrightarrow{f} & \mathrm{A}' \\ {\scriptstyle \xi}\downarrow & & \downarrow{\scriptstyle \xi'} \\ \mathrm{A}^\vee & \xleftarrow[f^\vee]{} & \mathrm{A}'^\vee \end{array}$$

commute.

Definition 2.2. Let K_0 be a totally real number field with ring of integers $\mathcal{O}_{K_0}$ and let k be a field. For

$$(\mathrm{A}, \xi, \iota), (\mathrm{A}', \xi', \iota') \in \mathbf{POrd}_{k,K_0}$$

and $\mu \in \mathcal{O}_{K_0}$, we define a *$\mu$-isogeny* $f : (\mathrm{A}, \xi, \iota) \to (\mathrm{A}', \xi', \iota')$ to be a morphism $f : (\mathrm{A}, \iota) \to (\mathrm{A}', \iota')$ in $\mathbf{Ord}_{k,K_0}$ such that the diagram

$$\begin{array}{ccccc} \mathrm{A} & \xleftarrow{\iota(\mu)} & \mathrm{A} & \xrightarrow{f} & \mathrm{A}' \\ & {\scriptstyle \xi}\searrow & & & \downarrow{\scriptstyle \xi'} \\ & & \mathrm{A}^\vee & \xleftarrow[f^\vee]{} & \mathrm{A}'^\vee \end{array}$$

commutes.

2.2 Hilbert modular forms

Definition 2.3. Let K_0 be a totally real number field of degree g over $\mathbb{Q}$ with ring of integers $\mathcal{O}_{K_0}$. Let $\mathcal{N}$ be an invertible $\mathcal{O}_{K_0}$-ideal. Then the matrix group $\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{N})$ is defined as

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(K_0) : a, d \in \mathcal{O}_{K_0},\, b \in \mathcal{N},\, c \in \mathcal{N}^{-1} \right\}.$$

Let $\mathbb{H}$ be the complex upper half plane. We want to view objects in $\mathbf{POrd}_{\mathbb{C},K_0}$ as elements of $\mathbb{H}^g$, where g is the degree of K_0 over $\mathbb{Q}$. We will be interested in the action of matrix groups with entries in K_0 on elements of $\mathbb{H}^g$, hence it is much more convenient to work with $K_0 \otimes \mathbb{C}$ instead of $\mathbb{C}^g$. To this end, we fix once for all a $\mathbb{C}$-algebra isomorphism

$$\mathbb{C}^g \longrightarrow K_0 \otimes \mathbb{C} \tag{1}$$

and we define $K_0 \otimes \mathbb{H}$ to be the image of $\mathbb{H}^g$ under this isomorphism. Observe that $K_0 \otimes \mathbb{H}$ does not depend on the choice of isomorphism. Let the group of 2×2 matrices with entries in K_0 that have totally positive determinant be denoted by $\mathrm{GL}_2(K_0)^+$. The group $\mathrm{GL}_2(K_0)^+$ acts on $K_0 \otimes \mathbb{H}$ as

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau \mapsto (a\tau + b)(c\tau + d)^{-1}.$$

Lemma 2.4. Let K_0 be a totally real number field of degree g over $\mathbb{Q}$ with ring of integers $\mathcal{O}_{K_0}$, and write $\mathcal{O}_{K_0}^\vee$ for the trace dual of $\mathcal{O}_{K_0}$. Then there is a bijection

$$\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)\backslash(K_0 \otimes \mathbb{H}) \longrightarrow \{(\mathrm{A}, \xi, \iota) \in \mathbf{POrd}_{\mathbb{C},K_0}\}_{/\cong}$$

where the image of $\tau \in \mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)\backslash(K_0 \otimes \mathbb{H})$ is

$$\mathrm{A} = (K_0 \otimes \mathbb{C})/(\tau\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee)$$

with the natural embedding ι and the polarisation induced by the Riemann form $E : (K_0 \otimes \mathbb{C}) \times (K_0 \otimes \mathbb{C}) \longrightarrow \mathbb{R}$ given by

$$E(\tau u_1 + u_2, \tau v_1 + v_2) = \mathrm{tr}_{(K_0 \otimes \mathbb{R})/\mathbb{R}}(u_1 v_2 - u_2 v_1)$$

for $u_1, u_2, v_1, v_2 \in K_0 \otimes \mathbb{R}$.

Proof. See [Gee88, Chapter IX, Section 1]. □

Definition 2.5. Let κ be an integer, and let τ be in $K_0 \otimes \mathbb{H}$. Then the *weight function* w_κ is defined by

$$\begin{array}{ccc} \mathrm{GL}_2(K_0)^+ \times (K_0 \otimes \mathbb{H}) & \longrightarrow & \mathbb{C} \\ (M, \tau) & \mapsto & (\mathrm{N}_{K_0/\mathbb{Q}}(\det(M))^{-\frac{1}{2}} \mathrm{N}_{(K_0 \otimes \mathbb{C})/\mathbb{C}}(c\tau + d))^\kappa, \end{array}$$

where we choose the positive square root.

Definition 2.6. Let $\mathrm{GL}_2(K_0)^+$ and $K_0 \otimes \mathbb{H}$ be as above. Let M be any matrix in $\mathrm{GL}_2(K_0)^+$, and let $f : K_0 \otimes \mathbb{H} \to \mathbb{C}$ be a holomorphic map. Then we define $f|_{[M]_\kappa}$ by

$$\begin{array}{rccc} f|_{[M]_\kappa}: & K_0 \otimes \mathbb{H} & \to & \mathbb{C} \\ & \tau & \mapsto & w_\kappa(M,\tau)^{-1} f(M\tau). \end{array}$$

It is straightforward to check that for $M, N \in \mathrm{GL}_2(K_0)^+$, we have

$$(f|_{[M]_\kappa})|_{[N]_\kappa} = f|_{[MN]_\kappa}.$$

Definition 2.7. Let $\mathrm{GL}_2(K_0)^+$ and $K_0 \otimes \mathbb{H}$ be as above, and assume that $g > 1$. Let Γ be a congruence subgroup of $\mathrm{GL}_2(K_0)^+$. We say that $f : K_0 \otimes \mathbb{H} \to \mathbb{C}$ is a *Hilbert modular form* of weight κ for Γ if and only if it is holomorphic and for all $M \in \Gamma$ and $\tau \in K_0 \otimes \mathbb{H}$, we have

$$f|_{[M]_\kappa}(\tau) = f(\tau).$$

From this point on, if f is a Hilbert modular form of weight κ, then for $M \in \mathrm{GL}_2(K_0)^+$ we will write $f|_M$ for $f|_{[M]_\kappa}$.

Remark 2.8. For $g = 1$, we also have to impose holomorphicity at the cusps.

Definition 2.9. With notation as in Definition 2.7, if $\varphi = f/g$ is the quotient of Hilbert modular forms for Γ of equal weight, then we say that φ is a *Hilbert modular function* for Γ.

Definition 2.10. Suppose that $g = 2$. Then for $f \in \mathcal{M}_{K_0,k}$, if for every $(\tau_1, \tau_2) \in K_0 \otimes \mathbb{H} = \mathbb{H}^2$ we have

$$f(\tau_1, \tau_2) = f(\tau_2, \tau_1),$$

we say that f is *symmetric*.

Definition 2.11. Let $\mathcal{O}_{K_0}^\vee$ be the trace dual of $\mathcal{O}_{K_0}$. We define $\mathcal{M}_{K_0,\kappa}$ to be the $\mathbb{C}$-vector space of Hilbert modular forms for $\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)$ of weight κ, and we define

$$\mathcal{M}_{K_0} = \bigoplus_\kappa \mathcal{M}_{K_0,\kappa}$$

to be the graded $\mathbb{C}$-algebra of all Hilbert modular forms for $\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)$. For $f \in \mathcal{M}_{K_0}$, let $\mathrm{coeffs}(f)$ be the set of coefficients of the q-expansion of f around the cusp at infinity. For a ring R, we define

$$\mathcal{M}_{K_0,\kappa}(R) = \{f \in \mathcal{M}_{K_0,\kappa} : \ \mathrm{coeffs}(f) \subseteq R\},$$

and

$$\mathcal{M}_{K_0}(R) = \{f \in \mathcal{M}_{K_0} : \ \mathrm{coeffs}(f) \subseteq R\}.$$

Theorem 2.12. *(Baily-Borel Theorem)*
Let $\mathcal{M}_{K_0}$ be the graded ring of Hilbert modular forms for $\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)$. Then the normal complex analytic space of $\mathrm{Proj}(\mathcal{M}_{K_0})$ is a compactification of

$$V = \mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee) \backslash (K_0 \otimes \mathbb{H}).$$

Proof. See [Gee88, p. II.7.1]. □

Definition 2.13. We define the *Hilbert modular variety* $\overline{V}$ to be the normal complex analytic space of $\mathrm{Proj}(\mathcal{M}_{K_0})$. We will also refer to this as the *Baily-Borel compactification of* V.

Proposition 2.14. (Rapoport)
$\mathcal{M}_{K_0,\kappa}(\mathbb{Z})$ is a finitely generated $\mathbb{Z}$-module.

Proof. See [Rap78, Proposition 6.6]. □

Lemma 2.15. (Rapoport)

$$\mathcal{M}_{K_0}(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{C} = \mathcal{M}_{K_0}.$$

Proof. See the proof of [Rap78, Lemma 6.12]. □

Proposition 2.16. Let K_0 be a quadratic number field of discriminant 5, 8, 13 or 17. Then $\mathcal{M}_{K_0}(\mathbb{Q})$ is a finitely generated $\mathbb{Q}$-algebra, and the q-expansions of a choice of generators are known.

Proof. For discriminant 5 see [Mue85] or [May07], for discriminant 8 see [Mue83], and for discriminants 13 and 17 see [May07]. □

Remark 2.17. In everything that follows, we will assume that $\mathcal{M}_{K_0}(\mathbb{Q})$ is a finitely generated $\mathbb{Q}$-algebra.

3 Defining RM isomorphism invariants

As before, let K_0 be a totally real number field of degree g over $\mathbb{Q}$, and let $\overline{V}$ be the Hilbert modular variety for $\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^{\vee})$, as defined in Definition 2.13. The aim of this section is to prove Proposition 3.1.

For completeness, we recall here the definition of RM isomorphism invariants from above.

Definition 1.1. *A d-tuple of $\mathbb{Q}$-linearly independant, non-constant Hilbert modular functions*

$$(J_1, \ldots, J_d) \in \mathbb{Q}(\mathcal{M}_{K_0}(\mathbb{Z}))^{\times d}$$

such that

$$\mathbb{C}(\overline{V}) = \mathbb{C}(J_1, \ldots, J_d)$$

is a choice of RM isomorphism invariants *for* K_0.

Proposition 3.1. Write $\mathbb{Q}(\mathcal{M}_{K_0}(\mathbb{Z}))$ for the $\mathbb{Q}$-algebra of quotients of Hilbert modular forms in $\mathcal{M}_{K_0}(\mathbb{Z})$ of equal weight. There exists $d \in \mathbb{Z}$ and a choice

$$J_1, \ldots, J_d \in \mathbb{Q}(\mathcal{M}_{K_0}(\mathbb{Z}))$$

of RM isomorphism invariant for K_0. Furthermore, for such $J_1, \ldots, J_d$, there exists a Zariski-open affine subvariety U of $\overline{V}$ such that the map

$$(J_1, \ldots, J_d) : U \longrightarrow \mathbb{A}^d_{\mathbb{C}}$$

is a well-defined injective morphism.

Proof. Write $\mathbb{C}(\mathcal{M}_{K_0})$ for the field of quotients of elements of $\mathcal{M}_{K_0}$ of equal weight. By definition of $\overline{V}$ (see Definition 2.13), we have that $\mathbb{C}(\overline{V}) = \mathbb{C}(\mathcal{M}_{K_0})$, and by Lemma 2.15, we know that

$$\mathbb{Q}(\mathcal{M}_{K_0}(\mathbb{Z})) \otimes_{\mathbb{Q}} \mathbb{C} = \mathbb{C}(\mathcal{M}_{K_0}).$$

So let $J_1, \ldots, J_d$ be generators of the $\mathbb{Q}$-algebra $\mathbb{Q}(\mathcal{M}_{K_0}(\mathbb{Z}))$, so that

$$\mathbb{C}(J_1, \ldots, J_d) = \mathbb{C}(\overline{V}),$$

and write W for the image of $(J_1, \ldots, J_d)$ in $\mathbb{A}^d_{\mathbb{C}}$. Then by [Har77, Corollary I.4.5], there are non-empty Zariski-open subsets $U \subseteq \overline{V}$ and $U' \subseteq W$ such that U is isomorphic to U'. □

Example 3.2. If $g = 1$, so that $K_0 = \mathbb{Q}$, then we have that

$$\mathrm{SL}_2(\mathcal{O}_{K_0} \oplus \mathcal{O}^\vee_{K_0}) \backslash K_0 \otimes \mathbb{H} = \mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H}.$$

The j-invariant for elliptic curves defines an isomorphism

$$j : \mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H} \longrightarrow \mathbb{A}^1_{\mathbb{C}}.$$

Hence setting

$$V = \mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H}, \quad \overline{V} = \mathbb{P}^1_{\mathbb{C}}, \quad U = V, \text{ and } \quad J_1 = j$$

gives us $\mathbb{C}(\overline{V}) = \mathbb{C}(J_1)$ and an injective morphism $J_1 : U \to \mathbb{A}^1_{\mathbb{C}}$.

4 Algorithm to compute a set of Hilbert modular polynomials

As before, in what follows, K_0 is a totally real number field of degree g over $\mathbb{Q}$ with ring of integers $\mathcal{O}_{K_0}$. From this point on, we fix RM isomorphism invariants $(J_1, \ldots, J_d) \in \mathbb{Q}(\mathcal{M}_{K_0}(\mathbb{Z}))^{\times d}$, and a non-empty Zariski-open subvariety U of the Hilbert modular variety $\overline{V}$ such that

$$(J_1, \ldots, J_d) : U \longrightarrow \mathbb{A}^d_{\mathbb{C}}$$

defines an injective morphism.

For $i = 1, \ldots, d$, we choose f_i and g_i to be elements of $\mathcal{M}_{K_0}(\mathbb{Z})$ of weight k_i such that

$$J_i = f_i / g_i. \tag{2}$$

Definition 4.1. Let $\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}^\vee_{K_0})$ be as in Definition 2.3 and let μ be a totally positive prime element of $\mathcal{O}_{K_0}$. Define

$$\Gamma^0(\mu) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}^\vee_{K_0}) : b \in \mu \mathcal{O}^\vee_{K_0} \right\}.$$

For any $x \in K_0$ define

$$\underline{x} := \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}.$$

Given a Hilbert modular form $f \in \mathcal{M}_{K_0}(\mathbb{Z})$, for every $N \in \mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}^\vee_{K_0})$, the function $f|_{\underline{\mu^{-1}} N}$ depends only on the class of N in

$$\Gamma^0(\mu) \backslash \mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}^\vee_{K_0}).$$

Definition 4.2. Denote by $\mathcal{C}$ a choice of coset representatives for the quotient of groups

$$\Gamma^0(\mu)\backslash \mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee).$$

We then further define

$$\Phi_\mu(Y) := \prod_{M \in \mathcal{C}} \left(g_1|_{\underline{\mu^{-1}} M} Y - f_1|_{\underline{\mu^{-1}} M} \right)$$

and for each $i = 2, \ldots, d$,

$$\Psi_{\mu,i}(Y, Z_i) := \sum_{M \in \mathcal{C}} \left\{ \left(g_i|_{\underline{\mu^{-1}} M} Z_i - f_i|_{\underline{\mu^{-1}} M} \right) \cdot \prod_{\substack{M' \in \mathcal{C} \\ M' \neq M}} \left(g_1|_{\underline{\mu^{-1}} M'} Y - f_1|_{\underline{\mu^{-1}} M'} \right) \right\}.$$

Note that the definitions of $\Phi_\mu(Y)$ and $\Psi_{\mu,i}(Y, Z_i)$ do not depend on the choice of coset representatives for $\Gamma^0(\mu)\backslash \mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)$.

Remark 4.3. We have that

$$\Phi_\mu(Y) \in \mathcal{M}_{K_0}(\mathbb{Z})[Y] \quad \text{and} \quad \Psi_{\mu,i}(Y, Z_i) \in \mathcal{M}_{K_0}(\mathbb{Z})[Y, Z_i].$$

Proof. Recall that for $M \in \mathcal{C}$ and $N \in \mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)$, for every $f \in \mathcal{M}_{K_0}$, we have that

$$(f|_{\underline{\mu^{-1}} M})|_N(\tau) = f|_{\underline{\mu^{-1}} MN}(\tau).$$

In particular, acting by $|_N$ on the coefficients of $\Phi_\mu(Y)$ (and $\Psi_{\mu,i}(Y, Z_i)$) just permutes the factors (or terms) of the defining product (or sum), leaving $\Phi_\mu(Y)$ (and $\Psi_{\mu,i}(Y, Z_i)$) unchanged, hence the coefficients are modular forms for $\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)$. □

As Φ_μ is a univariate polynomial with coefficients that are modular forms for $\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)$ of equal weight, the discriminant $\Delta\Phi_\mu$ is also a modular form for $\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)$. In particular, whether or not $(\Delta\Phi_\mu)(\tau) = 0$ depends only on the class of τ in V.

Proposition 4.4. Fix notation as in Definition 4.2 and recall from Definition 1.3 the definition of a μ-isogeny $\tau \to \tau'$ for $\tau, \tau' \in K_0 \otimes \mathbb{H}$. For any $\tau, \tau' \in K_0 \otimes \mathbb{H}$ such that the classes $[\tau]$ and $[\tau']$ of τ and τ' in $\overline{V}$ are in

$$(U \cap V) - \{x \in (U \cap V) : (\Delta\Phi_\mu)(x) = 0\},$$

there exists a μ-isogeny $\tau \to \tau'$ if and only if for every $i = 2, \ldots, d$, evaluating $\Phi_\mu(Y)$ and $\Psi_{\mu,i}(Y, Z_i)$ at $(Y, Z_2, \ldots, Z_d) = (J_1([\tau']), \ldots, J_d([\tau']))$, and then evaluating the resulting modular forms at τ, gives

$$\left(\Phi_\mu(J_1([\tau']))\right)(\tau) = 0 \quad \text{and} \quad \left(\Psi_{\mu,i}(J_1([\tau']), J_i([\tau']))\right)(\tau) = 0.$$

Lemma 4.5. If μ is a totally positive prime element of $\mathcal{O}_{K_0}$ then the set $\Gamma^0(\mu)\backslash \mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)$ has $\mathrm{Norm}_{K_0/\mathbb{Q}}(\mu) + 1$ elements.

Proof. Define

$$k := \max\{n \in \mathbb{Z} : (\mathcal{O}_{K_0}^\vee)^{-1} \subseteq \mu^n \mathcal{O}_{K_0}\}.$$

There is a bijection of sets

$$\begin{array}{ccccc} \Gamma^0(\mu)\backslash \mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee) & \longleftrightarrow & (\underline{\mu^k}\Gamma^0(\mu)\underline{\mu^{-k}})\backslash(\underline{\mu^k}\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)\underline{\mu^{-k}}) \\ M & \mapsto & \underline{\mu^k} M \underline{\mu^{-k}}. \end{array}$$

We claim that

$$\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathcal{O}_{K_0}/\mu\mathcal{O}_{K_0} \right\} \cup \left\{ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\}$$

is in bijection with $(\underline{\mu^k}\Gamma^0(\mu)\underline{\mu^{-k}})\backslash(\underline{\mu^k}\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)\underline{\mu^{-k}})$. Let

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \underline{\mu^k}\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)\underline{\mu^{-k}}.$$

Then $a, d \in \mathcal{O}_{K_0}$, $b \in \mu^k \mathcal{O}_{K_0}^\vee \subseteq (\mathcal{O}_{K_0})_{(\mu)}$ and $c \in \mu^{-k}(\mathcal{O}_{K_0}^\vee)^{-1} \subseteq (\mathcal{O}_{K_0})_{(\mu)}$, so that in particular, reduction by μ defines a group homomorphism

$$r : \underline{\mu^k}\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)\underline{\mu^{-k}} \to \mathrm{SL}_2(\mathcal{O}_{K_0}/\mu\mathcal{O}_{K_0}).$$

Now $\mathcal{O}_{K_0}/\mu\mathcal{O}_{K_0}$ is a field as $\mu\mathcal{O}_{K_0}$ is prime, and $\mathrm{SL}_2(\mathcal{O}_{K_0}/\mu\mathcal{O}_{K_0})$ acts on $\mathbb{P}^1(\mathcal{O}_{K_0}/\mu\mathcal{O}_{K_0})$ as

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot (x : y) \mapsto (ax + by : cx + dy).$$

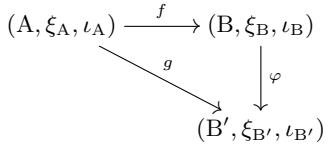
The stabilizer of $(0 : 1)$ is

$$\left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_{K_0}/\mu\mathcal{O}_{K_0}) \right\},$$

the pull-back of which under r is $\underline{\mu^k}\Gamma^0(\mu)\underline{\mu^{-k}}$, so the bijection follows from the orbit-stabilizer theorem. □

We will prove Proposition 4.4 by using the above lemma and a representation of μ-isogenies up to isomorphism.

Definition 4.6. We say μ-isogenies $f : (\mathrm{A}, \xi_\mathrm{A}, \iota_\mathrm{A}) \to (\mathrm{B}, \xi_\mathrm{B}, \iota_\mathrm{B})$ and $g : (\mathrm{A}, \xi_\mathrm{A}, \iota_\mathrm{A}) \to (\mathrm{B}', \xi_{\mathrm{B}'}, \iota_{\mathrm{B}'})$ are *isomorphic* if there exists a 1-isogeny $\varphi : (\mathrm{B}, \xi_\mathrm{B}, \iota_\mathrm{B}) \to (\mathrm{B}', \xi_{\mathrm{B}'}, \iota_{\mathrm{B}'})$ such that the diagram



commutes.

Definition 4.7. For every $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = M \in \mathrm{GL}_2(K_0)^+$ and for every $\tau \in K_0 \otimes \mathbb{H}$, we define $\varphi_{M,\tau}$ to be the element of $\mathrm{Hom}_{\mathbf{Ord}_{\mathbb{C},K_0}}(\tau, M\tau) \otimes \mathbb{Q}$ that is multiplication by $(c\tau + d)^{-1}$ on $K_0 \otimes \mathbb{C}$.

Note that

$$\varphi_{B,A\tau} \circ \varphi_{A,\tau} = \varphi_{BA,\tau} \tag{3}$$

and

$$\varphi_{M,\tau}^{-1} = \varphi_{M^{-1},M\tau}. \tag{4}$$

Lemma 4.8. We have that $\varphi_{M,\tau}$ is an isomorphism in $\mathbf{POrd}_{\mathbb{C},K_0}$ if and only if $M \in \mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)$.

Proof. Write $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and for any $\tau' \in K_0 \otimes \mathbb{H}$ let $E_{\tau'}$ be the Riemann form

$$E_{\tau'}(u_1\tau + u_2, v_1\tau' + v_2) = \mathrm{tr}_{K_0/\mathbb{Q}}(u_1v_2 - u_2v_1).$$

We get commutative diagram of unpolarised abelian varieties, where the dashed arrows are automorphisms of $K_0 \otimes \mathbb{C}$ that may or may not induce actual maps of abelian varieties:

$$\begin{array}{ccc} (K_0 \otimes \mathbb{C})/(\tau\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee) & \overset{\varphi_{M,\tau} := (c\tau+d)^{-1}}{- - - - - \to} & (K_0 \otimes \mathbb{C})/(M\tau\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee) \\ & \overset{f := \mathrm{id}_{(K_0 \otimes \mathbb{C})}}{\searrow} & \Big\downarrow{\scriptstyle c\tau+d} \\ & & (K_0 \otimes \mathbb{C})/((a\tau + b)\mathcal{O}_{K_0} + (c\tau + d)\mathcal{O}_{K_0}^\vee). \end{array}$$

Now f, and hence ϕ defines an isomorphism on lattices if and only if $M \in \mathrm{GL}(\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee)$. Suppose now that $M \in \mathrm{GL}(\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee)$. It remains to show that $\det(M) = 1$ if and only if ϕ is an isomorphism in $\mathbf{POrd}_{\mathbb{C},K_0}$, that is, if

$$E_\tau(\alpha, \beta) = E_{M\tau}(\phi(\alpha), \phi(\beta)).$$

Write $E_\tau = \mathrm{tr}_{K_0/\mathbb{Q}} \circ S_\tau$ and $E_{M\tau} = \mathrm{tr}_{K_0/\mathbb{Q}} \circ S_{M\tau}$. The matrices of S_τ and $\phi^* S_{M\tau}$ with respect to the $(K_0 \otimes \mathbb{R})$-basis $\{\tau, 1\}$ of $K_0 \otimes \mathbb{C}$ are

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

and

$$M \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} M^t$$

respectively, so $S_\tau = \phi^* S_{M\tau}$ if and only if $\det(M) = 1$ and the result follows. □

Lemma 4.9. Fix a totally positive prime element $\mu \in K_0$. Then for any $\tau \in K_0 \otimes \mathbb{H}$, there is a map

$$\begin{array}{rccc} i: & \Gamma^0(\mu)\backslash \mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee) & \longrightarrow & \left\{ \mu\text{-isogenies from } \tau \right\}_{/\cong} \\ & M & \mapsto & \varphi_{\underline{\mu^{-1}},M\tau} \circ \varphi_{M,\tau}, \end{array}$$

and i defines a bijection of sets.

Proof. Observe that $\mathrm{id}_{K_0\otimes\mathbb{C}}$ defines a μ-isogeny

$$\begin{aligned}\varphi_{\underline{\mu^{-1}},\tau} : \big((K_0\otimes\mathbb{C})/(\tau\mathcal{O}_{K_0}+\mathcal{O}_{K_0}^\vee),\xi,\iota\big)\\ \longrightarrow \big((K_0\otimes\mathbb{C})/(\mu^{-1}\tau\mathcal{O}_{K_0}+\mathcal{O}_{K_0}^\vee),\mu\xi,\iota\big),\end{aligned}$$

where $\xi = (\tau-\overline{\tau})^{-1}$, which in other words is a μ-isogeny $\tau \to \mu^{-1}\tau$. Replacing τ by $M\tau$ with

$$M \in \Gamma^0(\mu)\backslash \mathrm{SL}(\mathcal{O}_{K_0}\oplus\mathcal{O}_{K_0}^\vee)$$

it is easy to see that i is well-defined on $\mathrm{SL}(\mathcal{O}_{K_0}\oplus\mathcal{O}_{K_0}^\vee)$.

We claim further that i is a well-defined injection of sets. Let $M,N \in \mathrm{SL}(\mathcal{O}_{K_0}\oplus\mathcal{O}_{K_0}^\vee)$ and suppose that $\varphi_{\underline{\mu^{-1}},M\tau}\circ\varphi_{M,\tau}$ and $\varphi_{\underline{\mu^{-1}},N\tau}\circ\varphi_{N,\tau}$ are isomorphic as μ-isogenies. That is, there exists an isomorphism

$$\psi : \underline{\mu^{-1}}M\tau \to \underline{\mu^{-1}}N\tau$$

such that

$$\psi\circ\varphi_{\underline{\mu^{-1}},M\tau}\circ\varphi_{M,\tau} = \varphi_{\underline{\mu^{-1}},N\tau}\circ\varphi_{N,\tau}, \tag{5}$$

hence by (3) and (4)

$$\psi = \varphi_{\underline{\mu^{-1}}NM^{-1}\underline{\mu},\underline{\mu^{-1}}M\tau}. \tag{6}$$

By Lemma 4.8, as ψ is an isomorphism, we have that

$$\underline{\mu^{-1}}NM^{-1}\underline{\mu} \in \mathrm{SL}(\mathcal{O}_{K_0}\oplus\mathcal{O}_{K_0}^\vee).$$

Define $X = NM^{-1}$ and $T = \underline{\mu^{-1}}NM^{-1}\underline{\mu}$. As T and $X \in \mathrm{SL}(\mathcal{O}_{K_0}\oplus\mathcal{O}_{K_0}^\vee)$, we get further that $X \in \Gamma^0(\mu)$. Conversely, suppose that $NM^{-1} \in \Gamma^0(\mu)$. Then $\underline{\mu^{-1}}NM^{-1}\underline{\mu} \in \mathrm{SL}(\mathcal{O}_{K_0}\oplus\mathcal{O}_{K_0}^\vee)$, so ψ defined by (6) is an isomorphism. Hence i is a well-defined injection of sets.

To show that i is in fact a bijection we proceed by counting. By Lemma 4.5 the set $\mathcal{C}$ has $\mathrm{Norm}_{K_0/\mathbb{Q}}(\mu)+1$ elements, so we just need to show that there are at most $\mathrm{Norm}_{K_0/\mathbb{Q}}(\mu)+1$ non-isomorphic μ-isogenies from any given $\tau \in K_0\otimes\mathbb{H}$. If $f : (\mathrm{A},\xi_\mathrm{A},\iota_\mathrm{A}) \to (\mathrm{B},\xi_\mathrm{B},\iota_\mathrm{B})$ is a μ-isogeny, then

$$\ker(f) \subseteq \ker(\mu) \cong (\mathcal{O}_{K_0}/\mu\mathcal{O}_{K_0})^{\times 2}.$$

Also, as for every $\alpha \in \mathcal{O}_{K_0}$ the following diagram commutes:

$$\begin{array}{ccccc}\ker(f) & \longrightarrow & \mathrm{A} & \xrightarrow{f} & \mathrm{B}\\ \downarrow & & \downarrow{\scriptstyle \iota_\mathrm{A}(\alpha)} & & \downarrow{\scriptstyle \iota_\mathrm{B}(\alpha)}\\ \ker(f) & \longrightarrow & \mathrm{A} & \xrightarrow{f} & \mathrm{B},\end{array}$$

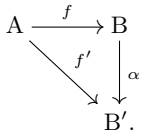
the kernel of f is an $\mathcal{O}_{K_0}$-module, and hence an $\mathcal{O}_{K_0}/\mu\mathcal{O}_{K_0}$ sub-vector space of $(\mathcal{O}_{K_0}/\mu\mathcal{O}_{K_0})^{\times 2}$. Then, as $\deg(f) = \mathrm{Norm}_{K_0/\mathbb{Q}}(\mu)$, there are at most $\mathrm{Norm}_{K_0/\mathbb{Q}}(\mu)+1$ distinct kernels of μ-isogenies from any given τ (or equivalently any given $(\mathrm{A},\xi,\iota) \in \mathbf{POrd}_{\mathbb{C},K_0}$). Therefore it remains to show that there do not exist non-isomorphic μ-isogenies

$$f : (\mathrm{A},\xi_\mathrm{A},\iota_\mathrm{A}) \to (\mathrm{B},\xi_\mathrm{B},\iota_\mathrm{B})$$

and

$$f' : (\mathrm{A}, \xi_{\mathrm{A}}, \iota_{\mathrm{A}}) \to (\mathrm{B}', \xi_{\mathrm{B}'}, \iota_{\mathrm{B}'})$$

with the same kernel. By the universal property of quotient maps there exists an isomorphism α (of unpolarised abelian varieties) such that the following diagram commutes:



We claim that α is a 1-isogeny. Consider the following diagram:

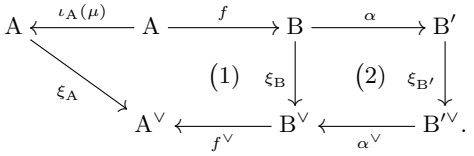


Diagram (1) commutes as f is a μ-isogeny and the diagram formed by the outside arrows commutes as f' is a μ-isogeny, hence diagram (2) commutes. Similarly, consider the following diagram:

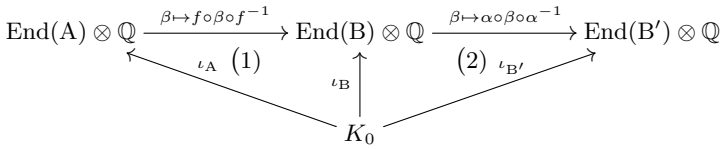


Diagram (1) commutes as f is a μ-isogeny and the diagram formed by the outside arrows commutes as f' is a μ-isogeny and

$$f' \circ \beta(f')^{-1} = (\alpha \circ f) \circ \beta \circ (\alpha \circ f)^{-1} = \alpha \circ (f \circ \beta \circ f^{-1}) \circ \alpha^{-1}.$$

Hence (2) commutes, so α is a 1-isogeny and f and f' are isomorphic as μ-isogenies. □

Proof of Proposition 4.4. Suppose first that there exists a μ-isogeny $\tau \to \tau'$. Then by Lemma 4.9, there exists $N \in \mathcal{C} = \Gamma^0(\mu) \backslash \mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)$ such that this μ-isogeny is isomorphic to a μ-isogeny $\tau \to \mu^{-1} N\tau$, so we can identify τ' with $\mu^{-1} N\tau$. Plugging this into the definitions of $\Phi_\mu(Y)$ and $\Psi_{\mu,i}(Y, Z_i)$, we get

$$\Phi_\mu(J_1(\mu^{-1} N\tau)) = 0$$

and

$$\Psi_{\mu,i}(J_1(\mu^{-1} N\tau), J_i(\mu^{-1} N\tau)) = 0.$$

Suppose now that $(Y_0, Z_{2,0}, \ldots, Z_{d,0})$ is a common root of $\Phi_\mu(Y)$ and $\Psi_{\mu,i}(Y, Z_i)$. One can see directly from the definition of Φ_μ and $\Psi_{\mu,i}$ that under the discriminant condition, the set of common roots of (4.2) is exactly the set

$$\{(J_1(\mu^{-1} M\tau), \ldots, J_d(\mu^{-1} M\tau)) : M \in \mathcal{C}\}.$$

Therefore, there exists $N \in \mathcal{C}$ such that

$$(Y_0, Z_{2,0}, \ldots, Z_{d,0}) = (J_1(\mu^{-1}N\tau), \ldots, J_d(\mu^{-1}N\tau)),$$

and by Lemma 4.9 there exists a μ-isogeny

$$\tau \to \mu^{-1}N\tau.$$

□

5 Computing the RM isomorphism invariants for a given genus 2 curve

In Definition 1.1, we defined RM isomorphism invariants for elements of $\mathbf{POrd}_{\mathbb{C},K_0}$. Restrict now to the dimension 2 case. It is however not immediately clear how to compute these given the equation of a genus 2 curve. We have a computational advantage in genus 2, which is that there already exist Igusa-Clebsch invariants to determine a curve up to isomorphism.

Definition 5.1. For a curve C of genus 2 over a field k with $\mathrm{char}(k) \neq 2$, there exists a hyperelliptic model $y^2 = f(x)$ of C, where f is a separable polynomial of degree 6. Fix such a model, denote by c the leading coefficient of f, fix an ordering $x_1, \ldots, x_6$ of the roots of f in its splitting field, and denote by (ij) the difference $x_i - x_j$. For $\mathrm{char}(k) \neq 2, 3, 5$, we define the *Igusa-Clebsch invariants* of C to be

$$\begin{aligned}
I_2 &= c^2 \sum (12)^2(34)^2(56)^2, \\
I_4 &= c^4 \sum (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2, \\
I_6 &= c^6 \sum (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2(14)^2(25)^2(36)^2, \\
I_{10} &= c^{10} \prod (12)^2,
\end{aligned}$$

where each sum and product runs over the distinct expressions obtained by applying a permutation to the index set $\{1, \ldots, 6\}$.

These invariants are integral whenever f is integral. The Igusa-Clebsch invariants are 'invariants for the Siegel moduli space'. Before making this more precise, we recall some facts about the Siegel moduli space.

Definition 5.2. We define

$$\mathrm{Sym}_2(\mathbb{C}) = \left\{ \begin{pmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{C}) \right\},$$

and for $\tau \in \mathrm{Sym}_2(\mathbb{C})$, we write $\mathrm{Im}(\tau) > 0$ for '$\mathrm{Im}(\tau)$ is positive definite'.

Definition 5.3. The *Siegel upper half space* is defined to be

$$\mathbb{H}_2 = \left\{ \tau = \begin{pmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_4 \end{pmatrix} \in \mathrm{Sym}_2(\mathbb{C}) : \mathrm{Im}(\tau) > 0 \right\},$$

and the symplectic group

$$\mathrm{Sp}_2(\mathbb{Z}) = \left\{ \gamma \in \mathrm{GL}_4(\mathbb{Z}) : \gamma \begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix} \gamma^{\mathrm{tr}} = \begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix} \right\}$$

acts on $\mathbb{H}_2$ via

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \cdot \tau = (A\tau + B)(C\tau + D)^{-1}.$$

The field of rational functions of the coarse moduli space for hyperelliptic curves of genus 2 can be generated by three Siegel modular functions, as shown by Igusa in [Igu60]. Following the notation in the Echidna database [Echidna], we choose as generators three Siegel modular functions

$$i_1, i_2, i_3 : \mathrm{Sp}_2(\mathbb{Z})\backslash\mathbb{H}_2 \longrightarrow \mathbb{C}$$

such that, if C is a curve of genus 2, and $[\tau] \in \mathrm{Sp}_2(\mathbb{Z})\backslash\mathbb{H}_2$ is the point in the moduli space corresponding to C, then

$$i_1(\tau) = (I_4 I_6 / I_{10})(C), \tag{7}$$

$$i_2(\tau) = (I_2^3 I_4 / I_{10})(C), \tag{8}$$

$$i_3(\tau) = (I_2^2 I_6 / I_{10})(C). \tag{9}$$

Now, for a totally real quadratic number field K_0, the forgetful functor

$$\begin{array}{ccc} \mathbf{POrd}_{\mathbb{C},K_0} & \longrightarrow & \mathbf{POrd}_{\mathbb{C},2} \\ (\mathrm{A}, \xi, \iota) & \mapsto & (\mathrm{A}, \xi) \end{array}$$

induces a map

$$\phi : \mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^{\vee})\backslash K_0 \otimes \mathbb{H} \to \mathrm{Sp}_2(\mathbb{Z})\backslash\mathbb{H}_2,$$

which is generically 2-1. We will refer to this as the *modular map*. The image of this map is called the *Humbert surface for* K_0, and is denoted as $\mathcal{H}_{K_0}$. That is, the modular map ϕ induces a degree 2 map

$$\phi : \mathcal{M}_{K_0} \longrightarrow \mathcal{H}_{K_0}.$$

In particular, as there exist 2 algebraically independent Siegel modular functions f_1 and f_2 in

$$\mathbb{C}(\mathcal{H}_{K_0}) \subseteq \mathbb{C}(i_1, i_2, i_3),$$

we get 2 algebraically independent Hilbert modular functions

$$J_1 = \phi^* f_1 \quad \text{and} \quad J_2 = \phi^* f_2 \tag{10}$$

in $\mathbb{C}(\mathcal{M}_{K_0})$. Also, by construction, we get that J_1 and J_2 are *symmetric*, that is, that if σ is the generator of $\mathrm{Gal}(K_0/\mathbb{Q})$, then for all $\tau \in K_0 \otimes \mathbb{H}$, we have that

$$J_1(\sigma(\tau)) = J_1(\tau) \quad \text{and} \quad J_2(\sigma(\tau)) = J_2(\tau).$$

By Proposition 2.14 and Lemma 2.15, we have that $\mathbb{C}(\overline{V})$ is a finite separable field extension of $\mathbb{C}(J_1, J_2)$ and hence is generated by one element; choose such an element and denote it by J_3. Write $m(X) \in \mathbb{C}(J_1, J_2)[X]$ for the minimal polynomial of J_3; then $m(X)$ is the pullback along ϕ of a polynomial in $\mathbb{C}(i_1, i_2, i_3)[X]$.

The subtlety of how to choose the root of $m(X)$ in practice is addressed in Algorithm 6.4, Step 2.

Example 5.4. Gundlach [Gun63] and Müller [Mue85] computed formulae for a choice of isomorphism invariants J_1, J_2, and J_3 for $K_0 = \mathbb{Q}(\sqrt{5})$, and gave the functions from which J_1, J_2, and J_3^2 (here $m(X)$ is quadratic and without a linear term) are pulled back along ϕ:

$$J_1 = \phi^* \left(\frac{2^{-6}3^{-3}i_1^2 i_2^2 + 2^{-3}3^2 i_1 i_2^2 - 2^{-4}3^{-3} i_1 i_3^3 + 2^{-5}3^2 i_2 i_3^2}{i_1^2 i_2^2 + 2^2 3^5 i_1 i_2^2} \right), \tag{11}$$

$$J_2 = \phi^* \left(\frac{2^9 i_1^3 i_2^2 + 2^{11} 3^5 i_1^2 i_2^2}{i_1^2 i_2^2 + 2^2 i_1 i_3^3 - 2 \cdot 3^5 i_2 i_3^2} \right), \tag{12}$$

$$\begin{aligned} J_3^2 = {} & 5^5 - 2^{-1}5^3 J_1 J_2 + 2^{-4} J_2 + 2^{-1}3^2 5^2 J_2^2 J_1^3 - 2^{-3} J_1^2 J_2^2 \\ & - 2 \cdot 3^3 J_2^3 J_1^5 + 2^{-4} J_2^3 J_1^4. \end{aligned} \tag{13}$$

Remark 5.5. For each choice of K_0, we have to recalculate RM isomorphism invariants J_1, J_2, and J_3. In [LNY16, Theorem 2.2], Lauter, Naehrig, and Yang give a method to calculate a choice of Siegel modular functions f_1 and f_2 as in (10), but the minimal polynomial of J_3 over $\mathbb{Q}(J_1, J_2)$ is not known in general.

Recall from Lemma 2.15 that $\mathbb{C}(\overline{V}) = \mathbb{Q}(\mathcal{M}_{K_0}(\mathbb{Z})) \otimes \mathbb{C}$, so that in particular a choice of $\mathbb{Q}$-algebra generators $J_1, \ldots, J_d$ for $\mathbb{Q}(\mathcal{M}_{K_0}(\mathbb{Z}))$ is also a choice of $\mathbb{C}$-algebra generators for $\mathbb{C}(\overline{V})$. In the cases for which a complete set of generators is known, namely K_0 of discriminant 5, 8, 13, and 17, we can choose RM isomorphism invariants $J_1, J_2, J_3 \in \mathbb{Q}(\mathcal{M}_{K_0}(\mathbb{Z}))^{\times 3}$ for which J_1 and J_2 are symmetric Hilbert modular functions (as above) and $J_3^2 \in \mathbb{Q}(J_1, J_2)$. For simplicity, we restrict to this case in all that follows.

5.1 The algorithm

Given the coefficients of the q-expansions of the numerators and denominators of $J_1, \ldots, J_d$ up to a high enough precision (see the implementation at `www.martindale.info/research` for details on the precision), using Lemma 6.2 and the formulae for $\Phi_\mu(Y)$ and $\Psi_{\mu,i}(Y, Z_i)$ given in Definition 4.2 we can write out explicit formulae for the q-expansions of the coefficients (with respect to Y and Z_i) up to some precision of $\Phi_\mu(Y)$ and $\Psi_{\mu,i}(Y, Z_i)$. Fix $\mathbb{Q}$-algebra generators of $\mathcal{M}_{K_0}(\mathbb{Q})$ to be $\gamma_1, \ldots, \gamma_s \in \mathcal{M}_{K_0}(\mathbb{Z})$ of weights $\kappa_1, \ldots, \kappa_s$ respectively (recall from Remark 2.17 that we assumed s to be finite), and assume that we also know sufficiently many coefficients of the q-expansions of $\gamma_1, \ldots, \gamma_s$. Then for each coefficient $f \in \mathcal{M}_{K_0}(\mathbb{Z})$ of $\Phi_\mu(Y)$ or $\Psi_{\mu,i}(Y, Z_i)$ it is just linear algebra to determine integers $h_1, \ldots, h_s$ and rational numbers $b_{\underline{h}}$, where

$\underline{h} = (h_1, \ldots, h_s)$, such that

$$f = \sum_{\left\{\underline{h} \in (\mathbb{Z}_{\geq 0})^s : \sum_{j=1}^{s} h_j \kappa_j = k\right\}} b_{\underline{h}} \prod_{j}^{s+1} \gamma_j^{h_j}, \tag{14}$$

where k is the weight of f. To deduce the Hilbert modular polynomials G_μ and $H_{\mu,i}$ from Φ_μ and $\Psi_{\mu,i}$, we first have to scale Φ_μ and $\Psi_{\mu,i}$ so that the coefficients are in $\mathbb{Q}(\mathcal{M}_{K_0}(\mathbb{Z}))$. To do this, we construct a ring homomorphism

$$\mathcal{M}_{K_0}(\mathbb{Z}) \longrightarrow \mathbb{Q}(\mathcal{M}_{K_0}(\mathbb{Z})).$$

To this end, we define

$$d = \gcd(\{\kappa : \mathcal{M}_{K_0,\kappa} \neq \emptyset\})$$

and choose w_1 and w_2 such that $\mathcal{M}_{K_0,w_1}(\mathbb{Z}), \mathcal{M}_{K_0,w_2}(\mathbb{Z}) \neq \emptyset$ and $d = w_1 - w_2$. Then choose

$$\varphi \in \mathcal{M}_{K_0,w_2}(\mathbb{Z}) \quad \text{and} \quad \psi \in \mathcal{M}_{K_0,w_1}(\mathbb{Z}), \tag{15}$$

and define

$$\varphi_i = \varphi^{\kappa_i/d} \quad \text{and} \quad \psi_i = \psi^{\kappa_i/d}.$$

This defines a map

$$\begin{array}{ccc} \mathcal{M}_{K_0,\kappa_i}(\mathbb{Z}) & \longrightarrow & \mathbb{Q}(\mathcal{M}_{K_0}(\mathbb{Z})) \\ \gamma_i & \mapsto & \frac{\varphi_i}{\psi_i}\gamma_i \end{array}$$

which extends $\mathbb{Z}$-linearly to a map

$$\rho : \mathcal{M}_{K_0}(\mathbb{Z}) \longrightarrow \mathbb{Q}(\mathcal{M}_{K_0}(\mathbb{Z})), \tag{16}$$

which is in fact a ring homomorphism. In Algorithm 5.8, we will assume that the representations of $\rho(\gamma_1), \ldots, \rho(\gamma_s)$ as rational functions in $J_1, \ldots, J_d$ are known.

Example 5.6. Müller [Mue85] defined four elements $(\gamma_1, \gamma_2, \gamma_3, \gamma_4) = (g_2, s_5, g_6, s_{15})$ of $\mathcal{M}_{\mathbb{Q}(\sqrt{5})}(\mathbb{Z})$ of weights 2, 5, 6, and 15 respectively that generate $\mathcal{M}_{\mathbb{Q}(\sqrt{5})}(\mathbb{Q})$ as a $\mathbb{Q}$-algebra and defined modular functions

$$(J_1, J_2, J_3) = \left(\frac{g_2^5}{s_5^2}, \frac{s_6}{g_2^3}, \frac{s_5^3}{s_{15}}\right), \tag{17}$$

such that $\mathbb{Q}(\mathcal{M}_{K_0}(\mathbb{Z})) = \mathbb{Q}(J_1, J_2, J_3)$. In this case, we get that $d = 1$, we choose $w_1 = 5$ and $w_2 = 4$, and we choose $\varphi = g_2^2$ and $\psi = s_5$. Then

$$\begin{aligned} \gamma_1 = g_2 &\mapsto \frac{g_2^5}{s_5^2} = J_1 \\ \gamma_2 = s_5 &\mapsto \frac{g_2^{10}}{s_5^4} = \left(\frac{g_2^5}{s_5^2}\right)^2 = J_1^2 \\ \gamma_3 = s_6 &\mapsto \frac{g_2^{12} s_6}{s_5^6} = \left(\frac{g_2^5}{s_5^2}\right)^3 \frac{s_6}{g_2^3} = J_1^3 J_2 \\ \gamma_4 = s_{15} &\mapsto \frac{g_2^{30} s_{15}}{s_5^{15}} = \left(\frac{g_2^5}{s_5^2}\right)^6 \frac{s_{15}}{s_5^3} = J_1^6 J_3^{-1}. \end{aligned}$$

The choice given in Equation (17) is the choice in the implementation of Algorithm 5.8 that can be found at `www.martindale.info/research`.

The following algorithm computes a set of Hilbert modular polynomials in the sense of Definition 1.5.

Lemma 5.7. Let k_i be the weight of ψ_i (the denominator of J_i). Let $\Phi_\mu(Y)$ and $\Psi_{\mu,i}(Y, Z_i)$ be as in Definition 4.2. There exist modular forms $y_0, \ldots, y_{|\mathcal{C}|} \in \mathcal{M}_{K_0}$ of weight $|\mathcal{C}|k_1$, and for $i = 2, \ldots, d$, there exist modular forms $z_{i,0}, z'_{i,0}, \ldots, z_{i,|\mathcal{C}|-1}, z'_{i,|\mathcal{C}|-1} \in \mathcal{M}_{K_0}$ of weight $(|\mathcal{C}| - 1)k_1 + k_i$ such that

$$\Phi_\mu(Y) = \sum_{n=0}^{|\mathcal{C}|} y_n Y^n$$

and

$$\Psi_{\mu,i}(Y, Z_i) = \sum_{n=0}^{|\mathcal{C}|-1} (z_{i,n} Z_i - z'_{i,n}) Y^n.$$

Proof. This follows from the explicit formulae in Definition 4.2. □

Algorithm 5.8.
INPUT: A totally real number field K_0 of degree g over $\mathbb{Q}$, the q-expansions of generators $\gamma_1, \ldots, \gamma_s$ of the $\mathbb{Q}$-algebra $\mathcal{M}_{K_0}(\mathbb{Q})$ (up to a certain precision), the images of $\gamma_1, \ldots, \gamma_s$ under ρ as rational functions of $J_1, \ldots, J_d$, and a totally positive element $\mu \in \mathcal{O}_{K_0}$ that generates a prime ideal.
OUTPUT: Polynomials

$$G_\mu(X_1, \ldots, X_d, Y) \in \mathbb{Z}[X_1, \ldots, X_d, Y]$$
$$H_{\mu,i}(X_1, \ldots, X_d, Y, Z_i) \in \mathbb{Z}[X_1, \ldots, X_d, Y, Z_i],$$

for $i = 2, \ldots, d$, satisfying the conclusions of Theorem 1.4.

1. Compute the q-expansions of the coefficients of Φ_μ and $\Psi_{\mu,i}$ up to precision P. For more details in genus 2, see Remark 6.3. For details on how to compute the required precision, see the MAGMA code, which can be found at `www.martindale.info/research`.
2. As in (14), write each coefficient of Φ_μ and $\Psi_{\mu,i}$ as elements of $\mathbb{Z}[\gamma_1, \ldots, \gamma_s]$ using linear algebra on the q-expansions (here it is necessary to have chosen the precision of the q-expansions to be sufficiently large).
3. For each i, the input contains an expression

   $$\tilde{\rho}(\gamma_i) \in \mathbb{Q}(X_1, \ldots, X_d)$$

   such that

   $$\tilde{\rho}(\gamma_i)(J_1, \ldots, J_d) = \rho(\gamma_i).$$

   Define

   $$G_\mu(X_1, \ldots, X_d, Y) \in \mathbb{Z}[X_1, \ldots, X_d, Y]$$

   to be the numerator of $\tilde{\rho}(\Phi_\mu(Y))$ and

   $$H_{\mu,i}(X_1, \ldots, X_d, Y, Z_i) \in \mathbb{Z}[X_1, \ldots, X_d, Y, Z_i]$$

   to be the numerator of $\tilde{\rho}(\Psi_{\mu,i}(Y, Z_i))$.

We have implemented a more optimised version of this in MAGMA for $K_0 = \mathbb{Q}(\sqrt{5})$ and $K_0 = \mathbb{Q}(\sqrt{2})$, see Section 6. That the output of Algorithm 5.8 is correct was in the statement of Theorem 1.4, which we now prove:

Proof of Theorem 1.4. Define $D_1 \in \mathcal{M}_{K_0}(\mathbb{Z})[Y]$ to be the denominator of $\rho(\Phi_\mu(Y))$ and

$$D_i \in \mathcal{M}_{K_0}(\mathbb{Z})[Y, Z_i]$$

to be the denominator of $\rho(\Psi_{\mu,i}(Y, Z_i))$. Let

$$S = \{[\tau] \in U \cap V : D_1(J_1(\tau)) = 0\} \cup \{[\tau] :\in U \cap V : D_i(J_1(\tau), J_i(\tau)) = 0\}.$$

Then S is a finite set, as D_1 and D_i have finitely many roots, and for any value $r \in \mathbb{C}$ and any $1 \leq i \leq d$, there are finitely many $[\tau]$ such that $J_i(\tau) = r$ as J_i extends to a holomorphic function on the compact set $\overline{V}$.

It is immediate from Proposition 4.4 that the roots of $(\Phi_\mu(Y))(\tau)$ are given by the first isomorphism invariant $J_1(\tau')$ of all the $\tau' \in K_0 \otimes \mathbb{H}$ that are μ-isogeneous to τ, up to isomorphism. If all the $J_1(\tau')$ are distinct then it also follows from Proposition 4.4 that the unique root of $(\Psi_{\mu,i}(J_1(\tau'), Z_i))(\tau)$ is $J_i(\tau')$. If they are not distinct then $(\Delta\Phi_\mu)(\tau) = 0$, so as $[\tau] \notin S$, we have that $\Delta G_\mu(J_1(\tau), \ldots, J_d(\tau), Y) = 0$. Hence, for every

$$[\tau], [\tau'] \in (U \cap V) - S \cup \{x \in (U \cap V) : \Delta G_\mu(J_1(x), \ldots, J_d(x), Y) = 0\},$$

there exists a μ-isogeny $\tau \to \tau'$ if and only if $(\Phi_\mu(J_1(\tau')))(\tau) = 0$ and for $i = 2, \ldots, d$, we have that $(\Psi_{\mu,i}(J_1(\tau'), J_i(\tau')))(\tau) = 0$. But for every

$$[\tau], [\tau'] \in (U \cap V) - S \cup \{x \in (U \cap V) : \Delta G_\mu(J_1(x), \ldots, J_d(x), Y) = 0\},$$

we have that $(\Phi_\mu(J_1(\tau')))(\tau) = 0$ if and only if

$$G_\mu(J_1(\tau), \ldots, J_d(\tau), J_1(\tau') = 0$$

and, for $i = 2, \ldots, d$, we have that $(\Psi_{\mu,i}(J_1(\tau'), J_i(\tau')))(\tau) = 0$ if and only if

$$H_{\mu,i}(J_1(\tau), \ldots, J_d(\tau), J_1(\tau'), J_i(\tau')) = 0,$$

so the theorem follows. □

6 Complexity and simplifications for genus two

We only implemented an algorithm to compute the set of Hilbert modular polynomials in genus 2, and only for small quadratic fields K_0, due to the fact that we do not know explicit q-expansions for the RM invariants $J_1, \ldots, J_d$ in any other larger genus. Hence, we restrict now to the genus 2 case, and for simplicity, we set $d = 3$.

Lemma 6.2 gives one simplification of the formulae for genus 2: in this case K_0 is quadratic, so that $\mathcal{O}_{K_0}$ and $\mathcal{O}_{K_0}^\vee$ are isomorphic as $\mathcal{O}_{K_0}$-modules. This means that we may define the Hilbert modular variety as a compactification of $\mathrm{SL}_2(\mathcal{O}_{K_0})\backslash(K_0 \otimes \mathbb{H})$ instead of $\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)\backslash(K_0 \otimes \mathbb{H})$. When we do this, in Lemma 4.9, we must replace the matrix group $\Gamma^0(\mu)$ with the matrix group $\Gamma^0(\mu)'$, which we now define.

Definition 6.1. For a totally real number field K_0 of degree 2 over $\mathbb{Q}$, with ring of integers $\mathcal{O}_{K_0}$, and a totally positive element $\mu \in K_0$, we define

$$\Gamma^0(\mu)' = \left\{ \begin{pmatrix} a & \mu b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_{K_0}) : a, b, c, d \in \mathcal{O}_{K_0} \right\}.$$

Lemma 6.2. For a totally real number field K_0 of degree 2 over $\mathbb{Q}$ with ring of integers $\mathcal{O}_{K_0}$, and a totally positive element $\mu \in \mathcal{O}_{K_0}$ that generates a prime ideal, the set

$$\mathcal{C} = \left\{ \begin{pmatrix} 1 & \omega \\ 0 & 1 \end{pmatrix} : \omega \in \mathcal{O}_{K_0}/\mu\mathcal{O}_{K_0} \right\} \bigcup \left\{ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\}$$

is a choice of coset representatives for the quotient of groups $\Gamma^0(\mu)'\backslash \mathrm{SL}_2(\mathcal{O}_{K_0})$.

Proof. The matrix group $\mathrm{SL}_2(\mathcal{O}_{K_0})$ acts on $\mathbb{P}^1(\mathcal{O}_{K_0}/\mu\mathcal{O}_{K_0})$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot (x : y) = (ax + by : cx + dy).$$

Then in particular, the stabilizer of $(0 : 1)$ is given by $\Gamma^0(\mu)'$, and hence by the orbit-stabilizer theorem, there exists a natural bijection from $\mathcal{C}$ to $\Gamma^0(\mu)'\backslash \mathrm{SL}_2(\mathcal{O}_{K_0})$. □

Remark 6.3. Using the representation of $\Gamma^0(\mu)'\backslash \mathrm{SL}_2(\mathcal{O}_{K_0})$ given in Lemma 6.2, we can write out explicit q-expansions of the coefficients of Φ_μ and $\Psi_{\mu,i}$ via the following. Let f be a modular form for $\mathrm{SL}_2(\mathcal{O}_{K_0})$ of weight k with q-expansion

$$f(\tau) = \sum_{t \in (\mathcal{O}_{K_0}^\vee)^+} \alpha(t) e^{2\pi i \mathrm{tr}(t\tau)},$$

and let $\ell = \mathrm{Norm}_{K_0/\mathbb{Q}}(\mu)$.

1. For $\omega \in \mathcal{O}_{K_0}/\mu\mathcal{O}_{K_0}$ and $M = \begin{pmatrix} 1 & \omega \\ 0 & 1 \end{pmatrix}$, we have that

$$f|_{\underline{\mu^{-1}} M\tau} = \ell^{-k/2} \sum_{t \in (\mathcal{O}_{K_0}^\vee)^+} \zeta_\ell^{\mathrm{tr}(\ell\mu^{-1}t\omega)} \alpha(t) e^{2\pi i \mathrm{tr}(\mu^{-1}t\tau)},$$

   where $(\mathcal{O}_{K_0}^\vee)^+$ denotes the totally positive elements of $\mathcal{O}_{K_0}^\vee$.

2. For $M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, we have that

$$f|_{\underline{\mu^{-1}} M\tau} = \ell^{k/2} \sum_{t \in (\mathcal{O}_{K_0}^\vee)^+} \alpha(t) e^{2\pi i \mathrm{tr}(\mu t\tau)},$$

   where $(\mathcal{O}_{K_0}^\vee)^+$ denotes the totally positive elements of $\mathcal{O}_{K_0}^\vee$.

Algorithm 5.8 is extremely slow and uses a lot of memory, and so we give here some practical improvements on the computation time and memory usage. First of all, we do not compute the third modular polynomial $H_{\mu,3}(X_1, X_2, X_3, Y, Z_3)$; Algorithm 6.4 shows that, given $(\mathrm{A}, \xi, \iota) \in \mathbf{POrd}_{\mathrm{C},K_0}$, we can compute every abelian surface μ-isogenous to it without using $H_{\mu,3}$.

Algorithm 6.4.
INPUT: The first 2 Hilbert modular polynomials $G_\mu(X_1, X_2, X_3, Y)$ and $H_{\mu,2}(X_1, X_2, X_3, Y, Z_2)$, as defined in Definition 1.5, the RM isomorphism invariants $(j_1, j_2, j_3) \in \mathbb{C}^3$ of some $(\mathrm{A}, \xi, \iota) \in \mathbf{POrd}_{\mathbb{C},K_0}$, as defined in Definition 1.1, and the minimal polynomial $m(X) \in \mathbb{Q}(J_1, J_2)[X]$ of J_3, as in Section 5.
OUTPUT: The RM isomorphism invariants of each $(\mathrm{A}', \xi', \iota') \in \mathbf{POrd}_{\mathbb{C},K_0}$ that is μ-isogenous to (A, ξ, ι), or failure.

1. Set L to be the list of the $\mathrm{Norm}_{K_0/\mathbb{Q}}(\mu)+1$ roots of $G_\mu(j_1, j_2, j_3, Y)$. If the roots are not distinct, output failure.
2. For every $j_1' \in L$:
   (a) set j_2' to be the unique element of $\mathbb{C}$ for which $H_{\mu,2}(j_1, j_2, j_3, j_1', j_2') = 0$,
   (b) set L_0 to be the list of the roots of $m(X)$ evaluated at $(J_1, J_2) = (j_1', j_2')$.
   (c) for every $l \in L_0$, check if $G_\mu(j_1', j_2', l, j_1) = 0$. If true for exactly one l, set $j_3' = l$. Else, output failure.
   (d) add (j_1', j_2', j_3') to list L'.
3. Return L'.

The second major improvement is to do computations in finite fields in place of in $\mathbb{Q}$ and $\mathbb{Q}(\zeta_{\mathrm{Norm}_{K_0/\mathbb{Q}}(\mu)})$ and then use the Chinese Remainder Theorem.

One advantage of working over a finite field in place of $\mathbb{Q}$ is that while the algorithm is running over $\mathbb{Q}$, the coefficients of the q-expansions blow up, using up memory space and slowing down computations, so that Algorithm 6.5 is significantly faster than Algorithm 5.8.

Algorithm 6.5.
INPUT:

1. A totally real number field K_0 of degree 2 over $\mathbb{Q}$.
2. The q-expansions of generators $\gamma_1, \ldots, \gamma_s \in \mathcal{M}_{K_0}(\mathbb{Z})$ of the $\mathbb{Q}$-algebra $\mathcal{M}_{K_0}(\mathbb{Q})$.
3. The images of $\gamma_1, \ldots, \gamma_s$ under ρ as rational functions of J_1, J_2, J_3, where ρ is as defined in (16).
4. A totally positive element $\mu \in K_0$ that generates a prime ideal.
5. An upper bound B on the absolute values and a common denominator D of the rational coefficients of the coefficients of $\Phi_\mu(Y)$ and $\Psi_{\mu,2}(Y, Z_2)$ when represented as formal polynomials $\gamma_1, \ldots, \gamma_s$.
6. A prime p_0 such that for every prime $p \geq p_0$, the q-expansion coefficients in Step 1 of Algorithm 5.8 have denominator coprime to p, and when replacing $\mathbb{Q}$ and $\mathbb{Q}(\zeta_\ell)$ by $\mathbb{F}_p$ and $\mathbb{F}_p(\zeta_\ell)$, the system of linear equations in Step 2 of Algorithm 5.8 still has a unique solution.

OUTPUT: The first 2 polynomials

$$G_\mu(X_1, X_2, X_3, Y) \in \mathbb{Z}[X_1, X_2, X_3, Y], \text{ and}$$
$$H_{\mu,2}(X_1, X_2, X_3, Y, Z_2) \in \mathbb{Z}[X_1, X_2, X_3, Y, Z_2]$$

of Definition 1.5.

1. Create a list L of primes in the following way:
   (a) Set $i = 0$.
   (b) Set $b = p_i$.
   (c) Set $p_{i+1} = \min\{n \in \mathbb{Z}_{>b} : n \text{ prime}, n \equiv 1 \bmod \mathrm{Norm}_{K_0/\mathbb{Q}}(\mu)\}$. (This condition is to speed up the computations as the $\mathrm{Norm}_{K_0/\mathbb{Q}}(\mu)^{\text{th}}$ roots of unity are then in $\mathbb{F}_p$.)
   (d) Reduce the coefficients of the q-expansions of $\gamma_1, \ldots, \gamma_s$ mod p_{i+1} to get
   $$\overline{\gamma_1}, \ldots, \overline{\gamma_s} \in \mathcal{M}_{K_0}(\mathbb{Z})/p_{i+1}\mathcal{M}_{K_0}(\mathbb{Z}).$$
   If $\overline{\gamma_1}, \ldots, \overline{\gamma_s}$ generate $\mathcal{M}_{K_0}(\mathbb{Z})/p_{i+1}\mathcal{M}_{K_0}(\mathbb{Z})$ as a $\mathbb{F}_{p_{i+1}}$-algebra, go to step (e). Else, set $b = p_{i+1}$ and go to step (c).
   (e) If $\prod_{j=1}^{i+1} p_j < 2BD$ then set $i = i + 1$ and go to (b). Else return
   $$L = \{p_1, \ldots, p_{i+1}\}.$$
2. Write the coefficients mod p of $\Phi_\mu(Y)$ and $\Psi_{\mu,2}(Y)$ as formal polynomials in $\gamma_1, \ldots, \gamma_s$ for every $p \in L$ by following Step 1 and 2 of Algorithm 5.8, with $\mathbb{Q}$ (and $\mathbb{Q}(\zeta_{\mathrm{Norm}_{K_0/\mathbb{Q}}})$) replaced by $\mathbb{F}_p$. (This can be done in parallel.)
3. Use the Chinese Remainder Theorem to compute the coefficients of $D\Phi_\mu(Y)$ and $D\Psi_{\mu,2}(Y)$ as formal polynomials in $\gamma_1, \ldots, \gamma_s$ with integer coefficients.
4. Compute G_μ and $H_{\mu,2}$ following Step 3 of Algorithm 5.8.

Remark 6.6. Heuristically, we expect that for large primes p and most (A, ξ) and $(\mathrm{A}', \xi') \in \mathbf{POrd}_{\mathbb{F}_p, K_0}$, there exists a μ-isogeny $(\mathrm{A}, \xi) \to (\mathrm{A}', \xi')$ if and only if

$$\begin{aligned} &G_\mu(J_1(\mathrm{A}), J_2(\mathrm{A}), J_3(\mathrm{A}), J_1(\mathrm{A}')) \\ \equiv &H_{\mu,1}(J_1(\mathrm{A}), J_2(\mathrm{A}), J_3(\mathrm{A}), J_1(\mathrm{A}'), J_2(\mathrm{A}')) \\ \equiv &0 \bmod p \end{aligned}$$

and $J_3(\mathrm{A}')$ is the same as the output of Step 2 of Algorithm 6.4 (with $\mathbb{C}$ replaced by $\mathbb{F}_p$) with

$$(j_1, j_2, j_3, j_1', j_2') = (J_1(\mathrm{A}), J_2(\mathrm{A}), J_3(\mathrm{A}), J_1(\mathrm{A}'), J_2(\mathrm{A}')).$$

The disadvantage of Algorithm 6.5 is that we have to guess the input values B, D, and p_0. However, the speed up is quite significant: for $\mathrm{Norm}_{K_0/\mathbb{Q}}(\mu) = 11$, Algorithm 5.8 took 1 week and Algorithm 6.5 took 90 minutes (on the same machine). Also, we can heuristically check the output by looking at the behaviour of the polynomials, for example by attempting to run Algorithm 6.4. Even with these improvements, there is still a long way to go before this algorithm is practical for larger values of $\mathrm{Norm}_{K_0/\mathbb{Q}}(\mu)$; Table 1 gives the timings for the computations that we have done so far.

$\mathrm{Disc}(K_0)$	8	5	5	5	5	5
$\mathrm{N}_{K_0/\mathbb{Q}}(\mu)$	2	4	5	9	11	19
Time	2s	63s	90s	$\sim$ 4m	$\sim$ 90m	$\sim$ 3d

Table 1: Timings for computation of Hilbert modular polynomials

Remark 6.7. Choosing the representations of the invariants in such a way to minimise the coefficients of the Hilbert modular polynomials would give a very siginificant speed-up, especially taking into account Algorithm 6.5. We leave this for furture work.

Remark 6.8. Dudeanu, Jetchev, Robert, and Vuille [DJRV17] have presented an algorithm to compute a μ-isogeny directly from its kernel. When the isogeny class of a given $(\mathrm{A}, \xi, \iota) \in \mathbf{POrd}_{\mathbb{F}_p, K_0}$ is large enough, it should be possible to determine the coefficients of the Hilbert modular polynomial modulo p by looking at a large set of roots (found using the algorithm of [DJRV17]) and applying linear algebra. In combination with the Chinese remainder theorem, under the heuristics of Remark 6.6, this could give a more efficient algorithm to compute Hilbert modular polynomials. We leave this for future work.

7 Applications

There are many potential applications for these polynomials, some of which have already been explored. We give three of these applications below.

7.1 Point counting

One natural application is a generalisation of the Schoof-Elkies-Aktin point-counting algorithm to genus 2 curves. Schoof [Sch95] gave an algorithm to count points on elliptic curves over finite fields in polynomial time. Schoof's algorithm was improved by Atkin using factorisations of modular polynomials, and later improved further by Elkies. Although there already exists a theoretical polynomial-time algorithm to count points on genus 2 curves over finite fields due to Pila [Pil90], it is natural to study the factorisation patterns of the Hilbert modular polynomials presented in this paper to attempt to generalise Atkin's improvements to Schoof's algorithm to genus 2 curves with maximal real multiplication. This generalisation is given by Ballentine, Guillevic, Lorenzo-Garcia, Massierer, Martindale, Smith, and Top in [BGLGMMST17]; the asymptotic complexity gives an improvement on Pila's method.

7.2 Walking on isogeny graphs

Another natural application is the 'navigation' of isogeny graphs of genus 2 curves. There has been a growing interest in the isogeny graphs of elliptic curves over finite fields recently due to the development of isogeny-based cryptography [FJP14; DKS18; CLMPR18]. Every such protocol relies on the ability to compute 'neighbours' in an ℓ-isogeny graph, that is, given an elliptic curve $E/\mathbb{F}_q$, to compute all the elliptic curves that are

ℓ-isogenous to E (up to isomorphism). In the case of elliptic curves, there are many different options for doing this, such as Vélu's formulas [Vé71], or division polynomials in combination with Kohel's algorithm [Koh96, Section 2.4], or modular polynomials in combination with Kohel's algorithm. Modular polynomials are rarely the most efficient option, although for some applications they do prove to be the best choice, e.g. [BLMP18, Appendix D].

There is a case for attempting to generalise these protocols to genus 2, especially given the recent research [RSSB16] suggesting that genus 2 arithmetic can be more efficient than elliptic curve arithmetic. The protocol presented in [DKS18] should generalise to genus 2 curves with maximal real multiplication directly–given that the structure of isogeny graphs for principally polarised simple ordinary abelian surfaces with maximal real multiplication is the same as for ordinary elliptic curves defined over $\mathbb{F}_q$ [Mar18; BJW17]. In order to actually implement such a protocol, there has to be a method of navigating the isogeny graphs, that is, of computing all the surfaces that are μ-isogenous to a given surface. Dudeanu, Jetchev, Robert, and Vuille [DJRV17] have presented an algorithm to compute a μ-isogeny from its kernel as an ideal in the endomorphism ring; this can be thought of as a genus 2 analogue of Vélu's formulas. The Hilbert modular polynomials presented in this paper give another method for computing neighbours in the μ-isogeny graph. The Hilbert modular polynomial method is currently more viable for small μ with $K_0 = \mathbb{Q}(\sqrt{5})$ and large (cryptographic size) p.

7.3 Computing class polynomials

A third natural application is the generalisation of Sutherland's algorithm for computing Hilbert class polynomials [Sut11] to genus 2. A Hilbert class polynomial over a field k for a given maximal order $\mathcal{O}$ in a imaginary quadratic field is a polynomial whose roots are given by the j-invariants of all the elliptic curves over k for which the endomorphism ring is isomorphism to $\mathcal{O}$. Via these polynomials it is possible to construct an elliptic curve over $\mathbb{F}_p$ with a given number of points. Sutherland [Sut11] gives a method to compute these polynomials using modular polynomials, which should generalise in a natural way to genus 2 using the polynomials presented in this paper. We leave the details to future work.

References

[BGLGMMST17] S. Ballentine, A. Guillevic, E. Lorenzo-García, M. Massierer, C. Martindale, B. Smith, and J. Top. "Isogenies for point counting on genus two hyperelliptic curves with maximal real multiplication". In: *Algebraic Geometry for Coding Theory and Cryptography*. Vol. 9. Association for Women in Mathematics Series. Springer Int. Pub., 2017, pp. 63–94. ISBN: 978-3-319-63931-4.

[BJW17] E.H. Brooks, D. Jetchev, and B. Wesolowski. "Isogeny graphs of ordinary abelian varieties". In: *Research in Number Theory* 3 (2017). ISSN: 2363-9555.

[BLMP18] D. Bernstein, T. Lange, C. Martindale, and L. Panny. *Quantum circuits for the CSIDH: optimizing quantum evaluation of isogenies*. (upcoming). 2018.

[CLMPR18] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes. *CSIDH: An Efficient Post-Quantum Commutative Group Action*. IACR Cryptology ePrint Archive 2018/383. 2018. URL: `https://ia.cr/2018/383`.

[DJRV17] A. Dudeanu, D. Jetchev, D. Robert, and M. Vuille. *Cyclic Isogenies for Abelian Varieties with Real Multiplication*. 2017.

[DKS18] L. De Feo, J. Kieffer, and B. Smith. *Towards practical key exchange from ordinary isogeny graphs*. IACR Cryptology ePrint Archive 2018/485. 2018. URL: `https://ia.cr/2018/485`.

[Dup06] R. Dupont. "Moyenne Arithmético-géométrique, Suites de Borchant et Applications". PhD thesis. École Polytechnique, 2006. URL: `http://www.lix.polytechnique.fr/Labo/Regis.Dupont/these_soutenance.pdf`.

[Echidna] D. Kohel. *The Echidna Database*. URL: `https://www.i2m.univ-amu.fr/perso/david.kohel/dbs/index.html`.

[FJP14] L. De Feo, D. Jao, and J. Plût. "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies". In: *Journal of Mathematical Cryptology* 8.3 (2014). IACR Cryptology ePrint Archive 2011/506., pp. 209–247. URL: `https://ia.cr/2011/506`.

[Gee88] G. van der Geer. *Hilbert modular surfaces*. Vol. 16. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]. Springer-Verlag, Berlin, 1988, pp. x+291. ISBN: 3-540-17601-2.

[Gun63] K.-B. Gundlach. "Die Bestimmung der Funktionen zur Hilbertschen Modulgruppe des Zahlkörpers $Q(\sqrt{5})$". In: *Math. Ann.* 152 (1963), pp. 226–256. ISSN: 0025-5831.

[Har77] R. Hartshorne. *Algebraic geometry*. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977, pp. xvi+496. ISBN: 0-387-90244-9.

[Igu60] J. Igusa. "Arithmetic variety of moduli for genus two". In: *Ann. of Math. (2)* 72 (1960), pp. 612–649. ISSN: 0003-486X.

[Koh96] D. Kohel. "Endomorphism rings of elliptic curves over finite fields". PhD thesis. University of California, Berkeley, 1996, p. 117. ISBN: 978-0591-32123-4.

[LNY16] K. Lauter, M. Naehrig, and T. Yang. "Hilbert theta series and invariants of genus 2 curves". In: *J. Number Theory* 161 (2016), pp. 146–174. ISSN: 0022-314X.

[Mar18] C. Martindale. "Isogeny Graphs, Modular Polynomials, and Applications". PhD thesis. Universiteit Leiden and Université de Bordeaux, 2018. URL: `http://www.martindale.info/research/Thesis.pdf`.

[May07] S. Mayer. "Hilbert Modular Forms for the Fields $Q(\sqrt{5})$, $Q(\sqrt{13})$ and $Q(\sqrt{17})$". PhD thesis. Rheinisch-Westfälischen Technischen Hochschule Aachen, 2007. URL: `http://www.matha.rwth-aachen.de/~mayer/homepage/dissertation-S-Mayer-revised-edition.pdf`.

[Mue83] R. Mueller. "Hilbertsche Modulformen und Modulfunktionen zu $\mathbf{Q}(\sqrt{8})$". In: *Math. Ann.* 266.1 (1983), pp. 83–103. ISSN: 0025-5831.

[Mue85] R. Mueller. "Hilbertsche Modulformen und Modulfunktionen zu $\mathbf{Q}(\sqrt{5})$". In: *Arch. Math. (Basel)* 45.3 (1985), pp. 239–251. ISSN: 0003-889X.

[Pil90] J. Pila. “Frobenius maps of abelian varieties and finding roots of unity in finite fields”. In: *Math. Comp.* 55.192 (1990), pp. 745–763.

[Rap78] M. Rapoport. “Compactifications de l’espace de modules de Hilbert-Blumenthal”. In: *Compositio Math.* 36.3 (1978), pp. 255–335. ISSN: 0010-437X.

[RSSB16] J. Renes, P. Schwabe, B. Smith, and L. Batina. “μKummer: efficient hyperelliptic signatures and key exchange on microcontrollers.” In: Lecture Notes in Computer Science (2016). URL: `https://doi.org/10.1007/978-3-662-53140-2_15`.

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

[Sut11] A.V. Sutherland. “Computing Hilbert class polynomials with the Chinese remainder theorem”. In: *Math. Comp.* 80.273 (2011), pp. 501–538. ISSN: 0025-5718.

[Sut18] A. Sutherland. *Modular Polynomials*. Online database. 2018. URL: `https://math.mit.edu/~drew/~ClassicalModPolys.html`.

[Vé71] J. Vélu. “Isogénies entre courbes elliptiques”. In: *Comptes Rendus de l’Académie des Sciences de Paris* 273 (1971), pp. 238–241.