CONSTRUCTING GENUS 3 HYPERELLIPTIC JACOBIANS WITH CM

JENNIFER S. BALAKRISHNAN, SORINA IONICA, KRISTIN LAUTER,
AND CHRISTELLE VINCENT

Abstract. Given a CM sextic field K, we give an explicit method for finding and constructing all genus 3 hyperelliptic curves defined over number fields whose Jacobians have complex multiplication by the maximal order of this field. Our algorithm works in complete generality, for any CM sextic field K, and for any period matrix for the Jacobian.

1. Introduction

We consider the problem of constructing genus 3 hyperelliptic curves defined over number fields with the property that their Jacobians are simple and admit complex multiplication (CM) by the maximal order of a sextic field. The interest in this question stems from the situation in genera 1 and 2, where the construction of curves over a finite field that have CM by a given field can be done by first computing curves defined over number fields that have CM by the field of interest and then reducing these curves modulo a prime ideal, under some hypotheses that guarantee that the endomorphism ring does not become larger.

In genus 3, however, the situation is more interesting. Up to isomorphism over $\mathbb{C}$, every simple principally polarized abelian variety (ppav) of dimension 3 is the Jacobian of a complete smooth projective curve of genus 3. Furthermore, if X is such a curve, then by Riemann-Roch, X is isomorphic either to a hyperelliptic or a plane quartic curve. If A is a simple ppav of dimension 3 that is isomorphic to the Jacobian of a hyperelliptic curve, resp. a plane quartic curve, we will call it a *hyperelliptic Jacobian*, resp. a *plane quartic Jacobian*. We note that the subspace of hyperelliptic Jacobians has codimension 1 in the moduli space of ppav of dimension 3.

If we are interested only in generating hyperelliptic curves whose Jacobians have CM, then given a sextic CM field K, we consider the set of simple ppav having CM by the maximal order $\mathcal{O}_K$ and ask some natural questions: Does this set contain hyperelliptic Jacobians? What conditions on K determine if this set contains hyperelliptic Jacobians? Do there exist fields K such that this set contains both hyperelliptic and plane quartic Jacobians?

This question is closely related to the construction and use in cryptography of genus 3 hyperelliptic Jacobians defined over finite fields, with CM by a given sextic field. Indeed, it is well known that discrete log attacks on plane quartic Jacobians are more efficient than on genus 3 hyperelliptic Jacobians [7, 5]. Consequently, evaluating the security of a genus 3 hyperelliptic Jacobian needs a good understanding of the type of Jacobians appearing in its isogeny class [18].

Our work takes steps toward answering these questions by presenting an algorithm that, given a CM sextic field K, first constructs a period matrix for each isomorphism class of simple, ppav with CM by $\mathcal{O}_K$, then verifies computationally if the abelian variety is the

2010 *Mathematics Subject Classification.* Primary 11G15; Secondary 11G30, 14H42, 14Q05.

Jacobian of a hyperelliptic curve. If this is the case, it computes a model for the hyperelliptic curve. The code we have written is available on GitHub [1].

Using this algorithm, we have carried out the computations described above for all Galois CM sextic fields K with class number 1. Some examples of the models computed can be found in §6, along with a list of such fields K that admit a hyperelliptic Jacobian. We also validate that the hyperelliptic curves we computed have CM. We conjecture that this list is complete: there are exactly four hyperelliptic curves, up to isomorphism, with CM by a Galois sextic field of class number 1. This replicates results found in the literature [25] and confirms that our algorithm works as intended.

In forthcoming work, we plan to use this algorithm to explore the case of general K. Currently the issues that prevent us from carrying out these computations have to do with precision: we need to give better precision estimates for the algorithm so that we can ensure *a priori* that our results are correct to a certain precision. To obtain these estimates, we need an algorithm that takes any period matrix Z and computes a representative in the same $\mathrm{Sp}_6(\mathbb{Z})$-equivalence class belonging to a fundamental domain suitable for convergence of the theta series. We give more details in §6.

In the body of the paper we present some background and references for our algorithm, as well as some results which were needed to carry out the computation. In particular, in Example 4.3 we present an example of a period matrix in a Γ_2-equivalence class not previously considered by Mumford [14] to make our algorithm truly applicable to any period matrix. In §4 we also verify, using Mumford's [14, 15] and Poor's work [16], that the Thomae formulae can be used to compute hyperelliptic models starting from any period matrix, without making a specific choice for the basis for homology. Although similar computations have been performed before [24, 25], we were not able to find a proof of these formulae in the literature.

This paper is organized as follows. In §2 we present the results of Weng [25], as well as quickly introduce the algorithm of Koike and Weng [12] to enumerate period matrices of abelian varieties with CM by a fixed field K, with more details presented in Appendix A. In §3, we introduce a set of maps denoted Ξ_g, first defined by Poor [16], and show how to attach such a map to a hyperelliptic Jacobian. In §4, we introduce theta functions, the Vanishing Criterion and a formula to compute the model of a hyperelliptic curve given the period matrix of its Jacobian. In §5 we give, and provide justification for, our algorithm to compute the map η attached to a hyperelliptic Jacobian. Finally in §6 we present our complete algorithm, as well as selected examples of the curves we have computed.

2. Preliminaries

2.1. **Previously completed computations and general observations.** This work considers natural questions in the geometry of genus 3 curves, some of which have been previously considered in the literature. Most notably, in 2001, Weng [25] carried out computations identical to those presented here. She showed that if A is a simple ppav of dimension 3 having CM by the maximal order of a sextic field K such that $\mathbb{Q}(i) \subset K$, then A is the Jacobian of a hyperelliptic curve. Restricting to sextic fields K satisfying this hypothesis, she computed models for several hyperelliptic curves of genus 3 with CM by K. In particular, she exhibited 3 hyperelliptic curves with CM whose model is defined over $\mathbb{Q}$. Unfortunately, Weng's implementation is not publicly available, so we began our investigations anew.

The example of $K = \mathbb{Q}(\zeta_7)$ is classical: One can compute that there is a single isomorphism class of simple ppav with CM by the full ring of integers of $\mathbb{Q}(\zeta_7)$. This abelian variety is a hyperelliptic Jacobian, and a model for the hyperelliptic curve is given in [11].

It is of interest to lift the hypothesis that K contain complex roots of unity, with the aim of determining experimentally if this is a necessary condition for K to admit a hyperelliptic Jacobian. So far we have been unable to find such a counterexample. We have also not yet found any examples of a field K admitting both a hyperelliptic and a plane quartic Jacobian. These explorations will be the subject of further work.

2.2. **Computing period matrices.** Given a CM field K, to compute ppav with CM by the full ring of integers of K, we rely on the CM theory of Shimura and Taniyama [17]. In genus 3, an explicit construction was presented by Koike and Weng [12]. We use their algorithm and present here a single result needed to complete our work, as well as the most basic facts needed to put this result in context. For further details, we refer the reader to Lang [13] or Birkenhake and Lange [2].

We will use the term *period matrix* to refer to an element $Z \in \mathcal{H}_g$, where

$$\mathcal{H}_g = \{M \in M_{g\times g}(\mathbb{C}) : M^T = M, \mathrm{Im}(M) > 0\}. \tag{1}$$

To such a period matrix we can associate a lattice L_Z generated by the columns of the matrix $(1_g, Z)$, where 1_g is the $g \times g$ identity matrix.

This lattice gives rise to an abelian variety A whose underlying torus is isomorphic to $\mathbb{C}^g/L_Z$. In this paper, we focus on the case where $\mathrm{End}(A) = \mathcal{O}_K$, for $\mathcal{O}_K$ the ring of integers of a CM field K of degree $2g$. We will say that such an A has *CM by* K, and by this we will always mean that the endomorphism ring of A is the full ring of integers $\mathcal{O}_K$.

To each abelian variety of dimension g defined over $\mathbb{C}$ with CM by K is attached a g-tuple of complex embeddings of K, no two of which are complex conjugates, called the variety's *CM type*. Conversely, when constructing such an abelian variety, we must first choose a CM type. An abelian variety over $\mathbb{C}$ with CM by the ring of integers $\mathcal{O}_K \subset K$ is given by $A = \mathbb{C}^g/\Phi(\mathfrak{a})$, where $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$ and Φ is a CM type. This variety is said to be of CM type (K, Φ).

We are interested only in constructing *simple* abelian varieties, a property which is completely controlled by the choice of CM type. Indeed, fix (K, Φ) a CM type and let L be the Galois closure of K over $\mathbb{Q}$. Throughout, let G be the Galois group $\mathrm{Gal}(L/\mathbb{Q})$, and set $H = \mathrm{Gal}(L/K)$. Define the sets

$$S = \{\sigma \in G : \sigma|_K = \phi_i, \text{ for one of } i = 1, \ldots, g\}, \quad \text{and} \quad H' = \{\gamma \in G : \gamma S = S\}.$$

A CM type (K, Φ) is called *primitive* (or *simple* in Lang [13]) if $H = H'$. It can be shown that an abelian variety of CM type (K, Φ) is simple if and only if its CM type is primitive. Since we are interested in constructing complex ppav that are simple, we will restrict our attention to primitive CM types. Two CM types Φ_1 and Φ_2 are said to be *equivalent* if there is an automorphism σ of K such that $\Phi_1 = \Phi_2\sigma$. We have the following result:

Proposition 2.1 (Streng [21, Lemmata I.5.4 and I.5.6])**.** *Let A_1 and A_2 be abelian varieties over $\mathbb{C}$ with CM types Φ_1 and Φ_2, where Φ_1 and Φ_2 are primitive CM types for a common CM field K. If A_1 and A_2 are isomorphic, then the two CM types are equivalent. Moreover, if two CM types Φ_1 and Φ_2 are equivalent, then the set of isomorphism classes of ppav with CM type Φ_1 coincides with the set of isomorphism classes of ppav with CM type Φ_2.*

Since we are interested in enumerating abelian varieties with CM by a certain field up to isomorphism, it suffices to consider only one CM type from each equivalence class of equivalent CM types. In our case of interest, $g = 3$ and K is a sextic CM field. There are thus four possible isomorphism classes of Galois groups G of the Galois closure L of K over $\mathbb{Q}$: $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times S_3$, $(\mathbb{Z}/2\mathbb{Z})^3 \rtimes \mathbb{Z}/3\mathbb{Z}$ or $(\mathbb{Z}/2\mathbb{Z})^3 \rtimes S_3$. (Note that Weng [25] has a typo in the orientation of the symbol $\rtimes$.) Weng determines primitive CM types for each isomorphism class of G, and with this it is straightforward to determine the equivalence classes of equivalent CM types:

Proposition 2.2. *Let K be a CM sextic field.*

(1) *If $G \cong \mathbb{Z}/6\mathbb{Z}$, K has six primitive CM types, and they are all equivalent.*
(2) *If $G \cong \mathbb{Z}/2\mathbb{Z} \times S_3$, K has six primitive CM types, and three equivalence classes of equivalent primitive CM types.*
(3) *If $G \cong (\mathbb{Z}/2\mathbb{Z})^3 \rtimes \mathbb{Z}/3\mathbb{Z}$ or $G \cong (\mathbb{Z}/2\mathbb{Z})^3 \rtimes S_3$, K has eight primitive CM types, and four equivalence classes of equivalent primitive CM types.*

Proof. In any case, K has $2^3 = 8$ CM types. For each case, the number and characterization of primitive CM types follow from Weng's work [25, Lemma 3.1]. In part 1, the fact that all primitive CM types are equivalent follows again from Weng [25, Theorem 3.5]. For the other parts, we use the fact that $\mathrm{Aut}(K)$ contains only the identity and complex multiplication. Therefore, a primitive CM type is only equivalent to its complex conjugate. □

With these results giving us a complete list of equivalence classes of equivalent primitive CM types for a given field K, we can apply Koike and Weng's [12] algorithm to enumerate data for all isomorphism classes of simple ppav with CM by K. We briefly recall this method in Algorithm 2, presented in Appendix A, and refer the reader to [12] for full details.

3. The map η attached to a hyperelliptic period matrix

Given a hyperelliptic period matrix Z, Mumford [14] constructs a certain map η. This map is crucial to the understanding of hyperelliptic Jacobians: First, its values control the vanishing of certain theta functions in such a way that the hyperelliptic Jacobians can be characterized by this vanishing property. Secondly, knowledge of a map η attached to a period matrix allows one to recover a model for the hyperelliptic curve. These two phenomena are explained in §4. Here we begin by describing the set of such maps η that arise from hyperelliptic Jacobians and showing how to construct these maps given a hyperelliptic period matrix.

Throughout this section, we will take the convention that if $x \in \mathbb{C}^{2g}$, then $x = (x_1, x_2)$, with $x_i \in \mathbb{C}^g$; in other words x_1 will denote the vector of the first g entries of x, and x_2 will denote the vector of the last g entries of x. For a vector x, we will write x^T for the transpose, and whenever matrix multiplication is involved, x is taken to be a column vector.

3.1. **Eta maps.** Throughout, we let $B = \{1, 2, \ldots, 2g+1, \infty\}$. For any two subsets $S_1, S_2 \subset B$, we define

$$S_1 \circ S_2 = (S_1 \cup S_2) - (S_1 \cap S_2),$$

the symmetric difference of the two sets. For $S \subset B$ we also define $S^c = B - S$, the complement of S in B. Then we have that the set

$$\{S \subset B : \#S \equiv 0 \pmod 2\}/\{S \sim S^c\}$$

is a commutative group under the operation $\circ$, of order 2^{2g}, with identity $\emptyset \sim B$. Since $S \circ S = \emptyset$ for all $S \subset B$, this is a group of exponent 2. Therefore this group, which we denote G_B, is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{2g}$.

We also need some functions on elements of $(1/2)\mathbb{Z}^{2g}$. Given $\xi \in (1/2)\mathbb{Z}^{2g}$, we continue to write $\xi = (\xi_1, \xi_2)$, as explained at the beginning of this section.

Definition 3.1. *For $\xi \in (1/2)\mathbb{Z}^{2g}$, let $e_*(\xi) = \exp(4\pi i \xi_1^T \xi_2)$.*

Definition 3.2. *For $\xi, \zeta \in (1/2)\mathbb{Z}^{2g}$, let $e_2(\xi, \zeta) = \exp(4\pi \xi^T J \zeta)$, with $J = \begin{pmatrix} 0 & 1_g \\ -1_g & 0 \end{pmatrix}$.*

We note that these two functions are related by the following formula: For $\xi_i \in (1/2)\mathbb{Z}^{2g}$,

$$e_*\left(\sum_{i=1}^{k} \xi_i\right) = \prod_{i<j} e_2(\xi_i, \xi_j) \prod_{i=1}^{k} e_*(\xi_i).$$

We are now ready to define the set of maps of interest.

Definition 3.3. *Following Poor [16], we define the set Ξ_g to contain the maps $\eta\colon P(B) \to (1/2)\mathbb{Z}^{2g}$, where $P(B)$ is the power set of B, satisfying the following properties:*

1. *$\eta(\{\infty\}) = 0$.*
2. *For all $S \subset B$, $\eta(S) = \sum_{i \in S} \eta(\{i\})$.*
3. *$\eta\colon G_B \cong (1/2)\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$ is a group isomorphism.*
4. *For all sets S_1 and S_2 such that $\#S_1, \#S_2 \equiv 0 \pmod 2$, $e_2(\eta(S_1), \eta(S_2)) = (-1)^{\#(S_1 \cap S_2)}$.*
5. *There is $U_\eta \subset B$ such that $\#U_\eta \equiv g+1 \pmod 4$ and for all S such that $\#S \equiv 0 \pmod 2$, we have $e_*(\eta(S)) = (-1)^{(g+1-\#(S \circ U_\eta))/2}$.*

Remark. As noted in the proof of Lemma 1.4.13 of [16], the set U_η is none other than $\{i \in B - \{\infty\} : e_*(\eta(\{i\})) = -1\} \cup \{\infty\}$.

For ease of notation, for any map $\eta \in \Xi_g$, we will henceforth denote

$$\eta_1 = \eta(\{1\}), \ldots, \eta_{2g+1} = \eta(\{2g+1\}),$$

and for any set $S \subset B$, we write $\eta_S = \eta(S)$.

Definition 3.4. *Two maps η and θ in Ξ_g are said to be in the same* class *if they are equal as maps into $(1/2)\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$.*

Because of property (2) in Definition 3.3, any map $\eta \in \Xi_g$ is determined by its values $\eta_1, \ldots \eta_{2g+1}$. We have the following converse:

Proposition 3.5. *Any ordered tuple (α_i) of $2g+1$ vectors in $(1/2)\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$ gives rise to a class of maps $\eta \in \Xi_g$ via $\eta_i \equiv \alpha_i \pmod{\mathbb{Z}^{2g}}$ and property (2) if it satisfies the following conditions:*

1. *The α_i's span $(1/2)\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$ as an $\mathbb{F}_2$ vector space.*
2. *$\sum_{i=1}^{2g+1} \alpha_i = 0$.*
3. *$e_2(\alpha_i, \alpha_j) = -1$ for each pair $i \neq j$.*

In fact, there is a bijection between the set of such tuples (α_i) and the classes of maps in Ξ_g.

We note that an ordered tuple satisfying these three conditions is commonly called an *asygetic basis* in the literature. We will avoid this technical term and simply speak of the values $\eta_1, \ldots \eta_{2g+1}$ of a given class of maps η, where η is understood to be any representative of the class, and the entries of the values η_i have all been reduced modulo $\mathbb{Z}$.

3.2. **Associating a map η to a hyperelliptic period matrix.** In this section, let X be a smooth complete hyperelliptic curve of genus g defined over $\mathbb{C}$. As explained in the literature, for example [2], a choice of period matrix $Z \in \mathcal{H}_g$ is equivalent to a choice of symplectic basis, A_i, B_i, for the homology group $H_1(X, \mathbb{Z})$ of the curve. Indeed, without any further choice, there exists a unique basis ω_i of holomorphic differentials on X such that

$$\int_{A_i} \omega_i = 1 \quad \text{and} \quad \int_{A_i} \omega_j = 0,\ i \neq j.$$

Then Z is the matrix given by $\int_{B_i} \omega_j$. Conversely, any period matrix is obtained in this manner.

Still without any further choices, we can obtain an Abel-Jacobi map

$$AJ\colon \mathrm{Jac}(X) \to \mathbb{C}^g/L_Z, \qquad \sum_{k=1}^{s} P_k - \sum_{k=1}^{s} Q_k \mapsto \left(\sum_{k=1}^{s} \int_{Q_k}^{P_k} \omega_i \right)_i,$$

which is well-defined since the value of each path integral on X is well-defined up to the value of integrating the ω_i's along the basis elements A_i, B_i, and thus up to elements of L_Z.

We can further choose to label the $2g+2$ branch points of the hyperelliptic map $\pi\colon X \to \mathbb{P}^1$, $P_1, P_2, \ldots, P_{2g+1}, P_\infty$. Given this second choice, we can give a group isomorphism (see [15, Corollary 2.11] for details) between the 2-torsion of the Jacobian of X and the group G_B in the following manner: To each set $S \subset B$ such that $\#S \equiv 0 \pmod 2$, associate the divisor class of the divisor

$$e_S = \sum_{i \in S} P_i - (\#S) P_\infty. \tag{2}$$

In turn, this isomorphism gives rise to a class of maps $\eta \in \Xi_g$ by sending $S \subset B$ to the unique vector η_S in $(1/2)\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$ such that $AJ(e_S) = (\eta_S)_2 + Z(\eta_S)_1$. Since there are $(2g+2)!$ different ways to label the $2g+2$ branch points of a hyperelliptic curve X of genus g, there are several ways to assign a class in Ξ_g to a matrix $Z \in \mathcal{H}_g$.

Definition 3.6. *We say that the class of the map $\eta \in \Xi_g$ is associated to the period matrix $Z \in \mathcal{H}_g$ if there is a labeling of the branch points of the hyperelliptic map such that for all $S \subset B$ with $\#S \equiv 0 \pmod 2$, we have $AJ(e_S) = (\eta_S)_2 + Z(\eta_S)_1$, where the Abel-Jacobi map is defined by the symplectic basis used to compute the period matrix Z.*

Example 3.7 (Mumford)**.** *In* [15, Chapter 5]*, Mumford chooses an explicit symplectic basis for homology and computes the associated class in Ξ_g. He obtains the values*

$$\tilde{\eta}_{2i-1} = \left(0 \ldots 0 \overbrace{\tfrac{1}{2}}^{i} 0 \ldots 0 \underbrace{\tfrac{1}{2}}_{g+1} \tfrac{1}{2} \ldots \tfrac{1}{2} \underbrace{0}_{g+i} 0 \ldots 0\right) \quad \textit{for } i = 1, \ldots g+1 \textit{ and}$$

$$\tilde{\eta}_{2i} = \left(0 \ldots 0 \overbrace{\tfrac{1}{2}}^{i} 0 \ldots 0 \underbrace{\tfrac{1}{2}}_{g+1} \tfrac{1}{2} \ldots \tfrac{1}{2} \underbrace{\tfrac{1}{2}}_{g+i} 0 \ldots 0\right) \quad \textit{for } i = 1, \ldots g.$$

One can show using Proposition 3.5 that this indeed gives rise to a class of maps in Ξ_g, which we denote by $\tilde{\eta}$ throughout the paper.

The set $U_{\tilde{\eta}}$ associated to this map is $\{2, 4, \dots 2g, \infty\}$. He also computes

$$\tilde{\eta}_U = \left(\frac{1}{2} \cdots \frac{1}{2} \quad \frac{g}{2} \quad \frac{g-1}{2} \cdots \frac{3}{2} \quad 1 \quad \frac{1}{2}\right).$$

Finally, there is a transitive action of the group $\mathrm{Sp}_{2g}(\mathbb{Z})$ on the set Ξ_g given by matrix multiplication on the left on the codomain of a map η where $\mathrm{Sp}_{2g}(\mathbb{Z})$ is the group of $2g \times 2g$ matrices symplectic with respect to the bilinear form $A(x, y) = x_1^T y_2 - x_2^T y_1$ and with coefficients in $\mathbb{Z}$. We also define

$$\Gamma_2 = \{\gamma \in \mathrm{Sp}_{2g}(\mathbb{Z}) : \gamma \equiv 1_{2g} \pmod 2\},$$

the principal congruence subgroup of level 2.

We have the following:

Proposition 3.8 (Igusa [10, Chapter V, Section 6])**.** *The quotient group $\mathrm{Sp}_{2g}(\mathbb{Z})/\Gamma_2$ acts freely and transitively on the classes in Ξ_g.*

Proof. Use the isomorphism $(1/2)\mathbb{Z}^{2g}/\mathbb{Z}^{2g} \cong \mathbb{F}_2^{2g}$, then $\mathrm{Sp}_{2g}(\mathbb{Z})/\Gamma_2 \cong \mathrm{Sp}_{2g}(\mathbb{F}_2)$ is exactly the group of symplectic matrices for the non-degenerate bilinear mapping given by $e(x, y) = (-1)^{x_1^T y_2 - x_2^T y_1}$ for $x, y \in \mathbb{F}_2^{2g}$. □

Thanks to this action, we need only one example of a class of maps $\eta \in \Xi_g$ to obtain a representative from each class, which is given to us by Mumford's explicit computation.

4. The Vanishing Criterion and Thomae's formulae

4.1. **Theta functions, theta characteristics, and theta constants.** For $\omega \in \mathbb{C}^g$ and $Z \in \mathcal{H}_g$, we define the following important theta series:

$$\vartheta(\omega, Z) = \sum_{n \in \mathbb{Z}^g} \exp(\pi i n^T Z n + 2\pi i n^T \omega). \tag{3}$$

Recall that given a period matrix $Z \in \mathcal{H}_g$, we denote by L_Z the lattice that is generated by the columns of the matrix $(1_g, Z)$. This gives a set of coordinates on the torus $\mathbb{C}^g/L_Z$ in the following way: A vector $x \in [0, 1]^{2g}$ gives the point $x_2 + Zx_1 \in \mathbb{C}/L_Z$, where as in the previous section x_1 denotes the first g entries and x_2 denotes the last g entries of a vector of length $2g$.

Of interest to us will be the values of $\vartheta(\omega, Z)$ at points $\omega \in \mathbb{C}^g$ that, under the natural quotient map $\mathbb{C}^g \to \mathbb{C}^g/L_Z$, map to 2-torsion points. These points are of the form $\omega = \xi_2 + Z\xi_1$ for $\xi \in (1/2)\mathbb{Z}^{2g}$. This motivates the following definition:

$$\vartheta[\xi](Z) = \exp(\pi i \xi_1^T Z \xi_1 + 2\pi i \xi_1^T \xi_2)\vartheta(\xi_2 + Z\xi_1, Z).$$

In this context, ξ is customarily called a *characteristic* or *theta characteristic*. The value $\vartheta[\xi](Z)$ is called a *theta constant*. It is the special value $\vartheta[\xi](0, Z)$ of the theta function with characteristic ξ, which is defined in [14, p. 123].

Definition 4.1. *We say that a characteristic $\xi \in (1/2)\mathbb{Z}^{2g}$ is* even *if $e_*(\xi) = 1$ and* odd *if $e_*(\xi) = -1$. If ξ is even we call $\vartheta[\xi](Z)$ an* even theta constant *and if ξ is odd we call $\vartheta[\xi](Z)$ an* odd theta constant*.*

We have the following fact about the series $\vartheta[\xi](\omega, Z)$ [14, Chapter II, Proposition 3.14]: For $\xi \in (1/2)\mathbb{Z}^{2g}$,

$$\vartheta[\xi](-\omega, Z) = e_*(\xi)\vartheta[\xi](\omega, Z).$$

From this we conclude that all odd theta constants vanish.

Finally, we will most often only be concerned about the vanishing or non-vanishing of certain values $\vartheta[\xi](Z)$ for ξ even. In this case, because of the transformation

$$\vartheta[\xi + n](Z) = \exp(2\pi i \xi_1^T n_2)\vartheta[\xi](Z),$$

we note that the vanishing depends only on the equivalence class of ξ in $(1/2)\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$.

4.2. **The Vanishing Criterion.** We are finally in a position to state the Mumford-Poor Vanishing Criterion:

Theorem 4.2 (Poor [16, Main Theorem 2.6.1])**.** *Let $Z \in \mathcal{H}_g$ and $\eta \in \Xi_g$. Then the following statements are equivalent:*

- *Z is the period matrix of a simple abelian variety and satisfies the following equations:*

(4) $\vartheta[\eta_S](Z) = 0$ *for each* $S \subset B$ *with* $\#S \equiv 0 \pmod 2$ *and* $\#(S \circ U_\eta) \neq g + 1$.

- *There is a hyperelliptic curve of genus g whose Jacobian has period matrix Z and η is one of the maps associated to Z.*

We note that the original idea behind the Vanishing Criterion is due to Mumford [15]. In Chapter 3, Corollary 6.7 of *loc. cit.*, Mumford shows that with his specific choice of symplectic basis for the homology group of the hyperelliptic curve, the period matrix obtained satisfies the vanishing criterion (4) above. In Theorem 9.1, he then presents a partial converse and states that if there is a map η whose distinguished set U_η has $g + 1$ elements such that Z satisfies the vanishing criterion (4) for the map η, then Z is a hyperelliptic period matrix.

We state Poor's result above because this Theorem 9.1 does not cover every hyperelliptic period matrix, as shown by this example:

Example 4.3. *Consider Mumford's choice of symplectic basis and his choice of labeling for the branch points of the hyperelliptic curve, exhibited at the beginning of* [15, Chapter 5]*. Act on this basis by the symplectic matrix*

$$\bar{\gamma} = \begin{pmatrix} 1 & 1 & 1 & -1 & 1 & 1 \\ 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 & 1 & 1 \\ -1 & -1 & -1 & 2 & -1 & -1 \\ 0 & 0 & -1 & 1 & -1 & -1 \\ 0 & -1 & -1 & -1 & 1 & 0 \end{pmatrix}, \tag{5}$$

without changing the labeling of the points. As computed by Poor [16]*, if $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{Sp}_{2g}(\mathbb{Z})$ acts on a symplectic basis with associated map $\tilde{\eta}$, then after the change of basis, if the branch points are not relabeled, the map associated to the new basis will be given by $\gamma^*\tilde{\eta}$, where $\gamma^* = \left(\begin{smallmatrix} A & -B \\ -C & D \end{smallmatrix}\right)$. In our particular case, after performing this action, the class of the new map*

$\bar{\eta} = \gamma^* \tilde{\eta}$ *is given by the values*

$$\bar{\eta}_1 = \left(\tfrac{1}{2} \quad 0 \quad 0 \quad \tfrac{1}{2} \quad 0 \quad 0\right), \quad \bar{\eta}_2 = \left(0 \quad 0 \quad \tfrac{1}{2} \quad \tfrac{1}{2} \quad \tfrac{1}{2} \quad \tfrac{1}{2}\right)$$
$$\bar{\eta}_3 = \left(0 \quad \tfrac{1}{2} \quad 0 \quad \tfrac{1}{2} \quad \tfrac{1}{2} \quad 0\right), \quad \bar{\eta}_4 = \left(\tfrac{1}{2} \quad 0 \quad \tfrac{1}{2} \quad 0 \quad 0 \quad \tfrac{1}{2}\right)$$
$$\bar{\eta}_5 = \left(\tfrac{1}{2} \quad \tfrac{1}{2} \quad 0 \quad 0 \quad \tfrac{1}{2} \quad \tfrac{1}{2}\right), \quad \bar{\eta}_6 = \left(0 \quad \tfrac{1}{2} \quad \tfrac{1}{2} \quad \tfrac{1}{2} \quad 0 \quad \tfrac{1}{2}\right)$$
$$\bar{\eta}_7 = \left(\tfrac{1}{2} \quad \tfrac{1}{2} \quad \tfrac{1}{2} \quad 0 \quad \tfrac{1}{2} \quad 0\right),$$

where each entry is reduced modulo $\mathbb{Z}$*. The map* $\bar{\eta}$ *given by these values has distinguished set* U *equal to all of* B*, which does not have cardinality* $g+1 = 4$*. Furthermore, we will show in Lemma 5.4 that if a period matrix is associated to* $\bar{\eta}$*, then it will only be associated to maps with* $\#U = 8$*.*

4.3. **Takase's modified formula.** Given a hyperelliptic period matrix Z and one of its associated maps η, we can construct a model for the hyperelliptic curve via Thomae's formulae. To state the formulae, we set up some notation. If Z is a period matrix satisfying the Vanishing Criterion (4) for some map $\eta \in \Xi_g$, then Z is the period matrix of a hyperelliptic Jacobian. Further, the map η comes equipped with a labeling of the branch points of the hyperelliptic map $\pi\colon X \to \mathbb{P}^1$, $P_1, \ldots, P_{2g+1}, P_\infty$. Let x be a choice of x-coordinate such that the hyperelliptic curve has a model of the form $y^2 = f(x)$, for f of degree $2g+1$, with $x(P_\infty) = \infty$. Then we write $a_i = x(P_i)$ for $i = 1, \ldots, 2g+1$, and these are all finite values in $\mathbb{C}$.

Theorem 4.4 (Thomae [15, Chapter III, Theorem 8.1])**.** *Let* Z *satisfy the Vanishing Criterion for a map* $\eta \in \Xi_g$*. Then for all sets* $S \subset B - \{\infty\}$*,* $\#S$ *even, and with notation as above, there is a constant* c *independent of* S *such that*

$$\vartheta[\eta_S](Z)^4 = \begin{cases} 0 & \text{if } \#S \circ U_\eta \neq g+1, \\ c \cdot (-1)^{(\#S \cap U)} \cdot \prod_{\substack{i \in S \circ U_\eta, \\ j \in B - S \circ U_\eta - \{\infty\}}} (a_i - a_j)^{-1} & \text{if } \#S \circ U_\eta = g+1. \end{cases}$$

Proof. We note here the slight modifications to Mumford's proof that are necessary to ensure that the proof applies to any period matrix, and not only those considered by Mumford (see the remarks immediately above Example 4.3 for more details).

The proof of Mumford's Theorem 8.1 logically relies on Proposition 6.3, which we assume here to be true about any map η, and Theorem 7.6. Theorem 7.6 in turn relies on Part 3 of Theorem 5.3 and Corollary 7.4. The proof of part 3 of Theorem 5.3 is valid, as long as δ is replaced with the vector η_U for a map η associated with the period matrix Z and η_k is as in our definitions. The argument of Corollary 7.4 relies only on the Generalized Frobenius Theta Formula (Theorem 7.1), which Mumford shows only for maps η with $\#U_\eta = g+1$, but which is shown in full generality by Poor [16, Proposition 1.6.10]. Therefore we conclude that the Thomae formulae are valid for any period matrix, since the Generalized Frobenius Theta Formula is. □

Then we have the following:

Theorem 4.5 (Takase [22])**.** *Let* Z *a period matrix and* $\eta \in \Xi_g$ *be such that the Vanishing Criterion (4) is satisfied. Then, again with notation as above, for any disjoint decomposition*

$B - \{\infty\} = V \sqcup W \sqcup \{k, l, m\}$ *with* $\#V = \#W = g - 1$, *we have*

$$\frac{a_k - a_l}{a_k - a_m} = \epsilon(k,l,m) \left(\frac{\vartheta[U \circ (V \cup \{k,l\})] \cdot \vartheta[U \circ (W \cup \{k,l\})]}{\vartheta[U \circ (V \cup \{k,m\})] \cdot \vartheta[U \circ (W \cup \{k,m\})]} \right)^2,$$

with

$$\epsilon(k,l,m) = \begin{cases} 1 & \text{if } k < l, m \text{ or } l, m < k \\ -1 & \text{if } l < k < m \text{ or } m < k < l, \end{cases}$$

and where to lighten the notation we denote $\vartheta[\eta_S](Z)$ *by* $\vartheta[S]$.

Proof. The proof follows as in [22] for any period matrix Z, once we replace Mumford's $\tilde{\eta}$ with any η associated to our period matrix Z and U with the set U_η. □

Finally, to fix a model for our hyperelliptic curve of genus 3, we require that $x(P_1) = 0$ and $x(P_2) = 1$ and compute the Rosenhain model

$$y^2 = x(x-1)(x-a_3)(x-a_4)(x-a_5)(x-a_6)(x-a_7)$$

of the curve. This allows us to compute a_i, $i = 3, \ldots, 7$ directly using the formula above, with the choice $k = 1$ and $m = 2$ for each i.

5. Computing the map η

We now show how to give a map η associated with a period matrix given only the values of the even theta constants. We note that throughout this section, we will be concerned with computing the *class* of a map η associated to Z. To apply Theorem 4.5, we then lift each value $\eta_i \pmod{\mathbb{Z}^6}$ to a value in $(1/2)\mathbb{Z}^6$ in the naive way, and then use these values to compute η_S for the other $S \subset B$ using Property 2 of Definition 3.3.

We have already remarked that with Mumford's map $\tilde{\eta}$ and the transitive action of $\mathrm{Sp}_{2g}(\mathbb{F}_2)$ on the classes of Ξ_g, we can compute a representative of each class. It would suffice then to verify if Z satisfies the Vanishing Criterion for each class of maps until we find one that works. Unfortunately, the size of the group $\mathrm{Sp}_{2g}(\mathbb{F}_2)$ grows quickly as g grows which makes this unmanageable. For this reason, in this section we provide a faster way to construct a map η attached to a period matrix for the case $g = 3$. Throughout, we will need the group $\Gamma_{1,2}$, where for Q the quadratic form $Q(x) = x_1^T x_2$,

$$\Gamma_{1,2} = \{\gamma \in \mathrm{Sp}_{2g}(\mathbb{Z}) : Q(\gamma x) \equiv Q(x) \pmod 2\}.$$

We note that the quotient $\Gamma_{1,2}/\Gamma_2$ is isomorphic to the special orthogonal group of matrices that preserve the $2g$-ary positive definite quadratic form of Arf invariant 0 over $\mathbb{F}_2$.

5.1. Characterizing hyperelliptic Jacobians when $g = 3$.

To recognize hyperelliptic Jacobians in our situation, we use the following theorem:

Theorem 5.1 (Igusa [9, Lemmata 10 and 11])**.** *When* $g = 3$, *the Vanishing Criterion (4) reduces to the following: If* Z *is the period matrix of a simple ppav of dimension* 3, *then* Z *is the period matrix of a hyperelliptic Jacobian if and only if* $\vartheta[\xi](Z)$ *vanishes for a single equivalence class* $\xi \in (1/2)\mathbb{Z}^6/\mathbb{Z}^6$ *with* $e_*(\xi) = 1$.

Proof. This is done by noticing that if Z is the period matrix of a simple ppav of dimension 3, then $\Sigma_{140}(Z) \neq 0$, so at most one even theta constant vanishes. But in this case, Z is hyperelliptic if and only if $\chi_{18}(Z)$ vanishes, which implies that at least one even theta constant vanishes. □

Definition 5.2. *Let Z be the period matrix of a simple hyperelliptic Jacobian. Then we denote by δ the unique vector in $(1/2)\mathbb{Z}^6/\mathbb{Z}^6$ such that $\vartheta[\delta](Z) = 0$ and $e_*(\delta) = 1$, and call it the* vanishing even characteristic.

Proposition 5.3. *Suppose that Z is the period matrix of a simple hyperelliptic Jacobian and $g = 3$. Then for any η associated to Z, the vanishing even characteristic of Z is η_U. Conversely, if Z has vanishing even characteristic δ and $\delta = \eta_U$ for some map η, then Z satisfies the Vanishing Criterion (4) for the map η.*

Proof. Let η be a map associated to Z, with distinguished set U_η. By part 5 of Definition 3.3, we have that $\#(U_\eta \circ U_\eta) = 0$, so that $e_*(\eta_U) = (-1)^{4/2} = 1$ and η_U is an even characteristic. We also have that $\#U_\eta = 4$ or 8 and $\#(U_\eta \circ U_\eta) \neq 4$ so $\vartheta[\eta_U](Z) = 0$ by the Vanishing Criterion. Therefore η_U is the unique vanishing even theta constant.

Now for the converse, suppose that there is a map η with $\eta_U = \delta$, where δ is the unique vanishing even characteristic of Z. Then we need to show that for any S of even cardinality such that $\#(S \circ U_\eta) \neq g + 1 = 4$, $\vartheta[\eta_S](Z) = 0$.

Because $\#(S \circ U_\eta) = \#U_\eta + \#S - 2\#(S \cap U_\eta)$, the possibilities for $\#(S \circ U_\eta)$, excluding $\#(S \circ U_\eta) = 4$, are 0, 2, 6 or 8. If $\#(S \circ U_\eta) = 2$ or 6, then $e_*(\eta_S) = (-1)^{(4-\#(U_\eta \circ S))/2} = -1$ by property 5 of Definition 3.3, and so $\vartheta[\eta_S](Z) = 0$ because it is an odd theta constant.

In the case where $\#(S \circ U_\eta) = 0$ or 8, we must have $S = U_\eta$ or $S = U_\eta^c$, respectively. In that case $\eta_S = \eta_U = \delta$ and $\vartheta[\eta_S](Z) = 0$ by assumption. □

5.2. **Computing the maps η.** There are two cases to this computation: We first consider the case where $\delta \neq 0$, and then the case where $\delta = 0$.

Lemma 5.4. *Let Z be the period matrix of a simple hyperelliptic Jacobian. Then $\vartheta[0](Z) = 0$ if and only if for every map η associated to Z, $\#U_\eta = 8$.*

Proof. For ξ even and any map η associated to Z, $\vartheta[\xi](Z) = 0$ if and only if $\xi = \eta_U$. In turn, $\eta_{S_1} = \eta_{S_2}$ if and only if $S_1 = S_2$ or $S_1 = S_2^c$, and $\eta_\emptyset = 0$. This forces $\#U_\eta = 0$ or 8, but since $\infty \in U_\eta$, $\#U_\eta = 8$. □

Remark. This shows that when the map $\bar{\eta}$ from Example 4.3 is associated to a period matrix Z, then the vanishing even characteristic of Z will be $\delta = 0$, which forces every other map η associated to Z to have $\#U_\eta = 8$.

Proposition 5.5. *Suppose that Z is irreducible and satisfies $\vartheta[\delta](Z) = 0$ for exactly one even characteristic, and $\delta \neq 0$. Then there is $\gamma \in \Gamma_{1,2}$ such that Z satisfies the Vanishing Condition for the map $\eta = \gamma\tilde{\eta}$. Furthermore, this γ can be taken to be any such that $\gamma(\frac{1}{2}\ \frac{1}{2}\ \frac{1}{2}\ \frac{1}{2}\ 0\ \frac{1}{2}) = \delta \pmod{\mathbb{Z}^6}$.*

Proof. Since Z is irreducible and has one vanishing even theta constant, Z is the period matrix of a hyperelliptic Jacobian. Therefore there are several maps in Ξ_g such that Z satisfies the Vanishing Condition for these maps. Choose any such and denote it η^*. Then the cardinality of the distinguished set U_{η^*} is 4 by Lemma 5.4.

Recall that $\eta_i^* = AJ(P_i - P_\infty)$, by equation (2). Relabel the points $\{P_1, \ldots, P_7\}$ so that if $e_*(AJ(P_i - P_\infty)) = 1$, then $i \in \{1, 3, 5, 7\}$ and if $e_*(AJ(P_i - P_\infty)) = -1$ then $i \in \{2, 4, 6\}$. This is possible because exactly three values of $i \in \{1, \ldots, 7\}$ are such that $e_*(\eta_i^*) = -1$. This relabelling gives rise to a different map η which is still associated to Z.

We now have $e_*(\eta_i) = e_*(\tilde{\eta}_i)$ for each i, and there is $\gamma \in \mathrm{Sp}_6(\mathbb{F}_2)$ with $\gamma\tilde{\eta} = \eta \pmod{\mathbb{Z}^6}$. We show that in fact $\gamma \in \Gamma_{1,2}/\Gamma_2$ by showing that for all $\xi \in (1/2)\mathbb{Z}^6/\mathbb{Z}^6$, $e_*(\gamma\xi) = e_*(\xi)$.

For any class $\eta \in \Xi_3$, the values η_i for $i = 1, \ldots 6$ form a basis of the $\mathbb{F}_2$ vector space $(1/2)\mathbb{Z}^6/\mathbb{Z}^6$. Therefore any $\xi \in (1/2)\mathbb{Z}^6/\mathbb{Z}^6$ can be written as a sum of elements in this basis, say $\xi = \sum_{k\in S} \tilde{\eta}_k$, and since $e_2(\tilde{\eta}_i, \tilde{\eta}_j) = -1$ whenever $i \neq j$,

$$e_*(\xi) = (-1)^{\binom{\#S}{2}} \prod_{k\in S} e_*(\tilde{\eta}_k).$$

On the other hand, $\gamma\xi = \gamma \sum_{k\in S} \tilde{\eta}_k = \sum_{k\in S} \gamma\tilde{\eta}_k$ and applying the same argument to the map η, we have

$$e_*(\gamma\xi) = (-1)^{\binom{\#S}{2}} \prod_{k\in S} e_*(\gamma\tilde{\eta}_k).$$

But $e_*(\gamma\tilde{\eta}_k) = e_*(\eta_k) = e_*(\tilde{\eta}_k)$ by assumption and so $e_*(\gamma\xi) = e_*(\xi)$ and $\gamma \in \Gamma_{1,2}$.

We also have

$$\eta_U = \sum_{i\in U_\eta} \eta_i = \sum_{i\in U_{\tilde{\eta}}} \gamma\tilde{\eta}_i = \gamma \sum_{i\in U_{\tilde{\eta}}} \tilde{\eta}_i = \gamma(\tfrac{1}{2}\ \tfrac{1}{2}\ \tfrac{1}{2}\ \tfrac{1}{2}\ 0\ \tfrac{1}{2}) = \delta,$$

which completes the proof. □

Proposition 5.6. *Suppose that Z is irreducible and satisfies $\vartheta[0](Z) = 0$. Then Z satisfies the Vanishing Criterion for $\bar{\eta}$ defined in Example 4.3.*

Proof. By Proposition 5.3, it suffices to show that for the map $\bar{\eta}$, $\bar{\eta}_U = 0$. This follows since $U_{\bar{\eta}} = B$, and $\sum_{i\in B} \bar{\eta}_i = 0$. □

6. Implementation, examples and results

We implemented the algorithms described here in Sage and PARI/GP; our code is available at [1]. Our search for hyperelliptic curves and their construction uses Algorithm 1.

The software implements the different steps in Algorithm 1 as follows:

- Algorithm 2 is implemented in Sage [20] and all computations are done symbolically. The running time of this step is negligible.
- The computation of theta constants is performed by a PARI/GP program. This is the most time-consuming part of the algorithm. Indeed, in order to compute a theta constant, we approximate $\theta[\xi](Z)$ by

$$S_{\xi,B} = \sum_{n\in[-B,B]^3} \exp\left(\pi i((n + \frac{1}{2}\xi_1)^T Z(n + \frac{1}{2}\xi_1) + 2(n + \frac{1}{2}\xi_1)^T(\frac{1}{2}\xi_2))\right),$$

  with $B > 0$. To ensure that our computation is correct for N bits of precision, we would need to estimate the error bound as a function of B and N. In genera 1 and 2, this was previously done by computing with period matrices in the fundamental domain (see [8, 6]). In genus 3, no method for computing matrices in the fundamental domain is known. To make sure we computed correctly with precision t, we computed

Algorithm 1 Computing the Rosenhain model

INPUT: A sextic CM field K

OUTPUT: A hyperelliptic curve with CM by K, if it exists.

1: Compute a period matrix Z using Algorithm 2.
2: Compute all even theta constants and the set T of characteristics for which the theta constants are 0.
3: **if** T has exactly one element δ **then**
4: **if** $\delta \neq 0$ **then**
5: Compute $\gamma \in \Gamma_{1,2}$ such that $\delta = \gamma(\frac{1}{2}\ \frac{1}{2}\ \frac{1}{2}\ \frac{1}{2}\ 0\ \frac{1}{2})$. This can be computed once and for all and stored for each of the 35 possible δs.
6: **else if** $\delta = 0$ **then**
7: Let $\gamma = \bar{\gamma}$ from equation 5
8: **end if**
9: Compute the Rosenhain coefficients using the formulae from Theorem 4.5, and $\eta_i = \gamma\tilde{\eta}_i$, for all $i \in \{3, \ldots, 7\}$.
10: **end if**

$S_{\xi,B}$ for several values of B until we obtained $|S_{\xi,B'} - S_{\xi,B}| < 2^{-t}$ for two consecutive values $B' > B$.

- Recognition of the modular function values – the Rosenhain coefficients a_i – as algebraic integers is done using the algebraic dependence testing algorithm [3], implemented in PARI/GP by the function `algdep`. We obtain a conjectured minimal polynomial λ_i for each coefficient a_i. Note that the amount of precision needed for this computation to end successfully depends on the dimension of the lattice fed to `algdep`, i.e. on the degree of the minimal polynomial of the Rosenhain coefficients. This degree depends on the class number of K (see [4] for details). In practice, since we only computed with sextic fields of class number one, 53 bits of precision sufficed, and the degrees of the polynomials were at most 12. However, we expect the amount of precision needed for this computation to increase dramatically once the class number of K is increased.
- In order to validate the polynomials λ_i, we compute a Weil number over a prime p which splits completely in K and construct a curve defined over $\mathbb{F}_p$ whose Jacobian has CM by $\mathcal{O}_K$. The Rosenhain coefficients of this curve are roots of the polynomials we obtained (modulo p). We check that the Jacobian of this curve has cardinality equal to $N_{K/\mathbb{Q}}(1-\pi)$, for π a prime above p.

6.1. **Galois CM sextic fields with class number 1 giving hyperelliptic curves.** There are 17 sextic CM fields K with class number 1 that are Galois over $\mathbb{Q}$. Of these, four admit a hyperelliptic Jacobian. They are as follows:

(1) $K = \mathbb{Q}(\zeta_7)$
(2) $K = \mathbb{Q}[X]/(X^6 + 5X^4 + 6X^2 + 1)$
(3) $K = \mathbb{Q}[X]/(X^6 + 6X^4 + 9X^2 + 1)$
(4) $K = \mathbb{Q}[X]/(X^6 + 13X^4 + 50X^2 + 49)$

For each of these fields, we compute that there is a single isomorphism class of ppav with CM by K. All of these examples were found by Weng [25] or, in the case of $\mathbb{Q}(\zeta_7)$, have long

been known. We conjecture that these four examples are all of the hyperelliptic curves with CM by a Galois sextic field having class number one.

Example 6.1. *Let K be field number (2) above. The tuple $(\lambda_3(x), \lambda_4(x), \lambda_5(x), \lambda_6(x), \lambda_7(x))$ of minimal polynomials for the Rosenhain coefficients is:*

$$(x^3 + 22x^2 - 16x - 8, x^3 - 4x^2 + 3x + 1, -8x^3 + 8x^2 + 2x - 1,$$
$$x^3 - 9x^2 - x + 1, x^3 + 2x^2 - x - 1).$$

For this field, Weng computed the minimal polynomials of the Shioda invariants (the class polynomials) $(h_1(x), h_2(x), h_3(x), h_4(x), h_5(x))$. These polynomials have degree one, but their coefficients are larger than those of the minimal polynomials of the Rosenhain invariants:

$$(1048576x - 2187, 131072x - 24373629, 16384x + 11632436487,$$
$$16384000000000x + 2952169653573, 2048000000000000x - 1168038669244419).$$

This serves as evidence that the minimal polynomials of the Rosenhain invariants have smaller coefficients, but higher degree than those of the Shioda invariants. This is similar to the genus 2 case, where the Rosenhain invariants were compared to the Igusa invariants [4].

Example 6.2. *Let $K = \mathbb{Q}(\zeta_7)$. We obtain the tuple of Rosenhain minimal polynomials*

$$(x^6 - 5x^5 + 11x^4 - 13x^3 + 9x^2 - 3x + 1, x^6 - 2x^5 + 4x^4 - 8x^3 + 9x^2 - 4x + 1,$$
$$x^6 - x^5 + x^4 - x^3 + x^2 - x + 1, x^6 - 3x^5 + 9x^4 - 13x^3 + 11x^2 - 5x + 1,$$
$$x^6 - 4x^5 + 9x^4 - 8x^3 + 4x^2 - 2x + 1).$$

Finally, our algorithm works for any $\mathrm{Gal}(L/\mathbb{Q})$, where L is the Galois closure of K:

Example 6.3. *Let $K = \mathbb{Q}[X]/(X^6 + 9X^4 + 18X^2 + 1)$. Then $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times S_3$. We obtain the following tuple of minimal polynomials for the Rosenhain coefficients:*

$$(x^3 - 69x^2 + 198x - 49, 8x^3 - 448x^2 - 2042x + 2401, x^3 - 43x^2 - 606x - 441,$$
$$x^3 - 169x^2 + 6479x + 2401, x^3 - 58x^2 - 96x + 72).$$

Acknowledgements

This collaboration started at the workshop Sage Days 42: Women in Sage, and we are grateful to Sarah Chisholm for her contribution toward an early version of the algorithm. We thank Léo Ducas and Enea Milio for helpful discussions. The second author thanks Microsoft Research and the University of California, San Diego for hospitality during a visit when part of this work was performed. We also thank ICERM for facilitating a productive working environment which allowed us to complete this project.

Appendix A. An algorithm for computing period matrices of abelian varieties with CM

It is well-known that all abelian varieties with CM by a given field K have complex points given by $\mathbb{C}^g/\Phi(\mathfrak{a})$, for $\mathfrak{a}$ a fractional ideal of K and Φ a CM type. To identify which ones are principally polarizable, we must verify if the lattice $\Phi(\mathfrak{a})$ admits a principal polarization. Spallek [19], based on the work of Shimura and Taniyama, shows that this is the case if and only if there is $\xi \in K$ such that $-\xi^2$ is totally positive in K_0, the totally real subfield of K

of degree g, $\mathrm{Im}(\phi_i(\xi)) > 0$ for $i = 1, \ldots, g$, and the ideal $(\mathcal{D}_{K/\mathbb{Q}}\mathfrak{a}\bar{\mathfrak{a}})^{-1}$, for $\mathcal{D}_{K/\mathbb{Q}}$ the different of K, is principal and generated by ξ.

Let U_K denote the group of units of K, let U^+ be the subgroup of totally positive units of the group of units of the totally real subfield K_0, and let be U_1 the subgroup of U^+ containing only units of the form $\epsilon\bar{\epsilon}$ for $\epsilon \in \mathcal{O}_K^\times$. Then to find a suitable ξ given an ideal $\mathfrak{a}$ such that $(\mathcal{D}_{K/\mathbb{Q}}\mathfrak{a}\bar{\mathfrak{a}})^{-1}$ is principal and a generator b of this principal ideal, it is enough to multiply b by a set of coset representatives of U_K/U^+. If we can find one such suitable ξ, all different possibilities – each giving a different principal polarization – differ from this first element by an element of the quotient U^+/U_1, by a theorem of van Wamelen [23, Theorem 5]. In their paper, Koike and Weng [12] give a procedure to compute representatives for the quotient groups U_K/U^+ and U^+/U_1, which we also use.

Algorithm 2 Generating all period matrices

INPUT: A sextic CM field K

OUTPUT: A list of tuples $(\Phi, \mathfrak{a}, \xi)$ for each isomorphism class of simple ppav with CM by K

1: Compute a representative Φ for each equivalence class of equivalent CM types of K
2: Run through the ideal class group of K and compute a representative $\mathfrak{a}$ for each ideal class such that $(\mathfrak{a}\bar{\mathfrak{a}}\mathcal{D}_{K/\mathbb{Q}})^{-1}$ is principal, and a generator b of the ideal $(\mathfrak{a}\bar{\mathfrak{a}}\mathcal{D}_{K/\mathbb{Q}})^{-1}$
3: **for** each pair (Φ, b) **do**
4: Running through representatives $\{u_1, \ldots, u_e\}$ of the finite quotient U_K/U^+, check if $u_j b$ satisfies the conditions for $\xi = u_j b$ to give a principal polarization for any j
5: **if** such a u_j can be found, write $\xi = u_j b$ **then**
6: Output the pairs $(\Phi(\mathfrak{a}), \epsilon_i\xi)$ for ϵ_i running through representatives of the finite quotient U^+/U_1. These are the data of all of the nonisomorphic ppav with underlying torus $\mathbb{C}^g/\Phi(\mathfrak{a})$
7: **else if** none is found **then**
8: There is no ppav with underlying torus $\mathbb{C}^g/\Phi(\mathfrak{a})$
9: **end if**
10: **end for**

References

[1] J. S. Balakrishnan, S. Ionica, K. Lauter, and C. Vincent, *Genus 3*, https://github.com/christellevincent/genus3, 2016.

[2] C. Birkenhake and H. Lange, *Complex abelian varieties*, second ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 302, Springer-Verlag, Berlin, 2004.

[3] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993.

[4] C. Costello, A. Deines-Schartz, K. Lauter, and T. Yang, *Constructing abelian surfaces for cryptography via Rosenhain invariants*, LMS J. Comput. Math. **17** (2014), no. suppl. A, 157–180.

[5] C. Diem, *An index calculus algorithm for plane curves of small degree*, Algorithmic Number Theory-ANTS VII, LLNCS, no. 4076, Springer, 2006.

[6] R. Dupont, *Moyenne arithmético-géométrique, suites de Borchardt et applications*, Ph.D. thesis, École Polytechnique, 2006.

[7] P. Gaudry, E. Thomé, N. Thériault, and C. Diem, *A double large prime variation for small genus hyperelliptic index calculus*, Math.Comp. **76** (2007), 475–492.

[8] E. Gottschling, *Explizite Bestimmung der Randflächen des Fundamentalbereiches der Modulgruppe zweiten Grades*, Math. Ann. **138** (1959), 103–124.
[9] J. Igusa, *Modular forms and projective invariants*, Amer. J. Math. **89** (1967), 817–855.
[10] ———, *Theta functions*, Springer-Verlag, New York-Heidelberg, 1972, Die Grundlehren der mathematischen Wissenschaften, Band 194.
[11] N. Koblitz, *Algebraic aspects of cryptography*, Algorithms and Computation in Mathematics, vol. 3, Springer-Verlag, Berlin, 1998, With an appendix by A. J. Menezes, Y.-H. Wu and R. J. Zuccherato.
[12] K. Koike and A. Weng, *Construction of CM Picard curves*, Math. Comp. **74** (2005), no. 249, 499–518.
[13] S. Lang, *Complex multiplication*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 255, Springer-Verlag, New York, 1983.
[14] D. Mumford, *Tata lectures on theta. I*, Modern Birkhäuser Classics, Birkhäuser Boston, Inc., Boston, MA, 2007, With the collaboration of C. Musili, M. Nori, E. Previato and M. Stillman, Reprint of the 1983 edition.
[15] ———, *Tata lectures on theta. II*, Modern Birkhäuser Classics, Birkhäuser Boston, Inc., Boston, MA, 2007, Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura, Reprint of the 1984 original.
[16] C. Poor, *The hyperelliptic locus*, Duke Math. J. **76** (1994), no. 3, 809–884.
[17] G. Shimura and Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publications of the Mathematical Society of Japan, vol. 6, The Mathematical Society of Japan, Tokyo, 1961.
[18] Benjamin Smith, *Isogenies and the Discrete Logarithm Problem in Jacobians of Genus 3 Hyperelliptic Curves*, Journal of Cryptology **22** (2009), no. 4, 505–529.
[19] A.-M. Spallek, *Kurven von geschelcht 2 und ihre anwendung in public key kryptosystemen*, Ph.D. thesis, Institut für Experimentelle Mathematik, Universität GH Essen, 1994.
[20] W. A. Stein et al., *Sage Mathematics Software (Version 6.10)*, The Sage Development Team, 2015, `http://www.sagemath.org`.
[21] M. Streng, *Complex multiplication of abelian surfaces*, Ph.D. thesis, Universiteit Leiden, 2010.
[22] K. Takase, *A generalization of Rosenhain's normal form for hyperelliptic curves with an application*, Proc. Japan Acad. Ser. A Math. Sci. **72** (1996), no. 7, 162–165.
[23] P. van Wamelen, *Examples of genus two CM curves defined over the rationals*, Math. Comp. **68** (1999), no. 225, 307–320.
[24] H.-J. Weber, *Hyperelliptic simple factors of $J_0(N)$ with dimension at least* 3, Experiment. Math. **6** (1997), no. 4, 273–287.
[25] A. Weng, *A class of hyperelliptic CM-curves of genus three*, J. Ramanujan Math. Soc. **16** (2001), no. 4, 339–372.

Jennifer S. Balakrishnan, Mathematical Institute, University of Oxford, Woodstock Road, Oxford OX2 6GG, UK
E-mail address: `balakrishnan@maths.ox.ac.uk`

Sorina Ionica, MIS, Université de Picardie Jules Verne, 33 Rue Saint Leu, 80000 Amiens, France
E-mail address: `sorina.ionica@m4x.org`

Kristin Lauter, Microsoft Research, 1 Microsoft Way, Redmond, WA 98062, USA
E-mail address: `klauter@microsoft.com`

Christelle Vincent, Department of Mathematics and Statistics, The University of Vermont, 16 Colchester Avenue, Burlington VT 05401, USA
E-mail address: `christelle.vincent@uvm.edu`