RIGOROUS COMPUTATION OF THE ENDOMORPHISM RING OF A JACOBIAN

EDGAR COSTA, NICOLAS MASCOT, JEROEN SIJSLING, AND JOHN VOIGHT

Abstract. We describe several improvements to algorithms for the rigorous computation of the endomorphism ring of the Jacobian of a curve defined over a number field.

Contents

1. Introduction

1.1. **Motivation.** The computation of the geometric endomorphism ring of the Jacobian of a curve defined over a number field is a fundamental question in arithmetic geometry. For curves of genus 2 over $\mathbb{Q}$, this was posed as a problem in 1996 by Poonen [Poo96, §13]. The structure of the endomorphism ring and its field of definition has important implications for the arithmetic of the curve, for example on the identification of the automorphic realization of its L-function [BSS$^+$16b].

Let F be a number field with algebraic closure F^{alg}. Let X be a nice curve over F and let J be its Jacobian. In this article, to *compute the geometric endomorphism ring* of J means to compute an abstractly presented $\mathbb{Z}$-algebra B (associative with 1 and free of finite rank as a $\mathbb{Z}$-module), equipped with an action of $\mathrm{Gal}(F^{\mathrm{alg}} \mid F)$, and a computable ring isomorphism

$$\iota\colon B \xrightarrow{\sim} \mathrm{End}(J_{F^{\mathrm{alg}}}) \tag{1.1.1}$$

that commutes with the action of $\mathrm{Gal}(F^{\mathrm{alg}} \mid F)$. (In this overview, we are agnostic about how to encode elements of $\mathrm{End}(J_{F^{\mathrm{alg}}})$ in bits; see below for a representation in terms of correspondences.) Lombardo [Lom16, §5] has shown that the geometric endomorphism ring can be computed in principle using a day-and-night algorithm—but this algorithm would be hopelessly slow in practice.

Date: May 24, 2017.

For a curve X of genus 2, there are practical methods to compute the geometric endomorphism ring developed by van Wamelen [vW99a, vW99b, vW00] for curves with complex multiplication (CM) and more recently by Kumar–Mukamel [KM16] for curves with real multiplication (RM). A common ingredient to these approaches, also described by Smith [Smi05] and in its Magma [BCP97] implementation by van Wamelen [vW06], is a computation of the *numerical endomorphism ring*, in the following way. First, we embed F into $\mathbb{C}$ and by numerical integration we compute a period matrix for X. Second, we compute putative endomorphisms of J by computing integer matrices (with small coefficients) that preserve the lattice generated by these periods, up to the computed precision. Finally, from the tangent representation of a putative endomorphism, we compute a correspondence on X whose graph is a divisor $Y \subset X \times X$; the divisor Y may then be rigorously shown to give rise to an endomorphism $\alpha \in \mathrm{End}(J_K)$ over an extension $K \supseteq F$ by exact computation. From this computation, we can also recover the multiplication law in $\mathrm{End}(J_{F^{\mathrm{alg}}})$ and its Galois action [BSS+16a, §6].

In the work of van Wamelen [vW99b] and Kumar–Mukamel [KM16], in the last step the divisor Y representing the correspondence and endomorphism is found by interpolation, as follows. Let $P_0 \in X(F^{\mathrm{alg}})$ be a Weierstrass point on X. Given a point $P \in X(F^{\mathrm{alg}})$, by inverting the Abel–Jacobi map we compute the (generically unique) pair of points $Q_1, Q_2 \in X(F^{\mathrm{alg}})$ such that

$$\alpha([P - P_0]) = [Q_1 + Q_2 - 2P_0] \in J(F^{\mathrm{alg}}) = \mathrm{Pic}^0(X)(F^{\mathrm{alg}}). \tag{1.1.2}$$

In this approach, the points Q_1, Q_2 are computed numerically, and the divisor Y is found by linear algebra by fitting $\{(P, Q_1), (P, Q_2)\} \subset Y$ for a sufficiently large sample set of points P on X.

1.2. **Contributions.** In this paper, we revisit this strategy and seek to augment its practical performance in several respects. Our methods apply to curves of arbitrary genus as well as isogenies between Jacobians, but we pay particular attention to the case of the endomorphism ring of a curve of genus 2 and restrict to this case in the introduction. We present three main ideas which can be read independently.

First, in section 3, we develop more robust numerical infrastructure by applying methods of Khuri-Makdisi [KM04] for computing in the group law of the Jacobian. Instead of directly inverting the Abel–Jacobi map at point, we divide this point by a large power of 2 to bring it close to the origin where Newton iteration converges well, then we multiply back using methods of linear series. In this way, we obtain increased stability for computing the equality (1.1.2) numerically.

Second, in section 5, we show how to dispense entirely with numerical inversion of the Abel–Jacobi map (the final interpolation step) by working infinitesimally instead. Let $P_0 \in X(K)$ be a base point on X over a finite extension $K \supseteq F$. We then calculate the equality (1.1.2) with $P = \widetilde{P}_0 \in X(K[[t]])$ the formal expansion of P_0 with respect to a uniformizer t at P_0. On an affine patch, we may think of $\widetilde{P}_0$ as the local expansion of the coordinate functions at P_0 in the parameter t. The points Q_1, Q_2 accordingly belong a ring of Puiseux series, and we can compute Q_1, Q_2 using a successive lifting procedure with exact linear algebra to sufficient precision to fit the divisor Y. For completeness (and as a good warmup), we also consider in section 4 a hybrid method, where we compute (1.1.2) for a single suitable point $P \neq P_0$ and then successively lift over a ring of power series instead. In both cases, we obtain further speedups by working over finite fields and using a fractional version of the Chinese remainder theorem. These methods work quite well in practice.

Third, in section 7 we consider upper bounds on the dimension of the endomorphism algebra as a $\mathbb{Q}$-vector space, used to match the lower bounds above and thereby sandwiching the endomorphism ring. Lombardo [Lom16, §6] has given such upper bounds in genus 2, and we introduce another ingredient in this case: we find rigorous, sharp upper bounds on dimension of the subalgebra of $\mathrm{End}(J_{F^{\mathrm{alg}}})_{\mathbb{Q}}$ fixed under the Rosati involution by examining Frobenius polynomials.

We conclude in section 8 with some examples. Confirming computations of Lombardo [Lom16, §8.2], we also verify the correctness of the endomorphism data in the *L-functions and Modular Forms DataBase* (LMFDB) [LMF16] which containins 66 158 curves of genus 2 with small minimal discriminant.

The code is available online [CMS17], and has already been used to establish the paramodularity of an abelian threefold in the context of functoriality by Cunningham–Dembélé [CD17].

Acknowledgments. The authors would like to thank Kamal Khuri-Makdisi for helpful conversations. Voight was supported by an NSF CAREER Award (DMS-1151047).

2. Setup

To begin, we set up some notation and background, and we discuss representations of endomorphisms in bits.

2.1. **Notation.** Throughout this article, let $F \subset \mathbb{C}$ be a number field with algebraic closure F^{alg}, let X be a nice—i.e., smooth, projective and geometrically integral—curve over F, let g be the genus of X, and let J be its Jacobian. When discussing algorithms, we assume that X is presented in bits by equations in affine or projective space; by contrast, we will not need to describe J as a variety defined by equations, as we will only need to describe the points of J.

2.2. **Numerical endomorphisms.** The first step in computing the endomorphism ring is to compute a numerical approximation to it. This technique is explained in detail by van Wamelen [vW06] in its Magma [BCP97] implementation for hyperelliptic curves. See also the sketch by Booker–Sijsling–Sutherland–Voight–Yasaki [BSS+16b, §6.1] where with a little more care the Galois structure on the resulting approximate endomorphism ring is also recovered.

The main ingredients of the computation of the numerical endomorphism ring are the computation of a period matrix of X—i.e., the periods of an F-basis $\omega_1, \dots, \omega_g$ of the space of global differential 1-forms on X over a chosen symplectic homology basis—followed by lattice methods. (For more detail on period computations, see the next section.) The output of this numerical algorithm is a putative $\mathbb{Z}$-basis $R_1, \dots, R_d \in \mathrm{M}_{2g}(\mathbb{Z})$ for the ring $\mathrm{End}(J_{F^{\mathrm{alg}}})$. These matrices represent the action of the corresponding endomorphisms on a chosen basis of the cohomology group $H^1(X, \mathbb{Z})$, and accordingly, the corresponding ring structure is induced by matrix multiplication. If $\Pi \in \mathrm{Mat}_{g,2g}(\mathbb{C})$ is the period matrix of J, then the equality

$$M\Pi = \Pi R \qquad (2.2.1)$$

holds, where $M \in \mathrm{M}_g(\mathbb{C})$ is the representation on the tangent space $H^0(X, \omega_X)^*$, given by right multiplication. Equation (2.2.1) allows us to convert (numerically) between the matrices $R_i \in \mathrm{M}_{2g}(\mathbb{Z})$ and matrices $M_i \in \mathrm{M}_g(\mathbb{C})$ describing the action on the tangent space, which allows us to descend to $\mathrm{M}_g(F^{\mathrm{alg}})$ and hence to $\mathrm{M}_g(K)$ for extensions of K by using Galois theory.

We take this output as being given for the purposes of this article; our goal is to certify its correctness.

Remark 2.2.2. In other places in the literature, equation (2.2.1) is transposed.

Example 2.2.3. We will follow one example throughout this paper, followed by several other examples in the last section.

Consider the genus 2 curve $X : y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1$ with LMFDB label 262144.d.524288.1. As described above, we find the period matrix

$$\Pi \approx \begin{pmatrix} 1.851 - 0.1795i & 3.111 + 2.027i & -1.517 + 0.08976i & 1.851 \\ 0.8358 - 2.866i & 0.3626 + 0.1269i & -1.727 + 1.433i & 0.8358 \end{pmatrix} \tag{2.2.4}$$

(computed to 600 digits of precision). We then verify that X has numerical quaternionic multiplication. More precisely, we have numerical evidence that endomorphism ring is a maximal order in the quaternion algebra over $\mathbb{Q}$ with discriminant 6. For example, we identify the putative endomorphism $\alpha \overset{?}{\in} \mathrm{End}(J_{\mathbb{C}})$ with representations

$$M = \begin{pmatrix} 0 & \sqrt{2} \\ \sqrt{2} & 0 \end{pmatrix} \text{ and } R = \begin{pmatrix} 0 & -3 & 0 & -1 \\ -2 & 0 & 1 & 0 \\ 0 & -4 & 0 & -2 \\ 4 & 0 & -3 & 0 \end{pmatrix} \tag{2.2.5}$$

and $\alpha^2 = 2$.

The numerical stability of the numerical method outlined above has not been analyzed. The Magma implementation will occasionally throw an error because of intervening numerical instability (see Example 3.4.8 below); this can often be resolved by slightly transforming the defining equation of X.

Remark 2.2.6. General functionality for calculating the period matrix of a specified basis of global differentials is under development by Pascal Molin and Christian Neurohr. This functionality also promises to address numerical stability.

Remark 2.2.7. For hyperelliptic curves and plane quartics it is also possibly to use the arithmetic–geometric mean (AGM) to speed up the calculation of periods. So far this has been implemented in the hyperelliptic case [Sij16]. While this delivers an enormous speedup, the AGM introduces a change of basis of differentials, which makes us lose information regarding the Galois action.

3. Complex endomorphisms

In this section, we describe a numerically stable method for inversion of the Abel–Jacobi map.

3.1. **Abel–Jacobi setup.** Let $P_0 \in X(\mathbb{C})$ be a base point and let

$$\begin{aligned} \mathrm{AJ} : X &\to J \\ P &\mapsto [P - P_0] \end{aligned} \tag{3.1.1}$$

be the Abel–Jacobi map associated to P_0. (The map AJ depends on this choice of base point P_0, but to ease formulas we do not keep it in the subscript.) Complex analytically, we may identify $J(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda$ where $\Lambda \simeq \mathbb{Z}^{2g}$ is the period lattice of J, and under this isomorphism the Abel–Jacobi map is

$$\mathrm{AJ}(P) = \left(\int_{P_0}^{P} \omega_i \right)_{i=1,\dots,g} \in \mathbb{C}^g/\Lambda. \tag{3.1.2}$$

The numerical evaluation of these integrals is standard: we compute a low degree map $\varphi : X \to \mathbb{P}^1$, make careful choices of the branch cuts of φ, and then integrate along a polygonal path that avoids the ramification points of φ.

Example 3.1.3. Suppose X is a hyperelliptic curve of genus g given by an equation of the form $y^2 = f(x)$ where $f(x)$ is squarefree of degree $2g+1$ or $2g+2$. Then an F-basis of differentials is given by

$$\omega_1 = \frac{\mathrm{d}x}{y},\ \omega_2 = x\frac{\mathrm{d}x}{y}, \dots,\ \omega_g = x^{g-1}\frac{\mathrm{d}x}{y}. \tag{3.1.4}$$

In the x-plane, we draw a polygonal path γ_x from $x(P_0)$ to $x(P)$ staying away from the roots of $f(x)$ (other than P_0, P). We then lift γ_x to a continuous path γ on X.

Suppose for simplicity that P_0 is not a Weierstrass point, so $f(x(P_0)) \neq 0$. (The case where P_0 is a Weierstrass point can similarly be handled by a choice of square root and more careful analysis.) Then $y(P_0) = \sqrt{f(x(P_0))}$ selects a branch of the square root; to keep track of the branch of the square root along γ, we make four branch cuts along the (positive and negative) real and imaginary axes. On each segment of γ, we change the branch of the square root whenever $\operatorname{Re} f$ or $\operatorname{Im} f$ changes sign, so as to keep the branch cut away from the values of $f(x)$, as in Figure 1.

In this way, the integrals $\int_{P_0}^{P} \omega_i$ can be computed, and thereby the Abel–Jacobi map.

Now let $O_0 = O_{0,1} + \dots + O_{0,g}$ be an effective ("origin") divisor of degree g; we may choose the points $O_{0,i}$ distinct. As explained by Mumford, to a general point $[D] \in J(\mathbb{C}) = \mathrm{Pic}^0(X)(\mathbb{C})$, by Riemann–Roch we can write

$$[D] = [Q_1 + \dots + Q_g - O_0] \tag{3.1.5}$$

with $Q_1, \dots, Q_g \in X(\mathbb{C})$ unique up to permutation; this defines a rational map

$$\begin{aligned} \mathrm{Mum} : J &\dashrightarrow \mathrm{Sym}^g(X) \\ [D] &\mapsto \{Q_1, \dots, Q_g\}. \end{aligned} \tag{3.1.6}$$

When $O_0 = gP_0$, the composition $\mathrm{AJ} \circ \mathrm{Mum}$ is the identity map on J, so then Mum is a right inverse to AJ. Analytically, for $b \in \mathbb{C}^g/\Lambda$, we have $\mathrm{Mum}(b) = \{Q_1, \dots, Q_g\}$ where

$$\left(\sum_{i=1}^{g} \int_{O_{0,i}}^{Q_i} \omega_i \right)_{i=1,\dots,g} \equiv b \pmod{\Lambda}. \tag{3.1.7}$$

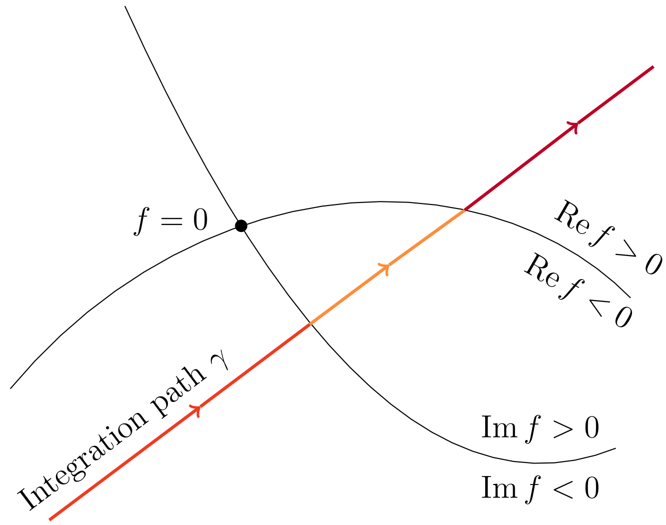

FIGURE 1. Changing the branches of $\sqrt{f(x)}$ along γ

Now let $\alpha \in \mathrm{End}(J_{\mathbb{C}})$ be a nonzero numerical endomorphism represented by the matrix $M \in \mathrm{M}_g(\mathbb{C})$ as in (2.2.1). Consider the following composed rational map

$$\alpha_X \colon\ X \xrightarrow{\mathrm{AJ}} J \xrightarrow{\alpha} J \overset{\mathrm{Mum}}{\dashrightarrow} \mathrm{Sym}^g(X)\ . \tag{3.1.8}$$

Then we have $\alpha_X(P) = \{Q_1, \ldots, Q_g\}$ if and only if

$$\alpha([P - P_0]) = [Q_1 + \cdots + Q_g - O_0]. \tag{3.1.9}$$

As mentioned in the introduction, the map α_X can be used to rigorously certify that α is an endomorphism of J by interpolation. We just saw how to compute the Abel–Jacobi map via integration, and the application of α amounts to matrix multiplication by M. So the tricky aspect is in computing the map Mum, inverting the Abel–Jacobi map. We will show in the next subsections how to accomplish this task in a more robust way than by naive inversion.

3.2. **Algorithms of Khuri-Makdisi.** Our method involves performing arithmetic in J, and for this purpose we use algorithms developed by Khuri-Makdisi [KM04]. Let $D_0 \in \mathrm{Div}(X)(\mathbb{C})$ be a divisor of degree $d_0 > 2g$ on X. By Riemann–Roch, every class in $\mathrm{Pic}^0(X)(\mathbb{C})$ is of the form $[D - D_0]$ where $D \in \mathrm{Div}(X)(\mathbb{C})$ is effective of degree d_0. We represent the class $[D - D_0]$ by the subspace

$$W_D := H^0(X, 3D_0 - D) \subseteq V := H^0(X, 3D_0). \tag{3.2.1}$$

The divisor D is not usually not unique, so the representation as a subspace of V is usually not unique. However, Khuri-Makdisi has exhibited a method [KM04, Proposition/Algorithm 4.3] that, given as input two subspaces W_{D_1} and W_{D_2} representing two classes in $\mathrm{Pic}^0(X)(\mathbb{C})$, computes as output a subspace W_{D_3} corresponding to a divisor D_3 such that $D_1 + D_2 + D_3 \sim 3D_0$ by performing linear algebra in the spaces V and $V_2 := H^0(X, 6D_0)$. In this way, we can compute explicitly with the group law in J.

Example 3.2.2. Suppose X is as in Example 3.1.3. We find a basis for V and V_2 as follows. A natural choice for D_0 is $(g+1)\infty_X$, where $\infty_X = \pi^{-1}(\infty)$ is the preimage of $\infty \in \mathbb{P}^1$ under the hyperelliptic map $x : X \to \mathbb{P}^1$. If f has even degree, then ∞_X is the sum of two distinct points; if f has odd degree, then ∞_X is twice a point. (The divisor $(g-1)\infty_X$ is a canonical divisor on X.) In either case, $\deg \infty_X = 2$ and by Riemann–Roch for $m \geq g+1$ the space $H^0(X, m\infty_X)$ has basis given by $1, x, \ldots, x^m, y, xy, \ldots, x^{m-g-1}y$.

In what follows, we represent functions in $V_2 \supsetneq V$ by their evaluation at any $N > 6d_0$ points of $X(\mathbb{C})$ disjoint from the support of D_0.

3.3. **Inverting the Abel–Jacobi map.** Let $b \in \mathbb{C}^g/\Lambda$ correspond to a divisor class $[C] \in \operatorname{Pic}^0(X)(\mathbb{C})$; for example, $b = M\,\mathrm{AJ}(P)$ for $P \in X(\mathbb{C})$ and M representing a putative endomorphism. We now explain how to compute $\mathrm{Mum}(b) = \{Q_1, \ldots, Q_g\}$ as in (3.1.7), under a genericity hypothesis.

If we start with arbitrary values for $Q_1, \ldots, Q_g$, we can adjust these points by Newton iteration until equality is satisfied to the desired precision. However, one has no guarantee about the convergence of the Newton iteration!

Step 1: Divide the point and Newton iterate. Following Mascot [Mas13, §3.5], we first replace b with a point b' very close to 0 modulo Λ and such that $2^m b' \equiv b \pmod{\Lambda}$ for some $m \in \mathbb{Z}_{\geq 0}$. For example, b' may be obtained by lifting b to $\mathbb{C}^g$ and dividing the resulting vector by 2^m.

As b' is very close to 0 modulo Λ, the equation (3.1.7) should have a solution $\{Q_i'\}_i$ with Q_i close to $O_{0,i}$ for $i = 1, \ldots, g$. Since the points $O_{0,i}$ were chosen distinct, the derivative of the Abel–Jacobi map AJ at O_0 is nonsingular. We start with $Q_i' = O_i$ as initial guesses, and then use Newton iteration until (3.1.7) holds to the desired precision. If Newton iteration does not seem to converge, we increase the value of m and start over. The probability of success of the method described above increases with m. In practice, we found that starting with $m = 10$ was a good compromise between speed and success rate.

In this way, we find points $Q_1', \ldots, Q_g'$ such that the linear equivalence

$$C \sim 2^m \left(\sum_{i=1}^{g} Q_i' - O_0 \right) \tag{3.3.1}$$

holds in $\operatorname{Div}(X)^0(\mathbb{C})$.

Step 2: Recover the divisor by applying an adaptation of the Khuri-Makdisi algorithm. From this, we want to compute $Q_1, \ldots, Q_g$ such that

$$C \sim \sum_{i=1}^{g} Q_i - O_0. \tag{3.3.2}$$

For this purpose, we work with divisors and the algorithms of the previous section. But these algorithms only deal with divisor classes of the form $[D - D_0]$ with $\deg D = d_0$ whereas we would like to work with $[\sum_{i=1}^{g} Q_i' - O_0]$. So we adapt the algorithms in the following way.

We choose $d_0 - g$ auxiliary points $P_1, \dots, P_{d_0-g} \in X(\mathbb{C})$ distinct from the points Q_i, the points $O_{0,i}$, and the support of D_0. Consider the divisors

$$\begin{aligned} D_+ &:= \sum_{i=1}^{g} Q_i + \sum_{i=1}^{d_0-g} P_i \\ D_- &:= O_0 + \sum_{i=1}^{d_0-g} P_i, \end{aligned} \tag{3.3.3}$$

both effective of degree d_0. We then compute the subspaces W_{D_+} and W_{D_-} of V, and apply the subtraction algorithm of Khuri-Makdisi: we obtain a subspace $W_{D'}$ corresponding to an effective divisor D' such that

$$D' - D_0 \sim \left(\sum_{i=1}^{g} Q'_i + \sum_{i=1}^{d_0-g} P_i \right) - \left(O_0 + \sum_{i=1}^{d_0-g} P_i \right) = \sum_{i=1}^{g} Q'_i - O_0. \tag{3.3.4}$$

We then repeatedly use the doubling algorithm to compute W_D, where D is a divisor such that $D - D_0 \sim 2^m(D' - D_0)$. We have thus computed a subspace W_D such that

$$D - D_0 \sim C \sim \sum_{i=1}^{g} Q_i - O_0. \tag{3.3.5}$$

To conclude, we recover the points $Q_1, \dots, Q_g$ from W_D in a few more steps. We proceed as in Mascot [Mas13, §3.6].

Step 3: Compute $E \sim \sum_i Q_i$. We apply the addition algorithm to W_D and W_{D_-} and negate the result. (In fact, Khuri-Makdisi's algorithm computes these two steps in one.) This results in a subspace W_Δ where Δ is an effective divisor with $\deg \Delta = d_0$ and

$$\Delta - D_0 \sim (D_0 - D) + (D_0 - D_-). \tag{3.3.6}$$

By (3.3.5), we have

$$\sum_{i=1}^{g} Q_i \sim E, \quad \text{where } E := 2D_0 - \Delta - \sum_{i=1}^{d_0-g} P_i \tag{3.3.7}$$

and $\deg(E) = g$.

Step 4: Compute $Z = H^0(X, E)$. Next, we compute

$$H^0(X, 3D_0 - \Delta) \cap H^0(X, 2D_0) \tag{3.3.8}$$

and the subspace Z of this intersection of functions that vanish at all P_i. Generically, we have

$$Z = H^0(X, E) \tag{3.3.9}$$

and since $\deg(E) = g$, by Riemann–Roch we have $\dim Z \geq 1$. The genericity assumption may fail, but we can detect its failure by comparing the (numerical) dimension of the spaces we compute with the value predicted by Riemann–Roch, and rectify its failure by restarting with different auxiliary points P_i.

Step 5: Recover the points Q_i. Now let $z \in Z$ be nonzero; then

$$\operatorname{div} z = Q - E \tag{3.3.10}$$

where Q is an effective divisor with $\deg Q = g$ and

$$Q \sim \sum_{i=1}^{g} Q_i \tag{3.3.11}$$

by (3.3.7); as we are always working up to linear equivalence, we may take $Q = \sum_{i=1}^{g} Q_i$ as desired. To compute $\operatorname{div} z$ and circumnavigate the unknown divisor Δ, we compute the subspace

$$Z' := \left\{ v \in V : vW_\Delta \subseteq zV \right\} \tag{3.3.12}$$

where $zV = H^0(X, 3D_0 - \operatorname{div} z)$ and $W_\Delta = H^0(X, 3D_0 - \Delta)$. Since $3D_0 - \Delta$ is basepoint-free (its degree exceeds $2g$), we conclude that

$$Z' = H^0\big(X, 3D_0 - \operatorname{div} z - (3D_0 - \Delta)\big) = H^0\left(X, 2D_0 - \sum_{i=1}^{d_0-g} P_i - \sum_{i=1}^{g} Q_i\right). \tag{3.3.13}$$

We then recover the divisor $\sum_i P_i + \sum_i Q_i$ as the intersection of the locus of zeros of the functions in Z', and then the points Q_i themselves whenever they are distinct from the chosen auxiliary points P_i, something that holds generically (and this genericity can similarly be verified and its failure rectified).

Example 3.3.14. In the case of a hyperelliptic curve, as in Example 3.2.2 with $D_0 = (g+1)\infty_X$, the method described above leads us to

$$T = H^0\left(X, (2g+2)\infty_X - \sum_{i=1}^{d_0-g} P_i - \sum_{i=1}^{g} Q_i\right), \tag{3.3.15}$$

which consists of functions which are linear combinations of x^n and $x^n y$ for $n \in \mathbb{Z}_{\geqslant 0}$. These linear combinations thus describe polynomial equations that the coordinates of the points P_i and Q_i must satisfy, which allows us to recover the Q_i.

Remark 3.3.16. Khuri-Makdisi's method relies only linear algebra operations in vector spaces of dimension $O(g \log g)$. As we are working numerically, we must rely upon numerical linear algebra, and in our implementation we performed most of these operations by QR decompositions, a good trade-off between speed and stability. In practice, our loss of precision was limited by at most 10 precision bits per Jacobian operation.

3.4. **Examples.** We give two examples of the above approach.

Example 3.4.1. We return to Example 2.2.3. Let $P_0 = (1, 0)$ and $P = (2, 5)$ Integrating, we find $\mathrm{AJ}([P - P_0]) \equiv b \pmod{\Lambda}$ where

$$b \approx (0.2525, 1.475) \tag{3.4.2}$$

We now apply the methods of section 3.3. The first step inverts the Abel–Jacobi map to obtain

$$2^{-10} M b = \mathrm{AJ}([Q_1' + Q_2' - O_{0,1} - O_{0,2}]) \tag{3.4.3}$$

where

$$Q'_1 \approx (0.9224 + 0.8521i,\ 1.103 - 1.909i)$$
$$Q'_2 \approx (0.3257 + 0.9592i,\ 2.146 - 0.3645i) \tag{3.4.4}$$
$$O_{0,1} \approx (0.9163 + 0.8483i,\ 1.104 - 1.884i)$$
$$O_{0,2} \approx (0.3311 + 0.9656i,\ 2.159 - 0.3835i)\,.$$

The remaining steps (adapting the algorithms of Khuri-Makdisi) compute Q_1 and Q_2 such that

$$2^{10}[Q'_1 + Q'_2 - O_{0,1} - O_{0,2}] \sim [Q_1 + Q_2 - 2P_0], \tag{3.4.5}$$

where

$$Q_i \approx (0.7500 \pm 0.4330i,\ -0.4419 \pm 0.7655i)\,. \tag{3.4.6}$$

Using the LLL algorithm [LLL82], we guess that the x-coordinates of Q_1 and Q_2 satisfy $x^2 - \frac{3}{2}x + \frac{3}{4} = 0$, and under this assumption we have

$$Q_i = \left(\frac{3 \pm i\sqrt{3}}{4}, 5\frac{-\sqrt{2} \pm i\sqrt{6})}{16}\right). \tag{3.4.7}$$

All the computations above were performed with at least 600 decimal digits.

Example 3.4.8. The MAGMAfunctions `ToAnalyticJacobian` and `FromAnalyticJacobian`, provides us similar functionality. However, we have found these algorithms to be numerically unstable. For example, for $X : y^2 = x^6 + 4x^5 + 6x^4 + 2x^3 + x^2 + 2x + 1$, a model for the modular curve $X_1(13)$, we were unable to perform

$$\texttt{FromAnalyticJacobian}\left(\begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \cdot \texttt{ToAnalyticJacobian}(P, X), X\right),$$

for a random point P. A workaround is as follows: replacing $\left(\begin{smallmatrix} 0 & i \\ -i & 0 \end{smallmatrix}\right)$ by $\left(\begin{smallmatrix} m & i \\ -i & m \end{smallmatrix}\right)$ for certain $m \in \mathbb{Z}_{>0}$ (equivalent for the purposes of rigorous certification, but at the cost of a larger degree endomorphism), the implementation works.

4. Newton lift

In the previous section, we showed how one can numerically compute the composite map

$$\alpha_X\colon\ X \xrightarrow{\text{AJ}} J \xrightarrow{\alpha} J \overset{\text{Mum}}{\dashrightarrow} \mathrm{Sym}^g(X) \tag{4.0.1}$$

given $\alpha \in \mathrm{End}(J_{\mathbb{C}})$. As explained in the introduction, by interpolation we can then fit a divisor $Y \subset X \times X$ representing the graph of the numerical endomorphism α. When this divisor is defined over a number field and the induced homomorphism on differentials as in Smith [Smi05, §3.5] is our given tangent matrix, then we have successfully verified the existence of the corresponding endomorphism. In this section—one that can be read as a warmup for the next section or as a hybrid method—we only use numerical approximation for a single point, after which we use a Newton lift to express the endomorphism in a formal neighborhood.

4.1. **Setup.** We retain the notation of the previous section. We further suppose that the base point $P_0 \in X(K)$ and origin divisor $O_0 = \sum_{i=1}^{g} O_{0,i} \in \mathrm{Div}^0(X)(K)$ are defined over a finite extension $K \supseteq F$. Enlarging K further if necessary, we choose $P \in X(K)$ distinct from P_0 and suppose (as computed in the previous section, or another way) that we are given points $Q_1, \dots, Q_g \in X(K)$ such that

$$\alpha_X(P) = \{Q_1, \dots, Q_g\}. \tag{4.1.1}$$

Moreover, possibly enlarging K again, we may assume the matrix M representing the action of α on differentials has entries in K.

For concreteness, we will exhibit the method for the case of a hyperelliptic curve; we restore generality in the next section. Suppose $X : y^2 = f(x)$ is hyperelliptic as in Example 3.1.3. Let $t := x - x(P)$; we think of t as a formal parameter. We further assume that t is a *uniformizer* at P: equivalently, $f(x(P)) \neq 0$, i.e., P is *not* a Weierstrass point. Since X is smooth at P, there exists a lift of P to a point $\widetilde{P} \in X(K[[t]])$ with

$$\begin{aligned} x(\widetilde{P}) &= x(P) + t = x \\ y(\widetilde{P}) &= y(P) + O(t). \end{aligned} \tag{4.1.2}$$

We can think of $\widetilde{P}$ as expressing the expansion of the coordinates x, y with respect to the parameter t. Indeed, we have

$$y(\widetilde{P}) = \sqrt{f(x(P) + t)} \in K[[t]] \tag{4.1.3}$$

expanded in the usual way, since $f(x(P)) \neq 0$ and the square root is specified by $y(\widetilde{P}) = y(P) + O(t)$. Alternatively, we can think of $\widetilde{P}$ as a formal neighborhood of P.

The Abel–Jacobi map, the putative endomorphism α, and the Mumford map extend to the ring $K[[t]]$. By a lifting procedure, we will compute points $\widetilde{Q}_1, \dots, \widetilde{Q}_g \in X(K[[t]])$ to arbitrary t-adic precision such that

$$\alpha_X\big(\widetilde{P}\big) = \big\{\widetilde{Q}_1, \dots, \widetilde{Q}_g\big\} \tag{4.1.4}$$

with

$$x\big(\widetilde{Q}_j\big) = x(Q_j) + O(t). \tag{4.1.5}$$

We then attempt to fit a divisor $Y \subset X \times X$ defined over K containing $\big\{(\widetilde{P}, \widetilde{Q}_j)\big\}_j$ instead of interpolation, and proceed as before.

4.2. **Lifting procedure.** For a generic choice of P, we may assume that $y(Q_j) \neq 0$ for all j and that the values $x(Q_j)$ are all distinct. In practice, we may also keep P and simply replace $\alpha \leftarrow \alpha + m$ with small $m \in \mathbb{Z}$ to achieve this.

Let $x_j(t) := x(\widetilde{Q}_j)$. The matrix $M = (m_{ij})_{i,j}$ describing the action of α on the F-basis of differentials $x^j \,\mathrm{d}x/y$ written out becomes

$$\sum_{j=1}^{g} \frac{x_j^i \,\mathrm{d}x_j}{\sqrt{f(x_j)}} = \left(\sum_{j=0}^{g-1} m_{ij} x^j\right) \frac{\mathrm{d}x}{\sqrt{f(x)}} \tag{4.2.1}$$

for all $i = 0, \dots, g-1$, where the branches of the square roots are chosen so that $\sqrt{f(x)} = y(P) + O(t)$ and that $\sqrt{f(x_j)} = y(P_j) + O(t)$ for all j. Dividing by $\mathrm{d}x = \mathrm{d}t$, (4.2.1) can be rewritten in matrix form:

$$WDx' = \frac{1}{\sqrt{f(x)}} Mw \tag{4.2.2}$$

where

$$\begin{aligned} W &:= \left(x_j^i\right)_{\substack{i=0,\ldots,g-1\\ j=1,\ldots,g}} = \begin{pmatrix} 1 & \cdots & 1 \\ x_1 & \cdots & x_g \\ \vdots & \ddots & \vdots \\ x_1^{g-1} & \cdots & x_g^{g-1} \end{pmatrix} \\ D &:= \operatorname{diag}\left(\sqrt{f(x_1)}^{-1}, \ldots, \sqrt{f(x_g)}^{-1}\right) \\ x' &:= (\mathrm{d}x_j/\mathrm{dt})_{j=1,\ldots,g}^{\mathsf{T}} = \left(\mathrm{d}x_1/\mathrm{dt}, \ldots, \mathrm{d}x_g/\mathrm{dt}\right)^{\mathsf{T}} \\ w &:= (x^j)_{j=0,\ldots,g-1}^{\mathsf{T}} = \left(1, \ldots, x^{g-1}\right)^{\mathsf{T}} \end{aligned} \tag{4.2.3}$$

where T denotes transpose. Since the values $x(Q_j) \in K$ are all distinct, the Vandermonde matrix W is invertible over $K[[t]]$. Therefore, equation (4.2.2) allows us to solve for x':

$$x' = \frac{1}{\sqrt{f(x)}} D^{-1} W^{-1} M w. \tag{4.2.4}$$

In practice, we use (4.2.4) to solve for the series $x_j(t) \in K[[t]]$ iteratively to any desired t-adic accuracy: if they are known up to precision $O(t^n)$ for some $n \in \mathbb{Z}_{\geq 1}$, we may apply the identity (4.2.4) and integrate to get the series up to $O(t^{n+1})$.

Example 4.2.5. We return to Example 3.4.1, and take $P = (2, 5)$ a non-Weierstrass point. We obtain

$$x_i(t) = \frac{1}{4}\left(3 \pm i\sqrt{3}\right) + \frac{1}{12} i \left(\sqrt{3} \pm 3i\right) t + \frac{1}{144}\left(9 \mp 11i\sqrt{3}\right) t^2 \pm \frac{5i}{36\sqrt{3}} t^3 + O\left(t^4\right), \tag{4.2.6}$$

where $t = x - 2$ is a uniformizer at P. Taking advantage of the evident symmetry of x_1, x_2, we find

$$x_1(t) + x_2(t) = \frac{4t+6}{(t+2)^2}, \quad x_1(t)x_2(t) = \frac{2t+3}{(t+2)^2} \tag{4.2.7}$$

Thus,

$$x_i(t) = \frac{2t + 3 \pm i\sqrt{(t+1)^2(2t+3)}}{(t+2)^2} \tag{4.2.8}$$

5. Puiseux lift

In the previous section, we lifted a single computation of $\alpha_X(P) = \sum_{j=1}^{g} Q_j - O_0$ to a formal neighborhood. In this section, we to dispense with even this one numerical computation to obtain an exact certification algorithm using only the matrix of a putative endomorphism.

We continue our notation but restore generality, allowing X to be again a general curve. We may for example represent X by a plane model that is smooth at P_0 (but with possible singularities elsewhere). Let $P_0 \in X(K)$ and let $M \in \mathrm{M}_g(K)$ be the tangent representation of a putative endomorphism α on an F-basis of $H^0(X, \omega_X)$.

5.1. **Setup.** We now make the additional assumption that P_0 is *not* a Weierstrass point, and we take $O_0 = gP_0$. Then by Riemann–Roch, the map

$$\begin{aligned} \operatorname{Sym}^g(X) &\to J \\ \{Q_1, \dots, Q_g\} &\mapsto \sum_{j=1}^{g} (Q_j - P_0) \end{aligned} \tag{5.1.1}$$

is locally an isomorphism.

Let $x \in F(X)$ be a local parameter for X at P_0. Since X is smooth at P_0, we obtain a canonical point $\widetilde{P}_0 \in X(F[[x]])$ such that $x(\widetilde{P}_0) = x \in F[[x]]$ lifting P_0, i.e., the image of $\widetilde{P}_0$ under the reduction map $X(F[[x]]) \to X(F)$ is equal to P_0. On an affine open set $U \ni P_0$ with U embedded into affine space over F, we may think of $\widetilde{P_0}$ as providing the local expansions of the coordinates at P_0 in the local ring at P_0.

We have

$$\alpha_X(\widetilde{P}_0) = \{\widetilde{Q}_1, \dots, \widetilde{Q}_g\} \in \operatorname{Sym}^g(X)(F[[x]]) \tag{5.1.2}$$

since (5.1.1) is locally an isomorphism at P_0. The reduction to F of $\{\widetilde{Q}_i\}_i$ is the g-fold multiple $\{P_0, \dots, P_0\} \in \operatorname{Sym}^g(X)(F)$. However, now the map $X^g \to \operatorname{Sym}^g(X)$ is ramified above $\{P_0, \dots, P_0\}$; so in general, we cannot expect to have $\widetilde{Q}_i \in X(F[[x]])$. Instead, consider the generic fiber of the point $\{\widetilde{Q}_i\}_i$, an element of $\operatorname{Sym}^g(X)(F((x)))$; this generic fiber lifts to a point of X^g defined over some finite extension of $F((x))$. Since $\operatorname{char} F = 0$, the algebraic closure of $F((x))$ is the field $F^{\mathrm{alg}}((x^{1/\infty}))$ of Puiseux series over F^{alg}. However, since X is smooth at P_0, the lift of $\{\widetilde{Q}_i\}_i$ is a point on X^g over the ring of integral Puiseux series $F^{\mathrm{alg}}[[x^{1/\infty}]]$.

In other words, if we allow ramification (fractional exponents) in our formal expansion, we can lift the trivial equality $\alpha_X(P_0) = \{P_0, \dots, P_0\}$ to a formal neighborhood.

5.2. **Lifting procedure.** The successive lifting procedure to carry out this method algorithmically is quite similar to the one of the previous section. For $i = 1, \dots, g$, let

$$\omega_i = f_i \, \mathrm{d}x \tag{5.2.1}$$

be an F-basis of $H^0(X, \omega_X)$ with $f_i \in F(X)$. The functions f_i are by definition regular at P_0, so they admit a power series expansion $f_i(x) \in F[[x]]$ in the uniformizing parameter x. Because P_0 is not a Weierstrass point, we may without loss of generality choose ω_i in row echelonized form, i.e., so that

$$\omega_i = (x^{i-1} + O(x^i)) \, \mathrm{d}x \tag{5.2.2}$$

for $i = 1, \dots, g$. (Or, if it is more convenient, we may work with a full echelonized basis.)

For $j = 1, \dots, g$, let

$$x_j = x(\widetilde{Q}_j) \in F^{\mathrm{alg}}[[x^{1/\infty}]]. \tag{5.2.3}$$

We will compute the Puiseux expansions x_j iteratively. Let $Y \subset X \times X$ be the graph of α, defined as the Zariski closure of the set

$$\{(P, Q_j) : P \in X(F^{\mathrm{alg}}),\ Q_j \in \alpha_X(P)\}. \tag{5.2.4}$$

Let π_1, π_2 be the two projection maps to X. Then on the basis ω_i, the operation $(\pi_2)_* \pi_1^*$ should induce the linear map $M = \alpha^*$. By definition, we have

$$\pi_1^{-1}(\widetilde{P}_0) = \{(\widetilde{P_0}, \widetilde{Q}_1), \dots, (\widetilde{P_0}, \widetilde{Q}_g)\}, \tag{5.2.5}$$

so if Y induces α, then on specialization the following infinitesimal equalities hold:

$$\sum_{j=1}^{g} x_j^*(\omega_i) = \alpha^*(\omega_i), \quad \text{for all } i = 1, \dots, g. \tag{5.2.6}$$

Written out, (5.2.6) becomes

$$\sum_{j=1}^{g} f_i(x_j)\,\mathrm{d}x_j = \sum_{j=1}^{g} m_{i,j} f_j(x)\,\mathrm{d}x, \quad i = 1, \dots, g, \tag{5.2.7}$$

or in matrix form

$$Wx' = Mf \tag{5.2.8}$$

where

$$\begin{aligned} W &= (f_i(x_j))_{i,j=1,\dots,g} \\ x' &= (\mathrm{d}x_j/\mathrm{d}x)_{j=1,\dots,g} \\ f &= (f_j)_{j=1,\dots,g} \end{aligned} \tag{5.2.9}$$

We iteratively solve the equations (5.2.7) as follows. We begin with the base case, and we seek to compute initial expansions

$$x_j = c_{j,\nu} x^{\nu} + O(x^{\nu+1/e}) \tag{5.2.10}$$

where

$$\nu := \min_{i,j}(\{j/i : m_{i,j} \neq 0\}) \in \mathbb{Q}_{>0} \tag{5.2.11}$$

which exists, since M is a full rank matrix. Typically, but not always, we have $\nu = 1/g$. Let e be the denominator of ν. Combining the notation above with (5.2.2) we obtain

$$\begin{aligned} x f_i(x_j)\,\mathrm{d}x_j &= ((c_{j,\nu}x^{\nu})^{i-1} + O(x^{i\nu}))\left(\nu c_{j,\nu} x^{\nu} + O(x^{\nu+1/e})\right)\mathrm{d}x \\ &= (\nu c_{j,\nu}^{i} x^{i\nu} + O(x^{i\nu+1/e}))\,\mathrm{d}x. \end{aligned} \tag{5.2.12}$$

Inspecting the leading terms of (5.2.7) for each i we obtain

$$\sum_{j=1}^{g} (\nu c_{j,\nu}^{i} x^{i\nu} + O(x^{i\nu+1/e}))\,\mathrm{d}x = \sum_{j=1}^{g} m_{i,j}(x^j + O(x^{j+1}))\,\mathrm{d}x, \tag{5.2.13}$$

therefore for all i we have

$$\nu \sum_{j=1}^{g} c_{j,\nu}^{i} = m_{i,i\nu}, \tag{5.2.14}$$

where $m_{i,i\nu} = 0$ if $i\nu \notin \mathbb{Z}$. The equations (5.2.14) are symmetric under S_g, and up to this action there is a unique nonzero solution by Newton's formulas, as we $m_{i,i\nu} \neq 0$ for some i.

Remark 5.2.15. In practice, to avoid a possible extension of K to solve (5.2.14), we work modulo a suitable large (split) prime and use a fractional version of the CRT to recover the answer (see also Remark 6.1.3).

Having the determined the expansions

$$x_j = c_{j,\nu}x^\nu + c_{j,\nu+1/e}x^{\nu+1/e} + \cdots + c_{j,\nu+n/e}x^{\nu+n/e} + O(x^{\nu+(n+1)/e}) \tag{5.2.16}$$

for $j = 1, \ldots, g$ up to some precision $n \geq 1$, we integrate (5.2.7) (or (5.2.8)) to iteratively solve for the next term in precision $n+1$. Introducing new variables $c_{j,\nu+(n+1)/e}$ for the next term and considering the coefficient of $x^{\nu+(n+1)/e-1}$ on both sides of (5.2.7), we obtain a inhomogeneous linear system; this system reduces to a Vandermonde matrix in $c_{1,\nu}, \ldots, c_{g,\nu}$, and so it is invertible when these values are distinct. This holds for a generic choice of a point P_0 as long as M is not a scalar matrix. In case of failure, we may replace $\alpha \leftarrow \alpha + m$ for $m \in \mathbb{Z}$: since the entries are of different degree with respect to the leading coefficients, eventually $\alpha + m$ will have branches with distinct leading terms.

The Puiseux series $x_j = x(\widetilde{Q}_j)$ for each j then determines the point $\widetilde{Q}_j$ because we assumed x to be a uniformizing element.

Remark 5.2.17. In practice and in the generic case, we refine the series x_j by successive Hensel lifting. This is possible because after integrating (5.2.7), we are asking for the zeroes of a multivariate function in the variables x_j, determined as a function of x; the initialization obtained corresponds to a constant solution starting from which the lifting process can be started.

Example 5.2.18. Revisiting our running example one last time, we compute Example 4.2.5 again, but starting afresh with just the matrix $M = \begin{pmatrix} 0 & \sqrt{2} \\ \sqrt{2} & 0 \end{pmatrix}$ and the point $P_0 = (0, \sqrt{-1})$. For display purposes, we work modulo a prime above 4001. We first expand

$$\widetilde{P_0} = (x, 3102 + 247x + 1714x^2 + 2082x^3 + 1505x^4 + O(x^5)). \tag{5.2.19}$$

By (5.2.11), we have $\nu = 1/2$. The equations (5.2.14) read:

$$\begin{aligned} c_{1,1/2} + c_{2,1/2} &= 2m_{1,1/2} = 0 \\ c_{1,1/2}^2 + c_{2,1/2}^2 &= 2m_{2,1} = 2\sqrt{2} \end{aligned} \tag{5.2.20}$$

so $c_{2,1/2} = -c_{1,1/2}$ and $c_{1,1/2}^2 = \sqrt{2}$, giving

$$c_{1,1/2} \equiv 2559 \pmod{4001}, \quad c_{2,1/2} \equiv -2559 \equiv 1442 \pmod{4001}. \tag{5.2.21}$$

Now iteratively solving the differential system (5.2.8), we find

(5.2.22)

$$\begin{aligned} \widetilde{Q_1} &= (2559x^{1/2} + 1445x + 2635x^{3/2} + O(x^2), 3102 + 3916x^{1/2} + 3938x + 1271x^{3/2} + O(x^2)) \\ \widetilde{Q_2} &= (1442x^{1/2} + 1445x + 1366x^{3/2} + O(x^2), 3102 + 85x^{1/2} + 3938x + 2730x^{3/2} + O(x^2)). \end{aligned}$$

Rather than computing the symmetric functions in the coordinates of these expansions, we use them directly to interpolate a divisor, as explained in detail in the next section.

6. Proving correctness

The procedure described in the previous sections works unimpeded for any matrix M, not necessarily an endomorphism. In order for M to represent an honest endomorphism $\alpha \in \operatorname{End}(J_K)$, we need to fit a divisor $Y \subset X \times X$ representing the graph of α.

6.1. **Fitting a divisor.** We now proceed to fit a divisor to either the points computed numerically or the Taylor or Puiseux series in a formal neighborhood computed exactly. The case of numerical interpolation was considered by Kumar–Mukamel [KM16], and the case of Taylor series is similar, so we focus on the latter two.

We suppose that X has a model in affine space. Then $X \times X$ has an affine open by the product, with two sets of variables. We then compute the subspace of polynomials of degree at most d that vanish on all of the points $(\widetilde{P_0}, \widetilde{Q}_j)$, iterating the degree d and the precision of the Puiseux series defining $\widetilde{Q}_j$, until a divisor is found: we just write down the corresponding monomials on these coordinates and solve a linear system. To verify that Y is correct, first using Gröbner basis methods we verify that Y is a divisor, and then we check that Y intersects $\{P_0\} \times X$ only in the point (P_0, P_0) with multiplicity g: this excludes the possibility that Y contains superfluous components, except possibly fibral ones (which induce the zero homomorphism at any rate). Examples of the divisors obtained in this way are given in the final section.

Remark 6.1.1. Because of its infinitesimal construction, the Puiseux approach has an advantage in that the verification on differentials in Smith [Smi05, §3.5] is superfluous when the divisor Y is irreducible, which is generically the case.

Remark 6.1.2. In a day-and-night algorithm, we would alternate this step with refining the numerical endomorphism ring by computing with increased precision of the period matrix. If M does not correspond to an endomorphism, then we will discover this in the numerical computation (provably so, if one kept track of errors in the numerical integration); if M does correspond to an endomorphism, then eventually a divisor will be found. Therefore we have a deterministic algorithm that takes a putative endomorphism represented by a matrix $M \in \mathrm{M}_g(F^{\mathrm{alg}})$ and returns `true` or `false` according as whether or not M represents an endomorphism of the Jacobian.

Remark 6.1.3. The algorithm above and both lifts can be significantly sped up further by determining the divisor D modulo many small primes and applying a version of the Chinese remainder theorem allowing denominators to recover equations from their reductions. To obtain the global coefficients one recovers them as small elements in a lattice. This approach can go wrong, and so some heuristics would be required for its analysis; however, for practical purposes, we can check the result obtained divisor a posteriori by determining the corresponding tangent representation.

6.2. **Symmetric functions.** In certain situations it might be more convenient directly to compute the rational map

$$\alpha_X : X \dashrightarrow \operatorname{Sym}^g(X). \tag{6.2.1}$$

Explicitly, we may represent an endomorphism by the elementary symmetric polynomials $e_k(x_1, \ldots, x_g)(x)$ for $k = 1, \ldots, g$, which lie in $K(x)$. See for example section 4.2.5. Given x_i as a Puiseux (or Newton) series, we may compute the power series associated to e_k identify them as rational fractions in x, which may be done by Padé approximants. Afterwards, we can compute the map induced by e_k on the tangent space and hopefully check that it corresponds exactly to our putative endomorphism $M \in \mathrm{M}_g(F^{\mathrm{alg}})$. In practice, we rationally reconstruct e_k using the extended Euclidean algorithm modulo many small primes. This is the method employed in van Wamelen [vW99b] to prove that a genus 2 curve has complex multiplication.

6.3. **Splitting the Jacobian.** The algorithms above can be generalized to the verification of the existence of homomorphisms $\mathrm{Jac}(X) \to \mathrm{Jac}(Y)$, which can be represented by either a rational map $X \dashrightarrow \mathrm{Sym}^{g_Y}(Y)$ or a divisor on $X \times Y$. In particular, this allows us to verify factors of the Jacobian variety that correspond to curves, as explained by Lombardo [Lom16, §6.2] in genus 2. For curves of genus 3, we can similarly identify curves of genus 2 that arise in their Jacobian, by reconstruction of these genus 2 curves from their period matrices.

6.4. **Saturation.** The methods above allow us to certify that the tangent representation $M \in \mathrm{M}_g(K)$ of a putative endomorphism is correct. If we are also given that the period matrix Π is correct up to some precision—for hyperelliptic curves, one may use Molin's double exponentiation algorithm [Mol10, Théorème 4.3]—we may also deduce that the geometric representation $R \in M_{2g}(\mathbb{Z})$ in (2.2.1) is also correct. Assuming that we have verified the geometric representation of all the generators of the endomorphism algebra, we can also recover the endomorphism ring, by considering possible superorders and ruling them out.

Example 6.4.1. For example, take $X : y^2 = -3x^6 + 8x^5 - 30x^4 + 50x^3 - 71x^2 + 50x - 27$ a simplified Weierstrass model for the genus 2 curve with LMFDB label 961.a.961.2, we can verify that the endomorphism algebra is $\mathbb{Q}(\sqrt{5})$, and $\sqrt{5}$ might be represented by

$$M = \begin{pmatrix} -1 & 2 \\ 2 & 1 \end{pmatrix} \quad \text{and} \quad R = \begin{pmatrix} -1 & 0 & 0 & -1 \\ 1 & 1 & 1 & 0 \\ 0 & 4 & -1 & 1 \\ -4 & 0 & 0 & 1 \end{pmatrix}. \tag{6.4.2}$$

From the above computation, we also deduce that the endomorphism ring is $\mathbb{Z}[\sqrt{5}]$ and not $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, as $\frac{1+R}{2} \notin M_4(\mathbb{Z})$.

7. Upper bounds in genus 2

In this section, we show how to read off heuristically the endomorphism algebra with rigorous upper bounds given Frobenius polynomials. Lombardo [Lom16, §6] has already given a practical method for this purpose; we consider a slightly different approach.

7.1. **Néron–Severi rank.** Suppose X has genus 2. Then J is a principally polarized abelian surface; let $\dagger$ denote the Rosati involution. In this case, we can take advantage of the relation between the Néron–Severi group $\mathrm{NS}(J)$ and $\mathrm{End}(J)_{\mathbb{Q}}$: by Mumford [Mum70, Section 21], we have an isomorphism of $\mathbb{Q}$-vector spaces

$$\mathrm{NS}(J)_{\mathbb{Q}} \simeq \{\phi \in \mathrm{End}(J)_{\mathbb{Q}} : \phi^{\dagger} = \phi\} \tag{7.1.1}$$

Let $\rho(J) := \operatorname{rk} \operatorname{NS}(J)$. Then by Albert's classification, we deduce that

$$\rho(J_F) = \begin{cases} 4 & \text{if } \operatorname{End}(J_F)_{\mathbb{R}} \simeq \mathrm{M}_2(\mathbb{C}); \\ 3 & \text{if } \operatorname{End}(J_F)_{\mathbb{R}} \simeq \mathrm{M}_2(\mathbb{R}); \\ 2 & \text{if } \operatorname{End}(J_F)_{\mathbb{R}} \simeq \mathbb{R}\times\mathbb{R}, \mathbb{C}\times\mathbb{C} \text{ or } \mathbb{C}\times\mathbb{R}; \\ 1 & \text{if } \operatorname{End}(J_F)_{\mathbb{R}} \simeq \mathbb{R}. \end{cases} \tag{7.1.2}$$

So if we had a way to compute $\rho(J_{F^{\mathrm{alg}}})$, we could limit the number of possibilities for $\operatorname{End}(J_{F^{\mathrm{alg}}})_{\mathbb{R}}$. To compute ρ, we look modulo primes.

Let $\mathfrak{p}$ be a prime of (the ring of integers of) F such that X has good reduction $X_{\mathbb{F}_\mathfrak{p}}$ at $\mathfrak{p}$, and write $J_{\mathbb{F}_\mathfrak{p}}$ for the reduction of J modulo $\mathfrak{p}$. Then there is a natural injective specialization homomorphism

$$s_p : \operatorname{NS}(J_{F^{\mathrm{alg}}}) \hookrightarrow \operatorname{NS}(J_{\overline{\mathbb{F}}_\mathfrak{p}}), \tag{7.1.3}$$

so $\rho(J_{F^{\mathrm{alg}}}) \leq \rho(J_{\overline{\mathbb{F}}_\mathfrak{p}})$.

Let $q = \#\mathbb{F}_\mathfrak{p}$ and let $\ell \nmid q$ be prime. Let

$$\begin{aligned} P_1(J_{\mathbb{F}_\mathfrak{p}}, T) &:= \det\left(1 - \operatorname{Frob}_\mathfrak{p} T \mid H^1(J_{F^{\mathrm{alg}}}, \mathbb{Q}_\ell)\right) = \det\left(1 - \operatorname{Frob}_\mathfrak{p} T \mid H^1(X_{F^{\mathrm{alg}}}, \mathbb{Q}_\ell)\right) \\ &= 1 + a_1 T + a_2 T^2 + a_1 q T^3 + q^2 T^4 \in 1 + T\mathbb{Z}[T]. \end{aligned} \tag{7.1.4}$$

Then

(7.1.5)

$$\begin{aligned} P_2(J_{\mathbb{F}_\mathfrak{p}}, t) &:= \det\left(1 - \operatorname{Frob}_\mathfrak{p} T \mid H^2(J_{F^{\mathrm{alg}}}, \mathbb{Q}_\ell)\right) \\ &= (1-qT)^2(1 + (2q - a_2)T + (2q + a_1^2 - 2a_2)qT^2 + (2q - a_2)q^2T^3 + q^4T^4). \end{aligned}$$

The Tate conjecture holds for abelian surfaces [Tat66], and it relates the Néron–Severi group of $J_{\mathbb{F}_\mathfrak{p}}$ with $P_2(J_{\mathbb{F}_\mathfrak{p}}, T)$ in the following way.

Proposition 7.1.6. *The following statements hold.*

(a) *$\rho(X_{\overline{\mathbb{F}}_\mathfrak{p}})$ is equal to the number of reciprocal roots of $P_2(J_{\mathbb{F}_\mathfrak{p}}, T)$ of the form q times a root of unity.*

(b) *We have*

$$\operatorname{disc}(\operatorname{NS}(J_{\mathbb{F}_\mathfrak{p}})) = \lim_{s\to 1} \frac{(-1)^{\rho(J_{\mathbb{F}_\mathfrak{p}})-1} P_2(J_{\mathbb{F}_\mathfrak{p}}, q^{-s})}{q(1-q^{1-s})^{\rho(J_{\mathbb{F}_\mathfrak{p}})}} \bmod \mathbb{Q}^{\times 2}. \tag{7.1.7}$$

Proof. For part (a), we know that $\rho(X_{\mathbb{F}_\mathfrak{p}})$ is equal to the multiplicity of q as a reciprocal root of $P_2(J_{\mathbb{F}_\mathfrak{p}}, T)$ by the Tate conjecture, and (a) follows by taking a power of the Frobenius. For part (b), the Tate conjecture implies the Artin–Tate conjecture [Mil75a, Theorem 6.1] and [Mil75b], which implies (b) after simplification using that $\#\operatorname{Br}(X)$ is a perfect square [LLR05]. ∎

We will use one other ingredient: we can rule out the possibility that $J_{F^{\mathrm{alg}}}$ has CM by looking at $P_1(J_{\mathbb{F}_\mathfrak{p}}, T)$ as follows.

Lemma 7.1.8. *Suppose that $\operatorname{End}(J_{F^{\mathrm{alg}}})_{\mathbb{Q}} = K$ is a quartic CM field. Let p be prime and let $\mathfrak{p}$ be a prime of F above p such that X has good reduction at $\mathfrak{p}$ and that splits completely in K. Then $P_1(J_{\mathbb{F}_\mathfrak{p}}, T)$ is irreducible and*

$$\mathbb{Q}[T]/(P_1(J_{\mathbb{F}_\mathfrak{p}}, T)) \simeq K. \tag{7.1.9}$$

Proof. Suppose that the CM for J is defined over $F' \supseteq F$, so $\mathrm{End}(J_{F'})_{\mathbb{Q}} = K$. Let $\mathfrak{p}'$ be a prime above $\mathfrak{p}$ in F'. Then by Oort [Oor88, (6.5.e)], if p splits in K then $J_{\mathbb{F}_\mathfrak{p}}$ is ordinary, so $\mathrm{End}(J_{\mathbb{F}_{\mathfrak{p}'}})_{\mathbb{Q}} = K$. Let $\pi \in \mathrm{End}(J)$ be the geometric Frobenius for $\mathfrak{p}$ and similarly $\pi' \in \mathrm{End}(J_{F'})$ for $\mathfrak{p}'$. Then by Tate [Tat66, Theorem 2], $\mathbb{Q}[\pi'] = K$ and in particular the characteristic polynomial $P_1(J_{\mathbb{F}_{\mathfrak{p}'}}, T)$ of π' is irreducible. But π' is a power of π, so $\mathbb{Q}[\pi] = \mathbb{Q}[\pi'] = K$, and the lemma follows. □

7.2. **Computing upper bounds.** We compute upper bounds on $\rho(J_{F^{\mathrm{alg}}})$ in the following way. By Proposition 7.1.6(a), we can compute $\rho(X_{\overline{\mathbb{F}}_\mathfrak{p}})$ for many good primes $\mathfrak{p}$ by counting points on $X_{\overline{\mathbb{F}}_\mathfrak{p}}$. We have two cases:

- If $\rho(J_{F^{\mathrm{alg}}})$ is even, then by Charles [Cha11, Theorem 1] (part (2) cannot occur) there are infinitely many primes such that $\rho(J_{F^{\mathrm{alg}}}) = \rho(J_{\overline{\mathbb{F}}_\mathfrak{p}})$.
- If $\rho(J_{F^{\mathrm{alg}}})$ is odd, there are infinitely many pairs of primes $(\mathfrak{p}_1, \mathfrak{p}_2)$ such that

$$\rho(J_{F^{\mathrm{alg}}}) + 1 = \rho(J_{\overline{F}_{\mathfrak{p}_1}}) = \rho(J_{\overline{F}_{\mathfrak{p}_2}}) \tag{7.2.1}$$

$$\mathrm{disc}(\mathrm{NS}(J_{\overline{\mathbb{F}}_{\mathfrak{p}_1}})) \not\equiv \mathrm{disc}(\mathrm{NS}(J_{\overline{\mathbb{F}}_{\mathfrak{p}_2}})) \bmod \mathbb{Q}^{\times 2}. \tag{7.2.2}$$

By (7.1.3), we then seek out the minimum values of $\min_\mathfrak{p} \rho(J_{\overline{\mathbb{F}}_\mathfrak{p}})$ over the first few primes $\mathfrak{p}$ of good reduction; and for those where equality holds, we check (7.2.2) using (7.1.7), improving our upper bound by 1 when the congruence fails. This upper bound for $\rho(J_{F^{\mathrm{alg}}})$ by gives an upper bound for $\mathrm{End}(J_{F^{\mathrm{alg}}})_{\mathbb{Q}}$ by (7.1.2), and a guess for $\mathrm{End}(J_{F^{\mathrm{alg}}})_{\mathbb{R}}$ except when $\rho(J_{F^{\mathrm{alg}}}) = 2$. For example, this approach allows us to quickly rule out the possibility that $J_{F^{\mathrm{alg}}}$ has quaternionic multiplication (QM) by showing that $\rho(J_{F^{\mathrm{alg}}}) \leq 2$.

To conclude, suppose that we are in the remaining case where, after many primes $\mathfrak{p}$, we compute $\rho(J_{F^{\mathrm{alg}}}) \leq 2$ and we believe that equality holds. Then the subalgebra $K_0 \subseteq \mathrm{End}(J_{F^{\mathrm{alg}}})_{\mathbb{Q}}$ fixed under the Rosati involution has dimension ≤ 2 over $\mathbb{R}$. We proceed as follows.

1. By the algorithms in the previous section, we can find and certify a nontrivial endomorphism. So with a day-and-night algorithm, eventually either we will find $\rho(J_{F^{\mathrm{alg}}}) = 1$ or we will have certified that the Rosati-fixed endomorphism algebra K_0 is of dimension 2.
2. Next, we check if K_0 is a field by factoring the minimal polynomial of the endomorphism generating K_0 over $\mathbb{Q}$. If $K_0 \simeq \mathbb{Q} \times \mathbb{Q}$ splits, then by section 6.3 we can split the Jacobian up to isogeny as the product of elliptic curves, and from there deduce the geometric endomorphism algebra and endomorphism ring.
3. To conclude, suppose that K_0 is a (necessarily real) quadratic field. Then by (7.1.2), we cannot have $\mathrm{End}(J_{F^{\mathrm{alg}}})_{\mathbb{R}} \simeq \mathbb{C} \times \mathbb{R}$, and we need to distinguish between RM and CM. We apply Lemma 7.1.8 to search for a candidate CM field or to rule out the CM possibility, by finding two nonisomorphic candidate CM fields. This approach is analogous to Lombardo's approach in [Lom16, §6.3], and we refer to his work for a careful exposition.

8. Examples

We now give some explicit illustrations of the methods developed above.

8.1. **Examples in genus 2.**

Example 8.1.1. Our first example is the curve of genus 2 with LMFDB label 12500.a.12500.1, the smallest curve with potential RM in the LMFDB. For convenience, we complete the square from the minimal Weierstrass model and work with the equation

$$X : y^2 = 5x^6 + 10x^3 - 4x + 1 = f(x) \tag{8.1.2}$$

so that $X \times X$ has affine patch described by $y_i^2 = f(x_i)$ with $i = 1, 2$.

Let α be a root of the polynomial $x^2 - x - 1$. Then the endomorphism ring of X is the maximal order in the quadratic field $\mathbb{Q}(\alpha)$ of discriminant 5. With basis of differentials $\mathrm{d}x/y, x\,\mathrm{d}x/y$, a generator has tangent representation $\begin{pmatrix} -\alpha & 0 \\ 0 & \alpha - 1 \end{pmatrix}$. For the base point $P_0 = (0, 1)$ a corresponding divisor in $X \times X$ is defined by the equations:

$$\begin{aligned}
&(2\alpha - 1)x_1^2x_2^2 - (\alpha + 2)x_1^2x_2 + x_1^2 - (\alpha + 2)x_1x_2^2 + \alpha x_1x_2 + x_2^2 = 0, \\
&(3\alpha + 1)x_1^2x_2y_2 - (2\alpha + 4)x_1^2y_2 - (3\alpha + 1)x_1y_1x_2^2 + (4\alpha + 3)x_1y_1x_2 \\
&\quad - (\alpha - 1)x_1y_1 - (4\alpha + 3)x_1x_2y_2 + (\alpha - 1)x_1y_2 + (2\alpha + 4)y_1x_2^2 \\
&\qquad + (1 - \alpha)y_1x_2 - y_1 + (\alpha + 1)x_2y_2 + y_2 = 0.
\end{aligned} \tag{8.1.3}$$

Alternatively, the image of a point $P = (v, w)$ of X under the morphism $X \to \mathrm{Sym}^2(X)$ is described by the equation $x^2 + a_1x + a_2 = 0$, $y = b_1x + b_2$, where

$$\begin{aligned}
a_1 &= \frac{-5\alpha v^2 + (\alpha + 2)v}{5v^2 - 5\alpha v + (2\alpha - 1)}, \\
a_2 &= \frac{(2\alpha - 1)v^2}{5v^2 - 5\alpha v + (2\alpha - 1)}, \\
b_1 &= \frac{-(7\alpha + 4)v^2w + (6\alpha + 2)vw - 2w}{5v^5 + 5(1 - 2\alpha)v^4 + (3 - \alpha)v^3 + (7\alpha - 1)v^2 - (2\alpha + 3)v + 1}, \\
b_2 &= \frac{(3\alpha + 1)v^2w - (2\alpha + 1)vw + w}{5v^5 + 5(1 - 2\alpha)v^4 + (3 - \alpha)v^3 + (7\alpha - 1)v^2 - (2\alpha + 3)v + 1}.
\end{aligned} \tag{8.1.4}$$

Example 8.1.5. As a second example, consider the curve with LMFDB label 20736.l.373248.1 with simplified Weierstrass model

$$X : y^2 = 24x^5 + 36x^4 - 4x^3 - 12x^2 + 1. \tag{8.1.6}$$

We find that this curve has QM over $\overline{\mathbb{Q}}$ by a non-Eichler order of reduced discriminant 36 in the indefinite quaternion algebra over $\mathbb{Q}$ with discriminant 6. The full ring of endomorphisms is only defined over $\mathbb{Q}(\theta)$ where θ is a root of $x^8 + 4x^6 + 10x^4 + 24x^2 + 36$, and accordingly its elements are difficult to write down. Over the smaller field $\mathbb{Q}(\sqrt{-3})$ we get endomorphism ring $\mathbb{Z}[3\sqrt{-1}]$. A generator has tangent representation

$$M = \begin{pmatrix} -\sqrt{-3} & \sqrt{-3} \\ 2\sqrt{-3} & \sqrt{-3} \end{pmatrix} \tag{8.1.7}$$

with square -9. When using the base point $P_0 = (0,1)$, a corresponding divisor on $X \times X$ is described by equations of the form

$$\begin{aligned}(8.1.8)\qquad &\left(-\frac{53568}{37}x_2^2 + \frac{137376}{37}x_2 + \frac{14256}{37}y_2 - 1296\right)x_1^{14} + \cdots + \frac{17-34\alpha}{111}y_1 - y_2 + 1 = 0,\\ &\left(-\frac{8640}{37}x_2^2 + \frac{29376}{37}x_2 + \frac{108}{37}y_2 - 324\right)x_1^{14} + \cdots + \frac{7-14\alpha}{74}y_1 + x_2^2 = 0,\end{aligned}$$

where $\alpha^2 - \alpha + 1 = 0$.

Example 8.1.9. A third example in genus 2 is 294.a.8232.1 with model

$$X : y^2 = x^6 - 8x^4 + 2x^3 + 16x^2 - 36x - 55. \tag{8.1.10}$$

The endomorphism ring of this curve is of index 2 in the ring $\mathbb{Z} \times \mathbb{Z}$ because it admits two maps of degree 2 to the elliptic curves

$$E_1 : y^2 = x^3 + 215/3x - 10582/27 \quad \text{and} \quad E_2 : y^2 = x^3 + 47/3x - 142/27. \tag{8.1.11}$$

The maps send a point (x,y) of X to

$$\left(\frac{6x^4 + 18x^3 + x^2 + x(-6y-50) - 18y - 50}{3(x+2)^2}, \frac{-4x^6 - 18x^5 - 2x^4 + 4x^3(y+24) - 2x^2(-9y-41) - 2x(93-9y) - 224}{(x+2)^3}\right) \tag{8.1.12}$$

on E_1 and

$$\left(\frac{6x^4 + 6x^3 - 23x^2 + 2x(3y-7) + 6y + 22}{3(x+2)^2}, \frac{24 + 22x^4 - 6x^5 - 4x^6 + x^2(-38-6y) + x^3(28-4y) + 8y + x(-30+6y)}{(x+2)^3}\right) \tag{8.1.13}$$

on E_2.

8.2. **Examples in higher genus.**

Example 8.2.1. The final hyperelliptic curve that we consider is the curve

$$X : y^2 = x^8 - 12x^7 + 50x^6 - 108x^5 + 131x^4 - 76x^3 - 10x^2 + 44x - 19 \tag{8.2.2}$$

of genus 3. This is a model for the modular curve $X_0(35)$ over $\mathbb{Q}$, and in fact this equation was obtained as a modular equation satisfied by modular forms of level 35. We could make some guesses about the endomorphism ring of its Jacobian by computing the space of cuspforms of weight 2 and level 35, but let us apply our algorithms as if we were ignorant of its modular provenance.

We find that the Jacobian of X splits into an elliptic curve and the Jacobian of a genus 2 curve. Its endomorphism algebra $\mathbb{Q} \times \mathbb{Q}(\sqrt{17})$ is generated by an endomorphism whose tangent representation with respect to the standard basis of differentials $\{x^i\,\mathrm{d}x/y\}_{i=1,2,3}$ is given by

$$\begin{pmatrix} 1 & 1 & -2 \\ 0 & -2 & -2 \\ -1 & 0 & 1 \end{pmatrix}. \tag{8.2.3}$$

which has characteristic polynomial $(t+1)(t^2-t-4)$. The curve X admits a degree 2 morphism to the elliptic curve $Y : x^3 + 6656/3x - 185344/27$ which is given by

$$(x, y) \longmapsto \left(\frac{64x^2 - 400x + 272}{3(x^2 - x - 1)}, \frac{224y}{(x^2 - x - 1)^2} \right). \tag{8.2.4}$$

Example 8.2.5. Our algorithms can equally well deal with more general curves. For example, it is known from work of Liang [Lia14] that the plane quartic

$$\begin{aligned} X : x_0^4 + 8x_0^3x_2 + 2x_0^2x_1x_2 + 25x_0^2x_2^2 - x_0x_1^3 + 2x_0x_1^2x_2 + 8x_0x_1x_2^2 + \\ 36x_0x_2^3 + x_1^4 - 2x_1^3x_2 + 5x_1^2x_2^2 + 9x_1x_2^3 + 20x_2^4 = 0 \end{aligned} \tag{8.2.6}$$

has real multiplication by the algebra $\mathbb{Q}(\zeta_7+\zeta_7^{-1})$. We have independently verified this result. Although the equations for the divisor are too large to reproduce here (they can be generated with the package [CMS17]), at least the tangent representation of the endomorphism with respect to an echelonized basis of differential forms at the base point $P_0 = (-2 : 0 : 1)$ is of the rather pleasing form

$$\begin{pmatrix} \zeta_7^5 + \zeta_7^2 & 0 & 0 \\ 0 & \zeta_7^4 + \zeta_7^3 & 0 \\ 0 & 0 & -\zeta_7^5 - \zeta_7^4 - \zeta_7^3 - \zeta_7^2 - 1 \end{pmatrix}. \tag{8.2.7}$$

Example 8.2.8. As a final aside, we consider Picard curves of the form $X : y^3 = a_4x^4 + a_2x^2 + a_0$. It can be shown [PS11] that the Sato–Tate group of a generic such curve is equal to $\mathrm{SU}(2) \times \mathrm{SU}(2)_2$. The corresponding Jacobian then splits into an elliptic curve with CM and the Jacobian of a curve of genus 2 that has QM. The latter factor, call it Y, can be identified explicitly using recent work of Ritzenthaler–Romagny [RR16], and our algorithms can be used to find an explicit correspondence between X and Y, as well as to determine the field of definition of the endomorphism rings involved.

References

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BSS+16a] Andrew R. Booker, Jeroen Sijsling, Andrew V. Sutherland, John Voight, and Dan Yasaki. A database of genus 2 curves over the rational numbers. *LMS J. Comput. Math.*, 19(suppl. A):235–254, 2016.

[BSS+16b] Andrew R. Booker, Jeroen Sijsling, Andrew V. Sutherland, John Voight, and Dan Yasaki. Sato-Tate groups and modularity for atypical genus 2 curves. `arXiv:1602.03715`, 2016.

[CD17] Clifton Cunningham and Lassina Dembélé. Lifts of hilbert modular forms and application to modularity of abelian varieties. `arXiv:1705.03054`, 2017.

[Cha11] François Charles. On the Picard number of K3 surfaces over number fields. `arXiv:1111.4117`, 2011.

[CMS17] Edgar Costa, Nicolas Mascot, and Jeroen Sijsling. Rigorous computation of the endomorphism ring of a jacobian. `https://github.com/edgarcosta/endomorphisms/`, 2017.

[KM04] Kamal Khuri-Makdisi. Linear algebra algorithms for divisors on an algebraic curve. *Math. Comp.*, 73(245):333–357, 2004.

[KM16] Abhinav Kumar and Ronen E. Mukamel. Real multiplication through explicit correspondences. *LMS J. Comput. Math.*, 19(suppl. A):29–42, 2016.

[Lia14] Dun Liang. *Explicit equations of non-hyperelliptic genus 3 curves with real multiplication by* $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$. PhD thesis, Louisiana State University, 2014.

[LLL82] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261(4):515–534, 1982.

[LLR05] Qing Liu, Dino Lorenzini, and Michel Raynaud. On the Brauer group of a surface. *Invent. Math.*, 159(3):673–676, 2005.

[LMF16] The LMFDB Collaboration. The l-functions and modular forms database. http://www.lmfdb.org, 2016. [Online; accessed 21 July 2016].

[Lom16] Davide Lombardo. Computing the geometric endomorphism ring of a genus 2 Jacobian. arXiv:1610.09674, 2016.

[Mas13] Nicolas Mascot. Computing modular Galois representations. *Rend. Circ. Mat. Palermo (2)*, 62(3):451–476, 2013.

[Mil75a] James S. Milne. On a conjecture of Artin and Tate. *Ann. of Math. (2)*, 102(3):517–533, 1975.

[Mil75b] James S. Milne. On a conjecture of Artin and Tate: addendum, 1975. http://www.jmilne.org/math/articles/add/1975a.pdf.

[Mol10] Pascal Molin. *Numerical integration and L functions computations*. Theses, Université Sciences et Technologies - Bordeaux I, October 2010.

[Mum70] David Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London, 1970.

[Oor88] Frans Oort. Endomorphism algebras of abelian varieties. In *Algebraic geometry and commutative algebra, Vol. II*, pages 469–502. Kinokuniya, Tokyo, 1988.

[Poo96] Bjorn Poonen. Computational aspects of curves of genus at least 2. In *Algorithmic number theory (Talence, 1996)*, volume 1122 of *Lecture Notes in Comput. Sci.*, pages 283–306. Springer, Berlin, 1996.

[PS11] Maria Petkova and Hironori Shiga. A new interpretation of the Shimura curve with discriminant 6 in terms of Picard modular forms. *Arch. Math. (Basel)*, 96(4):335–348, 2011.

[RR16] Christophe Ritzenthaler and Matthieu Romagny. On the Prym variety of genus 3 covers of elliptic curves. arXiv:1612.07033, 2016.

[Sij16] Jeroen Sijsling. arithmetic-geometric_mean; a package for calculating period matrices via the arithmetic-geometric mean. https://github.com/JRSijsling/arithmetic-geometric_mean/, 2016.

[Smi05] Benjamin Smith. *Explicit endomorphisms and correspondences*. PhD thesis, University of Sydney, 2005.

[Tat66] John Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.

[vW99a] Paul van Wamelen. Examples of genus two CM curves defined over the rationals. *Math. Comp.*, 68(225):307–320, 1999.

[vW99b] Paul van Wamelen. Proving that a genus 2 curve has complex multiplication. *Math. Comp.*, 68(228):1663–1677, 1999.

[vW00] Paul van Wamelen. Poonen's question concerning isogenies between Smart's genus 2 curves. *Math. Comp.*, 69(232):1685–1697, 2000.

[vW06] Paul B. van Wamelen. Computing with the analytic Jacobian of a genus 2 curve. In *Discovering mathematics with Magma*, volume 19 of *Algorithms Comput. Math.*, pages 117–135. Springer, Berlin, 2006.

Department of Mathematics, Dartmouth College, 6188 Kemeny Hall, Hanover, NH 03755, USA

E-mail address: edgarcosta@math.dartmouth.edu

URL: http://www.math.dartmouth.edu/~edgarcosta/

Department of Mathematics, University of Warwick, Coventry CV4 7AL, UK

E-mail address: n.a.v.mascot@warwick.ac.uk

URL: http://www2.warwick.ac.uk/fac/sci/maths/people/staff/mascot/

Universität Ulm, Institut für Reine Mathematik, D-89068 Ulm, Germany

E-mail address: sijsling@gmail.com

URL: https://sites.google.com/site/sijsling/

Department of Mathematics, Dartmouth College, 6188 Kemeny Hall, Hanover, NH 03755, USA

E-mail address: jvoight@gmail.com

URL: http://www.math.dartmouth.edu/~jvoight/