RIGOROUS COMPUTATION OF THE ENDOMORPHISM RING OF A JACOBIAN

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

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

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 have important implications for the arithmetic of the curve, for example when identifying of the automorphic realization of its L-function [BSS+16].

Let F be a number field with algebraic closure F^{al}. Let X be a nice curve over F, let J be its Jacobian, and J^{al} be its base change to F^{al}. 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 a continuous action of $\mathrm{Gal}(F^{\mathrm{al}} \mid F)$ (factoring through a finite quotient) together with a computable ring isomorphism

$$\iota \colon B \xrightarrow{\sim} \mathrm{End}(J^{\mathrm{al}}) \tag{1.1.1}$$

that commutes with the action of $\mathrm{Gal}(F^{\mathrm{al}} \mid F)$. (In this overview, we are agnostic about how to encode elements of $\mathrm{End}(J^{\mathrm{al}})$ 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.

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 find 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 such 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.

Date: March 30, 2020.

From this computation, we can also recover the multiplication law in $\mathrm{End}(J^{\mathrm{al}})$ and its Galois action [BSS+16, §6].

In the work on curves of genus 2 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 $P_0 \in X(F^{\mathrm{al}})$ be a Weierstrass point on X. Given a point $P \in X(F^{\mathrm{al}})$, by inverting the Abel–Jacobi map we compute the (generically unique) pair of points $Q_1, Q_2 \in X(F^{\mathrm{al}})$ such that

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

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 to 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. Our approach is similar to work of Couveignes–Ezome [CE15, §6.2], who also formally solve a differential system to compute equations for an isogeny between curves of genus 2. 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 by examining Frobenius polynomials; we consider a slightly different approach in this case by first bounding from above the dimension of the subalgebra of $\mathrm{End}(J^{\mathrm{al}})_{\mathbb{Q}}$ fixed under the Rosati involution (using the known Tate conjecture for the reduction of the abelian surface modulo primes). This specialized algorithm in genus 2 again is quite practical. We then generalize this approach to higher genus: applying work of Zywina [Zyw14], we

again find rigorous upper bounds and we show that these are sharp if the Mumford–Tate conjecture holds for the Jacobian and if a certain hypothesis on the independence of Frobenius polynomials holds.

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 contains 66 158 curves of genus 2 with small minimal absolute discriminant.

Our implementation of these results is available online [CMS17], and all examples in this paper can be inspected in detail by going to its subdirectory `endomorphisms/examples/paper`. This code has already been used by Cunningham–Dembélé to establish the paramodularity of an abelian threefold in the context of functoriality [CD17].

Acknowledgments. The authors would like to thank Kamal Khuri-Makdisi and David Zywina for helpful conversations, as well as the anonymous referees for their comments and suggestions. Mascot was supported by the EPSRC Programme Grant EP/K034383/1 "LMF: L-Functions and Modular Forms". Sijsling was supported by the Juniorprofessuren-Programm "Endomorphismen algebraischer Kurven" (7635.521(16)) from the Science Ministry of Baden–Württemberg. Voight was supported by an NSF CAREER Award (DMS-1151047) and a Simons Collaboration Grant (550029).

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, we use the following notation. Let $F \subset \mathbb{C}$ be a number field with algebraic closure F^{al}. Let X be a nice (i.e., smooth, projective and geometrically integral) curve over F of genus g. Let $J = \mathrm{Jac}(X)$ be the Jacobian of X. We abbreviate $J^{\mathrm{al}} = J_{F^{\mathrm{al}}}$ for the base change of J to F^{al}. 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+16, §6.1] where with a little more care the Galois structure on the resulting approximate endomorphism ring is recovered as well.

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 $\mathrm{End}(J^{\mathrm{al}})$. These matrices represent the action of the corresponding endomorphisms on a chosen basis of the homology group $H_1(X, \mathbb{Z})$, and accordingly, the corresponding ring structure is induced

by matrix multiplication. If $\Pi \in \mathrm{M}_{g,2g}(\mathbb{C})$ is the period matrix of J, then the equality

$$M\Pi = \Pi R \tag{2.2.1}$$

holds, where $M \in \mathrm{M}_g(\mathbb{C})$ is the representation on the tangent space $H^0(X, \omega_X)^*$, given by left multiplication. Equation (2.2.1) allows us to convert (numerically) between the matrices $R_j \in \mathrm{M}_{2g}(\mathbb{Z})$ and matrices $M_j \in \mathrm{M}_g(\mathbb{C})$ describing the action on the tangent space, which allows us to descend to $\mathrm{M}_g(F^{\mathrm{al}})$ 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. We chose this convention because it makes the map $\mathrm{End}(J) \to \mathrm{End}(H^0(X, \omega_X)^*)$ a ring homomorphism.

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 $X\colon y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1$ 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 in about 10 CPU seconds on a standard desktop machine). 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 can identify a putative endomorphism $\alpha \overset{?}{\in} \mathrm{End}(J_{\mathbb{C}})$ with representations

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

which satisfies $\alpha^2 = 2$.

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 3.4.9 below); this can often be resolved by slightly transforming the defining equation of X.

Remark 2.2.6. There are several available implementations to compute the period matrix and the Abel–Jacobi map in addition to Magma. A recent robust method to calculate period matrices of cyclic covers of the projective line was developed by Molin–Neurohr [MN17]. We also recommend the introduction of this reference for a survey of other available implementations.

Work continues: Neurohr is working on the generalization of these algorithms to (possibly singular) plane models of general algebraic curves, and for these curves a SageMath implementation by Nils Bruin and Alexandre Zotine is also in progress.

Remark 2.2.7. For hyperelliptic curves and plane quartics we may also speed up the calculation of periods through arithmetic–geometric mean (AGM) methods. So far this has been implemented in the hyperelliptic case [Sij16]. While this delivers an enormous speedup, the AGM method 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

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

be the Abel–Jacobi map associated to P_0. Complex analytically, using our chosen basis $\omega_1, \dots, \omega_g$ of $H^0(X, \omega_X)$ we identify $J(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda$ where $\Lambda \simeq \mathbb{Z}^{2g}$ is the period lattice of J. Under this isomorphism the Abel–Jacobi map is

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

The numerical evaluation of these integrals is standard: we compute a low degree map $\varphi \colon X \to \mathbb{P}^1$, 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 $f(x)$ different from 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 be handled similarly 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 square root along γ, we use four determinations of the square root over $\mathbb{C}$, with respective branch cuts along the half-axes $\operatorname{Re} z > 0$, $\operatorname{Re} z < 0$, $\operatorname{Im} z > 0$ and $\operatorname{Im} z < 0$. On each segment of γ_x, 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 $f(x)$. For instance, in the case illustrated by Figure 3.1.5, letting t be the parameter of integration and assuming we started with the determination whose branch cut is along $\operatorname{Im} z > 0$, we would first switch to the determination whose branch cut is along $\operatorname{Re} z < 0$ when $\operatorname{Im} f(\gamma_x(t))$ changes from negative to positive, and then to the determination whose branch cut is along $\operatorname{Im} z < 0$ when $\operatorname{Re} f(\gamma_x(t))$ changes from positive to negative, so that the branch cut is always at least $90°$ away from $f(\gamma_x(t))$. Of course, the sign of the square root may need to be corrected every time we switch from one determination to another, so as to get a continuous determination

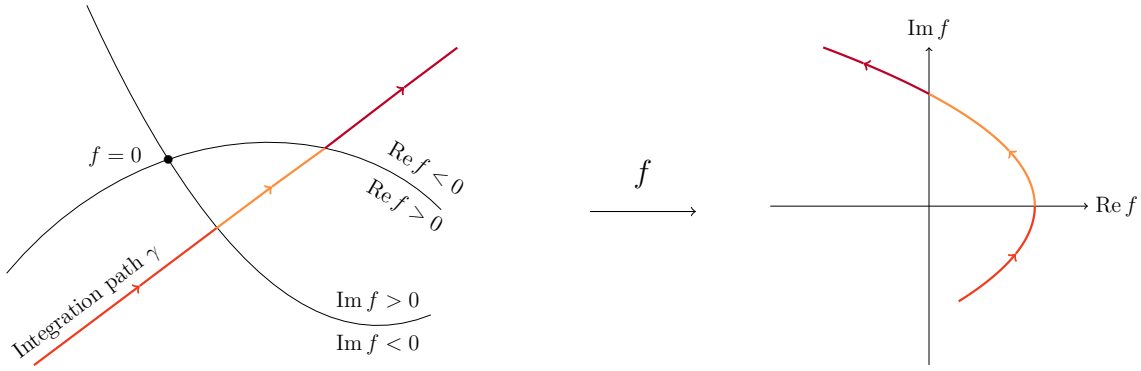

FIGURE 3.1.5. Changing the branches of $\sqrt{f(x)}$ along γ

of $\sqrt{f(\gamma(t))}$. Also note that by construction, the integration path avoids the roots of f, so the signs of $\operatorname{Re} f(\gamma(t))$ and $\operatorname{Im} f(\gamma(t))$ never change simultaneously.

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

Now let $O_0 = O_{0,1} + \cdots + O_{0,g}$ be an effective ("origin") divisor of degree g. Riemann–Roch ensures that for a generic choice of pairwise distinct points $O_{0,k} \in X(\mathbb{C})$, the derivative of the Abel–Jacobi map

$$\begin{aligned} \mathrm{AJ}\colon \mathrm{Sym}^g(X)(\mathbb{C}) &\to \mathbb{C}^g/\Lambda \\ \{Q_1, \cdots, Q_g\} &\mapsto \sum_{k=1}^{g} \left(\int_{O_{0,k}}^{Q_k} \omega_j \right)_{j=1,\cdots,g} \end{aligned} \tag{3.1.6}$$

is non-singular at O_0, so we assume that this is indeed the case from now on. As explained by Mumford, for a general point $[D] \in J(\mathbb{C}) = \mathrm{Pic}^0(X)(\mathbb{C})$, by Riemann–Roch we can write

$$[D] = [Q_1 + \cdots + Q_g - O_0] \tag{3.1.7}$$

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

$$\begin{aligned} \mathrm{Mum}\colon J &\dashrightarrow \mathrm{Sym}^g(X) \\ [D] &\mapsto \{Q_1, \ldots, Q_g\}. \end{aligned} \tag{3.1.8}$$

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 $\mathrm{Mum}(b) = \{Q_1, \ldots, Q_g\}$ where

$$\left(\sum_{k=1}^{g} \int_{O_{0,k}}^{Q_k} \omega_j \right)_{j=1,\ldots,g} \equiv b \pmod{\Lambda}. \tag{3.1.9}$$

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

$$\alpha_X\colon X \xrightarrow{\mathrm{AJ}} J \xrightarrow{\alpha} J \overset{\mathrm{Mum}}{\dashrightarrow} \mathrm{Sym}^g(X). \tag{3.1.10}$$

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

$$\alpha([P - P_0]) = [Q_1 + \cdots + Q_g - O_0]. \tag{3.1.11}$$

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 usually not unique, hence neither is this representation of a class in $\mathrm{Pic}^0(X)(\mathbb{C})$ as a subspace of V. 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 $x\colon X \to \mathbb{P}^1$. 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. In either case, the divisor $(g-1)\infty_X$ is a canonical divisor on X, and $\deg \infty_X = 2$; 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 $[C] \in \mathrm{Pic}^0(X)(\mathbb{C})$; 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 (3.1.9), 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, there are no guarantees on 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 (3.1.9) should have a solution $\{Q'_k\}_j$ with Q'_k close to $O_{0,k}$ for $k = 1, \ldots, g$ since the derivative of the Abel–Jacobi map AJ at O_0 is nonsingular by assumption. We start with $Q'_k = O_{0,k}$ as initial guesses, and then use Newton iteration until (3.1.9) 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 $Q'_1, \dots, Q'_g$ such that the linear equivalence

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

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

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

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

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 $[\sum_{k=1}^{g} Q'_k - O_0]$. 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'_k, the points $O_{0,k}$, and the support of D_0. Consider the divisors

$$\begin{aligned} D_+ &:= \sum_{k=1}^{g} Q'_k + \sum_{k=1}^{d_0-g} P_k \\ D_- &:= O_0 + \sum_{k=1}^{d_0-g} P_k, \end{aligned} \tag{3.3.3}$$

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

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

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

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

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 $E \sim \sum_k Q_k$. 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

$$\sum_{k=1}^{g} Q_k \sim E, \quad \text{where } E := 2D_0 - \Delta - \sum_{k=1}^{d_0-g} P_k \tag{3.3.7}$$

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_k. 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 resulting spaces with the value predicted by Riemann–Roch, and rectify its failure by restarting with different auxiliary points P_k.

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

$$Q \sim \sum_{k=1}^{g} Q_k \tag{3.3.11}$$

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

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

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

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

We then recover the divisor $\sum_k P_k + \sum_k Q_k$ as the intersection of the locus of zeros of the functions in Z', and then the points Q_k themselves whenever they are distinct from the chosen auxiliary points P_k. Once more, this procedure works for generic input, and we can check if we are in the generic case and rectify failure if this turns out not to be the case.

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

$$T = H^0\left(X, (2g+2)\infty_X - \textstyle\sum_{k=1}^{d_0 - g} P_k - \sum_{k=1}^{g} Q_k\right), \tag{3.3.15}$$

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_k and Q_k must satisfy, which allows us to recover the Q_k.

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 at most 10 precision bits per Jacobian operation.

3.4. **Examples.** We now present 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 $\mathrm{AJ}_{P_0}(P) \equiv b \pmod{\Lambda}$ where

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

We now apply the methods of section 3.3. We arbitrarily set

$$\begin{aligned} O_{0,1} &= (0.9163 + 0.8483i,\ 1.104 - 1.884i)\,, \\ O_{0,2} &= (0.3311 + 0.9656i,\ 2.159 - 0.3835i)\,. \end{aligned} \tag{3.4.3}$$

The first step inverts the Abel–Jacobi map to obtain

$$2^{-10}Mb = \mathrm{AJ}(\{Q_1', Q_2'\}) \tag{3.4.4}$$

where

$$\begin{aligned} Q_1' &\approx (0.9224 + 0.8521i,\ 1.103 - 1.909i)\,, \\ Q_2' &\approx (0.3257 + 0.9592i,\ 2.146 - 0.3645i)\,. \end{aligned} \tag{3.4.5}$$

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

$$2^{10}[Q_1' + Q_2' - O_{0,1} - O_{0,2}] = [Q_1 + Q_2 - 2P_0], \tag{3.4.6}$$

where

$$Q_k \approx (0.7500 \pm 0.4330i,\ -0.4419 \pm 0.7655i)\,. \tag{3.4.7}$$

Using the LLL algorithm [LLL82], we guess that the x-coordinates of Q_1 and Q_2 satisfy $4x^2 - 6x + 3 = 0$, and under this assumption we have

$$Q_k = \left(\frac{3 \pm i\sqrt{3}}{4},\ \frac{-5\sqrt{2} \pm 5i\sqrt{6}}{16}\right). \tag{3.4.8}$$

All the computations above were performed with at least 600 decimal digits. On a standard desktop machine, figuring out right number of points for the Gauss–Legendre quadrature and calculating b took less than 3 CPU seconds, and the computation of the points Q_1 and Q_2 took around 2 CPU minutes.

Example 3.4.9. The MAGMA functions `ToAnalyticJacobian` and `FromAnalyticJacobian` provide us similar functionality. However, we have found these algorithms to be sometimes numerically unstable (in v2.22-6).

For example, consider the curve with LMFDB label `169.a.169.1`, a model for the modular curve $X_1(13)$ with equation

$$X\colon y^2 = x^6 + 4x^5 + 6x^4 + 2x^3 + x^2 + 2x + 1. \tag{3.4.10}$$

We find a numerical endomorphism α with $\alpha^2 = 1$ defined over $\mathbb{Q}(\lambda)$ where $\lambda = 2\cos(2\pi/13)$, with matrix

(3.4.11)
$$M = \frac{1}{13}\begin{pmatrix} -7\lambda^5 - 8\lambda^4 + 32\lambda^3 + 27\lambda^2 - 27\lambda - 10 & -5\lambda^5 - 2\lambda^4 + 21\lambda^3 + 10\lambda^2 - 10\lambda - 9 \\ 2\lambda^5 + 6\lambda^4 - 11\lambda^3 - 17\lambda^2 + 17\lambda + 1 & 7\lambda^5 + 8\lambda^4 - 32\lambda^3 - 27\lambda^2 + 27\lambda + 10 \end{pmatrix}.$$

For a random point P, Magma is unable to compute

$$\texttt{FromAnalyticJacobian}\,(\alpha \cdot \texttt{ToAnalyticJacobian}(P, X), X)$$

in precision 600. A workaround in this case is to replace α by $\alpha + 1$ instead; it is unclear why such a modification restores numerical stability (sometimes a change of variables in the equation also suffices).

In comparison, if we set $P_0 = (0, 1)$, $P_1 = (-1, 1)$, and $O_0 = \{\infty_+, \infty_-\}$, then thanks to the above approach we can compute that

$$M\,\mathrm{AJ}_{P_0}(P_1) = \mathrm{AJ}(\{Q_1, Q_2\}), \tag{3.4.12}$$

or in other words

$$\alpha([P_1 - P_0]) = [Q_1 + Q_2 - \infty_+ - \infty_-], \tag{3.4.13}$$

where

$$\begin{aligned} Q_1 &\approx (-1.3772, 1.8730), \\ Q_2 &\approx (2.6511, 34.8995). \end{aligned} \tag{3.4.14}$$

With 600 decimal digits of accuracy, the computation takes about 1 CPU minute.

The LLL algorithm then suggests that

$$\begin{aligned} Q_1 &= (\theta^2 + 2\theta - 2,\ 11\lambda^5 + 18\lambda^4 - 43\lambda^3 - 66\lambda^2 + 26\lambda + 33), \\ Q_2 &= (-\theta^2 - \theta + 3,\ -6\lambda^5 + 6\lambda^4 + 31\lambda^3 - 19\lambda^2 - 21\lambda + 5), \end{aligned} \tag{3.4.15}$$

where $\theta = \lambda^5 - 5\lambda^3 + 6\lambda$, which holds to at least 500 decimal places.

Remark 3.4.16. In the example above, it is surprising that Q_1 and Q_2 are both defined (instead of being conjugate) over $\mathbb{Q}(\lambda)$ and that their x-coordinates are defined over the subfield $\mathbb{Q}(\theta)$. This happens because α turns out to be induced by a modular (sometimes called a *Fricke*) involution of $X_1(13)$ (to be precise, the one attached to the root of unity $e^{8\pi i/13}$), and because $X_1(13)(\mathbb{Q})$ only contains cusps, so that P_0, P_1, ∞_+, ∞_- and thus Q_1 and Q_2 are cusps.

4. Newton lift

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

$$\alpha_X \colon X \xrightarrow{\mathrm{AJ}_{P_0}} J \xrightarrow{\alpha} J \overset{\mathrm{Mum}}{\dashrightarrow} \mathrm{Sym}^g(X).$$

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 numerically we have

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

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 $X\colon y^2 = f(x)$ 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

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

with

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

We then attempt to fit a divisor $Y \subset X \times X$ defined over K to the point $\{(\widetilde{P}, \widetilde{Q}_j)\}_j$, and proceed as before. The only difference is that the divisor now interpolates this single infinitesimal point instead of many points of the form $(R, \alpha_X(R))$ with $R \in X(\mathbb{C})$.

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 fact that the matrix $M = (m_{ij})_{i,j}$ describes the action of α on the F-basis of differentials $x^j\,\mathrm{d}x/y$ implies (by an argument described in detail in the next

section) that

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

for all $k = 0, \ldots, g-1$. In this equation, the branches of the square roots are chosen so that $\sqrt{f(x)} = y(P) + O(t)$ and that $\sqrt{f(x_j)} = y(Q_j) + O(t)$ 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

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

where T denotes the 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

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

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

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

In Section 6 we will tackle the problem how to certify that α is indeed an endomorphism, and that the rational functions (4.2.7) are correct: see Example 6.1.6.

Here is another way: for genus 2 curves we have an upper bound for the degrees of $x_1(t)+x_2(t)$ and $x_1(t)x_2(t)$ as rational functions, given by

$$d := \mathrm{tr}(\alpha\alpha^\dagger) = \mathrm{tr}(RJR^{\mathsf{T}}J^{-1})/2 = \langle \alpha(\Theta), \Theta\rangle, \tag{4.2.9}$$

where $\dagger$ denotes the Rosati involution and J is the standard symplectic matrix; see van Wamelen [vW99b, §3] for more details and Remark 6.1.5 for a possible generalization to higher genus. Therefore, to deduce the pair $(x_1(t)+x_2(t), x_1(t)x_2(t))$ it is sufficient to compute $x_j(t)$ up to precision $O(t^{2d+1})$. Furthermore, we may sped up the process significantly by doing this modulo many small primes and applying a version of the Chinese remainder theorem with denominators (involving LLL).

In this example, we have $d=4$ and we deduced the pair $(x_1(t)+x_2(t), x_1(t)x_2(t))$ modulo 131 62-bit primes that split completely in $\mathbb{Q}(\sqrt{2},\sqrt{-3})$ by computing $x_j(t)$ up to precision $O(t^9)$. All together deducing $(x_1(t)+x_2(t), x_1(t)x_2(t))$ given (Q_1, Q_2) took less than 5 CPU seconds on a standard desktop machine.

(A third possible way to certify α using (4.2.7) is by following van Wamelen's approach [vW99b, §9].)

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 show how one can dispense with even this one numerical computation to obtain an exact certification algorithm for the matrix of a putative endomorphism.

5.1. **Setup.** We continue our notation but restore generality, once more allowing X to be a general curve. We may for example represent X by a plane model that is smooth at P_0 (but possibly with 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 $H^0(X,\omega_X)^*$.

We now make the additional assumption that P_0 is *not* a Weierstrass point. Then by Riemann–Roch, the map

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

is locally an isomorphism around $\{P_0,\dots,P_0\}$, in the sense that it is a birational map that restricts to an isomorphism in a neighborhood of said point.

Let $x \in F(X)$ be a local parameter for X at P_0. Then $x\colon X \to \mathbb{P}^1$ is also a rational function, and we use the same symbol for this map. Since X is smooth at P_0, we obtain a canonical point $\widetilde{P}_0 \in X(F[[x]])$ such that:

(i) $\widetilde{P}_0$ reduces to P_0 under the reduction map $X(F[[x]]) \to X(F)$, and
(ii) $x(\widetilde{P}_0) = x \in F[[x]]$.

On an affine open set $U \ni P_0$ of X 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.

Since (5.1.1) is locally an isomorphism at P_0, we can locally describe $\alpha_X(\widetilde{P}_0)$ uniquely as

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

The reduction to F of $\{\widetilde{Q}_i\}_i$ is the g-fold multiple $\{P_0, \dots, P_0\} \in \mathrm{Sym}^g(X)(F)$. The map $X^g \to \mathrm{Sym}^g(X)$ 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 $\mathrm{Sym}^g(X)(F((x)))$; 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 $F^{\mathrm{al}}((x^{1/\infty}))$ of Puiseux series over F^{al}. Since X is smooth at P_0, the lift of $\{\widetilde{Q}_i\}_i$ is even a point on X^g over the ring of integral Puiseux series $F^{\mathrm{al}}[[x^{1/\infty}]]$.

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

5.2. **Lifting procedure.** The lifting procedure to obtain this deformation algorithmically is similar to the one outlined in the previous section; here we provide complete details. 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 $i = 1, \dots, g$. (If it is more convenient, we may even work with a full echelonized basis.)

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

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

be the x-coordinates of the points $\widetilde{Q}_j$ on the graph of α above $\widetilde{P}$.

Proposition 5.2.4. *Let $\{\omega_1, \dots, \omega_g\}$ be a basis of $H^0(X, \omega_X)$, with $\omega_i = f_i \, \mathrm{d}x$ around P_0. Let $M = (m_{i,j})_{i,j}$ be the tangent representation of α with respect to the dual of this basis. Then we have*

$$\sum_{j=1}^{g} f_i(x_j) \, \mathrm{d}x_j = \sum_{j=1}^{g} m_{i,j} f_j(x) \, \mathrm{d}x \quad \text{for all } i = 1, \dots, g. \tag{5.2.5}$$

Proof. This is essentially proven by Smith [Smi05, §3.5]. Let Y be the divisor corresponding to α, and let π_1 and π_2 be the two projection maps from Y to X. Then $\alpha^* = (\pi_2)_* \pi_1^*$ (see *loc. cit.*), which in an infinitesimal neighborhood of P_0 becomes (5.2.5).

An alternative argument is as follows. By construction, we have

$$\sum_{j=1}^{g} (\widetilde{Q}_j - P_0) = \alpha(\widetilde{P}_0 - P_0). \tag{5.2.6}$$

On the tangent space, addition on the Jacobian induces the usual addition. Considering both sides of (5.2.6) over $F^{\mathrm{al}}[[x^{1/\infty}]]$ and substituting the resulting power series in the differential form ω_i, we obtain

$$\sum_{j=1}^{g} x_j^*(\omega_i) = x^*(\alpha^*(\omega_i))) \quad \text{for all } i = 1, \dots, g, \tag{5.2.7}$$

which also yields (5.2.5). □

We iteratively solve (5.2.5) as follows. We begin by computing initial expansions

$$x_j = c_{j,\nu}x^\nu + O(x^{\nu+1/e}) \tag{5.2.8}$$

where

$$\nu := \min_{i,j}(\{j/i : m_{i,j} \neq 0\}) \in \mathbb{Q}_{>0}, \tag{5.2.9}$$

and where e is the denominator of ν. Note that ν is well-defined since the matrix M has full rank; typically, but not always, we have $\nu = 1/g$. Combining the notation above with (5.2.2) we obtain

$$\begin{aligned} x f_i(x_j)\,\mathrm{d}x_j &= ((c_{j,\nu}x^\nu)^{i-1} + O(x^{i\nu}))\left(\nu c_{j,\nu}x^\nu + O(x^{\nu+1/e})\right)\mathrm{d}x \\ &= (\nu c_{j,\nu}^i x^{i\nu} + O(x^{i\nu+1/e}))\,\mathrm{d}x. \end{aligned} \tag{5.2.10}$$

Inspecting the leading terms of (5.2.5) for each i we obtain

$$\sum_{j=1}^{g}(\nu c_{j,\nu}^i x^{i\nu} + O(x^{i\nu+1/e}))\,\mathrm{d}x = \sum_{j=1}^{g} m_{i,j}(x^j + O(x^{j+1}))\,\mathrm{d}x, \tag{5.2.11}$$

therefore for all i we have

$$\nu\sum_{j=1}^{g} c_{j,\nu}^i = m_{i,i\nu}, \tag{5.2.12}$$

where $m_{i,i\nu} = 0$ if $i\nu \notin \mathbb{Z}$. The equations (5.2.12) are symmetric under the action of the permutation group S_g, and up to this action there is a unique nonzero solution by Newton's formulas, as $m_{i,i\nu} \neq 0$ for some i.

The equations (5.2.12) are of different degree with respect to the leading terms $c_{j,\nu}$. Therefore, replacing α by $\alpha + m$ with $m \in \mathbb{Z}$ will eventually result in a solution with distinct $c_{j,\nu}$. For purposes of rigorous verification it is the same to verify α as it is $\alpha + m$, so we may suppose that the values $c_{j,\nu}$ are distinct.

Having determined the expansions

$$x_j = c_{j,\nu}x^\nu + c_{j,\nu+1/e}x^{\nu+1/e} + \cdots + c_{j,\nu+n/e}x^{\nu+n/e} + O(x^{\nu+(n+1)/e}) \tag{5.2.13}$$

for $j = 1, \ldots, g$ up to some precision $n \geq 1$, we integrate (5.2.5) to iteratively solve for the next term in precision $n+1$. As at the end of the previous section, we then introduce new variables $c_{j,\nu+(n+1)/e}$ for the next term and consider the first coefficients on the left hand side of the equations (5.2.5) in which these new variables occur. Because of our echelonization and the presence of the derivative $\mathrm{d}x_j$, the exponents of x for which these coefficients occur are

$$\nu - 1 + (n+1)/e, 2\nu - 1 + (n+1)/e, \ldots, g\nu - 1 + (n+1)/e. \tag{5.2.14}$$

We obtain an inhomogeneous linear system in the new variables whose homogeneous part is described by a Vandermonde matrix in $c_{1,\nu}, \ldots, c_{g,\nu}$. This system has a unique solution since we have ensured that the latter coefficients are distinct. 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 5.2.15. In practice, we iterate the approximations x_j by successive Hensel lifting. Indeed, let F_i be the formal integral of the function f_i, and let F be the multivariate function $(F_1, \dots, F_g)$. Then the equation (5.2.5) is equivalent to solving for $x_1, \dots, x_g$ in

$$F(x_1, \dots, x_g) = \left(\sum_{j=1}^{g} m_{1,j} F_i(x), \dots, \sum_{j=1}^{g} m_{g,j} F_g(x) \right). \tag{5.2.16}$$

Our initialization is a sufficiently close approximation for the Hensel lifting process to take off.

Example 5.2.17. 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 $P_0 = (0, \sqrt{-1})$. In order to be able to display our results, we work modulo a prime above 4001 in $K = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$. We first expand

$$\widetilde{P_0} = (x, 3102 + 247x + 1714x^2 + 2082x^3 + 1505x^4 + O(x^5)). \tag{5.2.18}$$

By (5.2.9), we have $\nu = 1/2$. The equations (5.2.12) read:

$$\begin{aligned} c_{1,1/2} + c_{2,1/2} &= 2m_{1,1/2} = 0 \\ c_{1,1/2}^2 + c_{2,1/2}^2 &= 2m_{2,1} = 2\sqrt{2} \end{aligned} \tag{5.2.19}$$

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

$$c_{1,1/2} \equiv 2559 \pmod{4001}, \quad c_{2,1/2} \equiv -2559 \equiv 1442 \pmod{4001}. \tag{5.2.20}$$

Now iteratively solving the differential system (5.2.5), we find

$$\begin{aligned} \widetilde{Q_1} = (&2559x^{1/2} + 1445x + 2635x^{3/2} + O(x^2), \\ &3102 + 3916x^{1/2} + 3938x + 1271x^{3/2} + O(x^2)) \\ \widetilde{Q_2} = (&1442x^{1/2} + 1445x + 1366x^{3/2} + O(x^2), \\ &3102 + 85x^{1/2} + 3938x + 2730x^{3/2} + O(x^2)). \end{aligned} \tag{5.2.21}$$

We use these functions directly to interpolate a divisor in the next section (and we also consider the Cantor representation, involving in particular their symmetric functions).

6. Proving correctness

The procedures described in the previous sections work unimpeded for any matrix M, including those that do *not* correspond to actual endomorphisms. In order for M to represent an honest endomorphism $\alpha \in \mathrm{End}(J_K)$, we now need to fit a divisor $Y \subset X \times X$ representing the graph of α.

6.1. Fitting and verifying.

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 up until Proposition 6.1.1 below we focus on our infinitesimal versions.

Let $\pi_1, \pi_2 \colon X \times X \to X$ be the two projection maps. If the matrix M corresponds to an endomorphism, then the divisor Y traced out by the points $(\widetilde{P_0}, \widetilde{Q_j})$ has degree g with respect

to π_1 and degree d with respect to π_2 for some $d \in \mathbb{Z}_{\geq 1}$. Accordingly, we seek equations defining this divisor.

Choose an affine open $U \subset X$, with a fixed embedding into some ambient affine space. We then try to describe $D \subset U \times U$ by choosing degree bounds $n_1, n_2 \in \mathbb{Z}_{\geq 1}$ (with usually $n_2 = g$) and considering the K-vector space $K[U \times U]_{\leq (n_1,n_2)}$ of regular functions on $U \times U$ that are of degree at most n_1 when considered as functions on $U \times \{P_0\}$ and degree at most n_2 on $\{P_0\} \times U$. Let $N := \dim_K K[U \times U]_{\leq (n_1,n_2)}$ be the dimension of this space of functions. We then develop the points $(\widetilde{P}_0, \widetilde{Q}_j)$ to precision $N + m$ for some suitable global margin $m \geq 2$, and compute the subspace $Z \subseteq K[U \times U]_{\leq (n_1,n_2)}$ of functions that annihilates all these points to the given precision. If M is the representation of an actual endomorphism, then we will in this way eventually find equations satisfied by $(\widetilde{P}_0, \widetilde{Q}_j)$ by increasing n_1, n_2.

We show how to verify that a putative set of such equations is in fact correct. Assume that Z contains a nonzero function (on $U \times U$), and let E be the subscheme of $X \times X$ defined by the vanishing of Z.

Proposition 6.1.1. *Suppose that the second projection π_2 maps E surjectively onto X and that the intersection of E with $\{P_0\} \times X$ consists of a single point with multiplicity g. Then M defines an endomorphism of J_K.*

Proof. We have ensured that a nonzero function on $U \times U$ vanishes at E, so E cannot be all of $X \times X$. Yet the subscheme E cannot be of (Krull) dimension 0 either because E surjects to X. Therefore E is of dimension 1.

Let $Y \subset E$ be the union of the irreducible components of dimension 1 of E that contain the points $(\widetilde{P}_0, \widetilde{Q}_j)$. Because the degree of the projections to the second factor do not depend on the chosen base point, our hypothesis on the intersection of E with $\{P_0\} \times X$ ensures that $E \smallsetminus Y$ consists of a union of points and vertical divisors: these define the trivial endomorphism.

The subscheme $Y \subset X \times X$ defines a (Weil or Cartier) divisor whose projection to the second component is of degree g, and such a divisor defines an endomorphism [Smi05, §3.5]. The fact that Y contains the points $(\widetilde{P}_0, \widetilde{Q}_j)$, which we chose to satisfy (5.2.5) over K with a suitable nontrivial margin, then ensures without any further verification the endomorphism enduced by Y has tangent representation M. □

The hypotheses of Proposition 6.1.1 can be verified algorithmically, for example by using Gröbner bases. Indeed, the property that π_2 maps E surjectively to X can be verified by calculating a suitable elimination ideal, and the degree of the intersection with $\{P_0\} \times X$ is the dimension over K of the space of global sections of a zero-dimensional scheme. If desired, the construction of the divisor Y from E is also effectively computable, calculating irreducible components via primary decomposition.

In a day-and-night algorithm, we would alternate the step of seeking to fit a divisor (running through an enumeration of the possible values (n_1, n_2) above) 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 works with interval arithmetic to keep track of errors in the numerical integration). On the other hand, if M does correspond to an endomorphism, then eventually a divisor will be found, since increasing n_1 and n_2 eventually yields generators of the defining ideal of the divisor in $U \times U$ defined by M, which we can prove to be correct by

using Proposition 6.1.1. Therefore we have a deterministic algorithm that takes a putative endomorphism represented by a matrix $M \in \mathrm{M}_g(F^{\mathrm{al}})$ and returns true or false according to whether or not M represents an endomorphism of the Jacobian.

Remark 6.1.2. More sophisticated versions of the approach above are possible, for example by using products of Riemann–Roch spaces instead of using the square of the given ambient space. Additionally, the algorithm can be significantly sped up by determining the divisor Y modulo many small primes and applying a version of the Chinese remainder theorem with denominators (involving LLL) to recover the defining ideal of Y from its reductions.

Remark 6.1.3. Conversely, if we have a divisor $Y \subset X \times X$ (not necessarily obtained from the Taylor or Puiseux method), we can compute the tangent representation of the corresponding endomorphism as follows. Choose a point P_0 on X such that the intersection of $\{P_0\} \times X$ with Y is proper, with

$$Y \cap (\{P_0\} \times X) = \{Q_1, \dots, Q_e\} \tag{6.1.4}$$

the points Q_e taken with multiplicity. Then we can again develop the points Q_j infinitesimally, and as long as (5.2.5) is verified for the initial terms, the divisor Y induces an endomorphism with M as tangent representation.

Remark 6.1.5. While the above method will terminate as long as M corresponds to an actual endomorphism, Khuri-Makdisi has indicated an upper bound D of the degree of π_2 to us, namely $(g-1)!\,\mathrm{tr}(\alpha\alpha^\dagger)$, where $\dagger$ denotes the Rosati involution. Such an upper bound would allow us to rule out a putative tangent matrix M as one *not* corresponding to an endomorphism without resort to a numerical computation.

Indeed, having calculated the upper bound D, we can take $(n_1, n_2) = (D, g)$ above, and a suitably large N can be determined by applying a version of the Riemann-Roch theorem for surfaces. After determining the resulting equations, Proposition 6.1.1 can be used to tell us conclusively whether we actually obtain a suitable divisor or not. However, since our day-and-night algorithm is provably correct and functions very well in practice, we have not elaborated these details or implemented this approach.

Example 6.1.6. We revisit our running example one last time. Recall that

$$X\colon y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1 \tag{6.1.7}$$

and

$$M = \begin{pmatrix} 0 & \sqrt{2} \\ \sqrt{2} & 0 \end{pmatrix}. \tag{6.1.8}$$

While X may not have an obvious Weierstrass point, we can apply a trick that is useful for general hyperelliptic curves. Instead of X, we consider the quadratic twist of X by -1, namely

$$X'\colon y^2 = -(x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1), \tag{6.1.9}$$

which has the rational non-Weierstrass point $P_0 = (0, 1)$. While the curves X and X' are not isomorphic, their endomorphism rings are, because the isomorphism $(x, y) \to (x, \sqrt{-1}y)$ induces a scalar multiplication on global differentials, which disappears when changing basis by it.

We find a divisor with $d = 4$ with respect to π_2 (matching Khuri-Makdisi's estimate $(g-1)!\operatorname{tr}(\alpha\alpha^\dagger) = 4$ from Remark 6.1.5). Using a margin $m = 16$, the number of terms needed in the Puiseux expansion to find enough equations of Y equals 48. On a standard desktop machine, this calculation took less than 3 CPU seconds.

The equations defining the divisor Y representing M are quite long and unpleasant, so that we cannot reproduce them here. As mentioned in the introduction, they are available in the repository that contains our implementation. However, we can indicate the induced divisor mapped to $\mathbb{P}^1 \times \mathbb{P}^1$ under the hyperelliptic involution: it is given by

(6.1.10)
$$\begin{aligned}
&4x_2^4x_1^8 + 4x_2^4x_1^7 + (-96\sqrt{2}+29)x_2^4x_1^6 + 2(48\sqrt{2}-9)x_2^4x_1^5 + (-312\sqrt{2}+1193)x_2^4x_1^4 \\
&+ 4(216\sqrt{2}-891)x_2^4x_1^3 + 4(-210\sqrt{2}+959)x_2^4x_1^2 + 4(84\sqrt{2}-440)x_2^4x_1 + 4(-12\sqrt{2}+73)x_2^4 \\
&+ 4(2\sqrt{2}+2)x_2^3x_1^8 + 4(-39\sqrt{2}-65)x_2^3x_1^7 + 4(107\sqrt{2}+597)x_2^3x_1^6 + 4(-120\sqrt{2}-1864)x_2^3x_1^5 \\
&+ 4(152\sqrt{2}+2649)x_2^3x_1^4 + 4(-243\sqrt{2}-1945)x_2^3x_1^3 + 4(223\sqrt{2}+776)x_2^3x_1^2 + 4(-84\sqrt{2}-166)x_2^3x_1 \\
&+ 4(10\sqrt{2}+24)x_2^3 + 4(-2\sqrt{2}+2)x_2^2x_1^8 + 2(164\sqrt{2}+51)x_2^2x_1^7 + 2(-664\sqrt{2}-1543)x_2^2x_1^6 \\
&+ 4(340\sqrt{2}+3770)x_2^2x_1^5 + 2(-348\sqrt{2}-13363)x_2^2x_1^4 + 2(484\sqrt{2}+10499)x_2^2x_1^3 \\
&+ 4(-196\sqrt{2}-1841)x_2^2x_1^2 + 4(20\sqrt{2}+301)x_2^2x_1 + 4(12\sqrt{2}-46)x_2^2 + 4(-5\sqrt{2}-9)x_2x_1^8 \\
&+ 4(-24\sqrt{2}+12)x_2x_1^7 + 4(358\sqrt{2}+226)x_2x_1^6 + 4(-303\sqrt{2}-2210)x_2x_1^5 + 4(63\sqrt{2}+4242)x_2x_1^4 \\
&+ 4(-508\sqrt{2}-2960)x_2x_1^3 + 4(538\sqrt{2}+623)x_2x_1^2 + 4(-139\sqrt{2}+40)x_2x_1 + (8\sqrt{2}+33)x_1^8 \\
&+ 4(-2\sqrt{2}+4)x_1^7 + 4(-106\sqrt{2}+19)x_1^6 + 2(164\sqrt{2}+807)x_1^5 - 3348x_1^4 + 4(166\sqrt{2}+515)x_1^3 \\
&+ (-720\sqrt{2}-223)x_1^2 + 4(46\sqrt{2}-24)x_1 = 0.
\end{aligned}$$

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

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

This can be done as follows. Choose an affine model of $f(x,y) = 0$ for X. Then a generic divisor of degree g on X can be described by equations of the form

$$\begin{aligned}
x^g + a_1x^{g-1} + \cdots + a_{g-1}x + a_g &= 0, \\
y = b_1x^{g-1} + \cdots + b_{g-1}x + b_g,
\end{aligned} \tag{6.2.2}$$

which we call a Cantor representation. Using f one can determine g equations in the a_i and b_i that conversely determine when a generic point of the form (6.2.2) defines a divisor of degree g on X.

After fixing our origin in some point P_0 as before, (6.2.2) also gives a description of generic divisors of degree 0 on X. By taking a sufficiently precise development $(\widetilde{P}_0, \widetilde{Q}_j)$, we can obtain a_i and b_i as functions in $K(X)$, increasing this precision as we try functions of larger degree. In the end, we can verify these rational functions by checking that the equations (6.2.2) are satisfied and additionally checking that the corresponding tangent representation is correct. As above, we see that for this final step it suffices to check that the initial terms of the Puiseux approximation cancel (6.2.2).

6.3. **Splitting the Jacobian.** The algorithms above can be generalized to the verification of the existence of homomorphisms $\operatorname{Jac}(X) \to \operatorname{Jac}(Y)$, 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 reconstructing these genus 2 curves from their period matrices after choosing a suitable polarization.

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 (typically small) precision—for hyperelliptic curves, one may use Molin's double exponentiation algorithm [Mol10, Théorème 4.3]—we may also deduce that the geometric representation $R \in \mathrm{M}_{2g}(\mathbb{Z})$ 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 then also recover the endomorphism ring by considering possible superorders and ruling them out.

Example 6.4.1. For example, take $X\colon y^2 = -3x^6 + 8x^5 - 30x^4 + 50x^3 - 71x^2 + 50x - 27$ to be a simplified Weierstrass model for the genus 2 curve with LMFDB label `961.a.961.2`. We can then verify that the endomorphism algebra is $\mathbb{Q}(\sqrt{5})$, and $\sqrt{5}$ is 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 the superorder $\mathbb{Z}[(1+\sqrt{5})/2]$, as $1 + R \notin 2M_4(\mathbb{Z})$.

7. Upper bounds

In this section, we show how determining Frobenius action on X for a large set of primes often quickly leads to sharp upper bounds on the dimension of the endomorphism algebra of the Jacobian J of X.

7.1. **Upper bounds in genus 2 via Néron–Severi rank.** We begin with upper bounds for curves of genus 2. Lombardo [Lom16, §6] has already given a practical method for these curves; we consider a slightly different approach.

Suppose X has genus 2. Then its Jacobian J is naturally a principally polarized abelian *surface*; let $\dagger$ denote its 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 $\rho(J) := \operatorname{rk} \mathrm{NS}(J)$. By Albert's classification of endomorphism algebras,

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

So if we had a way to compute $\rho(J^{\mathrm{al}})$, we could limit the number of possibilities for $\mathrm{End}(J^{\mathrm{al}})_{\mathbb{R}}$, and hit it exactly in many cases including the typical case when $\mathrm{End}(J^{\mathrm{al}}) = \mathbb{Z}$. To compute $\rho(J^{\mathrm{al}})$, we look modulo primes.

Let $\mathfrak{p}$ be a nonzero prime of (the ring of integers of) F with residue field $\mathbb{F}_{\mathfrak{p}}$. Let $\mathbb{F}_{\mathfrak{p}}^{\mathrm{al}}$ be an algebraic closure of $\mathbb{F}_{\mathfrak{p}}$. Suppose that X has good reduction $X_{\mathbb{F}_{\mathfrak{p}}}$ at $\mathfrak{p}$. We write $J_{\mathfrak{p}} = J_{\mathbb{F}_{\mathfrak{p}}}$ for the reduction of J modulo $\mathfrak{p}$ and $J_{\mathfrak{p}}^{\mathrm{al}} = J_{\mathbb{F}_{\mathfrak{p}}^{\mathrm{al}}}$ its base change to $\mathbb{F}_{\mathfrak{p}}^{\mathrm{al}}$. (There is no ambiguity in this notation, as $(J^{\mathrm{al}})_{\mathfrak{p}}$ does not make sense.) Then there is a natural injective specialization homomorphism of $\mathbb{Z}$-lattices

$$s_p \colon \mathrm{NS}(J^{\mathrm{al}}) \hookrightarrow \mathrm{NS}(J_{\mathfrak{p}}^{\mathrm{al}}), \tag{7.1.3}$$

so $\rho(J^{\mathrm{al}}) \leq \rho(J_{\mathfrak{p}}^{\mathrm{al}})$.

Let $q = \#\mathbb{F}_{\mathfrak{p}}$, let $\mathrm{Frob}_{\mathfrak{p}}$ be the q-power Frobenius automorphism, and let $\ell \nmid q$ be prime. Let

$$\begin{aligned} c_{\mathfrak{p}}(T) &:= \det\left(1 - \mathrm{Frob}_{\mathfrak{p}}\, T \mid H^1_{\text{ét}}(J^{\mathrm{al}}, \mathbb{Q}_\ell)\right) \\ &= \det\left(1 - \mathrm{Frob}_{\mathfrak{p}}\, T \mid H^1_{\text{ét}}(X^{\mathrm{al}}, \mathbb{Q}_\ell)\right) \\ &= 1 + a_1 T + a_2 T^2 + a_1 q T^3 + q^2 T^4 \in 1 + T\mathbb{Z}[T]. \end{aligned} \tag{7.1.4}$$

Then

$$\begin{aligned} c_{\mathfrak{p}}^{\wedge 2}(T) &:= \det\left(1 - \mathrm{Frob}_{\mathfrak{p}}\, T \mid H^2_{\text{ét}}(J^{\mathrm{al}}, \mathbb{Q}_\ell)\right) \\ &= \det\left(1 - \mathrm{Frob}_{\mathfrak{p}}\, T \mid \textstyle\bigwedge^2 H^1_{\text{ét}}(J^{\mathrm{al}}, \mathbb{Q}_\ell)\right) \\ &= (1 - qT)^2(1 + (2q - a_2)T + (2q + a_1^2 - 2a_2)qT^2 + (2q - a_2)q^2T^3 + q^4T^4). \end{aligned} \tag{7.1.5}$$

The Tate conjecture holds for abelian varieties over finite fields [Tat66], and it relates $\mathrm{NS}(J_{\mathbb{F}_{\mathfrak{p}}})$, as a lattice with its intersection form, with $c_{\mathfrak{p}}^{\wedge 2}(T)$ in the following way.

Proposition 7.1.6. *The following statements hold.*

(a) *$\rho(J_{\mathfrak{p}}^{\mathrm{al}})$ is equal to the number of reciprocal roots of $c_{\mathfrak{p}}^{\wedge 2}(T)$ of the form q times a root of unity.*

(b) *We have*

$$\mathrm{disc}(\mathrm{NS}(J_{\mathfrak{p}})) = \lim_{s \to 1} \frac{(-1)^{\rho(J_{\mathfrak{p}})-1} c_{\mathfrak{p}}^{\wedge 2}(q^{-s})}{q(1 - q^{1-s})^{\rho(J_{\mathfrak{p}})}} \bmod \mathbb{Q}^{\times 2}. \tag{7.1.7}$$

Proof. For part (a), we know that $\rho(X_{\mathfrak{p}})$ is equal to the multiplicity of q as a reciprocal root of $c_{\mathfrak{p}}^{\wedge 2}(T)$ 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 by work of Milne [Theorem 6.1, Mil75a, Mil75b], which implies (b) after simplification using that $\#\,\mathrm{Br}(X)$ is a perfect square [LLR05]. □

We will use one other ingredient: we can rule out the possibility that J^{al} has CM by looking at $c_{\mathfrak{p}}(T)$ as follows.

Lemma 7.1.8. *Suppose that $\mathrm{End}(J^{\mathrm{al}})_{\mathbb{Q}} = L$ is a quartic CM field. Let $\mathfrak{p}$ be a prime of F of good reduction for X, let p be the prime of $\mathbb{Q}$ below $\mathfrak{p}$, and suppose that p splits completely in L. Then $c_{\mathfrak{p}}(T)$ is irreducible and*

$$L \simeq \mathbb{Q}[T]/(c_{\mathfrak{p}}(T)). \tag{7.1.9}$$

Proof. Suppose that the CM for J is defined over $F' \supseteq F$, so $\mathrm{End}(J_{F'})_{\mathbb{Q}} = L$. Let $\mathfrak{p}'$ be a prime above $\mathfrak{p}$ in F'. Then by Oort [Oor88, (6.5.e)], if p splits in L then $J_{\mathbb{F}_\mathfrak{p}}$ is ordinary, so $\mathrm{End}(J_{\mathbb{F}_{\mathfrak{p}'}})_{\mathbb{Q}} = L$. 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], $\mathbb{Q}[\pi'] = L$ and in particular the characteristic polynomial of π' is irreducible. But π' is a power of π, so we have the inclusions $L \supseteq \mathbb{Q}[\pi] \supseteq \mathbb{Q}[\pi'] = L$, and the lemma follows. □

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

- If $\rho(J^{\mathrm{al}})$ is even, then by Charles [Cha14, Theorem 1] (part (2) cannot occur) there are infinitely many primes such that $\rho(J^{\mathrm{al}}) = \rho(J^{\mathrm{al}}_\mathfrak{p})$.
- If $\rho(J^{\mathrm{al}})$ is odd, then also by Charles [Cha14, Proposition 18] (in our setting we must have $E = \mathbb{Q}$), there are infinitely many pairs of primes $(\mathfrak{p}_1, \mathfrak{p}_2)$ such that

$$\rho(J^{\mathrm{al}}) + 1 = \rho(J_{\mathbb{F}^{\mathrm{al}}_{\mathfrak{p}_1}}) = \rho(J_{\mathbb{F}^{\mathrm{al}}_{\mathfrak{p}_2}}) \tag{7.1.10}$$

$$\mathrm{disc}(\mathrm{NS}(J_{\mathbb{F}^{\mathrm{al}}_{\mathfrak{p}_1}})) \not\equiv \mathrm{disc}(\mathrm{NS}(J_{\mathbb{F}^{\mathrm{al}}_{\mathfrak{p}_2}})) \bmod \mathbb{Q}^{\times 2}. \tag{7.1.11}$$

By (7.1.3), we then seek out the minimum values of $\rho(J_{\mathbb{F}^{\mathrm{al}}_\mathfrak{p}})$ over the first few primes $\mathfrak{p}$ of good reduction; and for those where equality holds, we check (7.1.11) using (7.1.7), improving our upper bound by 1 when the congruence fails. This upper bound for $\rho(J^{\mathrm{al}})$ gives an upper bound for $\mathrm{End}(J^{\mathrm{al}})_{\mathbb{Q}}$ by (7.1.2), and a guess for $\mathrm{End}(J^{\mathrm{al}})_{\mathbb{R}}$ except when $\rho(J^{\mathrm{al}}) = 2$. For example, this approach allows us to quickly rule out the possibility that J^{al} has quaternionic multiplication (QM) by showing that $\rho(J^{\mathrm{al}}) \leq 2$.

To conclude, suppose that we are in the remaining case where, after many primes $\mathfrak{p}$, we compute $\rho(J^{\mathrm{al}}) \leq 2$ and we believe that equality holds. Then the subalgebra $L_0 \subseteq \mathrm{End}(J^{\mathrm{al}})_{\mathbb{Q}}$ 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 $\rho(J^{\mathrm{al}}) = 1$ or we will have certified that the Rosati-fixed endomorphism algebra L_0 is of dimension 2.
(2) Next, we check if L_0 is a field by factoring the minimal polynomial of the endomorphism generating L_0 over $\mathbb{Q}$. If $L_0 \simeq \mathbb{Q} \times \mathbb{Q}$ 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 L_0 is a (necessarily real) quadratic field. Then by (7.1.2) 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 [Lom16, §6.3], and we refer to his work for a careful exposition.

In practice, this method is very efficient to find sharp upper bounds, using only a few small primes.

Example 7.1.12. While computing the upper bound for all 66 158 genus 2 curves in the LMFDB database, we only had to study their reductions for $p \leq 53$ and for more than 96% of the curves $p \leq 19$ was sufficient. The unique curve requiring $p = 53$ was the curve `870400.a.870400.1`: the prime $p = 53$ is the first prime of good reduction for which the 2

elliptic curve factors are not geometrically isogenous modulo p. Altogether, computing these upper bounds took less than 7 CPU minutes.

7.2. **Endomorphism algebras over finite fields.** Starting in this section, we now consider upper bounds in higher genus. In this section, we compute the dimension of the geometric endomorphism algebra of an abelian variety over a finite field from the characteristic polynomial of Frobenius. We will apply this to reductions of an abelian variety in the next sections.

First a bit of notation. Let R be a (commutative) domain and let M be a free R-module of finite rank n. Let $\pi \in \mathrm{End}_R(M)$ be an R-linear operator, and let

$$c(T) = \det(1 - \pi T \mid M) \in 1 + TR[T] \tag{7.2.1}$$

be its characteristic polynomial acting on M. For $r \geq 1$, we define

$$\begin{aligned} c^{(r)}(T) &:= \det(1 - \pi^r T \mid M) \\ c^{\otimes r}(T) &:= \det(1 - \pi^{\otimes r} T \mid M^{\otimes r}) \end{aligned} \tag{7.2.2}$$

We have $\deg c^{(r)}(T) = \deg c(T) = n$ and $\deg c^{\otimes r}(T) = n^r$. If $c(T) = \prod_{i=1}^n (1 - z_i T)$ with $z_i \in R$, then $c^{(r)}(T) = \prod_{i=1}^n (1 - z_i^r T)$ and

$$c^{\otimes r}(T) = \prod_{1 \leq i_1, \dots, i_r \leq n} (1 - z_{i_1} \cdots z_{i_r} T). \tag{7.2.3}$$

We may compute $c^{\otimes 2}$ as a polynomial resultant

$$c^{\otimes 2}(T) := \mathrm{Res}_z(c(z), z^n c(T/z)) \in \mathbb{Z}[T]. \tag{7.2.4}$$

Let A be an abelian variety over the finite field $\mathbb{F}_q$ with $\dim A = g$, let $A^{\mathrm{al}} = A_{\mathbb{F}_q^{\mathrm{al}}}$ be its base change to an algebraic closure $\mathbb{F}_q^{\mathrm{al}}$, and let Frob_q be the q-power Frobenius automorphism. We write

$$c(T) := \det(1 - \mathrm{Frob}_q T \mid H^1_{\text{ét}}(A^{\mathrm{al}}, \mathbb{Q}_\ell)) \in 1 + T\mathbb{Z}[T] \tag{7.2.5}$$

for a prime $\ell \nmid q$ (with $c(T)$ independent of ℓ). Then $\deg c = 2g$. By the Riemann hypothesis (a theorem in this setting), the reciprocal roots of the polynomial $c^{\otimes 2}(T)$ have complex absolute value q. Factor

$$c^{\otimes 2}(T) = h(T) \prod_i \Phi_{k_i}(qT), \tag{7.2.6}$$

over $\mathbb{Z}[T]$ where $\Phi_{k_i}(T)$ is a cyclotomic polynomial (the minimal polynomial of a primitive k_ith root of unity) for each i and $h(T)$ is a polynomial with no reciprocal roots of the form q times a root of unity. (In the factorization (7.2.6), we allow repetition $k_i = k_j$ for $i \neq j$.)

We now recall a consequence of the (proven) Tate conjecture suitable for our algorithmic purposes.

Lemma 7.2.7. *The following statements hold.*

(a) *For all $r \geq 1$, factoring as in (7.2.6) we have*

$$\dim_{\mathbb{Q}} \mathrm{End}(A_{\mathbb{F}_{q^r}})_{\mathbb{Q}} = \sum_{k_i \mid r} \deg \Phi_{k_i}. \tag{7.2.8}$$

(b) *Let $k := \mathrm{lcm}\{k_i\}_i$. Then $\mathbb{F}_{q^k}$ is the minimal field over which $\mathrm{End}(A^{\mathrm{al}})$ is defined.*

Proof. Let $r \geq 1$. The Tate conjecture (proven by Tate [Tat66, Theorem 4]) applied to $A \times A$ over $\mathbb{F}_{q^r}$ implies

$$\operatorname{End}(A_{\mathbb{F}_{q^r}}) \otimes \mathbb{Q}_\ell \simeq (H^1_{\text{ét}}(A^{\text{al}}, \mathbb{Q}_\ell)^{\otimes 2}(1))^{\operatorname{Gal}(\mathbb{F}_q^{\text{al}} \mid \mathbb{F}_{q^r})}. \tag{7.2.9}$$

Factoring $c(T) = \prod_i (1 - z_i T) \in \mathbb{C}[T]$, so that $c^{\otimes 2}(T) = \prod_{i,j}(1 - z_i z_j T)$, we have

$$\begin{aligned} \dim_{\mathbb{Q}} \operatorname{End}(A_{\mathbb{F}_{q^r}})_{\mathbb{Q}} &= \#\{(i,j) : (z_i z_j)^r = q^r\} \\ &= \#\{(i,j) : z_i z_j = \zeta q \text{ with } \zeta^r = 1\} \\ &= \sum_{k_i \mid r} \deg \Phi_{k_i}. \end{aligned} \tag{7.2.10}$$

(Working over $\mathbb{F}_q$, in Tate's notation we have $\dim_{\mathbb{Q}} \operatorname{End}(A_{\mathbb{F}_q})_{\mathbb{Q}} = r(f,f)$, where f is the characteristic polynomial of Frobenius and $r(f,f)$ is the multiplicity of the root q in $f^{\otimes 2}$.) This proves (a).

The sum in (7.2.10) attains its maximum value for the first time when $r = k = \operatorname{lcm}_i\{k_i\}_i$, and by maximality we have $\operatorname{End}(A^{\text{al}}) = \operatorname{End}(A_{\mathbb{F}_{q^k}})$, which proves (b). □

We will make use of the following more specialized statement.

Corollary 7.2.11. *Suppose that $c(T)$ is separable and that the subgroup of $\overline{\mathbb{Q}}^\times$ generated by the (reciprocal) roots is torsion free. Then all endomorphisms of A^{al} are defined over $\mathbb{F}_q$ (i.e., $k = 1$) and*

$$\dim_{\mathbb{Q}} \operatorname{End}(A)_{\mathbb{Q}} = 2 \dim A.$$

Proof. Factor $c(T) = \prod_{i=1}^{2 \dim A}(1 - z_i T)$ over $\overline{\mathbb{Q}}$. Since $c(T)$ is separable, its reciprocal roots $z_i \in \overline{\mathbb{Q}}^\times$ are distinct. Suppose that $z_i z_j = \zeta q$ where ζ is a root of unity. By the (proven) Riemann hypothesis for abelian varieties, associated to z_i is a reciprocal root $z_{i'}$ such that $z_i z_{i'} = q$. By separability, the index i' is uniquely determined by i.

We now have $z_j / z_{i'} = \zeta$. Therefore $\zeta = 1$ since the subgroup generated by the roots is torsion free. By distinctness of the roots we obtain $i' = j$. So among the reciprocal roots $z_i z_j$ of $c^{\otimes 2}(T)$ there are exactly $2 \dim A$ pairs (i,j) with $z_i z_j = q$. We have shown that in the factorization (7.2.6) there are $2 \dim A$ factors $\Phi_1(qT) = 1 - qT$, all with $k_i = 1$, and no other cyclotomic factors. The result then holds by Lemma 7.2.7(a). □

Lemma 7.2.7 immediately implies that

$$\dim_{\mathbb{Q}} \operatorname{End}(A^{\text{al}})_{\mathbb{Q}} = \sum_i \deg \Phi_{k_i} \tag{7.2.12}$$

so we have direct access to the dimension of the geometric endomorphism algebra from the characteristic polynomial of Frobenius.

Remark 7.2.13. Although we will not use this in what follows, we can upgrade Lemma 7.2.7 from dimensions to a full description of the endomorphism algebra itself up to isomorphism by the use of Honda–Tate theory, as follows. Factor

$$c(T) = c_1(T)^{m_1} \cdots c_t(T)^{m_t} \tag{7.2.14}$$

where c_i are distinct, irreducible polynomials in $\mathbb{Z}[T]$. Applying Honda–Tate theory, see for example Waterhouse [Wat69, Chapter 2] and Waterhouse–Milne [WM71, Theorem 8], each irreducible polynomial $c_i(T)$ determines (by the p-adic valuation of its coefficients) a division

algebra B_i over $\mathbb{Q}$ such that B_i is central over the field $L_i := \mathbb{Q}[T]/(c_i(T))$ and $e_i^2 := \dim_{L_i} B_i$ has $e_i \mid m_i$; these combine to give

$$\operatorname{End}(A)_{\mathbb{Q}} \simeq B_1^{n_1} \times \ldots \times B_t^{n_t} \tag{7.2.15}$$

where $n_i = m_i/e_i$. This decomposition of the endomorphism algebra corresponds to the decomposition of A up to isogeny over $\mathbb{F}_q$ as

$$A \sim A_1^{n_1} \times \ldots \times A_t^{n_t} \tag{7.2.16}$$

where the abelian varieties A_i over $\mathbb{F}_q$ are simple and pairwise nonisogenous over $\mathbb{F}_q$, and $\operatorname{End}(A_i)_{\mathbb{Q}} \simeq B_i$.

We can apply this to compute the structure of the geometric endomorphism algebra by computing k as in Lemma 7.2.7 and applying the above to $c^{(k)}(T)$.

To conclude, we extract another description of the dimension of the endomorphism algebra, again due to Tate.

Lemma 7.2.17. *Factor $c(T) = \prod_i^s (1 - z_i T)^{m(z_i)} \in \mathbb{C}[T]$ with $z_i \in \mathbb{C}$ distinct. Then*

$$\dim_{\mathbb{Q}} \operatorname{End}(A)_{\mathbb{Q}} = \sum_{i=1}^{s} m(z_i)^2. \tag{7.2.18}$$

Proof. See Tate [Tat66, Theorem 1(a), Proof of Theorem 2(b)]; in his notation $f = c$ and the right hand side is $r(f, f)$. □

7.3. **Upper bounds in higher genus: decomposition into powers.** In the next two sections, we discuss how to produce tight upper bounds on the dimension of the geometric endomorphism algebra for a general abelian variety, under certain hypotheses. Our approach will be analogous to section 7.1, however, instead of studying the reduction homomorphism induced on the Néron–Severi lattice, we will study the reduction homomorphism induced on the endomorphism rings themselves.

These bounds come in two phases. In the first phase, described in this section, we describe a decomposition of an abelian variety over a number field into powers of geometrically simple abelian varieties. In the next phase, described in the next section, we refine this decomposition to bound the dimension of the geometric endomorphism algebra by examination of the center.

We work in slightly more generality in these two sections than in the rest of the paper. Let A be an abelian variety of a number field F (not necessarily the Jacobian of a curve). Let F_A be the minimal field over which $\operatorname{End}(A)$ is defined. Let $\mathfrak{p}$ be a nonzero prime of (the ring of integers) of F, let $\mathbb{F}_{\mathfrak{p}}$ be its residue field with $q = \#\mathbb{F}_{\mathfrak{p}}$, and let $\operatorname{Frob}_{\mathfrak{p}}$ be the q-power Frobenius automorphism. For $r \geq 1$, we denote $\mathbb{F}_{\mathfrak{p}^r} \supseteq \mathbb{F}_{\mathfrak{p}}$ the finite extension of degree r in an algebraic closure $\mathbb{F}_{\mathfrak{p}}^{\mathrm{al}}$.

Suppose that A has good reduction $A_{\mathfrak{p}}$ at $\mathfrak{p}$. Write

$$c_{\mathfrak{p}}(T) := \det(1 - \operatorname{Frob}_{\mathfrak{p}} T \mid H^1_{\text{ét}}(A_{\mathfrak{p}}^{\mathrm{al}}, \mathbb{Q}_\ell)) \in 1 + T\mathbb{Z}[T] \tag{7.3.1}$$

for the characteristic polynomial of $\operatorname{Frob}_{\mathfrak{p}}$ acting on the first ℓ-adic étale cohomology group (independent of $\ell \nmid q$).

The reduction (specialization) of an endomorphism modulo $\mathfrak{p}$ induces an injective ring homomorphism

$$s_{\mathfrak{p}}\colon \mathrm{End}(A^{\mathrm{al}}) \hookrightarrow \mathrm{End}(A^{\mathrm{al}}_{\mathfrak{p}}). \tag{7.3.2}$$

Therefore $\dim_{\mathbb{Q}} \mathrm{End}(A^{\mathrm{al}})_{\mathbb{Q}} \leq \dim_{\mathbb{Q}} \mathrm{End}(A^{\mathrm{al}}_{\mathfrak{p}})_{\mathbb{Q}}$. However, unless A is a CM abelian variety, this inequality will always be strict, so we undertake a more careful analysis.

Up to isogeny over F_A, we factor

$$A_{F_A} \sim A_1^{n_1} \times \cdots \times A_t^{n_t} \tag{7.3.3}$$

where A_i are geometrically simple and pairwise nonisogenous abelian varieties over F_A. Let $B_i := \mathrm{End}(A_i^{\mathrm{al}})_{\mathbb{Q}}$ be the geometric endomorphism algebra of A_i, let $L_i := Z(B_i)$ be the center of B_i, and write $e_i^2 := \dim_{L_i}(B_i)$ with $e_i \in \mathbb{Z}_{\geq 1}$. We have

$$\mathrm{End}(A^{\mathrm{al}})_{\mathbb{Q}} \simeq \mathrm{M}_{n_1}(B_1) \times \ldots \times \mathrm{M}_{n_t}(B_t). \tag{7.3.4}$$

For the prime $\mathfrak{p}$, we define $k_{\mathfrak{p}}$ to be the smallest integer such that $\mathrm{End}(A^{\mathrm{al}}_{\mathfrak{p}})$ is defined over $\mathbb{F}_{\mathfrak{p}^{k_{\mathfrak{p}}}}$. The polynomial $c_{\mathfrak{p},i}^{(k_{\mathfrak{p}})}(T)$ (see (7.2.2)) is the Frobenius polynomial for A_i over $\mathbb{F}_{\mathfrak{p}^{k_{\mathfrak{p}}}}$.

Proposition 7.3.5. *The following statements hold.*

(a) *For every $i = 1, \ldots, t$, there exists $g_{\mathfrak{p},i}(T) \in 1 + T\mathbb{Z}[T]$ such that*

$$c_{\mathfrak{p},i}^{(k_{\mathfrak{p}})}(T) = g_{\mathfrak{p},i}(T)^{e_i}. \tag{7.3.6}$$

(b) *We have*

$$2\sum_{i=1}^{t} e_i n_i^2 \dim A_i = \sum_{i=1}^{t} e_i^2 n_i^2 \deg g_{\mathfrak{p},i} \leq \dim_{\mathbb{Q}} \mathrm{End}(A^{\mathrm{al}}_{\mathfrak{p}})_{\mathbb{Q}} \tag{7.3.7}$$

and equality is obtained in (7.3.7) if and only if the polynomials $g_{\mathfrak{p},i}(T)$ in (a) *are separable and pairwise coprime.*

Proof. We begin by proving (a), and for this purpose we may assume $A = A_i$. Following Zywina [Zyw14, §2.3], let F_A^{conn} be the smallest extension of F such that the ℓ-adic monodromy group associated to A is connected over F_A^{conn}. Then F_A^{conn} is Galois over F and $F_A^{\mathrm{conn}} \supseteq F_A$, so all endomorphisms of A are defined over F_A^{conn}. If $F = F_A^{\mathrm{conn}}$, then (a) is proven by Zywina [Zyw14, Lemma 6.3(i)]: part (i) (but not the rest of his Lemma 6.3) only needs the hypothesis that $\mathfrak{p}$ is a prime of good reduction. The general case follows by applying the previous sentence to a prime in F_A^{conn} lying above $\mathfrak{p}$.

Now we prove (b). We first treat the case where $A = A_i$ is geometrically simple, and we drop the subscript i. Factor

$$g_{\mathfrak{p}}(T) = \prod_j (1 - \gamma_j T)^{m(\gamma_j)} \in \mathbb{C}[T] \tag{7.3.8}$$

where the reciprocal roots γ_j are pairwise distinct and occur with multiplicity $m(\gamma_j)$. Then

$$\deg g_{\mathfrak{p}} = \sum_j m(\gamma_j) \leq \sum_j m(\gamma_j)^2 \tag{7.3.9}$$

and the equality is attained if and only if $m(\gamma_j) = 1$ for all j, in other words, if $g_{\mathfrak{p},j}(T)$ is separable. By Lemma 7.2.17, since $c_{\mathfrak{p}}^{(k_{\mathfrak{p}})}(T) = g_{\mathfrak{p}}(T)^e$, we have

$$\dim_{\mathbb{Q}} \operatorname{End}(A_{\mathfrak{p}}^{\mathrm{al}})_{\mathbb{Q}} = \sum_j (em(\gamma_j))^2. \tag{7.3.10}$$

Since $2 \dim A = \deg c_{\mathfrak{p}}^{(k_{\mathfrak{p}})} = e \deg g_{\mathfrak{p}}$ we conclude

$$2e \dim A = e^2 \deg g_{\mathfrak{p}} \leq e^2 \sum_j m(\gamma_j)^2 = \dim_{\mathbb{Q}} \operatorname{End}(A_{\mathfrak{p}}^{\mathrm{al}})_{\mathbb{Q}} \tag{7.3.11}$$

as claimed.

Now we treat the general case. For $i = 1, \ldots, t$, in the notation of part (a), factor

$$g_{\mathfrak{p},i}(T) = \prod_j^s (1 - \gamma_{ij} T)^{m(\gamma_{ij})} \in \mathbb{C}[T]. \tag{7.3.12}$$

Adding up the inequality (7.3.11), multiplied by n_i^2 throughout, we obtain

$$\sum_i e_i^2 n_i^2 \deg g_{\mathfrak{p},i} \leq \sum_i e_i^2 n_i^2 \sum_j m(\gamma_{ij})^2 \leq \dim_{\mathbb{Q}} \operatorname{End}(A_{\mathfrak{p}}^{\mathrm{al}})_{\mathbb{Q}}. \tag{7.3.13}$$

As in the previous paragraph, the left-hand inequality is an equality if and only if for every i the polynomial $g_{\mathfrak{p},i}(T)$ is separable. By Lemma 7.2.17, the right-hand inequality is an equality if and only if

$$z_\ell = \gamma_{ij} \quad \text{and} \quad m(z_\ell) = e_i n_i m(\gamma_{ij}), \tag{7.3.14}$$

where

$$c_{\mathfrak{p}}^{(k)}(T) = \prod_\ell (1 - z_\ell T)^{m(z_\ell)} \tag{7.3.15}$$

with z_ℓ distinct. In other words, if and only if γ_{ij} are all distinct, or equivalently, if the polynomials $g_{\mathfrak{p},i}$ are pairwise coprime. □

We now try to deduce the decomposition (7.3.3) from factorizations as in Proposition 7.3.5. From the left-hand side of (7.3.7), we define the quantity

$$\eta(A^{\mathrm{al}}) := \sum_{i=1}^t e_i n_i^2 \dim A_i \tag{7.3.16}$$

which we would like to know. (The invariant $\eta(A^{\mathrm{al}})$ plays a similar role to that of $\rho(J^{\mathrm{al}})$ in the previous section.) Looking at the right-hand side of (7.3.7), for a prime $\mathfrak{p}$ of good reduction, we factor

$$c_{\mathfrak{p}}^{(k_{\mathfrak{p}})}(T) = \prod_{i=1}^{t_{\mathfrak{p}}} h_{\mathfrak{p},i}(T)^{m_{\mathfrak{p},i}} \in \mathbb{Z}[T] \tag{7.3.17}$$

into pairwise coprime irreducibles, where $k_{\mathfrak{p}}$ can be computed with Lemma 7.2.7 and $t_{\mathfrak{p}}$ is the number of pairwise distinct (simple) factors in the isogeny decomposition of $A_{\mathbb{F}_{\mathfrak{p}}^{k_{\mathfrak{p}}}}$. Now

we define the computable quantity

$$\eta(A_{\mathfrak{p}}^{\mathrm{al}}) := \sum_{i=1}^{t_{\mathfrak{p}}} m_{\mathfrak{p},i}^2 \deg h_{\mathfrak{p},i} \in 2\mathbb{Z}_{\geq 1}. \tag{7.3.18}$$

It follows from Lemma 7.2.17 that $\eta(A_{\mathfrak{p}}^{\mathrm{al}}) = \dim_{\mathbb{Q}} \mathrm{End}(A_{\mathfrak{p}}^{\mathrm{al}})_{\mathbb{Q}}$.

Corollary 7.3.19. (a) *For all good primes $\mathfrak{p}$, we have*

$$\eta(A^{\mathrm{al}}) \leq \tfrac{1}{2}\eta(A_{\mathfrak{p}}^{\mathrm{al}}). \tag{7.3.20}$$

(b) *If equality holds in (7.3.20), then $t \leq t_{\mathfrak{p}}$.*
(c) *If equality holds in (7.3.20) and $t = t_{\mathfrak{p}}$, then as multisets*

$$\{(m_{\mathfrak{p},i}, \tfrac{1}{2} m_{\mathfrak{p},i} \deg h_{\mathfrak{p},i})\}_{i=1}^{t_{\mathfrak{p}}} = \{(e_i n_i, n_i \dim A_i)\}_{i=1}^{t}. \tag{7.3.21}$$

Proof. The inequality $\eta(A^{\mathrm{al}}) \leq \frac{1}{2}\eta(A_{\mathfrak{p}}^{\mathrm{al}})$ is simply rewriting (7.3.7).

If equality holds in (7.3.20), then by Proposition 7.3.5(b), the t polynomials $g_{\mathfrak{p},i}(T)$ are separable and pairwise coprime, and there are $t_{\mathfrak{p}}$ distinct factors in total. Hence, $t \leq t_{\mathfrak{p}}$.

Moreover, if equality holds in (7.3.20) and $t = t_{\mathfrak{p}}$, then we have two factorizations of $c_{\mathfrak{p}}^{(k_{\mathfrak{p}})}(T)$ into powers of pairwise irreducibles, one in terms of $g_{\mathfrak{p},i}(T)$ and the other in terms of $h_{\mathfrak{p},i}(T)$. Therefore, as a multiset we have

$$\{(m_{\mathfrak{p},i}, h_{\mathfrak{p},i}(T))\}_{i=1}^{t_{\mathfrak{p}}} = \{e_i n_i, g_{\mathfrak{p},i}(T))\}_{i=1}^{t}. \tag{7.3.22}$$

Taking the degree of the second entry and multiplying it by the first entry, we get

$$\{(m_{\mathfrak{p},i}, m_{\mathfrak{p},i} \deg h_{\mathfrak{p},i})\}_{i=1}^{t_{\mathfrak{p}}} = \{(e_i n_i, e_i n_i \deg g_{\mathfrak{p},i})\}_{i=1}^{t}, \tag{7.3.23}$$

and the desired equality follows by noting that $2 \dim A_i = e_i \deg g_{\mathfrak{p},i}$. □

We now show that (conjecturally) there are an abundance of primes where we have an equality in (7.3.20), i.e., primes for which the endomorphism algebra grows in a controlled (minimal) way under reduction modulo $\mathfrak{p}$.

Let S be the set of primes $\mathfrak{p}$ of F with the following properties:

(i) The prime $\mathfrak{p}$ is a prime of good reduction for A.
(ii) $\mathrm{Nm}(\mathfrak{p})$ is prime, i.e., the residue field $\#\mathbb{F}_{\mathfrak{p}}$ has prime cardinality.
(iii) $\mathrm{End}(A_{\mathfrak{p}}^{\mathrm{al}})$ is defined over $\mathbb{F}_{\mathfrak{p}}$ (i.e., $k_{\mathfrak{p}} = 1$).
(iv) For all $i = 1, \ldots, t$, we have an isogeny $(A_i)_{\mathfrak{p}} \sim A_{\mathfrak{p},i}^{e_i}$ over $\mathbb{F}_{\mathfrak{p}}$ where $A_{\mathfrak{p},i}$ is simple; moreover, the abelian varieties $A_{\mathfrak{p},i}$ are pairwise nonisogenous.
(v) For all $i = 1, \ldots, t$, the algebra $\mathrm{End}(A_{\mathfrak{p},i}^{\mathrm{al}})_{\mathbb{Q}}$ is a field, generated by the Frobenius endomorphism.

Lemma 7.3.24. *For $\mathfrak{p} \in S$, we have $t = t_{\mathfrak{p}}$ and $2\eta(A^{\mathrm{al}}) = \eta(A_{\mathfrak{p}}^{\mathrm{al}})$.*

Proof. We have $t = t_{\mathfrak{p}}$ by the decomposition in (iv). By (7.3.6), $g_{\mathfrak{p},i}(T)$ is the characteristic polynomial of Frobenius for $A_{\mathfrak{p},i}$, and for every i, the polynomials $g_{\mathfrak{p},i}(T)$ are irreducible over $\mathbb{Q}$, otherwise the Honda–Tate theory would give a further splitting of $A_{\mathfrak{p}}$, see Remark 7.2.13. and pairwise coprime by (iv), so the equality holds by Proposition 7.3.5. □

The required analytic result about primes $\mathfrak{p} \in S$ is essentially proved by Zywina [Zyw14], as follows. For the statement of the Mumford–Tate conjecture, see Zywina [Zyw14, §2.5] and

the references given; although the conjecture is still open, many general classes of abelian varieties are known to satisfy the conjecture.

Proposition 7.3.25. *Suppose that the Mumford–Tate conjecture for A holds. Then the set S has positive density.*

Proof. We follow the proof of a result by Zywina [Zyw14, Theorem 1.4]. He shows that the set of primes with properties (i)–(iv) has positive density, and we obtain our full result by a refining his proof to obtain property (v) as a consequence, as follows.

As in the proof of Proposition 7.3.5, we first suppose that $F = F_A^{\mathrm{conn}}$. Zywina [Zyw14, Section 2.4] considers the set of primes satisfying (i)–(ii) and such that the Frobenius eigenvalues of each $A_{\mathfrak{p},i}$ generate a torsion-free subgroup of maximal rank in $(\mathbb{Q}^{\mathrm{al}})^\times$. Zywina shows that this set has density 1 and proves [Zyw14, Lemma 6.3] that the Frobenius eigenvalues of $A_{\mathfrak{p},i}$ are distinct. Next, among primes in this set, away from a set of primes of density zero [Zyw14, Proposition 6.6], the characteristic polynomial of Frobenius on $A_{\mathfrak{p},i}$ is irreducible [Zyw14, Lemma 6.7], so that (iv) holds. The hypotheses of Corollary 7.2.11 hold for the abelian variety $A_{\mathfrak{p},i}$ over $\mathbb{F}_{\mathfrak{p}}$, so all endomorphisms are defined over $\mathbb{F}_{\mathfrak{p}}$, so (iii) holds, and moreover $\dim_{\mathbb{Q}} \mathrm{End}(A_{\mathfrak{p},i})_{\mathbb{Q}} = 2 \dim A_{\mathfrak{p},i}$. Finally, since $A_{\mathfrak{p},i}$ is simple, the characteristic polynomial $g_{\mathfrak{p},i}(T)$ of Frobenius is irreducible with $\deg g_{\mathfrak{p},i}(T) = 2 \dim A_{\mathfrak{p},i}$, and so $\mathrm{End}(A_{\mathfrak{p},i}^{\mathrm{al}})_{\mathbb{Q}} = \mathrm{End}(A_{\mathfrak{p},i})_{\mathbb{Q}}$ contains as a subalgebra the field $\mathbb{Q}[T]/(g_{\mathfrak{p},i}(T))$ generated by Frobenius. By dimension counts, equality holds and (v) follows.

The general case follows by applying this argument to the set of primes $\mathfrak{p}$ of F such that a prime above $\mathfrak{p}$ in the Galois extension F_A^{conn} over F are in the above set: by the Chebotarev density theorem, this set has density $[F_A^{\mathrm{conn}} : F]^{-1}$. □

Proposition 7.3.26. *If the Mumford–Tate conjecture holds for A, then the following quantities are effectively computable:*

(i) *The integer $\eta(A^{\mathrm{al}})$;*
(ii) *The number t of geometrically simple factors of A; and*
(iii) *The set of tuples $\{(e_i n_i, n_i \dim A_i)\}_{i=1}^t$.*

Proof. We pursue a day-and-night approach. By day, we search for endomorphisms of A^{al}, find a (partial) decomposition

$$A_L \sim (A_1')^{n_1'} \times \ldots \times (A_{t'})^{n_{t'}'}, \tag{7.3.27}$$

and compute the quantity

$$\eta' = \sum_{i=1}^{t'} e_i'(n_i')^2 \dim A_i' \leq \eta(A^{\mathrm{al}}). \tag{7.3.28}$$

By night, by counting points on $A_{\mathfrak{p}}$ we compute $t_{\mathfrak{p}}$ and $\eta(A_{\mathfrak{p}}^{\mathrm{al}})$ for many good primes $\mathfrak{p}$ using (7.3.18). We continue in this way until we find a prime $\mathfrak{p}$ such that $t' = t_{\mathfrak{p}}$ and $2\eta' = \eta(A_{\mathfrak{p}}^{\mathrm{al}})$: Proposition 7.3.25 and Lemma 7.3.24 assure us that this will happen frequently, proving that the quantities (i) and (ii) are effectively computable. For (iii), we then appeal to Corollary 7.3.19. □

Remark 7.3.29. The statement of Proposition 7.3.26 can be proven in other ways without the Mumford–Tate conjecture, but the algorithm exhibited in the proof is quite practical! For example, we can expect to verify that the abelian variety A over F is geometrically a

power of a simple abelian variety (so $t = t_{\mathfrak{p}} = 1$) after examining $[F_A^{\mathrm{conn}} : F]$ Frobenius polynomials.

7.4. **Upper bounds in higher genus: bounding the center.** Now we refine the decomposition obtained in the previous section to bound the dimension of the geometric endomorphism algebra, by bounding the center. For a theoretical result, we refer again to Lombardo [Lom16, §5]. Our method in this section are heuristic in nature, as we lack an analytic result (Hypothesis 7.4.6) that assures us that our method terminates. That being said, our method is efficient, and if our method terminates then the output will be correct.

We start with some preliminary lemmas.

Lemma 7.4.1. *Let B be a central simple algebra over F and let N be a finite extension of F. Then there exists a maximal subfield $L \subseteq B$ such that L and N are linearly disjoint over F.*

Proof. We may assume N is Galois over F and exhibit L such that $L \cap N = F$. As a consequence of the Albert–Brauer–Hasse–Noether theorem (see e.g. Reiner [Rei03, Theorem 32.15]), we have an embedding $L \hookrightarrow B$ if and only if L satisfies finitely many local conditions (determined by the ramified primes in B). Choose a prime $\mathfrak{p}$ of F that splits completely in N disjoint from these finitely many conditions, and add the new local condition that $L_{\mathfrak{p}}$ is a field. By Chebotarev there are infinitely many fields L satisfying these conditions, and in $L \cap N$ we have $\mathfrak{p}$ both splitting completely and with a unique prime above it, so $F = L \cap N$. □

Lemma 7.4.2. *For $i = 1, 2$, let K_i be a number field and let B_i be a central simple algebra over K_i. Let $\varphi\colon B_1 \hookrightarrow B_2$ be an injective $\mathbb{Q}$-algebra homomorphism. If $\dim_{K_1} B_1 = \dim_{K_2} B_2 = m^2$, then $\varphi(K_1) \subseteq K_2$.*

Proof. Let L be a maximal subfield of B_1, so $\dim_{K_1} L = m$. Thus $\varphi(L)$ is a subfield of B_2, and $S := K_2\varphi(L) \subset B_2$, the subring of B_2 generated by K_2 and $\varphi(L)$, is a commutative K_2-subalgebra of B_2. Hence, $\dim_{K_2} S \leq m$.

Let $E = \varphi(K_1) \cap K_2 \subset B_2$ and N_2 be the normal closure of $\varphi(K_1)K_2$. We may choose L such that $\varphi(L)$ and N_2 are linearly disjoint by Lemma 7.4.1. Thus $\varphi(L) \otimes_E K_2 \xrightarrow{\sim} S$ and

$$\begin{aligned} m \geq \dim_{K_2} S = \frac{\dim_E S}{\dim_E K_2} &= \frac{\dim_E \varphi(L) \dim_E K_2}{\dim_E K_2} \\ &= \dim_E \varphi(L) = \dim_{\varphi(K_1)} \varphi(L) \dim_E \varphi(K_1) \geq m. \end{aligned} \tag{7.4.3}$$

Therefore, $\dim_E \varphi(K_1) = 1$ and $\varphi(K_1) \subseteq K_2$. □

We now recall the notation described in the previous section (starting with (7.3.3)), in particular $L_i = Z(B_i)$.

Corollary 7.4.4. *If the polynomial $g_{i,\mathfrak{p}}(T)$ in Proposition 7.3.5(a) is irreducible for some i, then L_i is isomorphic to a subfield of $\mathbb{Q}[T]/(g_{\mathfrak{p},i}(T))$.*

Proof. Apply Lemma 7.4.2 to the specialization homomorphism

$$s_{i,\mathfrak{p}}\colon \mathrm{End}(A_i^{\mathrm{al}})_{\mathbb{Q}} \hookrightarrow \mathrm{End}((A_i)_{\mathfrak{p}}^{\mathrm{al}})_{\mathbb{Q}}; \tag{7.4.5}$$

On the left we have center L_i and on the right we have center $\mathbb{Q}[T]/(g_{\mathfrak{p},i}(T))$ by Tate [Tat66, Theorem 2(a)]. □

Now we address the hypothesis that will allow us to deduce the candidate fields for the centers.

Hypothesis 7.4.6. *For every $i = 1, \dots, t$, there exists a nonempty, finite collection of primes $\mathfrak{p}_{ij} \in S$ such that K is a subfield of $\mathbb{Q}[T]/(g_{\mathfrak{p}_{ij}}(T))$ for all j if and only if K is a subfield of L_i.*

The hypothesis is known to hold for abelian surfaces by an explicit argument of Lombardo [Lom16, Theorem 6.10]. In our experiments with higher genus curves, every Jacobian variety we saw satisfied Hypothesis 7.4.6.

Proposition 7.4.7. *If the Mumford–Tate Conjecture and Hypothesis 7.4.6 hold for A, then the centers L_i are effectively computable.*

Proof. We continue with a day-and-night approach as described in the proof of Proposition 7.3.26. The decomposition of A by day into t factors allows us to decompose $A[\ell^r] \simeq (\mathbb{Z}/\ell\mathbb{Z})^{2\dim A}$ into t factors, and for r large enough we can keep track of the index i between different primes $\mathfrak{p}$: see Lombardo [Lom16, Lemma 5.2]. By night, we will have encountered an abundance of primes $\mathfrak{p}$ such that $t = t_{\mathfrak{p}}$ and $2\eta(A^{\mathrm{al}}) = \eta(A^{\mathrm{al}}_{\mathfrak{p}})$, and $c_{\mathfrak{p}}(T)$ factors as

$$g_{\mathfrak{p},i}(T)^{e_1 n_1} \cdots g_{\mathfrak{p},t}(T)^{e_t n_t} \tag{7.4.8}$$

with the polynomials $g_{\mathfrak{p},i}$ irreducible and pairwise coprime.

For these primes $\mathfrak{p}$, by Corollary 7.4.4 we have $L_i \hookrightarrow \mathbb{Q}[T]/(g_{\mathfrak{p},i}(T))$, immediately giving only finitely many possibilities for each L_i. Finally, by Hypothesis 7.4.6 the only field that embeds in all $\mathbb{Q}[T]/(g_{\mathfrak{p},i}(T))$ is L_i, and so by computing intersections of subfields we will eventually find L_i. □

Remark 7.4.9. Parallel to Remark 7.3.29, in practice the algorithm of Proposition 7.4.7 performs very well. In most cases, the abelian variety is geometrically a power and $L_i = \mathbb{Q}$, and in practice this can be quickly deduced by simply computing that the greatest common divisor of the discriminants $\operatorname{disc} \mathbb{Q}[T]/(g_{\mathfrak{p},i}(T))$ is equal to 1.

Remark 7.4.10. Many cohomological algorithms for counting points on a curve can be adapted to keep track of the index i between different primes $\mathfrak{p}$ rather than resorting to the ℓ-adic representation. For example, in those point counting algorithms that employ Monsky–Washnitzer cohomology, we may choose a basis of differentials that works for all good primes $\mathfrak{p}$ and use the decomposition of A into factors to decompose these differentials and thereby compute the action of Frobenius on each component. A similar argument applies to methods that compute the Hasse–Witt matrices.

8. Examples

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

8.1. Examples in genus 2.

Example 8.1.1. We begin with 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

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

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 we certify that 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 ideal

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

The second projection from the corresponding divisor to X has degree 2. 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

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

The first of these calculations need 40 terms in the Puiseux expansion, whereas the latter needs 172. The combination of these calculations takes around 2.5 CPU seconds.

Example 8.1.5. As a second example, we consider the curve 20736.1.373248.1 with simplified Weierstrass model

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

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 $x^8 + 4x^6 + 10x^4 + 24x^2 + 36$. Over the smaller field $\mathbb{Q}(\sqrt{-3})$ we get the endomorphism ring $\mathbb{Z}[3\sqrt{-1}]$. A generator α with $\alpha^2 = -9$ has tangent representation

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

Our algorithms can perform the corresponding verification over the field $\mathbb{Q}(\sqrt{-3})$ itself, by using the base point $P_0 = (0, 1)$. The second projection from the corresponding divisor to X has degree 18, and using the Cantor representation one needs functions of degree up to 105. The corresponding number of terms needed in the Puiseux expansion is 128 in the former case and 346 in the latter. This time the calculations take around 8.5 CPU seconds to finish.

Example 8.1.8. A third example in genus 2 is 294.a.8232.1 with model

$$X\colon y^2 = x^6 - 8x^4 + 2x^3 + 16x^2 - 36x - 55. \tag{8.1.9}$$

The endomorphism ring of this curve is of index 2 in the ring $\mathbb{Z} \times \mathbb{Z}$. The methods of 6.3 show that it admits two maps of degree 2 to the elliptic curves

$$E_1\colon y^2 = x^3 + 3440/3x - 677248/27 \quad \text{and} \quad E_2\colon y^2 = x^3 + x^3 + 752/3x - 9088/27 \tag{8.1.10}$$

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

$$\left(\frac{24x^4 + 72x^3 + 4x^2 - 24xy - 200x - 72y - 200}{3(x+2)^2}, \right. \\ \left. \frac{32x^6 + 144x^5 + 16x^4 - 32x^3y - 768x^3 - 144x^2y - 656x^2 - 144xy + 1488x + 1792}{(x+2)^3}\right) \tag{8.1.11}$$

on E_1 and

$$\left(\frac{24x^4 + 24x^3 - 92x^2 - 24xy - 56x - 24y + 88}{3(x+2)^2}, \right. \\ \left. \frac{-32x^6 - 48x^5 + 176x^4 + 32x^3y + 224x^3 + 48x^2y - 304x^2 - 48xy - 240x - 64y + 192}{(x+2)^3}\right) \tag{8.1.12}$$

on E_2. Finding these projections only requires 39 terms of the Puiseux series, and takes around 1 second.

8.2. **Examples in higher genus.**

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

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

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 cusp forms 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

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

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

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

Determining this projection again takes about a second. A curve that corresponds to the complementary factor dimension 2 can be found by using the results by Ritzenthaler–Romagny in [RR16].

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

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

has real multiplication by the algebra $\mathbb{Q}(\alpha)$, with $\alpha = 2\cos(2\pi/7)$. We have independently verified this result. The equations for the divisor are too large to reproduce here, but they can be generated with the package [CMS17]. 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

$$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha^2 - 2 & 0 \\ 0 & 0 & -\alpha^2 + \alpha + 1 \end{pmatrix}. \tag{8.2.7}$$

This verification takes about 7 CPU seconds and requires Puiseux series with 66 coefficients of precision.

Example 8.2.8. As a final aside, we consider Picard curves of the form

$$X\colon y^3 = a_0x^4 + a_2x^2 + a_4. \tag{8.2.9}$$

Petkova–Shiga [PS11] have shown that the connected component of the Sato–Tate group of a general such curve is equal to $\mathrm{U}(1) \times \mathrm{SU}(2)_2$. The endomorphism ring of such a general curve X is of index 4 in a maximal order of $\mathbb{Q}(\zeta_3) \times B$, where B is the indefinite quaternion algebra of discriminant 6.

The Jacobian of X therefore splits into an elliptic curve with CM and the Jacobian of a curve Y of genus 2 that has QM. Once again the curve Y can be identified explicitly using recent work of Ritzenthaler–Romagny [RR16]. It turns out that the field of definition of the endomorphism ring of X is the splitting field of the polynomial $t^6 - (2^4(a_4/a_0)(a_2^2 - 4a_0a_4))$. Using our algorithms, an explicit expression of the correspondence between X and Y can also be obtained.

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+16] 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.

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

[CE15] Jean-Marc Couveignes and Tony Ezome. Computing functions on Jacobians and their quotients. *LMS J. Comput. Math.*, 18(1):555–577, 2015.

[Cha14] François Charles. On the Picard number of K3 surfaces over number fields. *Algebra Number Theory*, 8(1):1–17, 2014.

[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] Arjen K. Lenstra, Hendrik W. Lenstra, Jr., and László 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.

[MN17] Pascal Molin and Christian Neurohr. Computing period matrices and the Abel-Jacobi map of superelliptic curves. arXiv:1707.07249, 2017.

[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.

[Rei03] Irving Reiner. *Maximal orders*, volume 28 of *London Mathematical Society Monographs. New Series*. The Clarendon Press, Oxford University Press, Oxford, 2003. Corrected reprint of the 1975 original, With a foreword by M. J. Taylor.

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

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

[vW00] Paul B. 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.

[Wat69] William C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2:521–560, 1969.

[WM71] William C. Waterhouse and James S. Milne. Abelian varieties over finite fields. In *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969)*, pages 53–64. Amer. Math. Soc., Providence, R.I., 1971.

[Zyw14] David Zywina. The splitting of reductions of an abelian variety. *Int. Math. Res. Not. IMRN*, (18):5042–5083, 2014.

Department of Mathematics 77 Massachusetts Ave., Bldg. 2-252B Cambridge, MA 02139, USA
Email address: edgarc@mit.edu
URL: https://edgarcosta.org/

Department of Mathematics Faculty of Arts and Sciences American University of Beirut P.O. Box 11-0236 Riad El Solh, Beirut 1107 2020 Lebanon
Email address: nm116@aub.edu.lb
URL: https://staff.aub.edu.lb/~nm116/

Universität Ulm, Institut für Reine Mathematik, D-89068 Ulm, Germany
Email address: jeroen.sijsling@uni-ulm.de
URL: https://jrsijsling.eu/

Department of Mathematics, Dartmouth College, 6188 Kemeny Hall, Hanover, NH 03755, USA
Email address: jvoight@gmail.com
URL: http://www.math.dartmouth.edu/~jvoight/