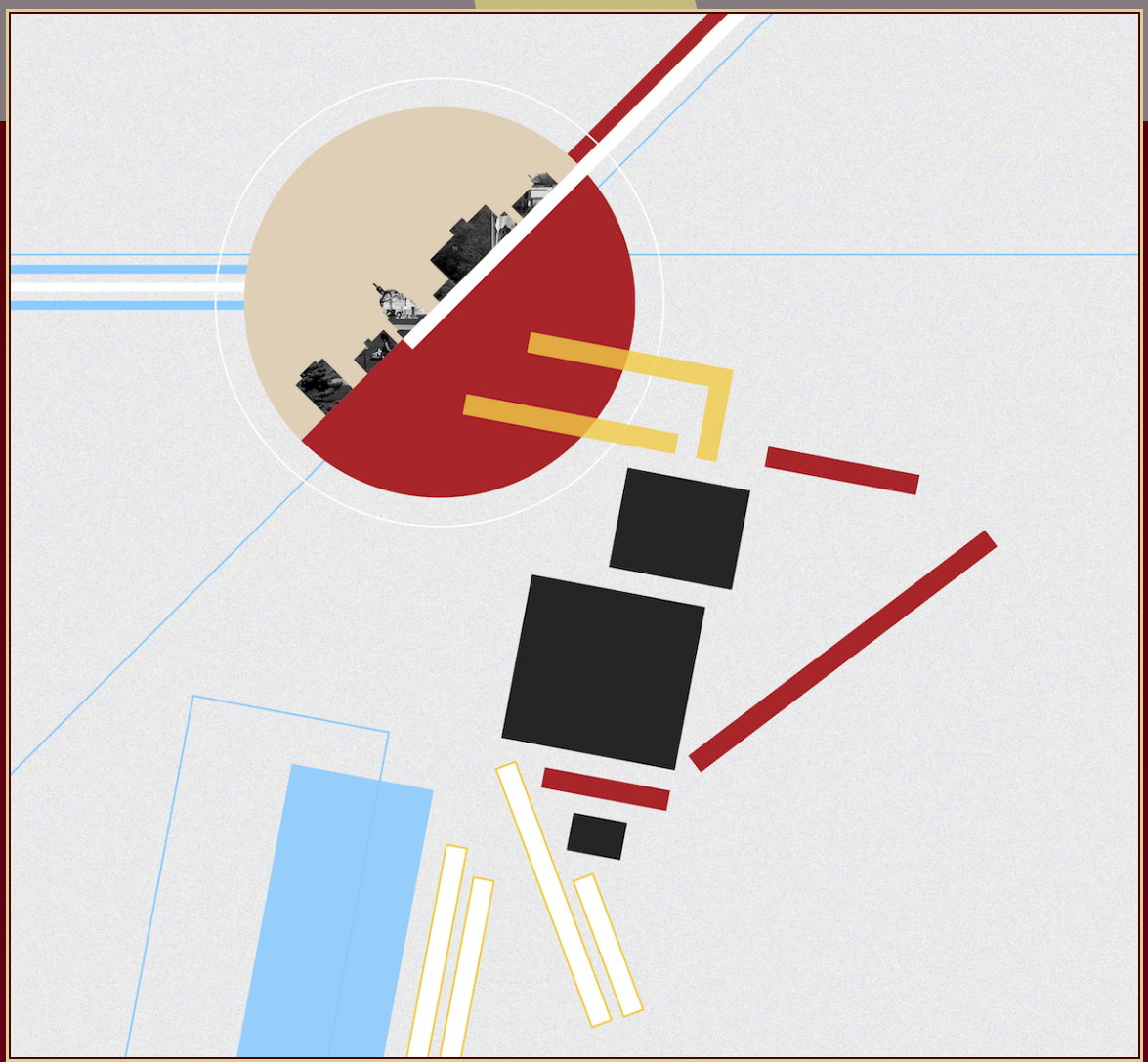
THE OPEN BOOK SERIES 2

# ANTS XIII
## Proceedings of the Thirteenth Algorithmic Number Theory Symposium

### Numerical computation of endomorphism rings of Jacobians

Nils Bruin, Jeroen Sijsling, and Alexandre Zotine



msp

THE OPEN BOOK SERIES 2 (2019)
**Thirteenth Algorithmic Number Theory Symposium**
dx.doi.org/10.2140/obs.2019.2.155

# Numerical computation of endomorphism rings of Jacobians

Nils Bruin, Jeroen Sijsling, and Alexandre Zotine

We give practical numerical methods to compute the period matrix of a plane algebraic curve (not necessarily smooth). We show how automorphisms and isomorphisms of such curves, as well as the decomposition of their Jacobians up to isogeny, can be calculated heuristically. Particular applications include the determination of (generically) non-Galois morphisms between curves and the identification of Prym varieties.

## 1. Introduction

Let $k$ be a field of characteristic 0 that is finitely generated over $\mathbb{Q}$. We choose an embedding of $k$ into $\mathbb{C}$. In this article, we consider nonsingular, complete, absolutely irreducible algebraic curves $C$ over $k$ of genus $g$. We represent such a curve $C$ by a possibly singular affine plane model

$$\widetilde{C} : f(x, y) = 0, \quad \text{where } f(x, y) \in k[x, y]. \tag{1-1}$$

Associated to $C$ is the Jacobian variety $J = \mathrm{Jac}(C)$ representing $\mathrm{Pic}^0(C)$. Classical results by Abel and Jacobi establish

$$J(\mathbb{C}) \cong \mathrm{H}^0(C_{\mathbb{C}}, \Omega^1_C)^*/\mathrm{H}_1(C(\mathbb{C}), \mathbb{Z}) \cong \mathbb{C}^g/\,\Omega\mathbb{Z}^{2g},$$

for a suitable $g \times 2g$ matrix $\Omega$, called a *period matrix* of $C$.

Let $J_1 = \mathrm{Jac}(C_1)$ and $J_2 = \mathrm{Jac}(C_2)$ be two such Jacobian varieties. The $\mathbb{Z}$-module $\mathrm{Hom}_{\bar{k}}(J_1, J_2)$ of homomorphisms defined over the algebraic closure $\bar{k}$ of $k$ is finitely generated and can be represented as the group of $\mathbb{C}$-linear maps $\mathbb{C}^{g_1} \to \mathbb{C}^{g_2}$ mapping the columns of $\Omega_1$ into $\Omega_2\mathbb{Z}^{g_2}$. As described in [10, §2.2], we can heuristically determine homomorphism modules, along with their tangent representations, from numerical approximations to $\Omega_1, \Omega_2$. These can then serve as input for rigorous verification as in [loc. cit.].

In this article we consider the problem of computing approximations to period matrices for arbitrary algebraic curves for the purpose of numerically determining homomorphism modules and endomorphism

The research of Bruin and Zotine is partially supported by NSERC, and Sijsling is supported by a Juniorprofessurprogramm of the Science Ministry of Baden-Württemberg.
*MSC2010*: 14H40, 14H37, 14H55, 14Q05.
*Keywords*: curves, Riemann surfaces, period matrices, automorphisms, endomorphisms, isogeny factors.

rings. We also describe how to identify the (finite) symplectic automorphism groups in these rings, and with that the automorphism group of the curve. We give several examples of how the heuristic determination of such objects can be used to obtain rigorous results.

There is extensive earlier work on computing period matrices for applications in scientific computing to Riemann theta functions and partial differential equations. For these applications, approximations that fit in standard machine precision tend to be sufficient. Number-theoretic applications tend to need higher accuracy and use arbitrary-precision approximation. Hyperelliptic curves have received most attention; see for instance van Wamelen's [28] implementation in Magma. In practice it is limited to about 2000 digits. Recent work by Molin and Neurohr [23] can reach higher accuracy and also applies to superelliptic curves.

For general curves, a Maple package based on work by Deconinck and van Hoeij [12] computes period matrices at system precision or (much more slowly) at arbitrary precision. Swierczewski's reimplementation in SageMath [26] only uses machine precision and no high-order numerical integration. During the writing of this article, another new and fast Magma implementation was developed by Neurohr [24]. See the introduction of [24] for a more comprehensive overview of the history and recent work on the subject.

Our approach is similar to the references above (in contrast to, for instance, the deformation approach taken in [25]) in that we basically use the definition of the period matrix to compute an approximation.

**Algorithm 1-2** (compute approximation to period matrix).

*Input*: $f$ as in (1-1) over a number field and a given working precision.

*Output*: Approximation of a period matrix of the described curve.

(1) Determine generators of the fundamental group of $C$ (Section 2C).

(2) Derive a symplectic basis $\{\alpha_1, \dots, \alpha_g, \beta_1, \dots, \beta_g\}$ of the homology group $H_1(C(\mathbb{C}), \mathbb{Z})$ (Section 2D).

(3) Determine a basis $\{\omega_1, \dots, \omega_g\}$ of the space of differentials $\mathrm{H}^0(C_{\mathbb{C}}, \Omega^1_C)$ (Section 3A).

(4) Approximate the period matrix $\Omega = \left(\int_{\alpha_j} \omega_i, \int_{\beta_j} \omega_i\right)_{i,j}$ using numerical integration (Section 3B).

We list some notable features of our implementation.

(a) We use *certified* homotopy continuation [19] to guarantee that the analytic continuations on which we rely are indeed correct. This allows us to guarantee that increasing the working precision sufficiently will improve accuracy.

(b) We base our generators of the fundamental group on a Voronoi cell decomposition to obtain paths that stay away from critical points. This is advantageous for the numerical integration.

(c) We determine homotopy generators by directly lifting the Voronoi graph to the Riemann surface via analytic continuation and taking a cycle basis of that graph. This avoids the relatively opaque procedure [27] used in [12; 24].

(d) We provide an implementation in a free and open mathematical software suite (SageMath version 8.0+), aiding verification of the implementation and adaptation and extension of its features.

We share the use of Voronoi decompositions with [28]. This is no coincidence, since Bruin suggested its use to van Wamelen at the time, while sharing an office in Sydney, and was eager to see its use tested for general curves. Dealing with hyperelliptic and superelliptic curves, [28; 23] use a shortcut in determining homotopy generators. The explicit use of a graph cycle basis in feature (c) above, while directly suggested by basic topological arguments, is to our knowledge new for an implementation in arbitrary precision.

The runtime of these implementations is in practice dominated by the numerical integration. The complexity for all these methods is essentially the same; see [24, §4.8] for an analysis, as well as a fairly systematic comparison. For a rough idea of performance we give here some timings for the computation of period matrices of the largest genus curves in each of our examples. Timings were done using Linux on a Intel Core i7-2600 3.40 GHz processor, at working precision of 30 decimal digits, 100 binary digits:

| curve | Maple 2018 | SageMath 8.3.beta0 |
|---|---|---|
| $C$ from Example 5A | 99.6 sec | 45.5 sec |
| $C$ from Example 5B | 133.2 sec | 8.59 sec |
| $D$ from Example 5C | 119.2 sec | 12.8 sec |

With recent work on rigorous numerical integration [17], which is now also available in SageMath, it would be possible to modify the program to return certified results. While this is worthwhile and part of future work, rigorous error bounds would make little difference for our applications, since we have no a priori height bound on the rational numbers we are trying to recognize from floating point approximations. One of our objectives is to provide input for the rigorous verification procedures described in [10].

Our main application is to find decompositions of $\mathrm{Jac}(C)$ via its endomorphism ring $\mathrm{End}(J) = \mathrm{End}_{\bar{k}}(J) = \mathrm{Hom}_{\bar{k}}(J, J)$. Idempotents of $\mathrm{End}(J)$ give rise to isogenies to products of lower-dimensional abelian varieties [5, Chapter 5; 18]. Furthermore, since $\mathrm{End}(J)$ has a natural linear action on $\mathrm{H}^0(C, \Omega^1_C)^*$, idempotents induce projections from the canonical model of $C$ in $\mathbb{P}\mathrm{H}^0(C, \Omega^1_C)^*$ to projective spaces of smaller dimension. For composition factors arising from a cover $\phi : C \to D$, the corresponding projection factors through $\phi$, so we can recover $\phi$ from it. In the process, we verify $\phi$ rigorously, as well as the numerically determined idempotent.

Finally, having determined $\mathrm{End}(J)$, we can compute the finite group automorphisms of $J$ that are fixed by the Rosati involution. Its action on $\mathrm{H}^0(C, \Omega^1_C)^*$ gives, via the Torelli theorem [21, Theorem 12.1], a representation of the automorphism group $\mathrm{Aut}(C) = \mathrm{Aut}_{\bar{k}}(C)$ of $C$ on a canonical model. There are other approaches to computing automorphism groups of curves, for instance [15]. The approach described here naturally finds a candidate for the *geometric* automorphism group (members of which are readily rigorously verified to give automorphisms) whereas more algebraically oriented approaches, such as the one in [15], tend only to find the automorphisms defined over a given base field or have prohibitive general running times. We describe the corresponding algorithm in Section 4B.

These results are applied to numerically identify some Prym varieties in higher genus. In particular, we find isogeny factors $\mathrm{Jac}(D)$ of Jacobians $\mathrm{Jac}(C)$ that do not come from any morphism $C \to D$, or come from a morphism that is not a quotient by automorphisms of $C$.

## 2. Computation of homology

We compute a homology basis for $C(\mathbb{C})$ from its fundamental group. We obtain generators for this group by pulling back generators of the fundamental group of a suitably punctured Riemann sphere covered by $C$. Such pullbacks can be found by determining the analytic continuations of appropriate algebraic functions. In order to make these continuations amenable to computation, we use paths that stay away from any ramification points.

The function $x$ on $\widetilde{C}$ induces a morphism $x : C \to \mathbb{P}^1$ and therefore expresses $C$ as a finite (ramified) cover of $\mathbb{P}^1$ of degree $n$ say. We collect terms with respect to $y$ and write

$$f(x, y) = f_n(x)y^n + f_{n-1}(x)y^{n-1} + \cdots + f_0(x),$$

where $f_0(x), \ldots, f_n(x) \in k[x]$, with $f_n(x) \neq 0$. We write $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$, and define the *finite critical locus* of $x$ as

$$S = \{x \in \mathbb{C} : \operatorname{disc}_y(f)(x) = 0\}.$$

We set $S_\infty = S \cup \{\infty\}$, so that $x$ induces an unramified cover $C - x^{-1}(S_\infty)$ of $\mathbb{C} - S$.

**2A.** ***Fundamental group of*** $\mathbb{C} - S$**.** We describe generators of the fundamental group of $\mathbb{C} - S$ by cycles in a planar graph that we build in the following way.

We approximate the circle with center $c_0 = (1/\#S) \sum_{s \in S} s$ and radius $2 \max_{s \in S} |s - c_0|$ using a regular polygon with vertices, say, $s'_1, \ldots, s'_6$. Then we compute the Voronoi cell decomposition (see, e.g., [2]) of $\mathbb{C}$ with respect to $S' = S \cup \{s'_1, \ldots, s'_6\}$. This produces a finite set of vertices $V = \{v_1, \ldots, v_r\} \subset \mathbb{C}$ and a set $E$ of line segments $e_{ij}$ between $v_i, v_j \in V$ such that the regions

$$F_s = \{x \in \mathbb{C} : |x - s| \leq |x - s'| \text{ for any } s' \in S' - \{s\}\}$$

have boundaries consisting of $e_{ij}$, together with some rays for unbounded regions. We define $F_\infty = \bigcup_{s \in S' - S} F_s$. Then we see that $F_s$ for $s \in S_\infty$ has a finite boundary, giving a loop separating $s$ from the rest of $S_\infty$. See Figure 1 for an illustration of the resulting graph for the curve $C : y^2 = x^3 - x - 1$. It illustrates the set $S = s_1, s_2, s_3$, together with the additional points $s'_1, \ldots, s'_6$, and the vertices $v_0, \ldots, v_{11}$ and edges between them, bounding the Voronoi cells $F_s$.

**Lemma 2-1.** (i) *The boundaries of the regions $F_s$ for $s \in S_\infty$ provide cycles that generate* $\mathrm{H}^1(\mathbb{C} - S, \mathbb{Z})$.

(ii) *The fundamental group $\pi_1(\mathbb{C} - S, v_i)$ is generated by cycles in the graph $(V, E)$.*

*Proof.* The first claim follows because the boundaries exactly form loops around each individual point $s$. The second claim follows because the graph is connected. Hence, we can find paths that begin and end in $v_i$ and (because of the first claim) provide a simple loop around a point $s \in S_\infty$. □

**2B.** ***Lifting the graph via homotopy continuation.*** Each of our vertices $v_i \in \mathbb{C}$ has exactly $n$ preimages $v_i^{(1)}, \ldots, v_i^{(n)}$, determined by the $n$ distinct simple roots of the equation $f(v_i, y) = 0$. We can parametrize

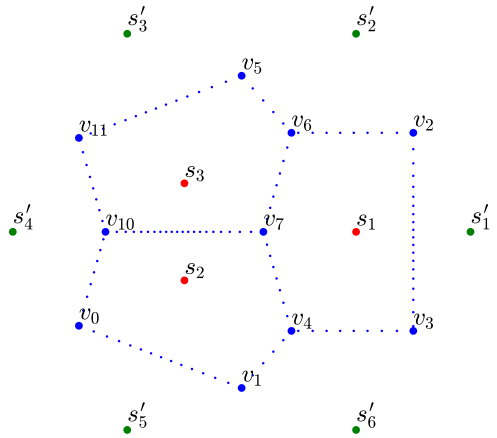



**Figure 1.** Paths for $C : y^2 = x^3 - x - 1$. The dots marking the edges indicate the step size used for the certified homotopy continuation.

each edge $e_{ij}$ from our graph by $x(t) = (1-t)v_i + tv_j$ for $t \in [0, 1]$. We lift $e_{ij}$ to paths $e_{ij}^{(1)}, \ldots, e_{ij}^{(n)}$ using the branches $y^{(k)}(t)$ defined by

$$f(x(t), y^{(k)}(t)) = 0 \quad \text{and} \quad y^{(k)}(0) = y(v_i^{(k)}).$$

Since $e_{ij}$ stays away from the critical locus, the function $y^{(k)}(t)$ is well defined by continuity. Moreover, it is analytic in a neighborhood of $e_{ij}^{(k)}$.

Given $k$, we have $y^{(k)}(1) = v_j^{k'}$ for some $k'$. Hence, every edge $e_{ij}$ determines a permutation $\sigma_{ij}$ such that $\sigma_{ij}(k) = k'$. The lifted edge $e_{ij}^{(k)}$ connects $v_i^{(k)}$ to $v_k^{(\sigma_{ij}(k))}$. We write $(V', E')$ for this lifted graph on $C(\mathbb{C})$. If we split up the path in sufficiently small steps, we can determine these permutations.

**Lemma 2-2.** *With the notation above and for given $i$, $j$, we can algorithmically determine a subdivision*

$$0 = t_0 < t_1 < t_2 < \cdots < t_{m_{ij}} = 1$$

*and real numbers $\varepsilon_0, \ldots, \varepsilon_{m_{ij}-1}$ such that for $t$, $m$ satisfying $t_m \le t \le t_{m+1}$, we have $|y^{(k')}(t) - y^{(k)}(t_m)| < \varepsilon_m$ if and only if $k' = k$.*

*Proof.* We construct the $t_m, \varepsilon_m$ iteratively, starting with $m = 0$. We set

$$\varepsilon_m = \tfrac{1}{3} \min\{|y^{(k_1)}(t_m) - y^{(k_2)}(t_m)| : k_1 \neq k_2\}.$$

Using [19, Theorem 2.1], we can determine from $f(x(t), y)$, $\varepsilon$, and $x(t_m)$ a value $\delta > 0$ such that for values $t$ satisfying $t_m \le t \le t_m + \delta$ we have that $|y^{(k)}(t) - y^{(k)}(t_m)| < \varepsilon_m$. It follows that we can set $t_{m+1} = \min(1, t_m + \delta)$. Inspection of the formulas for $\delta$ give us that if the distance of any critical point from the path is positive, then there is a finite $m$ such that $t_m = 1$. □

**Remark 2-3.** In Figure 1, the dots on the edges mark the sequence $x(t_0), x(t_1), \ldots, x(t_{m_{ij}})$. In particular, on the edge from $v_7$ to $v_{10}$ one can see that as the distance to the branch points $s_2, s_3$ gets smaller, the step sizes are reduced accordingly.

**Lemma 2-4.** *Given $\varepsilon < \varepsilon_m$, $t$ with $t_m < t \leq t_{m+1}$, and $\tilde{y}_m$ with $|\tilde{y}_m - y^{(k)}(t_m)| < \varepsilon$, we can use Newton iteration to compute $\tilde{y}$ such that $|\tilde{y} - y^{(k)}(t)| < \varepsilon$.*

*Proof.* We use Newton iteration to approximate a root of $f(t, y)$, with initial value $\tilde{y}_m$. We are looking for the unique root that lies within a radius of $\varepsilon_m$ of the initial value. If at any point the Newton iteration process escapes this disk, or if the iteration does not converge sufficiently quickly, we insert the point $(t_m + t)/2$ and restart. We know that if Newton iteration converges to a value in the disk, it must be the correct value. Furthermore, continuity implies that convergence will occur if $|t - t_m|$ is small enough. □

Since $x(t_0) \notin S$ we can use standard complex root-finding algorithms on $f(x(t_0), y) = 0$, to find approximations $\tilde{y}_0^{(k)}$ to any desired finite accuracy. We then use Lemma 2-4 iteratively to find an approximation $\tilde{y}_m^{(k)}$ to $y^{(k)}(t_m)$, for each $m = 1, \ldots, m_{ij}$.

The Voronoi graph $(V, E)$ generates the fundamental group of $\mathbb{C} - S$, so the lifted graph $(V', E')$ generates the fundamental group of the unramified cover $C(\mathbb{C}) - x^{-1}(S_\infty)$, and therefore also of $C(\mathbb{C})$. We have assumed that $C$ is an absolutely irreducible algebraic curve, so the graph is connected.

**Remark 2-5.** For computing integrals along $v_{ij}^{(k)}$ in Section 3B, we store for each relevant edge $e_{ij}$ the vectors $\{(t_m, \varepsilon_m, \tilde{y}_m^{(1)}, \ldots, \tilde{y}_m^{(n)}) : m \in \{0, \ldots, m_{ij}\}\}$. With this information we can quickly, reliably, and accurately approximate $y^{(k)}(t)$ for $t \in [0, 1]$ using Lemma 2-4.

**2C.** ***Computing the monodromy of $C \to \mathbb{P}^1$.*** We do not need this in the rest of the paper, but a side effect of computing the lifted graph is that we can also compute the monodromy of the cover $C \to \mathbb{P}^1$. To any path in the Voronoi graph we associate a permutation by composing the permutations associated with the constituent edges. For example, to the path $p = (v_1, v_2, v_3)$ we associate the permutation $\sigma_p = \sigma_{12}\sigma_{23}$ (assuming that our permutations act on the right). Choosing, say, $v_1$ as our base point, this provides us with a group homomorphism $\pi_1(\mathbb{C} - S, v_1) \to \mathrm{Sym}(n)$. The image gives the group of deck transformations of the cover or, in terms of field theory, a geometric realization of the Galois group of the degree $n$ field extension of $\mathbb{C}(x)$ given by $\mathbb{C}(x)[y]/(f(x, y))$. In particular, by taking a path that forms a loop around a single point $s \in C \cup \{\infty\}$, we can obtain the local monodromy of $s$. The cycle type of the corresponding permutation gives the ramification indices of the fiber over $s$. In particular, if the permutation is trivial, then $C \to \mathbb{P}^1$ is unramified over $s$.

**2D.** ***Symplectic homology basis.*** Since $C(\mathbb{C})$ is a Riemann surface, it is orientable and hence we have a symplectic structure on its first homology. The pairing on cycles can be computed in the following way. Suppose that $\alpha, \beta$ are two paths intersecting at $v_0^{(1)}$, and that $\alpha$ contains the segment $v_1^{(1)} \to v_0^{(1)} \to v_2^{(1)}$ and that $\beta$ contains the segment $v_3^{(1)} \to v_0^{(1)} \to v_4^{(1)}$. We define

$$\langle \alpha, \beta \rangle_{v_0^{(1)}} = \langle \alpha, \beta \rangle_{v_0^{(1)}}^{\text{in}} + \langle \alpha, \beta \rangle_{v_0^{(1)}}^{\text{out}}, \quad \text{and} \quad \langle \alpha, \beta \rangle = \sum_v \langle \alpha, \beta \rangle_v,$$


**Figure 2.** Examples of the intersection pairing.

where $\langle \alpha, \beta \rangle_{v_0^{(1)}} = 0$ if $\alpha$ or $\beta$ do not pass through $v_0^{(1)}$, and otherwise

$$\langle \alpha, \beta \rangle^{\text{in}}_{v_0^{(1)}} = \begin{cases} 0 & \text{if } v_3 = v_1 \text{ or } v_3 = v_2, \\ \frac{1}{2} & \text{if } v_1, v_3, v_2 \text{ are counterclockwise oriented around } v_0, \\ -\frac{1}{2} & \text{if } v_1, v_3, v_2 \text{ are clockwise oriented around } v_0, \end{cases}$$

$$\langle \alpha, \beta \rangle^{\text{out}}_{v_0^{(1)}} = \begin{cases} 0 & \text{if } v_3 = v_1 \text{ or } v_4 = v_2, \\ \frac{1}{2} & \text{if } v_1, v_2, v_4 \text{ are counterclockwise oriented around } v_0, \\ -\frac{1}{2} & \text{if } v_1, v_2, v_4 \text{ are clockwise oriented around } v_0. \end{cases}$$

At vertices where $\alpha, \beta$ meet transversely, this is clearly the usual intersection pairing on $H_1(C(\mathbb{C}), \mathbb{Z})$. A deformation argument verifies that the half-integer weights extend it properly to cycles with edges in common. An illustration of this intersection pairing is given in Figure 2.

**Lemma 2-6.** *By applying an algorithm by Frobenius* [14, §7] *we can find a* $\mathbb{Z}$*-basis* $\alpha_1, \ldots, \alpha_g, \beta_1, \ldots, \beta_g$ *for* $\mathrm{H}_1(C(\mathbb{C}), \mathbb{Z})$ *such that* $\langle \alpha_i, \alpha_j \rangle = \langle \beta_i, \beta_j \rangle = 0$ *and* $\langle \alpha_i, \beta_j \rangle = \delta_{ij}$.

*Proof.* We first compute a cycle basis for the lifted graph $(V', E')$ described in Section 2B, say $\gamma_1, \ldots, \gamma_r$ and compute the antisymmetric Gram matrix $G_\gamma = (\langle \gamma_i, \gamma_j \rangle)_{ij}$. Frobenius's algorithm yields an integral transformation $B$ such that $BG_\gamma B^T$ is in symplectic normal form, i.e., a block diagonal matrix with $g$ blocks

$$\begin{pmatrix} 0 & d_i \\ -d_i & 0 \end{pmatrix},$$

possibly followed by zeros, with $d_1 \mid d_2 \mid \cdots \mid d_g$. Because $C(\mathbb{C})$ is a complete Riemann surface, we know that $d_1 = \cdots = d_g = 1$ and that $g$ is the genus of $C(\mathbb{C})$. The matrix $B$ gives us $\alpha_1, \beta_1, \ldots, \alpha_g, \beta_g$ as $\mathbb{Z}$-linear combinations of our initial cycle basis $\gamma_1, \ldots, \gamma_r$. □

## 3. Computing the period lattice

**3A.** ***A basis for*** $\mathbf{H^0(C, \Omega^1_C)}$**.** From the adjunction formula [1] we know that $\mathrm{H}^0(C, \Omega^1_C)$ is naturally a subspace of the span of

$$\left\{ \frac{h\,dx}{\partial_y f(x, y)} : h = x^i y^j \text{ with } 0 \le i, j \text{ and } i + j \le n - 3 \right\}.$$

If the projective closure of $\widetilde{C}$ is nonsingular, then $\mathrm{H}^0(C, \Omega^1_C)$ is exactly this span. If $\widetilde{C}$ has only singularities at the projective points $(1:0:0)$, $(0:1:0)$, $(0:0:1)$, and $f$ satisfies some easily tested genericity conditions then Baker's theorem [4] states that we can take those $(i, j)$ for which $(i+1, j+1)$ is an interior point to the Newton polygon of $f(x, y)$. In even more general situations, the adjoint ideal [1, Appendix A, §2] specifies exactly which subspace of polynomials $g$ corresponds to the regular differentials on $C$. We use Baker's theorem when it applies and otherwise rely on Singular [11] to provide us with a basis

$$\left\{\omega_i = \frac{h_i dx}{\partial_y f(x, y)} : i = 1, \ldots, g\right\} \subset \mathrm{H}^0(C, \Omega^1_C).$$

**3B.** ***Computing the period matrix.*** Given a basis $\omega_1, \ldots, \omega_g$ for $\mathrm{H}^0(C, \Omega^1_C)$ and a symplectic basis $\alpha_1, \ldots, \alpha_g, \beta_1, \ldots, \beta_g$ for $\mathrm{H}_1(C(\mathbb{C}), \mathbb{Z})$, the corresponding *period matrix* is

$$\Omega_{\alpha\beta} = (\Omega_\alpha \mid \Omega_\beta) = \left(\int_{\alpha_j} \omega_i \;\middle|\; \int_{\beta_j} \omega_i\right)_{ij}.$$

The resulting *period lattice* is the $\mathbb{Z}$-span $\Lambda = \Omega_{\alpha\beta}\mathbb{Z}^{2g}$ of the columns in $\mathbb{C}^g$. As an analytic space, the Jacobian of $C$ is isomorphic to the complex torus $\mathbb{C}^g/\Lambda$. Our paths consist of lifted line segments, so we numerically approximate the integrals along the edges $e^{(k)}_{ij}$ that occur in our symplectic basis and compute $\Omega_{\alpha\beta}$ by taking the appropriate $\mathbb{Z}$-linear combinations of these approximations. To lighten notation we describe the process for the edge $e^{(1)}_{12}$. As in Section 2B we parametrize the edge by

$$x(t) = (1-t)v_1 + tv_2$$

and with the stored information (see Remark 2-5), we can quickly compute $y^{(k)}(t)$ for given values of $t$. We obtain

$$\int_{e^{(1)}_{12}} \omega_i = (v_2 - v_1) \int_{t=0}^{1} \frac{h_i(x(t)y(t))}{\partial_y f(x(t), y(t))}\, dt.$$

Note that our integrand is holomorphic, so well suited for high order integration schemes such as Gauss–Legendre and Clenshaw–Curtis. We implemented Gauss–Legendre with relatively naive node computation. While in our experiments this was sufficient, there is the theoretical drawback that for very high order approximations, the determination of the integration nodes becomes the dominant part. There are sophisticated methods for obtaining the nodes with a better complexity [6]. Alternatively, quadrature schemes like Clenshaw–Curtis may need more evaluation nodes to obtain the same accuracy, but allow for faster computation of these nodes.

Rather than compute guaranteed bounds, we have settled on a standard error estimation scheme, as described in, for instance, [3, §5] to adapt the number of evaluation nodes. Since our applications will not provide proven results anyway, this is sufficient for our purposes.

**Remark 3-1.** There is a split in literature on how to order the symplectic basis for the period matrix. With the normalization we use, one gets that

$$\Omega_\alpha^{-1}\Omega_{\alpha\beta} = (1 \mid \Omega_\alpha^{-1}\Omega_\beta) = (1 \mid \tau)$$

where $\tau$ is a Riemann matrix, i.e., a symmetric matrix with positive definite imaginary part. Here $\tau$ represents the corresponding lattice in Siegel upper half space. In [5], the period matrix is taken to be $\Omega_{\beta\alpha}$.

## 4. Homomorphism and isomorphism computations

**4A.** ***Computing homomorphisms between complex tori.*** Let $C_1$ and $C_2$ be two curves with Jacobians $J_1$ and $J_2$. Let $\Omega_1$, $\Omega_2$ be period matrices such that $J_1(\mathbb{C}) = \mathbb{C}^{g_1}/\,\Omega_1\mathbb{Z}^{2g_1}$ and $J_2(\mathbb{C}) = \mathbb{C}^{g_2}/\,\Omega_2\mathbb{Z}^{2g_2}$ as analytic groups.

A homomorphism $\phi : J_1 \to J_2$ induces a tangent map $\mathrm{H}^0(C_1, \Omega^1_{C_1})^* \to \mathrm{H}^0(C_2, \Omega^1_{C_2})^*$ and a map on homology $\mathrm{H}_1(C_1, \mathbb{Z}) \to \mathrm{H}_1(C_2, \mathbb{Z})$. After a choice of bases, these correspond to matrices $T = T_\phi \in M_{g_2,g_1}(\mathbb{C})$ and $R = R_\phi \in M_{2g_2,2g_1}(\mathbb{Z})$, which we call the *tangent representation* and the *homology representation* of $\phi$.

**Proposition 4-1.** *Let $\phi : J_1 \to J_2$ be a homomorphism and let $T$, $R$ be the induced matrices described above.*

(i) *The matrices $T = T_\phi$ and $R = R_\phi$ satisfy $T\Omega_1 = \Omega_2 R$.*

(ii) *A pair $(T, R)$ as in* (i) *comes from a uniquely determined homomorphism $\phi : J_1 \to J_2$.*

(iii) *Either of the elements $T$ and $R$ in* (i) *is determined by the other.*

(iv) *If the curves $C_1$ and $C_2$ as well as the chosen bases of differentials and $\phi$ are defined over $k \subset \overline{Q}$, then the matrix $T$ is an element of $M_{g_2,g_1}(k)$.*

*Proof.* These results are in [5, §1.2]. Writing $\overline{\Omega}_2$ for the elementwise complex conjugate of $\Omega_2$, we remark for part (iii) that we can determine $R$ from $T$ by considering

$$\begin{pmatrix} T\Omega_1 \\ \overline{T\Omega}_1 \end{pmatrix} = \begin{pmatrix} \Omega_2 \\ \overline{\Omega}_2 \end{pmatrix} R, \tag{4-2}$$

since the first matrix on the right-hand side of (4-2) is invertible. Conversely, we can determine $T$ from $R$ by considering the first $g_1$ columns on either side of $T\Omega_1 = \Omega_2 R$ since the corresponding matrices are invertible. □

We seek to recover these pairs $(T, R)$ numerically. This question was briefly touched upon in [7, §6.1], and before that in [28, §3], but here we give some more detail.

**Lemma 4-3.** *Given approximations of $\Omega_1$, $\Omega_2$ to sufficiently high precision, we can numerically recover a $\mathbb{Z}$-basis for* $\mathrm{Hom}(J_1, J_2)$, *represented by matrices $R \in M_{2g_2,2g_1}(\mathbb{Z})$ and $T \in M_{g_2,g_1}(\mathbb{C})$ as in Proposition 4-1.*

*Proof.* Following Remark 3-1, we can normalize $\Omega_i$ to be of the form $(1 \mid \tau_i)$. We write

$$R = \begin{pmatrix} D & B \\ C & A \end{pmatrix}, \quad \text{where } D, B, C, A \in M_{g_2,g_1}(\mathbb{Z}).$$

Then $T = D + \tau_2 C$, and

$$B + \tau_2 A = (D + \tau_2 C)\tau_1.$$

Considering real and imaginary parts separately, we obtain $m = 2g_1g_2$ equations with real coefficients in $n = 4g_1g_2$ integer variables, denoted by $M \in M_{m,n}(\mathbb{R})$. We recognize integer solutions that are small compared to the precision to which we calculated $\tau_1, \tau_2$ in the following way. Observe that such solutions correspond to short vectors in the lattice generated by the columns of $(I \mid \varepsilon^{-1}M)$, where $\varepsilon$ is some small real number. The LLL algorithm can find such vectors, and we keep the ones that lie in the kernel to the specified precision.

If sufficient precision is used, then we obtain a basis for $\mathrm{Hom}(J_1, J_2)$ in this way. (Heuristically, any approximation to high precision will do.) Proposition 4-1 shows how to recover the tangent representation $T$ from the corresponding homology representations $R$. □

**Remark 4-4.** An important tuning parameter for applications of LLL is the precision. We have an (estimated) accuracy of the entries in the matrix $M$. We choose $\varepsilon$ such that $\varepsilon^{-1}M$ has accuracy to within 0.5. If we have computed the period matrices to a precision of $b$ bits, then $M$ contains about $2g_1g_2b$ bits of information. We would therefore expect that the entries in the LLL basis have entries of size about $(2g_1g_2b)/(4g_1g_2) = b/2$. We only keep vectors that have entries of bit size at most half that.

In the context of Proposition 4-1(iv), the algebraic entries of $T$ can be recognized by another application of the LLL algorithm; the SageMath implementation number_field_elements_from_algebraics can be used to this end, for example. We emphasize that in order to recover this algebraicity, we need the original period matrices $\Omega_i$ with respect to a basis of $\mathrm{H}^0(C, \Omega^1_C)$ defined over $\overline{Q}$. A differential basis for which the period matrix takes the shape $(1 \mid \tau_i)$ usually has a transcendental field of definition.

For a Jacobian $J$, the natural principal polarization gives rise to the Rosati involution on $\mathrm{End}(J)$ [5, §5.1]. We choose a symplectic basis for $H_1(C(\mathbb{C}), \mathbb{Z})$ and denote the standard symplectic form by

$$E = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \in M_{2g,2g}(\mathbb{Z}).$$

**Proposition 4-5.** *Let $\phi : J \to J$ be an endomorphism with corresponding pair $(T, R)$ as in Proposition 4-1*(i)*. Then the Rosati involution $\phi^\dagger$ of $\phi$ corresponds to the pair $(T^\dagger, R^\dagger)$ with*

$$R^\dagger = -ER^tE.$$

*Proof.* Since we chose our homology basis to be symplectic, the Rosati involution of the endomorphism corresponding to $R$ corresponds to the adjoint with respect to the pairing defined by $E$, which is $ER^tE^{-1} = -ER^tE$. □

**Remark 4-6.** Proposition 4-1(iii) shows how to obtain $T^\dagger$ from $R^\dagger$.

Recall [5, Chapter 5] that any polarized abelian variety allows a decomposition up to isogeny

$$J \sim \prod_i A_i^{e_i} \tag{4-7}$$

into powers of simple polarized quotient abelian varieties $A_i$.

**Corollary 4-8.** *Let $J$ be the Jacobian of a curve $C$, and let $\Omega$ be a corresponding period matrix. If we know $\Omega$ to sufficiently high precision, then we can numerically determine the factors in (4-7). Furthermore, if $J$ is defined over $\overline{Q}$, we can numerically determine a field of definition for each of the conjectural factors $A_i$.*

*Proof.* Using Lemma 4-3 we can compute generators for $\mathrm{End}(J)$. We can then determine symmetric idempotent matrices $e \in M_{2g,2g}(\mathbb{Q})$ by using meataxe algorithms, or alternatively by directly solving $e^2 = e$ in the subring of $\mathrm{End}(J)$ fixed by the Rosati involution. The columns of $\Omega e$ span a complex torus of smaller dimension. By [18] all isogeny factors of $J$ occur this way.

In order to find a field of definition, we can determine the matrix $T$ corresponding to $e$ and recognize its entries as algebraic numbers. Then [18] shows that the image of the projection $T$ is still polarized, and defined over the corresponding field. □

**4B.** ***Computing symplectic isomorphisms.*** When $g_1 = g_2$, Lemma 4-3 allows us to recover possible isomorphisms between $J_1$ and $J_2$, as these correspond to the matrices $R$ with $\det(R) = \pm 1$.

In particular, this gives us a description of the automorphism group of a Jacobian variety $J$ as the subgroup of elements of $\mathrm{End}(J)$ with determinant 1. This group can be infinite. However, note that we have principal polarizations on $J_1$ and $J_2$. We take symplectic bases for the homology of both Jacobians, and let $\alpha : J_1 \to J_2$ be an isomorphism, represented by $R \in M_{2g,2g}(\mathbb{Z})$.

**Definition 4-9.** We say that $\alpha$ is *symplectic* if we have $R^t E_2 R = E_1$.

**Remark 4-10.** More intrinsically, the definition demands that the canonical intersection pairings $E_1$ and $E_2$ on $\mathrm{H}_1(C_1, \mathbb{Z})$ and $\mathrm{H}_1(C_2, \mathbb{Z})$ satisfy $\alpha^* E_2 = E_1$.

The symplectic automorphisms of $J$ form a group, which is called the *symplectic automorphism group* $\mathrm{Aut}(J, E)$ of the principally polarized abelian variety $(J, E)$.

**Theorem 4-11.** *Suppose that $C$ is a smooth curve of genus at least 2. Then we have the following*:

(i) *The symplectic automorphism group of $J$ is finite.*

(ii) *There is a canonical map* $\mathrm{Aut}(C) \to \mathrm{Aut}(J, E)$. *If $C$ is nonhyperelliptic, then this map is an isomorphism; otherwise it induces an isomorphism* $\mathrm{Aut}(C) \xrightarrow{\sim} \mathrm{Aut}(J, E)/\langle -1 \rangle$.

*Proof.* Part (i) is [5, Corollary 5.1.9], and (ii) is the Torelli theorem [21, Theorem 12.1]. □

This shows we can recover $\mathrm{Aut}(C)$ from $\mathrm{Aut}(J, E)$. In fact, from the linear action of the symplectic automorphism on $\mathrm{H}^0(C, \Omega^1_C)^*$ we can recover its action on a canonical model of $C$ in $\mathbb{P}\mathrm{H}^0(C, \Omega^1_C)^*$. For nonhyperelliptic curves this realizes the isomorphism $\mathrm{Aut}(J, E)/\langle -1 \rangle \simeq \mathrm{Aut}(C)$ explicitly. For hyperelliptic curves it recovers the *reduced* automorphism group, which can in fact be determined more efficiently by purely algebraic methods, as described in [20].

If $C$ is defined over $\overline{Q}$, then we can verify that the numerical automorphisms thus obtained are correct by working purely algebraically: by Proposition 4-1(iv) we obtain an algebraic expression for $T$. We can then check by exact calculation that it fixes the defining ideal of the canonical embedding of $C$.

More generally, given two Jacobians $J_1$ and $J_2$, we can determine the numerical symplectic isomorphisms between them. To this end, one proceeds as in the proof of [5, Theorem 5.1.8]: we have

$$R^t E_2 R = E_1 \tag{4-12}$$

or

$$(E_1^{-1} R^t E_2) R = 1. \tag{4-13}$$

In particular, we get

$$\operatorname{tr}((E_1^{-1} R^t E_2) R) = 2g \tag{4-14}$$

for the common genus $g$ of $C_1$ and $C_2$. Let $B = \{B_1, \ldots, B_d\}$ be a $\mathbb{Z}$-basis of $\operatorname{Hom}(J_1, J_2)$. Then we can write

$$R = \sum_{i=1}^{d} \lambda_i B_i. \tag{4-15}$$

The positivity of the Rosati involution implies that the set of solutions $\lambda_1, \ldots, \lambda_d$ of (4-14) is finite. Explicitly, these can be obtained by using the Fincke–Pohst algorithm [13]. For the finite set of solutions thus obtained, we check which yield matrices $R$ in (4-15) that numerically satisfy (4-13). These matrices constitute the homology representations $R$ of numerical isomorphisms $J_1 \to J_2$. From this, we can obtain the corresponding tangent representations $T$ by Proposition 4-1(iii), and we can verify these algebraically as above.

**Remark 4-16.** Using the same methods, one can determine the maps $C_1 \to C_2$ of a fixed degree $d$ by finding the $\alpha$ for which $\alpha_* E_1 = d E_2$. This is especially useful if the genus $g_2$ of $C_2$ is larger than 2, since then we can bound $d$ by $(2g_1 - 2)/(2g_2 - 2)$.

In this way, we obtain the following pseudocode.

**Algorithm 4-17** (compute isomorphisms between curves).

*Input*: Planar equations $f_1$, $f_2$ for two curves $C_1$, $C_2$, as well as a given working precision.

*Output*: A numerical determination of the set of isomorphisms $C_1 \to C_2$.

(1) Check if $g(C_1) = g(C_2)$ and that either both curves are hyperelliptic or both are nonhyperelliptic; if not, return the empty set.

(2) If $C_1$ and $C_2$ are both hyperelliptic, use the methods in [20].

(3) Otherwise, determine the period matrices $P_1$, $P_2$ of $C_1$, $C_2$ to the given precision, using Algorithm 1-2.

(4) Using Lemma 4-3 (see also [7, §6.1]), determine a $\mathbb{Z}$-basis of $\operatorname{Hom}(J_1, J_2) \subset M_{2g,2g}(\mathbb{Z})$ represented by integral matrices $R \in M_{2g,2g}(\mathbb{Z})$.

(5) Using Fincke–Pohst, determine the finite set $S = \{R \in \operatorname{Hom}(J_1, J_2) \mid \operatorname{tr}((E_1^{-1} R^t E_2) R) = 2g\}$.

(6) Using the canonical morphisms with respect to the chosen bases of differentials, return the subset of elements of $S$ that indeed induce an isomorphism $C_1 \to C_2$.

## 5. Examples

The examples in this section can be found online at [9] or in an online supplement.

**Example 5A.** Consider the curve

$$C : 4x^6 - 54x^5y - 729x^4 + 108x^3y^3 + 39366x^2 - 54xy^5 - 531441.$$

This is a nonhyperelliptic curve of genus 6. Theorem 4-11 shows that, at least numerically, its geometric automorphism group is of order 2 and generated by the involution $\iota : (x, y) \mapsto (-x, -y)$. Lemma 4-3 shows that its numerical geometric endomorphism ring is of index 6 in $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$.

The quotient of $C$ by its automorphism group gives a morphism of degree 2 to the genus 2 curve

$$D_1 : y^2 = x^6 - x^5 + 1.$$

This corresponds to the symmetric idempotent $e_1 = 1 - (1 + \iota)/2$ in the endomorphism algebra, whose tangent representation has numerical rank 4. Numerically, there are two other such symmetric idempotents $e_2$, $e_3$. Together, their kernels span $\mathrm{H}_1(C(\mathbb{C}), \mathbb{Z})$, and all of these are of dimension $4 = 2 \cdot 2$. This means that along with $A_1 = \mathrm{Jac}(D_1)$ there should be two other 2-dimensional abelian subvarieties $A_2$, $A_3$ of $\mathrm{Jac}(C)$ such that

$$\mathrm{Jac}(C) \sim A_1 \times A_2 \times A_3.$$

We now describe the abelian varieties $A_2$ and $A_3$.

The tangent representation of an idempotent $e_i$ corresponding to a factor $A_i$ has dimension 4. Its kernel is therefore a subspace $W_i$ of $\mathrm{H}^0(C, \Omega^1_C)^*$ of dimension 2. If the idempotent $e_i$ is induced by a map of curves $p : C \to D_i$, then $W_i = p^*\mathrm{H}^0(D_i, \Omega^1_{D_i})^*$ for some curve $D_i$ and some projection $p : C \to D_i$.

By composing the canonical map with the projection to the projective line $\mathbb{P}W_i$, all the idempotents $e_i$ give rise to a cover $C \to \mathbb{P}W_i$. Now if $e_i$ is induced by a projection $C \to D_i$ at all, then $D_i$ is a subcover of this map $C \to \mathbb{P}W_i$. It turns out that all $e_i$ give rise a subcover of the degree 6 non-Galois cover

$$C \to \mathbb{P}^1,$$
$$(x, y) \to y/x.$$

A monodromy calculation gives the Galois closure $Z \to \mathbb{P}^1$ of this cover: its Galois group $G$ is dihedral of order 12. In particular, considering the subgroups of $G$ that properly contain the degree 2 subgroup corresponding to $C \to \mathbb{P}^1$, we see that there exist exactly two nontrivial subcovers $p_1 : C \to D_1$ and $p_2 : C \to D_2$ of $C \to \mathbb{P}^1$. These subcovers have degree 2 and degree 3, respectively.

The curves $D_1$ and $D_2$ are both of genus 2. The first subcover $p_1$ is a quotient of $C$ and corresponds to the curve $D_1$ above. The second subcover $p_2$ is not a quotient of $C$, but using Galois theory for the normal closure still furnishes us with a defining equation of $D_2$, namely

$$D_2 : y^2 = -16x^5 - 40x^4 + 32x^3 + 88x^2 - 32x - 23.$$

We take $A_2$ to be the Jacobian of $D_2$.

Since we have exhausted all subcovers of the Galois closure $Z \to \mathbb{P}^1$, we conclude that $A_3$ does not arise from a cover $C \to D_3$. Still, using analytic methods we find that numerically the subvariety $A_3$ is simple and admits a (unique) principal polarization. It is therefore the Jacobian of a curve $D_3$ of genus 2. Calculating the Igusa invariants numerically, we reconstruct

$$D_3 : y^2 = x^6 + 3x^4 + 3x^2 + x + 1.$$

We can numerically check that there is a morphism of abelian varieties $\mathrm{Jac}(C) \to \mathrm{Jac}(D_3)$ that is compatible with the polarizations on both curves. A computation on homology again shows that this morphism cannot come from a morphism of curves $C \to D_3$; if it did, the degree of such a morphism would have to be 6, which is impossible in light of the Riemann–Hurwitz formula. An explicit correspondence between $C$ and $D_3$ can in principle be found by using the methods in [10]; however, this will still be a rather involved calculation, which we have therefore not performed yet.

**Example 5B.** Consider the plane model

$$C : f(x, y) = 1 + 7xy + 21x^2y^2 + 35x^3y^3 + 28x^4y^4 + 2x^7 + 2y^7 = 0$$

of the Macbeath curve from [16], which is due to Bradley Brock. Its automorphism group is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_8)$ and has order 504. We illustrate that the algorithm described in Section 4B indeed recovers that $\mathrm{Aut}(C)$ is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_8)$, that $C$ is indeed the Macbeath curve, and moreover that all the automorphisms of $C$ are already defined over the cyclotomic field $\mathbb{Q}(\zeta_7)$.

From the adjoint ideal computed by Singular [11] we find a $\mathbb{Q}$-rational basis of 7 global differentials of the form $h\omega$, where $\omega = \frac{\partial f}{\partial y}\,dx$ and where $h$ is one of

$$\{h_1, \ldots, h_7\} = \{4x^2y^2 + 3xy + 1, 2y^5 - x^3y - x^2, 2xy^4 + x^4 + y^3, \\ 4x^2y^3 + 3xy^2 + y, 4x^3y^2 + 3x^2y + x, 2x^4y + y^4 + x^3, 2x^5 - xy^3 - y^2\}.$$

We can determine a corresponding period matrix to binary precision 100 after about a minute's calculation, and find the corresponding numerical symplectic automorphism group. It indeed has cardinality 1008, and its elements are well approximated by relatively simple matrices in the cyclotomic field $\mathbb{Q}(\zeta_7)$ that also generate a group $G \subset \mathrm{GL}_7(\mathbb{Q}(\zeta_7))$ of order 1008 with $G \cap \mathbb{Q}(\zeta_7)^* = \langle -1 \rangle$ and with $G/\langle -1 \rangle \cong \mathrm{PSL}_2(\mathbb{F}_2^3)$. In practice this is of course indication enough that the automorphism group has been found.

To prove this, we choose two elements $T_1$, $T_2$ of $G$. The first of these is the diagonal matrix with entries $\{1, \zeta_7^2, \zeta_7^4, \zeta_7^6, \zeta_7, \zeta_7^3, \zeta_7^5\}$; the other has relatively modest entries but is still too large to write down here. We check that these matrices generate a subgroup of $G$ of cardinality 504 that projects isomorphically to $G/\langle -1 \rangle$. If we show that $T_1$ and $T_2$ indeed correspond to automorphisms of $C$, then our claims will be proved, since any curve of genus 7 with (at least) 504 automorphisms is birational to the Macbeath curve.

To verify this claim, one can use the canonical embedding of $C$ with respect to the given basis of global differentials $\{h_i\omega\}$. Alternatively, one observes that

$$x = h_5/h_1, \qquad y = h_4/h_1.$$

This means that after applying one of the transformations $T_1, T_2$ to the basis of global differentials to obtain the linear transformations $\{T_i(h_j\omega)\}_j$, we can recover corresponding transformations $x'$ and $y'$ in $x$ and $y$ via

$$x' = T_i(h_5\omega)/T_i(h_1\omega), \qquad y' = T_i(h_4\omega)/T_i(h_1\omega).$$

For $T_1$, we get

$$x' = \zeta_7 x, \qquad y' = \zeta_7^6 y,$$

while when evaluating natively for $T_2$ we get two decidedly unpleasant rational expressions the degree of whose denominator and numerator both equal 5. In either case, we can check that the corresponding substitutions leave the equation for $C$ invariant, which provides us with the desired verification of correctness of $T_1$ and $T_2$.

**Example 5C.** This example illustrates the value of being able to verify isogeny factors of Jacobians numerically. We consider a genus 4 curve $C$ and an unramified double cover $\pi : D \to C$. Then $D$ is of genus 7, and $\mathrm{Jac}(D)$ is isogenous to $\mathrm{Jac}(C) \times A$ for some 3-dimensional abelian variety $A$. The theory of Prym varieties shows that we can take $A$ to be principally polarized. It follows that generally $A$ is a quadratic twist of a Jacobian of a genus 3 curve $F$. In [22] W. P. Milne constructs a plane quartic $F$ from a genus 4 curve $C$ with data that amounts to specifying an unramified double cover of $C$. One would guess that $\mathrm{Jac}(F)$ is indeed the Prym variety of $D/C$. Here we check this numerically for a particular example. See [8] for a modern, systematic treatment of this construction.

Let $C$ be the canonical genus 4 curve in $\mathbb{P}^3$, described by $\Gamma_2 = \Gamma_3 = 0$, where

$$\Gamma_2 = x^2 + xy + y^2 + 3xz + z^2 - yw + w^2, \qquad \Gamma_3 = xyz + xyw + xzw + yzw.$$

A plane model for this curve is given by

$$\widetilde{C} : y^4w^2 - y^3w^3 + y^2w^4 + 2y^4w - y^3w^2 + 2yw^4 + y^4 - 2y^2w^2 + yw^3 + w^4 - y^2w - yw^2 + y^2 + 2yw + w^2 = 0.$$

Since $\Gamma_3$ has four nodal singularities in general position, it is a Cayley cubic. It admits a double cover unramified outside the nodes, obtained by adjoining the square root of the Hessian of $\Gamma_3$. Since $C$ does not pass through the nodes, this induces an unramified double cover $D$ of $C$. It is geometrically irreducible and admits a plane model

$$\widetilde{D} : u^4v^4 - 3u^4v^2 + u^4 - u^3v^3 - 2u^3v + u^2v^2 - u^2 + 3uv^3 + 2uv + v^4 + v^2 + 1 = 0.$$

Milne's construction yields a plane quartic

$$F : 5s^4 + 28s^3t + 28s^3 + 47s^2t^2 + 76s^2t + 44s^2 + 34st^3 + 82st^2 + 66st + 18s + 16t^4 + 34t^3 + 32t^2 + 18t + 1 = 0.$$

Numerical computation shows that $\mathrm{End}(\mathrm{Jac}(C)) = \mathbb{Z}$ and that $\mathrm{End}(\mathrm{Jac}(F)) = \mathbb{Z}$, which can be confirmed by the $\ell$-adic methods in [10]. It follows that $\mathrm{Hom}(\mathrm{Jac}(F), \mathrm{Jac}(C)) = 0$. Furthermore, we find that $\mathrm{Hom}(\mathrm{Jac}(C), \mathrm{Jac}(D))$ and $\mathrm{Hom}(\mathrm{Jac}(F), \mathrm{Jac}(D))$ are 1-dimensional, so it follows that $\mathrm{Jac}(D) \sim \mathrm{Jac}(C) \times \mathrm{Jac}(F)$ and that $\mathrm{Jac}(F)$ lies in the Prym variety of the cover $D \to C$. Thus, we obtain numerical evidence that Milne indeed provides a construction of a curve $F$ generating the Prym variety.

## Acknowledgments

We would like to thank Tim Dokchitser and Mark van Hoeij for references and comments on Baker's theorem in Section 3A, and Catherine Ray for pointing out errors in a previous version of Section 4.

## References

[1] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris, *Geometry of algebraic curves, I*, Grundlehren der Mathematischen Wissenschaften, no. 267, Springer, 1985. MR 770932

[2] Franz Aurenhammer, *Voronoi diagrams: a survey of a fundamental geometric data structure*, ACM Comput. Surv. **23** (1991), no. 3, 345–405.

[3] David H. Bailey, Karthik Jeyabalan, and Xiaoye S. Li, *A comparison of three high-precision quadrature schemes*, Experiment. Math. **14** (2005), no. 3, 317–329. MR 2172710

[4] H. F. Baker, *Examples of the application of Newton's polygon to the theory of singular points of algebraic functions*, Trans. Cambridge Philos. Soc. **15** (1893), 403–450.

[5] Christina Birkenhake and Herbert Lange, *Complex abelian varieties*, 2nd ed., Grundlehren der Mathematischen Wissenschaften, no. 302, Springer, 2004. MR 2062673

[6] I. Bogaert, *Iteration-free computation of Gauss–Legendre quadrature nodes and weights*, SIAM J. Sci. Comput. **36** (2014), no. 3, A1008–A1026. MR 3209728

[7] 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** (2016), suppl. A, 235–254. MR 3540958

[8] Nils Bruin and Emre Can Sertöz, *Prym varieties of genus four curves*, preprint, 2018. arXiv 1808.07881v1

[9] Nils Bruin, Jeroen Sijsling, and Alexandre Zotine, *Calculations with numerical Jacobians*, 2018.

[10] Edgar Costa, Nicolas Mascot, Jeroen Sijsling, and John Voight, *Rigorous computation of the endomorphism ring of a Jacobian*, Math. Comp. (online publication September 2018).

[11] Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, and Hans Schönemann, *Singular 4-4-1: a computer algebra system for polynomial computations*, 2018.

[12] Bernard Deconinck and Mark van Hoeij, *Computing Riemann matrices of algebraic curves: advances in nonlinear mathematics and science*, Phys. D **152–153** (2001), 28–46. MR 1837895

[13] U. Fincke and M. Pohst, *Improved methods for calculating vectors of short length in a lattice, including a complexity analysis*, Math. Comp. **44** (1985), no. 170, 463–471. MR 777278

[14] G. Frobenius, *Theorie der linearen Formen mit ganzen Coefficienten*, J. Reine Ang. Math. **86** (1879), 146–208. MR 1579769

[15] F. Hess, *An algorithm for computing isomorphisms of algebraic function fields*, Algorithmic number theory, Lecture Notes in Comput. Sci., no. 3076, Springer, 2004, pp. 263–271. MR 2137359

[16] Ruben A. Hidalgo, *About the Fricke–Macbeath curve*, Eur. J. Math. **4** (2018), no. 1, 313–325. MR 3782224

[17] Fredrik Johansson, *Numerical integration in arbitrary-precision ball arithmetic*, preprint, 2018. arXiv 1802.07942v1

[18] E. Kani and M. Rosen, *Idempotent relations and factors of Jacobians*, Math. Ann. **284** (1989), no. 2, 307–327. MR 1000113

[19] Stefan Kranich, *An epsilon-delta bound for plane algebraic curves and its use for certified homotopy continuation of systems of plane algebraic curves*, preprint, 2016. arXiv 1505.03432v2

[20] Reynald Lercier, Christophe Ritzenthaler, and Jeroen Sijsling, *Fast computation of isomorphisms of hyperelliptic curves and explicit Galois descent*, ANTS X — Proceedings of the Tenth Algorithmic Number Theory Symposium, Open Book Ser., no. 1, Math. Sci. Publ., Berkeley, CA, 2013, pp. 463–486. MR 3207427

[21] J. S. Milne, *Jacobian varieties*, Arithmetic geometry, Springer, 1986, pp. 167–212. MR 861976

[22] W. P. Milne, *Sextactic cones and tritangent planes of the same system of a quadri-cubic curve*, Proc. London Math. Soc. (2) **21** (1923), 373–380. MR 1575365

[23] Pascal Molin and Christian Neurohr, *Computing period matrices and the Abel–Jacobi map of superelliptic curves*, Math. Comp. (online publication May 2018).

[24] Christian Neurohr, *Efficient integration on Riemann surfaces and applications*, Ph.D. thesis, Carl von Ossietzky Universität Oldenburg, 2018.

[25] Emre Can Sertöz, *Computing periods of hypersurfaces*, preprint, 2018. arXiv 1803.08068v1

[26] Chris Swierczewski, *abelfunctions: a library for computing with Abelian functions, Riemann surfaces, and algebraic curves*, 2017.

[27] C. L. Tretkoff and M. D. Tretkoff, *Combinatorial group theory, Riemann surfaces and differential equations*, Contributions to group theory, Contemp. Math., no. 33, Amer. Math. Soc., Providence, RI, 1984, pp. 467–519. MR 767125

[28] Paul B. van Wamelen, *Computing with the analytic Jacobian of a genus 2 curve*, Discovering mathematics with Magma, Algorithms Comput. Math., no. 19, Springer, 2006, pp. 117–135. MR 2278925

Received 2 Mar 2018. Revised 18 Jun 2018.

NILS BRUIN: nbruin@sfu.ca
*Department of Mathematics, Simon Fraser University, Burnaby, BC, Canada*

JEROEN SIJSLING: jeroen.sijsling@uni-ulm.de
*Institut für Reine Mathematik, Universität Ulm, Ulm, Germany*

ALEXANDRE ZOTINE: sasha_zotine@sfu.ca
*Department of Mathematics, Simon Fraser University, Burnaby, BC, Canada*

VOLUME EDITORS

Renate Scheidler
University of Calgary
Calgary, AB T2N 1N4
Canada

Jonathan Sorenson
Butler University
Indianapolis, IN 46208
United States

The cover image is based on a design by Linh Chi Bui.

The contents of this work are copyrighted by MSP or the respective authors. All rights reserved.

Electronic copies can be obtained free of charge from http://msp.org/obs/2 and printed copies can be ordered from MSP (contact@msp.org).

The Open Book Series is a trademark of Mathematical Sciences Publishers.

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-02-6 (print), 978-1-935107-03-3 (electronic)

First published 2019.

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org http://msp.org

THE OPEN BOOK SERIES 2

# Thirteenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the thirteenth ANTS meeting, held July 16-20, 2018, at the University of Wisconsin-Madison. It includes revised and edited versions of 28 refereed papers presented at the conference.

Edited by Renate Scheidler and Jonathan Sorenson

## CONTRIBUTORS

Simon Abelard
Sonny Arora
Vishal Arul
Angelica Babei
Jens-Dietrich Bauch
Alex J. Best
Jean-François Biasse
Alin Bostan
Reinier Bröker
Nils Bruin
Xavier Caruso
Stephanie Chan
Qi Cheng
Gilles Christol
Owen Colman
Edgar Costa
Philippe Dumas
Kirsten Eisenträger
Claus Fieker
Shuhong Gao
Pierrick Gaudry
Alexandre Gélin
Alexandru Ghitza
Laurent Grémy
Jeroen Hanselman
David Harvey
Tommy Hofmann
Everett W. Howe
David Hubbard
Kiran S. Kedlaya
Thorsten Kleinjung
David Kohel
Wanlin Li
Richard Magner
Anna Medvedovsky
Michael Musty
Ha Thanh Nguyen Tran
Christophe Ritzenthaler
David Roe
J. Maurice Rojas
Nathan C. Ryan
Renate Scheidler
Sam Schiavone
Andrew Shallue
Jeroen Sijsling
Carlo Sircana
Jonathan Sorenson
Pierre-Jean Spaenlehauer
Andrew V. Sutherland
Nicholas Triantafillou
Joris van der Hoeven
Christine Van Vredendaal
John Voight
Daqing Wan
Lawrence C. Washington
Jonathan Webster
Benjamin Wesolowski
Yinan Zhang
Alexandre Zotine