Rigorous computation of the endomorphism ring of a Jacobian

Jeroen Sijsling
Universität Ulm

joint work with
Edgar Costa, Nicolas Mascot, and John Voight

Numerical Methods in Algebraic Geometry
Université de Rennes 1
February 23, 2018

Setup

Let F be a number field with algebraic closure F^{al}. Let X be a nice (smooth, projective, geometrically integral) curve over F of genus g given by equations. Let J be the Jacobian of X. We want to compute the endomorphism ring $\mathrm{End}(J)$.

Setup

Let F be a number field with algebraic closure F^{al}. Let X be a nice (smooth, projective, geometrically integral) curve over F of genus g given by equations. Let J be the Jacobian of X. We want to compute the endomorphism ring $\mathrm{End}(J)$.

We represent an element $\alpha \in \mathrm{End}(J)$ as follows. Fix a base point $P_0 \in X$. This determines a map

$$\begin{aligned} \iota : X &\to J \\ P &\mapsto [P] - [P_0] \end{aligned}$$

which is injective if $g > 0$. We get a composed map

$$\begin{aligned} \alpha \circ \iota : X &\to J \to J \\ P &\mapsto \alpha(\iota(P)) =: \sum_{i=1}^{g} \iota(Q_i). \end{aligned}$$

This traces out a divisor on $X \times X$, which determines α.

Alternative representations

$$\alpha \circ \iota : X \to J \to J$$

$$P \mapsto \alpha(\iota(P)) = \sum_{i=1}^{g} \iota(Q_i)$$

Alternatively, we can use a (possibly singular) plane equation $f(x, y) = 0$ for X. We can describe the points Q_i by giving a polynomial that vanishes on their x-coordinates, along with a second polynomial that interpolates the corresponding y-values. This leads to Cantor equations

$$x^g + a_1 x^{g-1} + \ldots + a_g = 0$$
$$b_1 x^{g-1} + \ldots + b_g = y$$

with $a_i, b_j \in F(X)$.

Alternative representations

The tangent space of J in 0 is naturally isomorphic to the dual of $H^0(X, \omega_X)$, and over $\mathbb{C}$ we have

$$J(\mathbb{C}) = H^0(X(\mathbb{C}), \omega_X)^\vee / H_1(X(\mathbb{C}), \mathbb{Z}).$$

If $D \subset X \times X$ is the divisor corresponding to α, then for $T = T\alpha$ we have

$$T = ((p_1)_*(p_2)^*)^\vee : H^0(X, \omega_X)^\vee \to H^0(X, \omega_X)^\vee.$$

Over $\mathbb{C}$, we also get a second, compatible map

$$R : H_1(X(\mathbb{C}), \mathbb{Z}) \to H_1(X(\mathbb{C}), \mathbb{Z}).$$

In practice, we choose bases and consider T as an element of $\mathrm{M}_g(F^{\mathrm{al}})$ and R as an element of $\mathrm{M}_{2g}(\mathbb{Z})$. For the period matrix Π of X we then have

$$T\Pi = \Pi R.$$

Our objective, more precisely

For us, to compute the endomorphism ring of J means to determine and represent the ring $\mathrm{End}(J_{F^{\mathrm{al}}})$ as a $\mathrm{Gal}(F^{\mathrm{al}} \,|\, F)$-module. In other words, we want to calculate

- a finite Galois extension $K \supseteq F$ with $\mathrm{End}(J_K) = \mathrm{End}(J_{F^{\mathrm{al}}})$,
- a $\mathbb{Z}$-basis for $\mathrm{End}(J_K)$, and
- the multiplication table as well as the action of $\mathrm{Gal}(K \,|\, F)$ (both with respect to the aforementioned basis).

This computational problem has many applications, for example in modularity.

First approach: some day the twain shall meet

Davide Lombardo has shown that there is a day-and-night algorithm to compute the geometric endomorphism ring of J. Briefly:

- By a theorem of Silverberg, $\mathrm{End}(J_{F^{\mathrm{al}}})$ is defined over $K = F(J[3])$.
- By day, we compute a lower bound by searching for endomorphisms by naively trying all maps $J \dashrightarrow J$.
- By night, we compute an upper bound by creeping up on the isomorphism

$$\mathrm{End}(J_K) \otimes \mathbb{Z}_\ell \simeq \mathrm{End}_{\mathrm{Gal}(F^{\mathrm{al}}|K)} T_\ell(J_K).$$

Eventually, the lower and upper bounds will meet.

Upper bounds in genus 2

We first study the rank of the algebra $\mathrm{End}(J_K) \otimes \mathbb{Q}$. Recall that

$$\mathrm{NS}(J_K) \otimes \mathbb{Q} \simeq \{\varphi \in \mathrm{End}(J_K) \otimes \mathbb{Q} : \varphi^\dagger = \varphi\}.$$

Let ρ be the rank of $\mathrm{NS}(J_K)$. In genus 2, the Albert classification shows that ρ only depends on $\mathrm{End}(J_K) \otimes \mathbb{R}$. More precisely, we have:

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

Upper bounds in genus 2

Let $\mathfrak{p}$ be a prime where X has good reduction, and denote the reduction of the Jacobian by $J/\mathfrak{p}$. Then there is an inequality $\rho \leq \rho_{\mathfrak{p}} := \rho(J/\mathfrak{p})$. Define

$$\begin{aligned} c_1(T) &= \det(1 - \mathrm{Frob}_{\mathfrak{p}}\, T \,|\, H^1(J/\mathfrak{p}, \mathbb{Q}_\ell)) \\ &= 1 + a_1 T + a_2 T^2 + a_1 q T^3 + q^2 T^4 \\ c_2(T) &= \det(1 - \mathrm{Frob}_{\mathfrak{p}}\, T \,|\, H^2(J/\mathfrak{p}, \mathbb{Q}_\ell)) \\ &= (1 - qT^2)(1 + (2q - a_2)T + (2q + a_1^2 - 2a_2)qT^2 \\ &\qquad\qquad + (2q - a_2)q^2 T^3 + q^4 T^4). \end{aligned}$$

The Tate conjecture shows:

(i) $\rho_{\mathfrak{p}}$ is the number of reciprocal roots of c_2 that are q times a root of unity;

(ii) if X has primitive CM by a quartic number field L and if $\mathfrak{p}$ splits completely in L, then c_1 is irreducible and defines L.

Upper bounds in genus 2

(i) $\rho_{\mathfrak{p}}$ is the number of reciprocal roots of c_2 that are q times a root of unity;

(ii) if X has primitive CM by a quartic number field L and if $\mathfrak{p}$ splits completely in L, then c_1 is irreducible and defines L.

Results by Charles show that if ρ is even, then there are infinitely many primes for which $\rho = \rho_{\mathfrak{p}}$. If ρ is odd, then $\rho + 1 = \rho_{\mathfrak{p}}$ for infinitely many primes, and moreover

$$\mathrm{disc}(\mathrm{NS}((J/\mathfrak{p}_1)^{\mathrm{alg}})) \not\equiv \mathrm{disc}(\mathrm{NS}((J/\mathfrak{p}_2)^{\mathrm{alg}})) \mod \mathbb{Q}^{\times 2}$$

for infinitely many pairs $\mathfrak{p}_1, \mathfrak{p}_2$.

In practice we very quickly hit the correct value for ρ while running over various $\mathfrak{p}$. Knowing ρ also gives the rank of $\mathrm{End}(J_K)$, except when $\rho = 2$, in which case we either get RM, CM, or a splitting. We can also tell these possibilities apart by using (ii).

A heuristic lower bound: numerical methods

To find a lower bound, we first approximate the numerical endomorphism ring of $J_{\mathbb{C}} = \mathbb{C}^g/\Lambda$. These methods were also used in genus $g = 2$ by Van Wamelen (CM) and Kumar–Mukamel (RM), using the former's Magma algorithms.

1. Embed $F^{\mathrm{al}} \hookrightarrow \mathbb{C}$, and compute (via Molin–Neurohr or Bruin) a period matrix Π for J to some precision, with period lattice Λ.
2. Use LLL to determine a basis of the $\mathbb{Z}$-module of matrices $R \in \mathrm{M}_{2g}(\mathbb{Z})$ such that $T\Pi = \Pi R$ for some T.
3. Determine the matrices T in the equality $T\Pi = \Pi R$ to obtain the representation of $\mathrm{End}(J_K)$ on the tangent space at 0, and recognize these using LLL as elements of $\mathrm{M}_g(K)$.
4. (!!!) By exact computation, certify the endomorphisms in the previous step.
5. Recover the Galois action $\mathrm{Gal}(K \,|\, F)$ by the action on the matrices T.

Computing divisorial correspondences

In the approach of Van Wamelen and Kumar–Mukamel, the endomorphism is verified by interpolating the divisor after calculating enough pairs $(P, Q_i) \in X \times X$ over $\mathbb{C}$.

To do this, we have to understand the composed map

$$X_{\mathbb{C}} \xrightarrow{\mathrm{AJ}} J_{\mathbb{C}} \xrightarrow{T} J_{\mathbb{C}} \overset{\mathrm{Mum}}{\dashrightarrow} \mathrm{Sym}^g(X_{\mathbb{C}})$$

The tricky part is the map Mum, which involves numerically inverting the Abel–Jacobi map AJ; given $b \in \mathbb{C}^g/\Lambda$, we want to find a g-tuple of points $\{Q_1, \ldots, Q_g\}$ that gives rise to it.

Robust Mumford map

We are given $b \in \mathbb{C}^g/\Lambda$, and we want to compute

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

where

$$\left(\sum_{i=1}^{g} \int_{P_0}^{Q_i} \omega_i \right)_{i=1,\ldots,g} \equiv b \pmod{\Lambda}.$$

This doesn't converge well! It converges better if we replace $\int_{P_0}^{Q_i}$ with $\int_{P_i}^{Q_i}$ with P_i distinct and b is close to 0 modulo Λ.

To improve things, compute with $b' = b/2^m$ with $m \in \mathbb{Z}_{>0}$ to find $\mathrm{Mum}(b') = \{Q'_1, \ldots, Q'_g\}$. Methods of Khuri–Makdisi allow us to (numerically) multiply back by 2^m to recover $\{Q_1, \ldots, Q_g\}$.

Dispense with numerical interpolation

But numerical computation comes with too many epsilons; it would be easier if we could avoid it, and in fact we can. We now describe an algorithm that:

- takes as input a putative tangent representation $T \in \mathrm{M}_g(K)$, and
- gives as output a proof whether or not T corresponds to an actual endomorphism α, along with a divisor D inducing T if it does.

Puiseux lift

Suppose that P_0 is a non-Weierstrass point. Our methods compute a high-order approximation of

$$\alpha([\widetilde{P}_0 - P_0]) = [\widetilde{Q}_1 + \cdots + \widetilde{Q}_g - gP_0]$$

where $\widetilde{P}_0 \in X(K[[x]])$ is the formal expansion of P_0 with respect to a suitable uniformizer x at P_0. The points $\widetilde{Q}_i$ are then defined over the ring of (integral) Puiseux series $F^{\mathrm{al}}[[x^{1/\infty}]]$.

To do this, we proceed as follows. For $j = 1, \ldots, g$, let

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

The required action by α on a basis ω_i of differentials implies:

$$\sum_{j=1}^{g} x_j^*(\omega_i) = T^*(\omega_i), \qquad \text{for all } i = 1, \ldots, g.$$

Puiseux lift

$$\sum_{j=1}^{g} x_j^*(\omega_i) = T^*(\omega_i), \qquad \text{for all } i = 1, \dots, g.$$

To do this, we first determine an initial expansion, typically

$$x_1 = c_{1,1} x^{1/g}, \dots, x_g = c_{g,1} x^{1/g}.$$

After this, we iterate. In terms of the parameter x, we get

$$\sum_{j=1}^{g} f_i(x_j) \frac{dx_j}{dx} = \sum_{j=1}^{g} T_{ij} f_j(x)$$

After integrating the f_i (as power series up to a certain precision), this becomes

$$\sum_{j=1}^{g} F_i(x_j(x)) = \sum_{j=1}^{g} T_{ij} F_j(x)$$

and we can find an implicit solution as usual.

Demonstration

Consider the curve

$$X : y^2 + (x^3 + x + 1)y = -x^5.$$

X has numerical RM by the quadratic order of discriminant 5. We verify this.

Updates: upper bounds

Modulo primes, a proven part of the Tate conjecture implies:

Theorem

The endomorphism algebra and geometric endomorphism algebra of $A/\mathfrak{p}$ are determined by

$$c_1(T) = \det(1 - \mathrm{Frob}_q\, T \,|\, H^1_{\text{ét}}((A/\mathfrak{p})^{\mathrm{alg}}, \mathbb{Q}_\ell)).$$

Now let

$$A \sim \prod_{i=1}^{t} A_i^{n_i}$$

be the decomposition of A up to isogeny over the field of definition of $\mathrm{End}(A)$. Let L_i be the center of $B_i = \mathrm{End}(A_i)$, and let $\dim_{L_i} B_i = e_i^2$.

Updates: upper bounds

$$A \sim \prod_{i=1}^{t} A_i^{n_i}, \; \dim_{L_i} B_i = e_i^2.$$

Theorem

If the Mumford–Tate conjecture holds for A, then we can compute

1. *The number of factors t;*
2. *The quantity $\sum_i e_i n_i^2 \dim A_i$;*
3. *The set of tuples $\{(e_i n_i, n_i \dim A_i)\}_i$.*
4. *The centers L_i (under an additional mild hypothesis).*

Updates: lower bounds

Since last time, we have managed to implement an approach that, instead of using polynomial ambient coordinates, finds equations for the requested divisor of bidegree (d, g) by determining the functions in

$$H^0(X, (d+g+1)P_0) \times H^0(X, (2g+1)P_0)$$

that vanish on it. (We can bound d in terms of the representation on homology due to an intersection-theoretic formula by Khuri–Makdisi.)

Updates: lower bounds

Since last time, we have managed to implement an approach that, instead of using polynomial ambient coordinates, finds equations for the requested divisor of bidegree (d, g) by determining the functions in

$$H^0(X, (d+g+1)P_0) \times H^0(X, (2g+1)P_0)$$

that vanish on it. (We can bound d in terms of the representation on homology due to an intersection-theoretic formula by Khuri–Makdisi.)

This attempt crashed and burned.

Conclusion

- A hybrid approach using Taylor expansions also works; we compute $\mathrm{Mum}(P) = \{Q_1, \ldots, Q_g\}$ once and then lift over a power series ring.
- We obtain further speedups by working over finite fields and reconstructing a divisor over F by using Sun Zi's theorem.
- Our method works just as well for isogenies and (particularly) projections.
- We have verified, decomposed and matched the 66,158 curves over $\mathbb{Q}$ of genus 2 in the *L-functions and modular form database* (LMFDB).
- The algorithms verify that the plane quartic defined by

  $$x^4 - x^3y + 2x^3z + 2x^2yz + 2x^2z^2 - 2xy^2z + 4xyz^2 - y^3z + 3y^2z^2 + 2yz^3 + z^4 = 0$$

  has complex multiplication.
- Try it: `https://github.com/edgarcosta/endomorphisms` .