Endomorphisms and decompositions of Jacobians

Jeroen Sijsling
Universität Ulm

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

ICERM, Providence
3 June 2019

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 $\operatorname{End}(J)$.

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 $\text{End}(J)$.

We represent an element $\alpha \in \text{End}(J)$ 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.

Main idea: And once 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. More effective versions of these upper bounds are themes of ongoing work by Lombardo et al.

State of the art on 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

- *The number of factors t;*
- *The quantity $\sum_i e_i n_i^2 \dim A_i$;*
- *The set of tuples $\{(e_i n_i, n_i \dim A_i)\}_i$.*
- *The centers L_i.*

Ye olde heuristic approache

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.

- 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.
- 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.
- 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 T as an element of $\mathrm{M}_g(K)$ using LLL.
- (!!!) By exact computation, certify the endomorphisms in the previous step.
- 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.

Theorem (CMSV, 2017)

There exists a deterministic algorithm that, given $T \in M_g(K)$, determines whether T corresponds to an actual endomorphism $\alpha \in \mathrm{End}(J)$, along with a divisor D inducing α 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:

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

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 implicit solutions x_j as usual via Hensel.

Remarks

- 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 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

$$\begin{aligned} X : x^4 - x^3y + 2x^3z + 2x^2yz + 2x^2z^2 - 2xy^2z + 4xyz^2 \\ - y^3z + 3y^2z^2 + 2yz^3 + z^4 = 0 \end{aligned}$$

  has complex multiplication (found in work with Kılıçer, Labrande, Lercier, Ritzenthaler, and Streng).
- Try it: `https://github.com/edgarcosta/endomorphisms` contains friendly button-push algorithms.

Demonstration

- We can check that the curve
$$X : y^2 + (x^3 + x + 1)y = -x^5.$$
has RM by the quadratic order of discriminant 5.
- We can check that conjectural fake elliptic curves over $\mathbb{Q}(\sqrt{-3})$ are genuine. (Ciaran Schembri)
- We can check that the projective curve defined by
$$\begin{aligned} -yz - 12z^2 + xw - 32w^2 &= 0, \\ y^3 + 108x^2z + 36y^2z + 8208xz^2 - 6480yz^2 + 74304z^3 + 96y^2w & \\ +2304yzw - 248832z^2w + 2928yw^2 - 75456zw^2 + 27584w^3 &= 0 \end{aligned}$$
is of GL_2-type, with endomorphism algebra $\mathbb{Q}(\zeta_8)$ over $\mathbb{Q}$; over $\overline{\mathbb{Q}}$, it is the fourth power of an elliptic curve. (David Zureick-Brown)

Decomposition

Let X be a genus-3 curve over F that is not simple. For simplicity, we assume that $\mathrm{End}(X) \otimes \mathbb{Q}$ is isomorphic to $\mathbb{Q} \times \mathbb{Q}$. Then

$$J = \mathrm{Jac}(X) \sim E \times \mathrm{Jac}(Y)$$

for curves E and Y of genus 1 and 2, respectively. The algorithms enable us to explicitly observe some rationality phenomena:

- The curve E is defined over F, as is the corresponding projection $\varphi : X \to E$ of degree d say;
- The complementary abelian subvariety $B = \ker^0(\varphi)$ carries a polarization of type $(1, d)$. To obtain a principally polarized variety B', we need to take an isogeny of degree d.
- When $d = p$ is prime, then there are $p + 1$ such isogenies, which typically form one Galois orbit.
- Curves Y' such that $\mathrm{Jac}(Y') = B'$ can be found using `https://github.com/jrsijsling/curve_reconstruction`.

Demonstration

We decompose the plane quartic curve

$$X := x^3z + 2x^2y^2 + x^2yz + 2x^2z^2 - xy^2z + xyz^2 - xz^3 + y^3z - y^2z^2 + yz^3 - z^4.$$

Crucial use is made of algorithms for calculating period matrices of plane curves due to Christian Neurohr (Oldenburg).

Gluing: $1 + 2 = 3$

We want to invert the previous considerations on decompositions and find a genus-3 curve from two other curves of genus 1 and 2. More precisely:

Definition

Let E (resp. Y) be a curve of genus 1 (resp. 2), and let $n \in \mathbb{N}$. An n-gluing of E and Y is a genus-3 curve X together with an isogeny

$$\mathrm{Jac}(E) \times \mathrm{Jac}(Y) \to \mathrm{Jac}(X)$$

under which the principal polarization on $\mathrm{Jac}(X)$ pulls back to n times the product principal polarization on $\mathrm{Jac}(E) \times \mathrm{Jac}(Y)$.

In what follows, we focus on 2-gluings: We want to find X given E and Y.

Gluing: geometric algorithms

Over $\mathbb{C}$, there is an obvious approach:

- Compute lattices $\Lambda_E \subset \mathbb{C}$ and $\Lambda_Y \subset \mathbb{C}^2$ corresponding to E and Y;
- Consider the product abelian variety

  $$\mathrm{Jac}(E) \times \mathrm{Jac}(Y) \cong (\mathbb{C} \times \mathbb{C}^2)/(\Lambda_E \times \Lambda_Y)$$

  and find an isotropic subgroup G of the 2-torsion $\frac{1}{2}(\Lambda_E \times \Lambda_Y)/(\Lambda_E \times \Lambda_Y)$ by using the Weil pairing;
- Reconstruct the curve X from the principally polarized quotient $(\mathrm{Jac}(E) \times \mathrm{Jac}(Y))/G$.

The last step uses algorithms for reconstruction of plane quartics with Lercier and Ritzenthaler, plus some refinements. These allow us to construct curves of genus up to 3 with given big (instead of merely small) period matrix.

Gluing: rationality questions

The quotient by G is defined over the base field iff G is stable under $\mathrm{Gal}(\overline{F} \,|\, F)$. This depends on the polynomials f_E and f_Y defining $E : y^2 = f_E$ and $Y : y^2 = f_Y$.

Proposition (Hanselman)

For a gluing over F to exist, the polynomial f_Y needs to contain a single quadratic or two linear factors. That is, $\mathrm{Jac}(Y)$ needs to contain a rational 2-torsion point.

Idea of proof: Since G cannot be a product, it maps surjectively to $\mathrm{Jac}(E)[2]$. The kernel is a distinguished subgroup H of $\mathrm{Jac}(Y)[2]$.

We have full criteria for there to exist a Galois-stable G, in which case our algorithms will find a curve X over F such that

$$\mathrm{Jac}(X) \cong (\mathrm{Jac}(E) \times \mathrm{Jac}(Y))/G.$$

Demonstration

The curves

$$E : y^2 = x^3 - x$$

and

$$Y : y^2 = x^5 + 20x^3 + 36x$$

give rise to 6 Galois-stable isotropic subgroups. The corresponding gluings X are given by

$$\begin{aligned}
x^4 + 48x^2yz - 288y^4 + 288y^2z^2 - 8z^4 &= 0, \\
x^4 - 48x^2yz - 288y^4 + 288y^2z^2 - 8z^4 &= 0, \\
x^4 + 24x^2yz - 720y^4 + 144y^2z^2 - 20z^4 &= 0, \\
x^4 - 24x^2yz - 720y^4 + 144y^2z^2 - 20z^4 &= 0, \\
x^4 + 48x^2yz + 1008y^4 - 432y^2z^2 + 28z^4 &= 0, \\
x^4 - 48x^2yz + 1008y^4 - 432y^2z^2 + 28z^4 &= 0.
\end{aligned}$$

Implementation: `https://github.com/jrsijsling/gluing`

Gluing: rationality questions

Given a genus-1 curve E of gonality 2 over a number field F, given by a defining equation

$$E : y^2 = a_0 x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4,$$

one can always realize E as part of a 2-gluing over F, as one sees by considering

$$X : y^2 = a_0 x^8 + a_1 x^6 + a_2 x^4 + a_3 x^2 + a_4.$$

Theorem (Hanselman)

Let Y be a genus-2 curve over F such that $\mathrm{Jac}(Y)$ contains a rational 2-torsion point. Then Y is part of a 2-gluing over F. In other words, there exist curves E and X of genus 1 resp. 3 over F such that X is a 2-gluing of E and Y.

Hanselman found a very explicit proof; another one can be obtained by degenerating an argument of Nils Bruin on Prym varieties.

Gluing: algebraic algorithms

Upcoming work by Hanselman and Schiavone will describe another approach, which works over any field. We sketch the steps here. Let E and Y of genus 1 and 2 be given.

- Construct the Kummer variety $K \subset \mathbb{P}^3$ of Y, for example by using the general formulas of Jan Steffen Müller;
- Choose two nodes P_1, P_2 on K.
- Consider the pencil of planes Λ through P_1 and P_2. For $H \in L$, the intersection $E_H = K \cap H$ is a plane curve of degree 3 with two nodes, and hence of genus 1;

Gluing: algebraic algorithms

- Find the planes $H_1, \ldots, H_6$ for which $j(E_{H_i}) = j(E)$;
- Construct the fiber products

$$\begin{tikzcd} X_i \arrow[r] \arrow[d] & E_{H_i} \arrow[d] \\ J \arrow[r] & K \end{tikzcd}$$

- The curves X_i are 2-gluings of E and Y over $\overline{F}$.

All these steps can be made completely effective. Note that in particular these algorithms work over finite fields! A corresponding implementation is in progress; a proof of concept is available in `Magma`. Further theoretical aspects remain to be explored.