Rigorous computation of the endomorphism ring of a Jacobian

Jeroen Sijsling
Universität Ulm

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

Intercity Number Theory Seminar
Science Park Amsterdam
19 May 2017

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.

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.

An endomorphism $\alpha \in \mathrm{End}(J)$ can be represented using the equations for X in one of the following equivalent ways:

1. by a divisor $D \subset X \times X$;

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.

An endomorphism $\alpha \in \mathrm{End}(J)$ can be represented using the equations for X in one of the following equivalent ways:

1. by a divisor $D \subset X \times X$;
2. by a correspondence $X \leftarrow Z \rightarrow X$;

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.

An endomorphism $\alpha \in \mathrm{End}(J)$ can be represented using the equations for X in one of the following equivalent ways:

1. by a divisor $D \subset X \times X$;
2. by a correspondence $X \leftarrow Z \rightarrow X$;
3. assuming X is presented as a (possibly singular) plane curve $f(x, y) = 0$, by Cantor equations

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

with $a_i, b_j \in K(X)$ rational functions.

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.

An endomorphism $\alpha \in \mathrm{End}(J)$ can be represented using the equations for X in one of the following equivalent ways:

1. by a divisor $D \subset X \times X$;
2. by a correspondence $X \leftarrow Z \rightarrow X$;
3. assuming X is presented as a (possibly singular) plane curve $f(x, y) = 0$, by Cantor equations

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

with $a_i, b_j \in K(X)$ rational functions.

(In (i), the fiber over a point P in the first factor is equivalent with $\alpha(P - P_0)$. In (iii), the Cantor equations also describe this divisor class.)

Our objective

For us, to compute the endomorphism ring of J means to determine and represent the ring $\mathrm{End}(J_{F^{\mathrm{al}}})$ as a $\mathrm{Gal}(K \mid F)$-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 and the action of $\mathrm{Gal}(K \mid F)$ on this 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:

1. By a theorem of Silverberg, $\mathrm{End}(J_{F^{\mathrm{al}}})$ is defined over $K = F(J[3])$.
2. By day, we compute a lower bound by searching for endomorphisms by naively trying all maps $J \dashrightarrow J$.
3. 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:

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

Upper bounds in genus 2

Let $\mathfrak{p}$ be a prime of good reduction of X. Then there is an inequality $\rho \leq \rho_{\mathfrak{p}} := \rho(J_{K_{\mathfrak{p}}})$. Define

$$P_1(T) = \det(1 - \mathrm{Frob}_{\mathfrak{p}}\ T \,|\, H^1(J_K, \mathbb{Q}_\ell))$$
$$P_2(T) = \det(1 - \mathrm{Frob}_{\mathfrak{p}}\ T \,|\, H^2(J_K, \mathbb{Q}_\ell))$$

The Tate conjecture shows:

1. $\rho_{\mathfrak{p}}$ is the number of reciprocal roots of P_2 that are q times a root of unity;
2. if X has primitive CM by a quartic number field K and if $\mathfrak{p}$ splits completely in K, then P_1 is irreducible and defines K.

Upper bounds in genus 2

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.

We can therefore refine our upper bound for ρ by running over the primes of good reduction, and we are guaranteed to find the upper bound (in practice this happens very quickly). We also obtain the rank of $\mathrm{End}(J_K)$ except when $\rho = 2$, in which case we either get RM or CM. Reducing at different primes, we can also tell these possibilities apart.

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 $F \hookrightarrow \mathbb{C}$, and compute 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 $\Lambda R \subseteq \Lambda$.
3. Determine the matrices M in the equality $M\Pi = \Pi R$ to obtain the representation of $\mathrm{End}(J_{\mathbb{C}})$ on the tangent space at 0, and recognize these using LLL as matrices $M \in \mathrm{M}_g(K)$.
4. (!!!) By exact computation, certify the endomorphisms in the previous step.
5. Recover the Galois action $\mathrm{Gal}(K \mid F)$ by the action on the matrices M.

Computing divisorial correspondences

In the approach of van Wamelen and Kumar–Mukamel, the endomorphism is computed and verified by interpolation. Choose a base point $P_0 \in X(K)$.

Let α be a putative endomorphism of J, with tangent representation $M \in \mathrm{M}_g(\mathbb{C})$. Then we have a composed rational map

$$\beta\colon\ X_{\mathbb{C}} \xrightarrow{\mathrm{AJ}} J_{\mathbb{C}} \xrightarrow{M} J_{\mathbb{C}} \xrightarrow{\mathrm{Mum}} \mathrm{Sym}^g(X_{\mathbb{C}})$$

where $\beta(P) = \{Q_1, \ldots, Q_g\}$ if

$$\beta([P - P_0]) = [Q_1 + \cdots + Q_g - gP_0].$$

The tricky part is the map Mum, which involves numerically inverting the Abel–Jacobi map AJ.

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.

In general, to obtain the latter, 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 we are allergic to numerical computation and want to reduce our symptoms.

We now describe a Turing machine that:

- takes as input a putative tangent representation $M \in \mathrm{M}_g(K)$ and
- if it terminates, certifies that M corresponds to an honest is an endomorphism α.

Puiseux lift

Suppose that P_0 is a non-Weierstrass point. Our methods compute

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

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 $F^{\mathrm{al}}[[x^{1/\infty}]]$.

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:

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

This is a differential equation for $(x_j)_j$ of the form $Wx' = M\omega$ which can be solved iteratively. We then use linear algebra to find a divisor.

Example: curve

Consider the curve

$$X : y^2 = 24x^5 + 36x^4 - 4x^3 - 12x^2 + 1.$$

(Click if time permits...)

X has numerical quaternionic multiplication (QM): more precisely, the numerical endomorphism ring is an order of reduced discriminant 36 in a quaternion algebra over $\mathbb{Q}$ with discriminant 6.

Example: system

$$X : y^2 = 24x^5 + 36x^4 - 4x^3 - 12x^2 + 1 = f(x).$$

Let us verify the putative endomorphism α with tangent representation $M = \begin{pmatrix} -\sqrt{-3} & \sqrt{-3} \\ 2\sqrt{-3} & \sqrt{-3} \end{pmatrix}$ in the basis $\omega_1 = \dfrac{\mathrm{d}x}{y}, \omega_2 = x\dfrac{\mathrm{d}x}{y}$. Note that $\alpha^2 = -9$.

We take $P_0 = (0, 1)$. Then

$$\widetilde{P}_0 = (x, \sqrt{f(x)}) = (x, 1 - 6x^2 - 2x^3 - 2x^6 + \ldots).$$

Our differential system is $(x_i' = \mathrm{d}x_i/\mathrm{d}x)$

$$\begin{pmatrix} 1 & 1 \\ x_1 & x_2 \end{pmatrix} \begin{pmatrix} x_1'/y_1 \\ x_2'/y_2 \end{pmatrix} = M \begin{pmatrix} 1/y \\ x/y \end{pmatrix}$$

where $x_i = x(\widetilde{Q}_i)$ and $y_i = y(\widetilde{Q}_i) = \sqrt{f(x_i)} = 1 + \ldots$

Example: solution

$$X : y^2 = 24x^5 + 36x^4 - 4x^3 - 12x^2 + 1 = f(x).$$

$$\begin{pmatrix} 1 & 1 \\ x_1 & x_2 \end{pmatrix} \begin{pmatrix} x_1'/y_1 \\ x_2'/y_2 \end{pmatrix} = \begin{pmatrix} -\sqrt{-3} & \sqrt{-3} \\ 2\sqrt{-3} & \sqrt{-3} \end{pmatrix} \begin{pmatrix} 1/y \\ x/y \end{pmatrix}$$

Computing the lowest degree terms on both sides, we start with the expansions

$$x_i = c_{i1} x^{1/2} + \dots$$

and see they must satisfy

$$\frac{1}{2} \begin{pmatrix} c_{11} + c_{21} \\ c_{11}^2 + c_{21}^2 \end{pmatrix} = \begin{pmatrix} 0 \\ 2\sqrt{-3} \end{pmatrix}$$

which has a unique solution $c_{11}, c_{21} = \pm\sqrt[4]{-12}$ up to permutation.

Having the determined the expansions to some precision, at each step of the lift we have a Vandermonde linear system which can be solved iteratively. Hensel lifting works even better!

Example: certificate

$$\langle -160704x_1^{14}x_2^2+412128x_1^{14}x_2+42768x_1^{14}y_2-143856x_1^{14}-596160x_1^{13}x_2^2-222912x_1^{13}x_2+136080x_1^{13}y_2-45360x_1^{13}+$$
$$14256\sqrt{-3}x_1^{12}y_1x_2^2-15552\sqrt{-3}x_1^{12}y_1x_2-3759696x_1^{12}x_2^2-2982096x_1^{12}x_2+66312x_1^{12}y_2+902664x_1^{12}-61344\sqrt{-3}x_1^{11}y_1x_2^2+$$
$$44064\sqrt{-3}x_1^{11}y_1x_2-432\sqrt{-3}x_1^{11}y_1y_2-40608\sqrt{-3}x_1^{11}y_1-3754080x_1^{11}x_2^2-2791728x_1^{11}x_2-605736x_1^{11}y_2+386568x_1^{11}-$$
$$227592\sqrt{-3}x_1^{10}y_1x_2^2+2016\sqrt{-3}x_1^{10}y_1x_2-4896\sqrt{-3}x_1^{10}y_1y_2-47664\sqrt{-3}x_1^{10}y_1+336312x_1^{10}x_2^2+450216x_1^{10}x_2-883836x_1^{10}y_2-$$
$$1050588x_1^{10}+6480\sqrt{-3}x_1^9y_1x_2^2-296712\sqrt{-3}x_1^9y_1x_2+18720\sqrt{-3}x_1^9y_1y_2+30168\sqrt{-3}x_1^9y_1+1882944x_1^9x_2^2+858312x_1^9x_2-$$
$$382140x_1^9y_2-808164x_1^9-287724\sqrt{-3}x_1^8y_1x_2^2-350064\sqrt{-3}x_1^8y_1x_2+113460\sqrt{-3}x_1^8y_1y_2+132420\sqrt{-3}x_1^8y_1+2191524x_1^8x_2^2+152868x_1^8x_2$$
$$+176946x_1^8y_2-294078x_1^8-288960\sqrt{-3}x_1^7y_1x_2^2+5664\sqrt{-3}x_1^7y_1x_2+15708\sqrt{-3}x_1^7y_1y_2+41016\sqrt{-3}x_1^7y_1+607920x_1^7x_2^2+216348x_1^7x_2+$$
$$400170x_1^7y_2-39138x_1^7+113058\sqrt{-3}x_1^6y_1x_2^2+134232\sqrt{-3}x_1^6y_1x_2-78120\sqrt{-3}x_1^6y_1y_2-57852\sqrt{-3}x_1^6y_1-966210x_1^6x_2^2-2112x_1^6x_2+$$
$$105894x_1^6y_2+201054x_1^6+160148\sqrt{-3}x_1^5y_1x_2^2+30798\sqrt{-3}x_1^5y_1x_2-20792\sqrt{-3}x_1^5y_1y_2-23830\sqrt{-3}x_1^5y_1-477396x_1^5x_2^2-124014x_1^5x_2-$$
$$109026x_1^5y_2+120012x_1^5+22148\sqrt{-3}x_1^4y_1x_2^2-17448\sqrt{-3}x_1^4y_1x_2+16321\sqrt{-3}x_1^4y_1y_2+7985\sqrt{-3}x_1^4y_1+136080x_1^4x_2^2-9792x_1^4x_2-$$
$$38379x_1^4y_2-21975x_1^4-25522\sqrt{-3}x_1^3y_1x_2^2-6864\sqrt{-3}x_1^3y_1x_2+5602\sqrt{-3}x_1^3y_1y_2+4346\sqrt{-3}x_1^3y_1+87882x_1^3x_2^2+18456x_1^3x_2+$$
$$12594x_1^3y_2-23874x_1^3-7946\sqrt{-3}x_1^2y_1x_2^2+684\sqrt{-3}x_1^2y_1x_2-1153\sqrt{-3}x_1^2y_1y_2-185\sqrt{-3}x_1^2y_1-5622x_1^2x_2^2+1008x_1^2x_2+$$
$$3999x_1^2y_2-597x_1^2+988\sqrt{-3}x_1y_1x_2^2+444\sqrt{-3}x_1y_1x_2-427\sqrt{-3}x_1y_1y_2-239\sqrt{-3}x_1y_1-5172x_1x_2^2-924x_1x_2-567x_1y_2+1389x_1+$$
$$376\sqrt{-3}y_1x_2^2+17\sqrt{-3}y_1y_2-17\sqrt{-3}y_1-111y_2+111,$$
$$-103680x_1^{14}x_2^2+352512x_1^{14}x_2+1296x_1^{14}y_2-143856x_1^{14}+452736x_1^{13}x_2^2-727488x_1^{13}x_2+89856x_1^{13}y_2-72576x_1^{13}+$$
$$432\sqrt{-3}x_1^{12}y_1x_2^2-12096\sqrt{-3}x_1^{12}y_1x_2-1709424x_1^{12}x_2^2-3901824x_1^{12}x_2+133272x_1^{12}y_2+883224x_1^{12}-24624\sqrt{-3}x_1^{11}y_1x_2^2+$$
$$60912\sqrt{-3}x_1^{11}y_1x_2+4104\sqrt{-3}x_1^{11}y_1y_2-53784\sqrt{-3}x_1^{11}y_1-3806064x_1^{11}x_2^2-2934432x_1^{11}x_2-390024x_1^{11}y_2+490104x_1^{11}-$$
$$98280\sqrt{-3}x_1^{10}y_1x_2^2+18144\sqrt{-3}x_1^{10}y_1x_2-14760\sqrt{-3}x_1^{10}y_1y_2-69336\sqrt{-3}x_1^{10}y_1-2461032x_1^{10}x_2^2+1257408x_1^{10}x_2-545940x_1^{10}y_2-$$
$$778644x_1^{10}+103608\sqrt{-3}x_1^9y_1x_2^2-280800\sqrt{-3}x_1^9y_1x_2-5124\sqrt{-3}x_1^9y_1y_2+22428\sqrt{-3}x_1^9y_1+737832x_1^9x_2^2+1184688x_1^9x_2-$$
$$257556x_1^9y_2-647220x_1^9-297588\sqrt{-3}x_1^8y_1x_2^2-321408\sqrt{-3}x_1^8y_1x_2+106500\sqrt{-3}x_1^8y_1y_2+133284\sqrt{-3}x_1^8y_1+3437796x_1^8x_2^2-140448x_1^8x_2$$
$$+38958x_1^8y_2-344562x_1^8-298500\sqrt{-3}x_1^7y_1x_2^2+17676\sqrt{-3}x_1^7y_1x_2+10614\sqrt{-3}x_1^7y_1y_2+41694\sqrt{-3}x_1^7y_1+1132956x_1^7x_2^2+61464x_1^7x_2+$$
$$312378x_1^7y_2-69414x_1^7+76538\sqrt{-3}x_1^6y_1x_2^2+117624\sqrt{-3}x_1^6y_1x_2-71194\sqrt{-3}x_1^6y_1y_2-46550\sqrt{-3}x_1^6y_1-1270878x_1^6x_2^2+48480x_1^6x_2+$$
$$96348x_1^6y_2+211308x_1^6+137674\sqrt{-3}x_1^5y_1x_2^2+25212\sqrt{-3}x_1^5y_1x_2-10231\sqrt{-3}x_1^5y_1y_2-20183\sqrt{-3}x_1^5y_1-558306x_1^5x_2^2-89376x_1^5x_2-$$
$$100671x_1^5y_2+109857x_1^5+32314\sqrt{-3}x_1^4y_1x_2^2-13620\sqrt{-3}x_1^4y_1x_2+15539\sqrt{-3}x_1^4y_1y_2+3415\sqrt{-3}x_1^4y_1+192642x_1^4x_2^2-13536x_1^4x_2-$$
$$26619x_1^4y_2-29499x_1^4-21684\sqrt{-3}x_1^3y_1x_2^2-6276\sqrt{-3}x_1^3y_1x_2+3058\sqrt{-3}x_1^3y_1y_2+3446\sqrt{-3}x_1^3y_1+93636x_1^3x_2^2+14700x_1^3x_2+$$
$$14112x_1^3y_2-21504x_1^3-8836\sqrt{-3}x_1^2y_1x_2^2+384\sqrt{-3}x_1^2y_1x_2-1349\sqrt{-3}x_1^2y_1y_2+407\sqrt{-3}x_1^2y_1-13080x_1^2x_2^2+1080x_1^2x_2+$$
$$2025x_1^2y_2+1065x_1^2+974\sqrt{-3}x_1y_1x_2^2+444\sqrt{-3}x_1y_1x_2-254\sqrt{-3}x_1y_1y_2-190\sqrt{-3}x_1y_1-5478x_1x_2^2-768x_1x_2-774x_1y_2+$$
$$1290x_1+424\sqrt{-3}y_1x_2^2+42\sqrt{-3}y_1y_2-42\sqrt{-3}y_1+444x_2^2\rangle$$

Conclusion

- A hybrid approach using Taylor expansions also works well: 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 using Sun Zi's theorem.
- The method works just as well for isogenies and projections.
- We have verified the endomorphism and decomposition data in the *L-functions and modular form database* (LMFDB), containing 66 158 curves of genus 2.