Rigorous computation of the endomorphism algebra of a Jacobian

Edgar Costa [1]
Nicolas Mascot [2] Jeroen Sijsling [1,3] John Voight [1]

[1]Dartmouth College

[2]University of Warwick

[3]Universität Ulm

ANTS, September 1st, 2016

Setup

Input: $X =$ genus 2 curve over a number field

Output: $\mathrm{End}(J_{\bar{\mathbb{Q}}}) \otimes \mathbb{Q}$ with a certificate, where $J = \mathrm{Jac}(X)$

Setup

Input: X = genus 2 curve over a number field

Output: $\mathrm{End}(J_{\bar{\mathbb{Q}}}) \otimes \mathbb{Q}$ with a certificate, where $J = \mathrm{Jac}(X)$

- Upper bound: a proof that $\mathrm{rk}\,\mathrm{End}(J_{\bar{\mathbb{Q}}}) \leq r$
- Lower bound and generators:
  a set of r linear independent endomorphisms, for each:
  1. a 2×2 matrix in a number field that represents the action on the tangent space at 0 of J, and
  2. the graph of the endomorphism as a divisor in $X \times X$, over the same number field

Upper bound for $\mathrm{rk}\,\mathrm{End}\left(J_{\overline{\mathbb{Q}}}\right)$

Example:
$$y^2 + (x^3 + 1)y = x^2 + x \quad (249.a.249.1)$$

- $p = 7$: $\mathrm{rk}\,\mathrm{NS}\left(J_{\overline{\mathbb{F}_p}}\right) = 2$, $\mathrm{disc}\,\mathrm{NS}\left(J_{\overline{\mathbb{F}_p}}\right) = -6 \bmod \mathbb{Q}^{\times 2}$;
- $p = 11$: $\mathrm{rk}\,\mathrm{NS}\left(J_{\overline{\mathbb{F}_p}}\right) = 2$, $\mathrm{disc}\,\mathrm{NS}\left(J_{\overline{\mathbb{F}_p}}\right) = -65 \bmod \mathbb{Q}^{\times 2}$;

$\Rightarrow \mathrm{rk}\,\mathrm{NS}\left(J_{\overline{\mathbb{Q}}}\right) = \mathrm{rk}\,\mathrm{End}\left(J_{\overline{\mathbb{Q}}}\right)^{\dagger} \leq 1$
$\Rightarrow \mathrm{rk}\,\mathrm{End}\left(J_{\overline{\mathbb{Q}}}\right) = 1$

Upper bound for $\mathrm{rk}\,\mathrm{End}\left(J_{\overline{\mathbb{Q}}}\right)$

Example:
$$y^2 + (x^3 + 1)y = x^2 + x \quad (249.a.249.1)$$

- $p = 7$: $\mathrm{rk}\,\mathrm{NS}\left(J_{\overline{\mathbb{F}_p}}\right) = 2$, $\mathrm{disc}\,\mathrm{NS}\left(J_{\overline{\mathbb{F}_p}}\right) = -6 \bmod \mathbb{Q}^{\times 2}$;
- $p = 11$: $\mathrm{rk}\,\mathrm{NS}\left(J_{\overline{\mathbb{F}_p}}\right) = 2$, $\mathrm{disc}\,\mathrm{NS}\left(J_{\overline{\mathbb{F}_p}}\right) = -65 \bmod \mathbb{Q}^{\times 2}$;

$\Rightarrow \mathrm{rk}\,\mathrm{NS}\left(J_{\overline{\mathbb{Q}}}\right) = \mathrm{rk}\,\mathrm{End}\left(J_{\overline{\mathbb{Q}}}\right)^{\dagger} \leq 1$
$\Rightarrow \mathrm{rk}\,\mathrm{End}\left(J_{\overline{\mathbb{Q}}}\right) = 1$

LMFDB ✓

Generators

Example:

$y^2 = -4x^6 + 20x^5 - 32x^4 + 16x^3 - 4x^2 + 4x \quad (262144.d.524288.1)$

1. Compute the action on the tangent space at 0 [van Wamelen]

$$\alpha = \begin{pmatrix} 0 & \zeta_8 - \zeta_8^3 \\ \zeta_8 - \zeta_8^3 & 0 \end{pmatrix}$$

Generators

Example:

$y^2 = -4x^6 + 20x^5 - 32x^4 + 16x^3 - 4x^2 + 4x \quad (262144.d.524288.1)$

1. Compute the action on the tangent space at 0 [van Wamelen]

$$\alpha = \begin{pmatrix} 0 & \zeta_8 - \zeta_8^3 \\ \zeta_8 - \zeta_8^3 & 0 \end{pmatrix}$$

2. and the corresponding divisor in $X \times X$
   - Either, for some P compute Q_1 and Q_2 such that

$$\alpha(2P - 2W) = Q_1 + Q_2 - 2W$$

$$e.g.: \quad P = (2, 2\zeta_8^3 + 2\zeta_8) \rightsquigarrow Q_i = \left(\left(17 \pm 2\sqrt{79}\right)/30, \mp\sqrt{\bullet}\right)$$

   and Newton lift the map above around P

Generators

Example:

$y^2 = -4x^6 + 20x^5 - 32x^4 + 16x^3 - 4x^2 + 4x \quad (262144.d.524288.1)$

1. Compute the action on the tangent space at 0 [van Wamelen]

$$\alpha = \begin{pmatrix} 0 & \zeta_8 - \zeta_8^3 \\ \zeta_8 - \zeta_8^3 & 0 \end{pmatrix}$$

2. and the corresponding divisor in $X \times X$
   - Either, for some P compute Q_1 and Q_2 such that

$$\alpha(2P - 2W) = Q_1 + Q_2 - 2W$$

$$e.g.: \quad P = (2, 2\zeta_8^3 + 2\zeta_8) \rightsquigarrow Q_i = \left(\left(17 \pm 2\sqrt{79}\right)/30, \mp\sqrt{\bullet}\right)$$

   and Newton lift the map above around P
   - Or directly Newton lift a *translation* of α using Puiseux series.