Computing isogenies from modular equations in genus 2

Jean Kieffer

Supervision: D. Robert, A. Page

Institut de Mathématiques de Bordeaux

Arithmetic Geometry, Cryptography, and Coding Theory
Luminy, 10–14 June 2019

Computing isogenies from modular equations

Problem

Let E_1, E_2/k be ℓ-isogenous elliptic curves: $\Phi_\ell(j(E_1), j(E_2)) = 0$.
Compute an ℓ-isogeny $\phi : E_1 \to E_2$?

- Known algorithms for elliptic curves (Elkies)
- Goal: generalize to Jacobians of genus 2 curves.
- Applications: point counting (SEA), explicit families, walking in isogeny graphs,...

Assumption: k has characteristic 0 or $p \gg \ell$.

Plan

1. The case of elliptic curves

2. From genus 1 to genus 2

Action on differential forms

$\phi : E_1 \to E_2$ induces $\phi^* : \Omega^1(E_2) \to \Omega^1(E_1)$.

$$E_1 : v^2 = u^3 + a_1 u + b_1 \qquad E_2 : y^2 = x^3 + a_2 x + b_2$$

$$\omega_1 = \frac{du}{v} \qquad\qquad \omega_2 = \frac{dx}{y}$$

- *Normalization matrix* $m \in \mathrm{GL}_1(k) = k^\times$: $\quad \phi^*(\omega_2) = m\,\omega_1$.

Action on differential forms

$\phi : E_1 \to E_2$ induces $\phi^* : \Omega^1(E_2) \to \Omega^1(E_1)$.

$$E_1 : v^2 = u^3 + a_1 u + b_1 \qquad E_2 : y^2 = x^3 + a_2 x + b_2$$

$$\omega_1 = \frac{du}{v} \qquad\qquad \omega_2 = \frac{dx}{y}$$

- *Normalization matrix* $m \in \mathrm{GL}_1(k) = k^\times$: $\quad \phi^*(\omega_2) = m\,\omega_1$.

Differential system: $\phi(u, v) = (x(u), v\,y(u))$

$$(S) \quad \begin{cases} \dfrac{x'(u)du}{v\,y(u)} = m\,\dfrac{du}{v} \\ (u^3 + a_1 u + b_1)y(u)^2 = x(u)^3 + a_2 x(u) + b_2 \end{cases}$$

- Compute m
- Solve (S).

Evaluating modular forms

$\tau \in \mathbb{H}_1$ gives

$$E(\tau) = \mathbb{C}/(\mathbb{Z} \oplus \tau\mathbb{Z}), \quad \omega(\tau) = dz.$$

Definition

- Given (E, ω) over $\mathbb{C}$, choose τ with $\eta : E \xrightarrow{\sim} E(\tau)$.

$$\omega = g\,\eta^*(dz), \quad g \in \mathrm{GL}_1(\mathbb{C})$$

- For f modular form of weight k: $f(E, \omega) := g^{-k} f(\tau)$.

$(E, \omega) \leftrightarrow$ Weierstrass equation.

Computing the normalization matrix (1)

We can find $\tau \in \mathbb{H}_1$ such that

$$\begin{tikzcd} E_1 \arrow[r, "\phi"] \arrow[d, "\simeq"] & E_2 \arrow[d, "\simeq"] \\ E(\tau) \arrow[r] & E(\tau/\ell). \end{tikzcd}$$

Weierstrass equations for E_1, E_2 give differential forms ω_1, ω_2:

$$\omega_1 = g_1\, dz, \quad \omega_2 = g_2\, dz \quad \text{for some } g_1, g_2 \in \mathrm{GL}_1(\mathbb{C}).$$

- $E(\tau) \to E(\tau/\ell)$ pulls dz back to dz
- Normalization matrix is $m = g_1^{-1} g_2$.

Computing the normalization matrix (2)

Key idea: use $\dfrac{dj}{d\tau}$, modular function of weight 2.

- Differentiate $\Phi_\ell(j(\tau), j(\tau/\ell)) = 0$:

$$\frac{dj}{d\tau}(\tau) = \frac{dj}{d\tau}(\tau/\ell) \cdot D$$

  D: partial derivatives of Φ_ℓ at $(j(E_1), j(E_2))$.
- $\dfrac{dj}{d\tau}(E, \omega) = \lambda\, j(E)\, \dfrac{b}{a}$ for $E : y^2 = x^3 + ax + b$.

Computing the normalization matrix (2)

Key idea: use $\dfrac{dj}{d\tau}$, modular function of weight 2.

- Differentiate $\Phi_\ell(j(\tau), j(\tau/\ell)) = 0$:

$$\frac{dj}{d\tau}(\tau) = \frac{dj}{d\tau}(\tau/\ell) \cdot D$$

  D: partial derivatives of Φ_ℓ at $(j(E_1), j(E_2))$.

- $\dfrac{dj}{d\tau}(E, \omega) = \lambda\, j(E)\, \dfrac{b}{a}$ for $E : y^2 = x^3 + ax + b$.

$$\frac{dj}{d\tau}(E_1, \omega_1) = g_1^{-2}\frac{dj}{d\tau}(\tau) = g_1^{-2}\frac{dj}{d\tau}(\tau/\ell)D = (g_1^{-1}g_2)^2\frac{dj}{d\tau}(E_2, \omega_2)D.$$

- We get $\pm g_1^{-1}g_2$. Valid over any field.

Solving the differential system

Differential system: $\phi(u, v) = (x(u), v\, y(u))$

$$\begin{cases} \dfrac{x'(u)du}{v\, y(u)} = m\, \dfrac{du}{v} \\ (u^3 + a_1 u + b_1)y(u)^2 = x(u)^3 + a_2 x(u) + b_2 \end{cases}$$

Solved locally around $\mathcal{O}_{E_1}$.

- Expand u, v, x, y as power series in z = uniformizer
- Newton iterations
- Recover $x(u) = \dfrac{N(u)}{D(u)}$.

Degree of N, D is $O(\ell)$, cost is $\widetilde{O}(\ell)$ operations in k.

Plan

1. The case of elliptic curves

2. From genus 1 to genus 2

From genus 1 to genus 2

$$E \,:\, v^2 = u^3 + au + b$$

$$J = \mathrm{Jac}(C)$$
$$C \,:\, v^2 = f_C(u),\ \deg f_C \in \{5, 6\}$$

$$\omega = \frac{du}{v}$$

$$\omega = \left(\frac{udu}{v}, \frac{du}{v}\right)$$

Problem

$\mathrm{Jac}(C_1)$, $\mathrm{Jac}(C_2)$ satisfying modular equations of level ℓ.
Compute an isogeny explicitly?

- Compute the normalization matrix $m \in \mathrm{GL}_2(k)$
- Solve a differential system.

Siegel modular forms: dictionary

$\mathrm{SL}_2(\mathbb{Z}) \circlearrowleft \mathbb{H}_1$	$\mathrm{Sp}_4(\mathbb{Z}) \circlearrowleft \mathbb{H}_2 = \left\{ \tau = \begin{pmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{pmatrix} \mid \mathrm{Im}(\tau) > 0 \right\}$
f of weight k	f vector-valued Siegel modular form of weight ρ: $\rho : \mathrm{GL}_2(\mathbb{C}) \to \mathrm{GL}(V)$, $f : \mathbb{H}_2 \to V$, $f((a\tau+b)(c\tau+d)^{-1}) = \rho(c\tau+d)f(\tau)$
$j(\tau)$	Igusa birational invariants j_1, j_2, j_3
$\Phi_\ell(j, J) = 0$	3 equations in $j_1, j_2, j_3, J_1, J_2, J_3$ (huge)
$\frac{dj}{d\tau}$ of weight 2	$\left(\frac{\partial j_1}{\partial \tau_1}, \frac{\partial j_1}{\partial \tau_2}, \frac{\partial j_1}{\partial \tau_3} \right)$ of weight $\rho = \mathrm{Sym}^2$ (dim. 3)
Polynomials in a, b	Covariants of the sextic $C : v^2 = f_C(u)$.

Derivatives of Igusa invariants

$$C \,:\, v^2 = f_C(u) = a_6 u^6 + \cdots + a_0$$

- Scalar-valued covariants: e.g. Igusa–Clebsch I_2, I_4, I_6, I_{10}
- Vector-valued covariants: f_C (dim. 7), y_1, y_2, y_3 (dim. 3),... (Notation from [Mestre 1991])

$$\frac{\partial j_1}{\partial \tau} \;=\; \lambda \frac{1}{I_{10}} \left(\frac{153}{8} I_4 I_2^2 y_1 - \frac{135}{2} I_2 I_6 y_1 + \frac{135}{2} I_4^2 y_1 \right. \\ \left. + \frac{46575}{4} I_2 I_4 y_2 - 30375\, I_6 y_2 + 1366875\, I_4 y_3 \right)$$

Numerical checks: high-precision computation of period matrices and theta functions.

Sketch of proof

Sketch of proof

1. Any holomorphic modular form g is a polynomial covariant.

$$\begin{array}{ccc} \widetilde{\mathcal{M}}_2 & \hookrightarrow & \widetilde{\mathcal{A}}_2 \\ \uparrow & & \uparrow \\ \mathcal{M}_2 & \hookrightarrow & \mathcal{A}_2 \end{array}$$

- $\widetilde{\mathcal{M}}_2$ moduli stack for semistable curves.
- g extends to $\widetilde{\mathcal{A}}_2$, so to $\widetilde{\mathcal{M}}_2$
- Up to a codimension 2 subvariety, universal curve over $k[a_0, \ldots, a_6]$ is semistable.

Sketch of proof

1. Any holomorphic modular form g is a polynomial covariant.

$$\begin{tikzcd} \widetilde{\mathcal{M}}_2 \arrow[r, hook] & \widetilde{\mathcal{A}}_2 \\ \mathcal{M}_2 \arrow[r, hook] \arrow[u, hook] & \mathcal{A}_2 \arrow[u, hook] \end{tikzcd}$$

- $\widetilde{\mathcal{M}}_2$ moduli stack for semistable curves.
- g extends to $\widetilde{\mathcal{A}}_2$, so to $\widetilde{\mathcal{M}}_2$
- Up to a codimension 2 subvariety, universal curve over $k[a_0, \ldots, a_6]$ is semistable.

2. $\exists\, g_{8,6}$ Siegel m.f. of weight $\det^8 \otimes \mathrm{Sym}^6$. Then $g_{8,6} = \lambda\, I_{10}\, f_C$
   - This space of covariants has dimension 1.

Already noted in [Cléry, Faber, Van der Geer, 2016].

Sketch of proof

1. Any holomorphic modular form g is a polynomial covariant.

$$
\begin{array}{ccc}
\widetilde{\mathcal{M}}_2 & \hookrightarrow & \widetilde{\mathcal{A}}_2 \\
\uparrow & & \uparrow \\
\mathcal{M}_2 & \hookrightarrow & \mathcal{A}_2
\end{array}
$$

- $\widetilde{\mathcal{M}}_2$ moduli stack for semistable curves.
- g extends to $\widetilde{\mathcal{A}}_2$, so to $\widetilde{\mathcal{M}}_2$
- Up to a codimension 2 subvariety, universal curve over $k[a_0, \ldots, a_6]$ is semistable.

2. $\exists\, g_{8,6}$ Siegel m.f. of weight $\det^8 \otimes \mathrm{Sym}^6$. Then $g_{8,6} = \lambda\, I_{10}\, f_C$
   - This space of covariants has dimension 1.

Already noted in [Cléry, Faber, Van der Geer, 2016].

3. We get q-expansions for $a_0, \ldots, a_6 \to$ linear algebra.
   - $I_{10}^3 \dfrac{dj_1}{d\tau}$ is a modular form, so lives in a finite dimensional space of covariants.

Computing the normalization matrix

$$\phi\,:\,\mathrm{Jac}(C_1) \to \mathrm{Jac}(C_2), \quad \phi^*\,:\,\Omega^1(C_2) \to \Omega^1(C_1)$$

Canonical bases ω_1, ω_2 of $\Omega^1(C_1), \Omega^1(C_2)$:

$$\phi^*\omega_2 = m\,\omega_1, \quad m \in \mathrm{GL}_2(k).$$

- Compute $\dfrac{\partial j_1}{\partial \tau_1}, \ldots$ at $(\mathrm{Jac}(C_1), \omega_1)$ and $(\mathrm{Jac}(C_2), \omega_2)$.
- Differentiate modular equations w.r.t. τ_1, τ_2, τ_3.
- We get $\mathrm{Sym}^2(m)$ as a 3×3 matrix: we find $\pm m$.

Representing the isogeny

$$\mathrm{Jac}(C_1) \xrightarrow{\phi} \mathrm{Jac}(C_2)$$

Representing the isogeny

$$\begin{tikzcd}
 & & C_2^2 \arrow[d] \\
 & & C_2^{2,sym} \arrow[d, dashed, "\sim"] \\
C_1 \arrow[r, hook] \arrow[rru, bend left, red, "\exists!"] & \mathrm{Jac}(C_1) \arrow[r, "\phi"] & \mathrm{Jac}(C_2)
\end{tikzcd}$$

- Pick $P_0 \in C_1(k)$:

$$C_1 \hookrightarrow \mathrm{Jac}(C_1), \quad Q \mapsto [Q - P_0]$$

Representing the isogeny

$$
\begin{tikzcd}
\operatorname{Spec} k[[z]] \arrow[rr, "\exists\ (x_1, y_1, x_2, y_2)"] \arrow[dd] & & C_2^2 \arrow[d] \\
& & C_2^{2,sym} \arrow[d, dashed, "\sim"] \\
C_1 \arrow[r, hook] \arrow[urr, bend left, red, "\exists!"] & \operatorname{Jac}(C_1) \arrow[r, "\phi"] & \operatorname{Jac}(C_2)
\end{tikzcd}
$$

- Pick $P_0 \in C_1(k)$:

$$C_1 \hookrightarrow \operatorname{Jac}(C_1), \quad Q \mapsto [Q - P_0]$$

- Choose an uniformizer z of C_1 at P_0.

[Couveignes, Ezome, 2014]

Differential system

$$\begin{cases} \dfrac{x_1 dx_1}{y_1} + \dfrac{x_2 dx_2}{y_2} & = & (m_{1,1} u + m_{1,2}) \dfrac{du}{v} \\ \dfrac{dx_1}{y_1} + \dfrac{dx_2}{y_2} & = & (m_{2,1} u + m_{2,2}) \dfrac{du}{v} \\ y_1^2 = f_{C_2}(x_1) \\ y_2^2 = f_{C_2}(x_2) \end{cases}$$

- Newton iterations
- Recover meaningful quantities in $C_2^{2,sym}$, e.g. $x_1 + x_2 \in k(u)$
- Degrees $O(\ell)$ for an ℓ-isogeny, cost $\widetilde{O}(\ell)$.

Hilbert modular equations

Modular equations on $\mathbb{H}_2$ are too big (only known for $\ell \leq 7$).

Use more structured isogenies:

- Jacobians with fixed real multiplication, e.g. by $K = \mathbb{Q}(\sqrt{5})$. Siegel threefold $\to$ Hilbert surface.
- Isogenies should respect the real multiplication.
- Use cyclic β-isogenies, $N(\beta) = \ell$.

Hilbert modular equations are smaller: we can reach $\ell = 97$.

Algorithm remains (essentially) the same.

Complexity comparison

	Siegel ℓ-isogeny	Hilbert β-isogeny	EC
Total size of Φ	$\gg \ell^{12}$	$\widetilde{O}(\ell^4)$?	$\widetilde{O}(\ell^3)$
$\deg \Phi(j, X)$	$\ell^3 + \ell^2 + \ell + 1$	$\ell + 1$	$\ell + 1$
Size of $\Phi(j, X)$	$\widetilde{O}(\ell^4)$	$\widetilde{O}(\ell^2)$	$\widetilde{O}(\ell^2)$
$\# \ker \phi$	ℓ^2	ℓ	ℓ
$\deg(N, D)$	$O(\ell)$	$O(\sqrt{\ell})$	$O(\ell)$

- Computations become feasible.

Example

Setting: $k = \mathbb{F}_{56311}$, real multiplication by $\mathbb{Q}(\sqrt{5})$, $N(\beta) = 11$.

$$f_{C_1}(u) = 4557u^6 + 11367u^5 + 26321u^4 + 49674u^3 + 55725u^2 + u$$
$$f_{C_2}(x) = 29024x^6 + 6872x^5 + 56082x^4 + 54138x^3 + 9838x^2 + 40828x + 1065$$

Jacobians are β-isogenous.

Example

Setting: $k = \mathbb{F}_{56311}$, real multiplication by $\mathbb{Q}(\sqrt{5})$, $N(\beta) = 11$.

$$f_{C_1}(u) = 4557u^6 + 11367u^5 + 26321u^4 + 49674u^3 + 55725u^2 + u$$
$$f_{C_2}(x) = 29024x^6 + 6872x^5 + 56082x^4 + 54138x^3 + 9838x^2 + 40828x + 1065$$

Jacobians are β-isogenous.

$$m = \begin{pmatrix} 2951\alpha + 29631 & 25196\alpha + 12598 \\ 15075\alpha + 35693 & 31443\alpha + 43877 \end{pmatrix} \text{ with } \alpha^2 + \alpha + 2 = 0.$$

Example

Setting: $k = \mathbb{F}_{56311}$, real multiplication by $\mathbb{Q}(\sqrt{5})$, $N(\beta) = 11$.

$$f_{C_1}(u) = 4557u^6 + 11367u^5 + 26321u^4 + 49674u^3 + 55725u^2 + u$$
$$f_{C_2}(x) = 29024x^6 + 6872x^5 + 56082x^4 + 54138x^3 + 9838x^2 + 40828x + 1065$$

Jacobians are β-isogenous.

$$m = \begin{pmatrix} 2951\alpha + 29631 & 25196\alpha + 12598 \\ 15075\alpha + 35693 & 31443\alpha + 43877 \end{pmatrix} \text{ with } \alpha^2 + \alpha + 2 = 0.$$

$$P_0 = (0,0), \quad z = \sqrt{u}$$
$$x_1(z) = 34291 + (343\alpha + 28327)z + 35342z^2 + \cdots$$

Example

Setting: $k = \mathbb{F}_{56311}$, real multiplication by $\mathbb{Q}(\sqrt{5})$, $N(\beta) = 11$.

$$f_{C_1}(u) = 4557u^6 + 11367u^5 + 26321u^4 + 49674u^3 + 55725u^2 + u$$
$$f_{C_2}(x) = 29024x^6 + 6872x^5 + 56082x^4 + 54138x^3 + 9838x^2 + 40828x + 1065$$

Jacobians are β-isogenous.

$$m = \begin{pmatrix} 2951\alpha + 29631 & 25196\alpha + 12598 \\ 15075\alpha + 35693 & 31443\alpha + 43877 \end{pmatrix} \text{ with } \alpha^2 + \alpha + 2 = 0.$$

$$P_0 = (0,0), \quad z = \sqrt{u}$$
$$x_1(z) = 34291 + (343\alpha + 28327)z + 35342z^2 + \cdots$$

$$x_1(u) + x_2(u) = \frac{12776u^6 + 25u^5 + 39114u^4 + \cdots}{u^6 + 26620u^5 + 24821u^4 + \cdots}$$

Questions ?

Thank you!