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 $\ell$-isogenous elliptic curves: $\Phi_\ell(j(E_1), j(E_2)) = 0$. Compute an $\ell$-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

\[ \phi : E_1 \to E_2 \text{ induces } \phi^* : \Omega^1(E_2) \to \Omega^1(E_1). \]

\[ E_1 : v^2 = u^3 + a_1 u + b_1 \quad E_2 : y^2 = x^3 + a_2 x + b_2 \]

\[ \omega_1 = \frac{du}{v} \quad \omega_2 = \frac{dx}{y} \]

- Normalization matrix \( m \in \text{GL}_1(k) = k^\times: \phi^*(\omega_2) = m \omega_1. \)
Action on differential forms

\[ \phi : E_1 \rightarrow E_2 \] induces \( \phi^* : \Omega^1(E_2) \rightarrow \Omega^1(E_1) \).

\[ E_1 : v^2 = u^3 + a_1 u + b_1 \quad E_2 : y^2 = x^3 + a_2 x + b_2 \]

\[ \omega_1 = \frac{du}{v} \quad \omega_2 = \frac{dx}{y} \]

> **Normalization matrix** \( m \in \text{GL}_1(k) = k^\times : \quad \phi^*(\omega_2) = m \omega_1. \)

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

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

> Compute \( m \)
> Solve \( (S) \).
Evaluating modular forms

\[ \tau \in \mathbb{H}_1 \text{ gives} \]

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

Definition

- Given \((E, \omega)\) over \(\mathbb{C}\), choose \(\tau\) with \(\eta : E \simarrow E(\tau)\).

\[ \omega = g \eta^*(dz), \quad g \in \text{GL}_1(\mathbb{C}) \]

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

\((E, \omega) \leftrightarrow \text{Weierstrass equation.}\)
Computing the normalization matrix (1)

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

\[
\begin{array}{ccc}
E_1 & \xrightarrow{\phi} & E_2 \\
\sim & & \sim \\
E(\tau) & \longrightarrow & E(\tau/\ell).
\end{array}
\]

Weierstrass equations for \( E_1, E_2 \) give differential forms \( \omega_1, \omega_2 \):

\[\omega_1 = g_1 \, dz, \quad \omega_2 = g_2 \, dz\]

for some \( g_1, g_2 \in \text{GL}_1(\mathbb{C}) \).

- \( E(\tau) \rightarrow E(\tau/\ell) \) pulls \( dz \) back to \( dz \)
- Normalization matrix is \( m = g_1^{-1} g_2 \).
Computing the normalization matrix (2)

Key idea: use $\frac{dj}{d\tau}$, 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 $\Phi_{\ell}$ at $(j(E_1), j(E_2))$.

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

Key idea: use $\frac{dj}{d\tau}$, 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 $\Phi_\ell$ at $(j(E_1), j(E_2))$.

- $\frac{dj}{d\tau}(E, \omega) = \lambda j(E) \frac{b}{a}$ 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: \( \phi(u, v) = (x(u), v y(u)) \)

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

Solved locally around \( \mathcal{O}_{E_1} \).

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

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

1. The case of elliptic curves

2. From genus 1 to genus 2
From genus 1 to genus 2

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

$$J = \text{Jac}(C)$$

$$C : \nu^2 = f_C(u), \text{ deg } f_C \in \{5, 6\}$$

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

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

Problem
Jac($C_1$), Jac($C_2$) satisfying modular equations of level $\ell$.
Compute an isogeny explicitly?

- Compute the normalization matrix $m \in \text{GL}_2(k)$
- Solve a differential system.
Siegel modular forms: dictionary

\( \text{SL}_2(\mathbb{Z}) \subset \mathbb{H}_1 \quad \text{Sp}_4(\mathbb{Z}) \subset \mathbb{H}_2 = \left\{ \tau = \begin{pmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{pmatrix} \mid \text{Im}(\tau) > 0 \right\} \)

\( f \) of weight \( k \) \hspace{1cm} \text{f vector-valued Siegel modular form of weight } \rho \ :
\begin{align*}
\rho : \text{GL}_2(\mathbb{C}) & \to \text{GL}(V) \\
 f : \mathbb{H}_2 & \to V \\
f((a\tau + b)(c\tau + d)^{-1}) & = \rho(c\tau + d)f(\tau)
\end{align*}

\( j(\tau) \) \hspace{1cm} \text{Igusa birational invariants } j_1, j_2, j_3

\( \Phi_\ell(j, J) = 0 \) \hspace{1cm} 3 equations in \( j_1, j_2, j_3, J_1, J_2, J_3 \) (huge)

\( \frac{dj}{d\tau} \) of weight 2 \hspace{1cm} \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 \( \rho = \text{Sym}^2 \) (dim. 3)

Polynomials in \( a, b \) \hspace{1cm} \text{Covariants of the sextic } C : \nu^2 = f_C(u).
Derivatives of Igusa invariants

\[ C : \nu^2 = f_C(u) = a_6 u^6 + \cdots + a_0 \]

- Scalar-valued covariants: e.g. Igusa–Clebsch \( l_2, l_4, l_6, l_{10} \)
- Vector-valued covariants: \( f_C \) (dim. 7), \( y_1, y_2, y_3 \) (dim. 3),...
  (Notation from [Mestre 1991])

\[
\frac{\partial j_1}{\partial \tau} = \lambda \frac{1}{l_{10}} \left( \frac{153}{8} l_4 l_2^2 y_1 - \frac{135}{2} l_2 l_6 y_1 + \frac{135}{2} l_4^2 y_1 \\
+ \frac{46575}{4} l_2 l_4 y_2 - 30375 l_6 y_2 + 1366875 l_4 y_3 \right)
\]

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

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

$\tilde{M}_2 \otimes \tilde{A}_2 \mapsto \tilde{M}_2 \moduli stack$ for semistable curves.

$g$ extends to $\tilde{A}_2$, so to $\tilde{M}_2$.

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 $\det 8 \otimes \text{Sym} 6$. 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 $a_0, \ldots, a_6 \rightarrow$ linear algebra.

$I_{310} dj_1 d\tau$ is a modular form, so lives in a finite dimensional space of covariants.
Sketch of proof

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

\[ \tilde{M}_2 \leftarrow \tilde{A}_2 \]

\[ \uparrow \quad \uparrow \]

\[ M_2 \leftarrow A_2 \]

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

\[ 13 / 20 \]
Sketch of proof

1. Any holomorphic modular form \( g \) is a polynomial covariant.

\[
\begin{array}{ccc}
\tilde{\mathcal{M}}_2 & \longrightarrow & \tilde{\mathcal{A}}_2 \\
\uparrow & & \uparrow \\
\mathcal{M}_2 & \longrightarrow & \mathcal{A}_2
\end{array}
\]

\( \tilde{\mathcal{M}}_2 \) moduli stack for semistable curves.

\( g \) extends to \( \tilde{\mathcal{A}}_2 \), so to \( \tilde{\mathcal{M}}_2 \)

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 \( \det^8 \otimes \text{Sym}^6 \). Then \( g_{8,6} = \lambda I_{10} f_C \)

\( \quad \text{This space of covariants has dimension 1.} \)

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

1. Any holomorphic modular form \( g \) is a polynomial covariant.

\[
\begin{array}{ccc}
\tilde{M}_2 & \longrightarrow & \tilde{A}_2 \\
\uparrow & & \uparrow \\
M_2 & \longrightarrow & A_2
\end{array}
\]

\( \tilde{M}_2 \) moduli stack for semistable curves.

\( g \) extends to \( \tilde{A}_2 \), so to \( \tilde{M}_2 \)

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 \( \text{det}^8 \otimes \text{Sym}^6 \). Then \( g_{8,6} = \lambda l_{10} f_C \)

\( \Rightarrow \) This space of covariants has dimension 1.

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

3. We get \( q \)-expansions for \( a_0, \ldots, a_6 \rightarrow \) linear algebra.

\( l_{10}^3 \frac{dj_1}{d\tau} \) is a modular form, so lives in a finite dimensional space of covariants.
Computing the normalization matrix

\[ \phi : \text{Jac}(C_1) \to \text{Jac}(C_2), \quad \phi^* : \Omega^1(C_2) \to \Omega^1(C_1) \]

Canonical bases \( \omega_1, \omega_2 \) of \( \Omega^1(C_1), \Omega^1(C_2) \):

\[ \phi^* \omega_2 = m \omega_1, \quad m \in \text{GL}_2(k). \]

- Compute \( \frac{\partial j_1}{\partial \tau_1} \), \ldots at \((\text{Jac}(C_1), \omega_1)\) and \((\text{Jac}(C_2), \omega_2)\).
- Differentiate modular equations w.r.t. \( \tau_1, \tau_2, \tau_3 \).
- We get \( \text{Sym}^2(m) \) as a \( 3 \times 3 \) matrix: we find \( \pm m \).
Representing the isogeny

\[ \text{Jac}(C_1) \xrightarrow{\phi} \text{Jac}(C_2) \]
Representing the isogeny

\[ \exists \left( x_1, y_1, x_2, y_2 \right) \sim \exists \phi \quad \text{Pick } P_0 \in C_1(k): \]

\[ C_1 \leftrightarrow \text{Jac}(C_1), \quad Q \mapsto [Q - P_0] \]
Representing the isogeny

\[ \text{Spec } k[[z]] \xrightarrow{\exists (x_1, y_1, x_2, y_2)} C_2^2 \]

\[ C_1 \xrightarrow{\exists!} C_2^{2, \text{sym}} \]

\[ C_1 \xhookleftarrow{} \text{Jac}(C_1) \xrightarrow{\phi} \text{Jac}(C_2) \]

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

\[ C_1 \xhookleftarrow{} \text{Jac}(C_1), \quad Q \mapsto [Q - P_0] \]

- Choose an uniformizer \( z \) of \( C_1 \) at \( P_0 \).

[Couveignes, Ezome, 2014]
Differential system

\[
\begin{align*}
\frac{x_1 dx_1}{y_1} + \frac{x_2 dx_2}{y_2} &= (m_{1,1}u + m_{1,2}) \frac{du}{v} \\
\frac{y_1}{dx_1} + \frac{y_2}{dx_2} &= (m_{2,1}u + m_{2,2}) \frac{du}{v} \\
y_1^2 &= f_{C_2}(x_1) \\
y_2^2 &= f_{C_2}(x_2)
\end{align*}
\]

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

16 / 20
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 $\rightarrow$ Hilbert surface.
- Isogenies should respect the real multiplication.
- Use cyclic $\beta$-isogenies, $N(\beta) = \ell$.

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

Algorithm remains (essentially) the same.
## Complexity comparison

<table>
<thead>
<tr>
<th></th>
<th>Siegel $\ell$-isogeny</th>
<th>Hilbert $\beta$-isogeny</th>
<th>EC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total size of $\Phi$</td>
<td>$\gg \ell^{12}$</td>
<td>$\tilde{O}(\ell^4)$?</td>
<td>$\tilde{O}(\ell^3)$</td>
</tr>
<tr>
<td>$\deg \Phi(j, X)$</td>
<td>$\ell^3 + \ell^2 + \ell + 1$</td>
<td>$\ell + 1$</td>
<td>$\ell + 1$</td>
</tr>
<tr>
<td>Size of $\Phi(j, X)$</td>
<td>$\tilde{O}(\ell^4)$</td>
<td>$\tilde{O}(\ell^2)$</td>
<td>$\tilde{O}(\ell^2)$</td>
</tr>
<tr>
<td>$# \ker \phi$</td>
<td>$\ell^2$</td>
<td>$\ell$</td>
<td>$\ell$</td>
</tr>
<tr>
<td>$\deg(N, D)$</td>
<td>$O(\ell)$</td>
<td>$O(\sqrt{\ell})$</td>
<td>$O(\ell)$</td>
</tr>
</tbody>
</table>

- 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 \( \beta \)-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 $\beta$-isogenous.

\[
m = \begin{pmatrix} 2951\alpha + 29631 & 25196\alpha + 12598 \\ 15075\alpha + 35693 & 31443\alpha + 43877 \end{pmatrix}
\]

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 \( \beta \)-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 $\beta$-isogenous.

$m = \begin{pmatrix}
2951\alpha + 29631 & 25196\alpha + 12598 \\
15075\alpha + 35693 & 31443\alpha + 43877
\end{pmatrix}$ 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!