Isogeny graphs in dimension 2
2014/12/17 — Cryptographic seminar — Caen

Gaëtan Bisson, Romain Cosset, Alina Dudeanu, Sorina Ionica, Dimitar Jetchev, David Lubicz, Chloë Martindale, Damien Robert
Outline

1. Isogenies on elliptic curves
2. Abelian varieties and polarisations
3. Maximal isotropic isogenies
4. Cyclic isogenies
5. Isogeny graphs in dimension 2
**Complex elliptic curve**

- Over \( \mathbb{C} \): an elliptic curve is a torus \( E = \mathbb{C}/\Lambda \), where \( \Lambda \) is a lattice \( \Lambda = \mathbb{Z} + \tau \mathbb{Z} \ (\tau \in \mathbb{H}_1) \).

- Let \( \wp(z, \Lambda) = \sum_{w \in \Lambda \setminus \{0\}} \left( \frac{1}{(z-w)^2} - \frac{1}{w^2} \right) \) be the Weierstrass \( \wp \)-function and \( E_{2k}(\Lambda) = \lambda_k \sum_{w \in \Lambda \setminus \{0\}} \frac{1}{w^{2k}} \) be the (normalised) Eisenstein series of weight \( 2k \).

- Then \( \mathbb{C}/\Lambda \to E, z \mapsto (\wp'(z, \Lambda), \wp(z, \Lambda)) \) is an analytic isomorphism to the elliptic curve

\[
y^2 = 4x^3 - 60E_4(\Lambda) - 140E_6(\Lambda).
\]
Isogenies between elliptic curves

Definition

An isogeny is a (non trivial) algebraic map \( f : E_1 \to E_2 \) between two elliptic curves such that \( f(P + Q) = f(P) + f(Q) \) for all geometric points \( P, Q \in E_1 \).

Theorem

An algebraic map \( f : E_1 \to E_2 \) is an isogeny if and only if \( f(0_{E_1}) = f(0_{E_2}) \).

Corollary

An algebraic map between two elliptic curves is either

- trivial (i.e. constant)
- or the composition of a translation with an isogeny.

Remark

Isogenies are surjective (on the geometric points). In particular, if \( E \) is ordinary, any curve isogenous to \( E \) is also ordinary.
Destructive cryptographic applications

- An isogeny \( f: E_1 \rightarrow E_2 \) transports the DLP problem from \( E_1 \) to \( E_2 \). This can be used to attack the DLP on \( E_1 \) if there is a weak curve on its isogeny class (and an efficient way to compute an isogeny to it).

**Example**

- extend attacks using Weil descent [GHS02]
- Transfert the DLP from the Jacobian of an hyperelliptic curve of genus 3 to the Jacobian of a quartic curve [Smi09].
One can recover informations on the elliptic curve $E$ modulo $\ell$ by working over the $\ell$-torsion.

But by computing isogenies, one can work over a cyclic subgroup of cardinal $\ell$ instead.

Since thus a subgroup is of degree $\ell$, whereas the full $\ell$-torsion is of degree $\ell^2$, we can work faster over it.

**Example**

- The SEA point counting algorithm [Sch95; Mor95; Elk97];
- The CRT algorithms to compute class polynomials [Sut11; ES10];
- The CRT algorithms to compute modular polynomials [BLS12].
Further applications of isogenies

- Splitting the multiplication using isogenies can improve the arithmetic [DIK06; Gau07];
- The isogeny graph of a supersingular elliptic curve can be used to construct secure hash functions [CLG09];
- Construct public key cryptosystems by hiding vulnerable curves by an isogeny (the trapdoor) [Tes06], or by encoding informations in the isogeny graph [RS06];
- Take isogenies to reduce the impact of side channel attacks [Sma03];
- Construct a normal basis of a finite field [CL09];
- Improve the discrete logarithm in $\mathbb{F}_q^*$ by finding a smoothness basis invariant by automorphisms [CL08].
Computing explicit isogenies

- If $E_1$ and $E_2$ are two elliptic curves given by Weierstrass equations, a morphism of curve $f : E_1 \rightarrow E_2$ is of the form
  \[ f(x,y) = (R_1(x,y), R_2(x,y)) \]
  where $R_1$ and $R_2$ are rational functions, whose degree in $y$ is less than 2 (using the equation of the curve $E_1$).
- If $f$ is an isogeny, $f(−P) = −f(P)$. If char $k > 3$ so we can assume that $E_1$ and $E_2$ are given by reduced Weierstrass forms, this mean that $R_1$ depends only on $x$, and $R_2$ is $y$ time a rational function depending only on $x$.
- Let $\omega_E = dx/2y$ be the canonical differential. Then $f^*\omega_{E'} = c\omega_E$, with $c$ in $k$.
- This shows that $f$ is of the form
  \[ f(x,y) = \left( \frac{g(x)}{h(x)}, cy \left( \frac{g(x)}{h(x)} \right)' \right). \]
  $h(x)$ gives (the $x$ coordinates of the points in) the kernel of $f$ (if we take it prime to $g$).
- If $c = 1$, we say that $f$ is normalized.
Vélu’s formula

- Let $E/k$ be an elliptic curve. Let $G = \langle P \rangle$ be a rational finite subgroup of $E$.
- Vélu constructs the isogeny $E \to E/G$ as
  
  \[
  X(P) = x(P) + \sum_{Q \in G \setminus \{0_E\}} (x(P + Q) - x(Q)) \\
  Y(P) = y(P) + \sum_{Q \in G \setminus \{0_E\}} (y(P + Q) - y(Q)).
  \]

  The choices are made so that the formulas give a normalized isogeny.
- Moreover by looking at the expression of $X$ and $Y$ in the formal group of $E$, Vélu recovers the equations for $E/G$.
- For instance if $E : y^2 = x^3 + ax + b = f_E(x)$ then $E/G$ is
  
  \[
  y^2 = x^3 + (a - 5t)x + b - 7w
  \]

  where $t = \sum_{Q \in G \setminus \{0_E\}} f'_E(Q)$, $u = 2 \sum_{Q \in G \setminus \{0_E\}} f_E(Q)$ and $w = \sum_{Q \in G \setminus \{0_E\}} x(Q)f'_E(Q)$. 

Complexity of Vélu’s formula

- Even if $G$ is rational, the points in $G$ may live to an extension of degree up to $\#G - 1$.
- Thus summing over the points in the kernel $G$ can be expensive.
- Let $h(x) = \prod_{Q \in G \setminus \{0_E\}} (x - x(Q))$. The symmetry of $X$ and $Y$ allows us to express everything in term of $h$.
- For instance is $E$ is given by a reduced Weierstrass equation $y^2 = f_E(x)$, we have

$$f(x, y) = \left( \frac{g(x)}{h(x)} , y \left( \frac{g(x)}{h(x)} \right)' \right),$$

with

$$\frac{g(x)}{h(x)} = \#G \cdot x - \sigma - f'_E(x) \frac{h'(x)}{h(x)} - 2f_E(x) \left( \frac{h'(x)}{h(x)} \right)' ,$$

where $\sigma$ is the first power sum of $h$ (i.e. the sum of the $x$-coordinates of the points in the kernel).
- When $\#G$ is odd, $h(x)$ is a square, so we can replace it by its square root.
- The complexity of computing the isogeny is then $O(M(\#G))$ operations in $k$. 
Here $k = \bar{k}$.

**Definition (Modular polynomial)**

The modular polynomial $\varphi_{\ell}(x, y) \in \mathbb{Z}[x, y]$ is a bivariate polynomial such that $\varphi_{\ell}(x, y) = 0 \iff x = j(E_1)$ and $y = j(E_2)$ with $E_1$ and $E_2$ \(\ell\)-isogeneous.

- Roots of $\varphi_{\ell}(j(E_1), \ldots) \iff$ elliptic curves \(\ell\)-isogeneous to $E_1$. There are $\ell + 1 = \#\mathbb{P}^1(\mathbb{F}_\ell)$ such roots if $\ell$ is prime.
- $\varphi_{\ell}$ is symmetric.
- The height of $\varphi_{\ell}$ grows as $O(\ell)$. 


Finding an isogeny between two isogenous elliptic curves

- Let $E_1$ and $E_2$ be $\ell$-isogenous abelian varieties (we can check that $\varphi_\ell(j_{E_1}, j_{E_2}) = 0$). We want to compute the isogeny $f : E_1 \to E_2$.
- The explicit forms of isogenies are given by Vélu’s formula, which give normalized isogenies. We first need to normalize $E_2$.
- Over $\mathbb{C}$, the equation of the normalized curve $E_2$ is given by the Eisenstein series $E_4(\ell \tau)$ and $E_6(\ell \tau)$. We have $j'(\ell \tau)/j(\ell \tau) = -E_6(\ell \tau)/E_4(\ell \tau)$. By differencing the modular polynomial, we recover the differential logarithms.
- We obtain that from $E_1 : y^2 = x^3 + ax + b$, a normalized model of $E_2$ is given by the Weierstrass equation
  \[ y^2 = x^3 + Ax + B \]
  where $A = -\frac{1}{48} \frac{j^2}{j_{E_2}(j_{E_2} - 1728)}$, $B = -\frac{1}{864} \frac{j^3}{j_{E_2}(j_{E_2} - 1728)}$ and $J = -\frac{18}{\ell} \frac{b \varphi'_\ell(x)}{a \varphi'_\ell(y)} \frac{j_{E_1} j_{E_2}}{j_{E_1}}$. \\

**Remark**

$E_2(\tau)$ is the differential logarithm of the discriminant. Similar methods allow to recover $E_2(\ell \tau)$, and from it $\sigma = \sum_{p \in K \setminus \{0\}} x(K)$. 
Finding the isogeny between the normalized models (Elkie’s method)

- We need to find the rational function $I(x) = g(x)/h(x)$ giving the isogeny $f: (x,y) \mapsto (I(x), yI'(x))$ between $E_1$ and $E_2$.
- Plugging $f$ into the equation of $E_2$ shows that $I$ satisfy the differential equation
  \[(x^3 + ax + b)I'(x)^2 = I(x)^3 + AI(x) + B.\]
- Using an asymptotically fast algorithm to solve this equation yields $I(x)$ in time quasi-linear ($\tilde{O}(\ell)$).
- Knowing $\sigma$ gains a logarithmic factor.
A 3-isogeny graph in dimension 1
Polarised abelian varieties over \( \mathbb{C} \)

**Definition**

A complex abelian variety \( A \) of dimension \( g \) is isomorphic to a compact Lie group \( V/\Lambda \) with

- A complex vector space \( V \) of dimension \( g \);
- A \( \mathbb{Z} \)-lattice \( \Lambda \) in \( V \) (of rank \( 2g \));

such that there exists an Hermitian form \( H \) on \( V \) with \( E(\Lambda, \Lambda) \subset \mathbb{Z} \) where \( E = \text{Im} \, H \) is symplectic.

- Such an Hermitian form \( H \) is called a polarisation on \( A \). Conversely, any symplectic form \( E \) on \( V \) such that \( E(\Lambda, \Lambda) \subset \mathbb{Z} \) and \( E(ix, iy) = E(x, y) \) for all \( x, y \in V \) gives a polarisation \( H \) with \( E = \text{Im} \, H \).
- Over a symplectic basis of \( \Lambda \), \( E \) is of the form.

\[
\begin{pmatrix}
0 & D_{\delta} \\
-D_{\delta} & 0
\end{pmatrix}
\]

where \( D_{\delta} \) is a diagonal positive integer matrix \( \delta = (\delta_1, \delta_2, \ldots, \delta_g) \), with \( \delta_1 | \delta_2 | \cdots | \delta_g \).

- The product \( \prod \delta_i \) is the degree of the polarisation; \( H \) is a principal polarisation if this degree is 1.
Principal polarisations

- Let $E_0$ be the canonical principal symplectic form on $\mathbb{R}^{2g}$ given by $E_0((x_1,x_2),(y_1,y_2)) = \langle x_1 \cdot y_2 - y_1 \cdot x_2 \rangle$;

- If $E$ is a principal polarisation on $A = V/\Lambda$, there is an isomorphism $j: \mathbb{Z}^{2g} \to \Lambda$ such that $E(j(x), j(y)) = E_0(x, y)$;

- There exists a basis of $V$ such that $j((x_1,x_2)) = \Omega x_1 + x_2$ for a matrix $\Omega$;

- In particular $E(\Omega x_1 + x_2, \Omega y_1 + y_2) = \langle x_1 \cdot y_2 - y_1 \cdot x_2 \rangle$;

- The matrix $\Omega$ is in $\mathfrak{H}_g$, the Siegel space of symmetric matrices $\Omega$ with $\text{Im} \Omega$ positive definite;

- In this basis, $\Lambda = \Omega \mathbb{Z}^g + \mathbb{Z}^g$ and $H$ is given by the matrix $(\text{Im} \Omega)^{-1}$. 
Let $A = V/\Lambda$ and $B = V'/\Lambda'$.

**Definition**

An isogeny $f : A \rightarrow B$ is a bijective linear map $f : V \rightarrow V'$ such that $f(\Lambda) \subset \Lambda'$. The kernel of the isogeny is $f^{-1}(\Lambda')/\Lambda \subset A$ and its degree is the cardinal of the kernel.

- Two abelian varieties over a finite field are isogenous iff they have the same zeta function (Tate);
- A morphism of abelian varieties $f : A \rightarrow B$ (seen as varieties) is a group morphism iff $f(0_A) = 0_B$. 
The dual abelian variety

**Definition**

If \( A = V/\Lambda \) is an abelian variety, its dual is \( \hat{A} = \text{Hom}_\mathbb{C}(V, \mathbb{C})/\Lambda^* \). Here \( \text{Hom}_\mathbb{C}(V, \mathbb{C}) \) is the space of anti-linear forms and \( \Lambda^* = \{ f | f(\Lambda) \subset \mathbb{Z} \} \) is the orthogonal of \( \Lambda \).

- If \( H \) is a polarisation on \( A \), its dual \( H^* \) is a polarisation on \( \hat{A} \). Moreover, there is an isogeny \( \Phi_H : A \to \hat{A} \):

\[
x \mapsto H(x, \cdot)
\]

of degree \( \text{deg} H \). We note \( K(H) \) its kernel.

- If \( f : A \to B \) is an isogeny, then its dual is an isogeny \( \hat{f} : \hat{B} \to \hat{A} \) of the same degree.

**Remark**

There is a canonical polarisation on \( A \times \hat{A} \) (the Poincaré bundle):

\[
(x, f) \mapsto f(x).
\]
Isogenies and polarisations

Definition

- An isogeny \( f : (A, H_1) \rightarrow (B, H_2) \) between polarised abelian varieties is an isogeny such that
  \[
  f^* H_2 := H_2(f(\cdot), f(\cdot)) = H_1.
  \]

- By abuse of notations, we say that \( f \) is an \( \ell \)-isogeny between principally polarised abelian varieties if \( H_1 \) and \( H_2 \) are principal and \( f^* H_2 = \ell H_1 \).

An isogeny \( f : (A, H_1) \rightarrow (B, H_2) \) respect the polarisations iff the following diagram commutes

\[
\begin{array}{ccc}
A & \xrightarrow{f} & B \\
\downarrow{\Phi_{H_1}} & & \downarrow{\Phi_{H_2}} \\
\hat{A} & \xleftarrow{\hat{f}} & \hat{B}
\end{array}
\]
An isogeny \( f : (A, H_1) \to (B, H_2) \) between polarised abelian varieties is an isogeny such that
\[
f^* H_2 := H_2(f(\cdot), f(\cdot)) = H_1.
\]
By abuse of notations, we say that \( f \) is an \( \ell \)-isogeny between principally polarised abelian varieties if \( H_1 \) and \( H_2 \) are principal and \( f^* H_2 = \ell H_1 \).

\( f : (A, H_1) \to (B, H_2) \) is an \( \ell \)-isogeny between principally polarised abelian varieties iff the following diagram commutes:

\[
\begin{align*}
A & \xrightarrow{f} B \\
\downarrow{[\ell]} & \downarrow{\Phi_{\ell H_1}} & \downarrow{\Phi_{H_2}} \\
A & \xrightarrow{\Phi_{H_1}} \hat{A} & \xleftarrow{\hat{f}} \hat{B}
\end{align*}
\]
Jacobians

- Let $C$ be a curve of genus $g$;
- Let $V$ be the dual of the space $V^*$ of holomorphic differentials of the first kind on $C$;
- Let $\Lambda \simeq H^1(C, \mathbb{Z}) \subset V$ be the set of periods (integration of differentials on loops);
- The intersection pairing gives a symplectic form $E$ on $\Lambda$;
- Let $H$ be the associated hermitian form on $V$;

\[ H^*(w_1, w_2) = \int_C w_1 \wedge w_2; \]

- Then $(V/\Lambda, H)$ is a principally polarised abelian variety: the Jacobian of $C$.

**Theorem (Torelli)**

Jac$C$ with the associated principal polarisation uniquely determines $C$.

**Remark (Howe)**

There exists an hyperelliptic curve $H$ of genus 3 and a quartic curve $C$ such that Jac$C \simeq$ Jac$H$ as non polarised abelian varieties!
Let \((A, H_0)\) be a principally polarised abelian variety over \(\mathbb{C}\):

\[
A = \mathbb{C}^g / (\Omega \mathbb{Z}^g + \mathbb{Z}^g) \quad \text{with} \quad \Omega \in \mathfrak{H}_g.
\]

**Theta functions with characteristics** \(a, b \in \mathbb{Q}^g\):

\[
\vartheta_{\left[ \begin{array}{c} a \\ b \end{array} \right]} (z, \Omega) = \sum_{n \in \mathbb{Z}^g} e^{\pi i (n+a)\Omega(n+a) + 2\pi i (n+a)(z+b)} \quad a, b \in \mathbb{Q}^g
\]

**Define** \(\vartheta_i = \vartheta_{\left[ \begin{array}{c} 0 \\ i/n \end{array} \right]} (., \frac{\Omega}{n})\) for \(i \in \mathbb{Z}(\overline{n}) = \mathbb{Z}^g / n\mathbb{Z}^g\)

\[
(\vartheta_i)_{i \in \mathbb{Z}(\overline{n})} = \begin{cases} \text{coordinates system} & n \geq 3 \\ \text{coordinates on the Kummer variety } A/ \pm 1 & n = 2 \end{cases}
\]
**The isogeny theorem**

**Theorem**

- Let $\varphi : \mathbb{Z}(\ell n) \rightarrow \mathbb{Z}(\ell n), x \mapsto \ell x$ be the canonical embedding.
- Let $K = A_2[\ell] \subset A_2[\ell n]$.
- Let $(\vartheta^A_i)_{i \in \mathbb{Z}(\ell n)}$ be the theta functions of level $\ell n$ on $A = \mathbb{C}^g/(\mathbb{Z}_g + \ell \Omega \mathbb{Z}_g)$.
- Let $(\vartheta^B_i)_{i \in \mathbb{Z}(\ell n)}$ be the theta functions of level $n$ of $B = A/K = \mathbb{C}^g/(\mathbb{Z}_g + \Omega \mathbb{Z}_g)$.
- We have:

\[
(\vartheta^B_i(x))_{i \in \mathbb{Z}(\ell n)} = (\vartheta^A_{\varphi(i)}(x))_{i \in \mathbb{Z}(\ell n)}
\]

**Example**

$f : (x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}) \mapsto (x_0, x_3, x_6, x_9)$ is a 3-isogeny between elliptic curves.
Theorem (Koizumi–Kempf)

Let $F$ be a matrix of rank $r$ such that $t^t FF = \ell \text{Id}_r$. Let $X \in (\mathbb{C}^g)^r$ and $Y = F(X) \in (\mathbb{C}^g)^r$. Let $j \in (\mathbb{Q}^g)^r$ and $i = F(j)$. Then we have

$$
\vartheta \left[ \frac{0}{i_1} \right] (Y_1, \frac{\Omega}{n}) \ldots \vartheta \left[ \frac{0}{i_r} \right] (Y_r, \frac{\Omega}{n}) = 
\sum_{t_1, \ldots, t_r \in \frac{1}{\ell} \mathbb{Z}^g / \mathbb{Z}^g} \vartheta \left[ \frac{0}{j_1} \right] (X_1 + t_1, \frac{\Omega}{\ell n}) \ldots \vartheta \left[ \frac{0}{j_r} \right] (X_r + t_r, \frac{\Omega}{\ell n}),
$$

(This is the isogeny theorem applied to $F_A : A^r \to A^r$.)

- If $\ell = a^2 + b^2$, we take $F = \left( \begin{array}{cc} a & b \\ -b & a \end{array} \right)$, so $r = 2$.
- In general, $\ell = a^2 + b^2 + c^2 + d^2$, we take $F$ to be the matrix of multiplication by $a + bi + cj + dk$ in the quaternions, so $r = 4$. 
The isogeny formula

\[ \ell \wedge n = 1, \quad B = \mathbb{C}^g / (\mathbb{Z}^g + \Omega \mathbb{Z}^g), \quad A = \mathbb{C}^g / (\mathbb{Z}^g + \ell \Omega \mathbb{Z}^g) \]

\[ \vartheta^B_b := \vartheta \left( \begin{bmatrix} 0 \\ \frac{b}{n} \end{bmatrix} \right) \left( \cdot, \frac{\Omega}{n} \right), \quad \vartheta^A_b := \vartheta \left( \begin{bmatrix} 0 \\ \frac{b}{n} \end{bmatrix} \right) \left( \cdot, \frac{\ell \Omega}{n} \right) \]

**Proposition**

Let \( F \) be a matrix of rank \( r \) such that \( t^t FF = \ell \text{Id}_r \). Let \( Y = (\ell x, 0, \ldots, 0) \) in \( (\mathbb{C}^g)^r \) and \( X = YF^{-1} = (x, 0, \ldots, 0)t_F \in (\mathbb{C}^g)^r \). Let \( i \in (\mathbb{Z}(n))^r \) and \( j = iF^{-1} \). Then we have

\[ \vartheta^A_{i_1}(\ell Z) \ldots \vartheta^A_{i_r}(0) = \sum_{t_1, \ldots, t_r \in \frac{1}{\ell} \mathbb{Z}^g/\mathbb{Z}^g} \vartheta^B_{j_1}(X_1 + t_1) \ldots \vartheta^B_{j_r}(X_r + t_r), \]

subject to \( F(t_1, \ldots, t_r) = (0, \ldots, 0) \).

**Corollary**

\[ \vartheta^A_k(0) \vartheta^A_0(0) \ldots \vartheta^A_0(0) = \sum_{t_1, \ldots, t_r \in K} \vartheta^B_{j_1}(t_1) \ldots \vartheta^B_{j_r}(t_r), \quad (j = (k, 0, \ldots, 0)F^{-1} \in \mathbb{Z}(n)) \]

subject to \( (t_1, \ldots, t_r)F = (0, \ldots, 0) \).
The Algorithm [Cosset, R.]

\[ x \in (A, \ell H_1) \rightarrow (x, 0, \ldots, 0) \in (A', \ell H_1 \ast \cdots \ast \ell H_1) \]

\[ y \in (B, H_2) \]

\[ \tilde{f} \]

We can compute the isogeny directly given the equations (in a suitable form) of the kernel \( K \) of the isogeny. When \( K \) is rational, this gives a complexity of \( \tilde{O}(\ell^g) \) or \( \tilde{O}(\ell^{2g}) \) operations in \( \mathbb{F}_q \) according to whether \( \ell \equiv 1 \) or 3 modulo 4.
The case \( \ell \equiv 1 \pmod{4} \)

- The isogeny formula assumes that the points are in affine coordinates. In practice, given \( A/\mathbb{F}_q \) we only have projective coordinates \( \Rightarrow \) we need to normalize the coordinates;
- We suppose that we have (projective) equations of \( K \) in diagonal form over the base field \( k \):
  \[
P_1(X_0, X_1) = 0
  
  \ldots
  
  X_nX_0^d = P_n(X_0, X_1)
\]
- By setting \( X_0 = 1 \) we can work with affine coordinates. The projective solutions can be written \((x_0, x_0x_1, \ldots, x_0x_n)\) so \( X_0 \) can be seen as the normalization factor.
- We work in the algebra \( \mathcal{A} = k[X_1]/(P_1(X_1)) \); each operation takes \( \tilde{O}(\ell^g) \) operations in \( k \)
- Let \( F = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \) where \( \ell = a^2 + b^2 \). Let \( c = -a/b \pmod{\ell} \). The couples in the kernel of \( F \) are of the form \((x, cx)\) for each \( x \in K \).
- So we normalize the generic point \( \eta \), compute \( c.\eta \) and then \( R := \vartheta^{A}_{j_1}(\eta)\vartheta^{A}_{j_2}(c.\eta) \in \mathcal{A} \).
- We need \( \sum_{x \in K} R(x_1) \in k \). In the euclidean division \( XRP'_1 = PQ + S \); this is simply \( Q(0) \).
An $(\ell, \ell)$-isogeny graph in dimension 2 [Bisson, Cosset, R.]
Let $f: (A, H_1) \rightarrow (B, H_2)$ be an isogeny between principally polarised abelian varieties;

When $\text{Ker} f$ is not maximal isotropic in $A[\ell]$ then $f^* H_2$ is not of the form $\ell H_1$;

How can we go from the principal polarisation $H_1$ to $f^* H_1$?
Theorem (Birkenhake-Lange, Th. 5.2.4)

Let $A$ be an abelian variety with a principal polarisation $\mathcal{L}_1$;

- Let $O_0 = \text{End}(A)^\text{sym}$ be the real algebra of endomorphisms symmetric under the Rosati involution;
- Let $\text{NS}(A)$ be the Néron-Severi group of line bundles modulo algebraic equivalence.

Then

- $\text{NS}(A)$ is a torsor under the action of $O_0$;
- This induces a bijection between polarisations of degree $d$ in $\text{NS}(A)$ and totally positive symmetric endomorphisms of norm $d$ in $O_0$;
- The isomorphic class of a polarisation $\mathcal{L}_f \in \text{NS}(A)$ for $f \in O_0^+$ correspond to the action $\varphi \mapsto \varphi^* f \varphi$ of the automorphisms of $A$. 
Cyclic isogeny

- Let \( f : (A, H_1) \to (B, H_2) \) be an isogeny between principally polarised abelian varieties with cyclic kernel of degree \( \ell \);
- There exists \( \varphi \) such that the following diagram commutes:

\[
\begin{array}{ccccc}
A & \xrightarrow{f} & B \\
\uparrow \varphi & & \uparrow \varphi_{H_2} & & \uparrow \varphi_{H_2} \\
A & \xleftarrow{\varphi_{H_1}} & \tilde{A} & \xleftarrow{\tilde{f}} & \tilde{B}
\end{array}
\]

- \( \varphi \) is an \((\ell, 0, \ldots, \ell, 0, \ldots)\)-isogeny whose kernel is not isotropic for the \( H_1 \)-Weil pairing on \( A[\ell] \)!
- \( \varphi \) commutes with the Rosatti involution so is a real endomorphism (\( \varphi \) is \( H_1 \)-symmetric). Since \( H_1 \) is Hermitian, \( \varphi \) is totally positive.
- \( \text{Ker} f \) is maximal isotropic for \( \varphi H_1 \); conversely if \( K \) is a maximal isotropic kernel in \( A[\varphi] \) then \( f : A \to A/K \) fits in the diagram above.
Descending a polarisation via \( \varphi \)

- The isogeny \( f \) induces a compatible isogeny between \( \varphi H_1 = f^* H_2 \) and \( H_2 \) where \( \varphi H_1 \) is given by the following diagram:

\[
\begin{array}{ccc}
  A & \xrightarrow{\varphi} & A \\
  \downarrow{\Phi_H} & \downarrow{\Phi_{H_1}} & \downarrow{\tilde{A}} \\
  \tilde{A} & & \\
\end{array}
\]

- \( \varphi \) plays the same role as \([\ell]\) for \( \ell \)-isogenies;

- We then define the \( \varphi \)-contragredient isogeny \( \tilde{f} \) as the isogeny making the following diagram commute:

\[
\begin{array}{ccc}
  x \in (A, \varphi^* H_1) & \xrightarrow{f} & y \in (B, \varphi H_2) \\
  \downarrow{\tilde{f}} & \downarrow{\varphi} & \downarrow{\tilde{f}} \\
  \tilde{f}(y) \in (A, H_1) & & \\
\end{array}
\]
We can use the isogeny theorem to compute $f$ from $(A, \varphi H_1)$ down to $(B, H_2)$ or $\tilde{f}$ from $(B, H_2)$ up to $(A, \varphi H_1)$ as before;

What about changing level between $(A, \varphi H_1)$ and $(A, H_1)$?

$\varphi H_1$ fits in the following diagram:

Applying the isogeny theorem on $\varphi$ allows to find relations between $\varphi^* H_1$ and $H_1$ but we want $\varphi H_1$. 
\( \varphi \)-change of level

- \( \varphi \) is a totally positive element of a totally positive order \( O_0 \);
- A theorem of Siegel show that \( \varphi \) is a sum of \( m \) squares in \( K_0 = O_0 \otimes \mathbb{Q} \);
- Clifford’s algebras give a matrix \( F \in \text{Mat}_r(K_0) \) such that \( \text{diag}(\varphi) = F^*F \);
- We can use this matrix \( F \) to change level as before: If \( X \in (\mathbb{C}^g)^r \) and \( Y = F(X) \in (\mathbb{C}^g)^r \), \( j \in (\mathbb{Q}^g)^r \) and \( i = F(j) \), we have (up to a modular automorphism)

\[
\vartheta \left[ \begin{smallmatrix} 0 \\ i_1 \\ \vdots \\ i_r \end{smallmatrix} \right] \left( Y_1, \frac{\Omega}{n} \right) \cdots \vartheta \left[ \begin{smallmatrix} 0 \\ i_r \end{smallmatrix} \right] \left( Y_r, \frac{\Omega}{n} \right) = \\
\sum_{t_1, \ldots, t_r \in K(\varphi H_i)} \vartheta \left[ \begin{smallmatrix} 0 \\ j_1 \\ \vdots \\ j_r \end{smallmatrix} \right] \left( X_1 + t_1, \frac{\varphi^{-1}\Omega}{n} \right) \cdots \vartheta \left[ \begin{smallmatrix} 0 \\ j_r \end{smallmatrix} \right] \left( X_r + t_r, \frac{\varphi^{-1}\Omega}{n} \right),
\]

Remark

- In general \( r \) can be larger than \( m \);
- The matrix \( F \) acts by real endomorphism rather than by integer multiplication;
- There may be denominators in the coefficients of \( F \).
The Algorithm for cyclic isogenies [Dudeanu, Jetchev, R.]

\[ B = \mathbb{C}^g / (\mathbb{Z}^g + \Omega \mathbb{Z}^g), \quad A = \mathbb{C}^g / (\mathbb{Z}^g + \varphi \Omega \mathbb{Z}^n), \quad \vartheta_b^B := \vartheta \left[ \frac{0}{b} \right] \left( \cdot, \frac{\Omega}{n} \right), \quad \vartheta_b^A := \vartheta \left[ \frac{0}{b} \right] \left( \cdot, \frac{\varphi \Omega}{n} \right) \]

**Theorem**

Let \( Y \in (\mathbb{C}^g)^r \) and \( X = YF^{-1} \in (\mathbb{C}^g)^r \). Let \( i \in (\mathbb{Z}(\overline{n}))^r \) and \( j = iF^{-1} \). Up to a modular automorphism:

\[
\vartheta_{i_1}^A(Y_1) \cdots \vartheta_{i_r}^A(Y_r) = \sum_{t_1, \ldots, t_r \in K(\varphi H_2)} \vartheta_{j_1}^B(X_1 + t_1) \cdots \vartheta_{j_r}^B(X_r + t_r),
\]

\( x \in (A, \varphi H_1) \to (x, 0, \ldots, 0) \in (A^r, \varphi H_1 \ast \cdots \ast \varphi H_1) \)

\( y \in (B, H_2) \to \tilde{f}(y) \in (A, H_1) \)

\( \varphi \)

\( tF \of(x, 0, \ldots, 0) \in (A^r, \varphi H_1 \ast \cdots \ast \varphi H_1) \)

\( F \of tF(x, 0, \ldots, 0) \in (A^r, H_1 \ast \cdots \ast H_1) \)
We normalize the coordinates by using multi-way additions;

The real endomorphisms are codiagonalisables (in the ordinary case), this is important to apply the isogeny theorem;

If \( g = 2 \), \( K_0 = \mathbb{Q}(\sqrt{d}) \), the action of \( \sqrt{d} \) is given by a standard \((d,d)\)-isogeny, so we can compute it using the previous algorithm for \( d \)-isogenies!

The important point is that this algorithm is such that we can keep track of the projective factors when computing the action of \( \sqrt{d} \).

Unlike the case of maximal isotropic kernels for the Weil pairing, for cyclic isogenies the Koizumi formula does not yield a product theta structure. We compute the action of the modular automorphism coming from \( F \) that gives a product theta structure.

**Remark**

Computing the action of \( \sqrt{d} \) directly may be expensive if \( d \) is big. If possible we replace it with Frobeniuses.
Abelian varieties with real and complex multiplication

- Let $K$ be a CM field (a totally imaginary quadratic extension of a totally real field $K_0$ of dimension $g$);

- An abelian variety with RM by $K_0$ is of the form $\mathbb{C}^g/(\Lambda_1 \oplus \Lambda_2 \tau)$ where $\Lambda_i$ is a lattice in $K_0$, $K_0$ is embedded into $\mathbb{C}^g$ via $K_0 \otimes \mathbb{Q} \mathbb{R} = \mathbb{R}^g \subset \mathbb{C}^g$, and $\tau \in \mathfrak{h}_1^g$;

- Furthermore the polarisations are of the form

$$H(z_1,z_2) = \sum_{\varphi_i : K \rightarrow \mathbb{C}} \varphi_i(\lambda z_1 \overline{z_2})/\Im \tau_i$$

for a totally positive element $\lambda \in K_0^{++}$. In other words if $x_i,y_i \in K_0$, then

$$E(x_1 + y_1 \tau, x_2 + y_2 \tau) = \text{Tr}_{K_0/\mathbb{Q}}(\lambda (x_2y_1 - x_1y_2)).$$

- An abelian variety with CM by $K$ is of the form $\mathbb{C}^g/\Phi(\Lambda)$ where $\Lambda$ is a lattice in $K$ and $\Phi$ is a CM-type.

- Furthermore, the polarisations are of the form

$$E(z_1,z_2) = \text{Tr}_{K/\mathbb{Q}}(\xi z_1 \overline{z_2})$$

for a totally imaginary element $\xi \in K$. The polarisation is principal iff $\xi \overline{\Lambda} = \Lambda^*$ where $\Lambda^*$ is the dual of $\Lambda$ for the trace.
Let $A$ be a principally polarised abelian surface over $\mathbb{F}_q$ with CM by $O \subset O_K$ and RM by $O_0 \subset O_{K_0}$;

Cyclic isogenies (between ppav) of degree $\ell$ correspond to kernels inside $A[\varphi]$ for an endomorphism $\varphi \in O_0^{++}$ of degree $\ell$. They preserve the real multiplication.

Let’s assume that $O_0$ is maximal and that we are in the split case: $(\ell) = (\varphi_1)(\varphi_2)$ in $O_0$ (where $\varphi_i$ is totally positive). Then $A[\ell] = A[\varphi_1] \oplus A[\varphi_2]$. We have two kind of cyclic isogenies: the $\varphi_1$-isogenies and the $\varphi_2$-isogenies.

When we look only at $\varphi_1$ isogenies, we recover the structure of a volcano: we have $O = O_0 + IO_K$ for a certain $O_0$-ideal $I$ such that the conductor of $O$ is $IO_K$.

- If $I$ is prime to $\varphi_1$, we have 2, 1, or 0 horizontal-isogenies according to whether $\varphi_1$ splits, is ramified or is inert in $O$, and the rest are descending to $O_0 + I\varphi_1 O_K$;
- If $I$ is not prime to $\varphi_1$ we have one ascending isogeny (to $O_0 + I/\varphi_1 O_K$) and $\ell$ descending ones;
- We are at the bottom when the $\varphi_1$-valuation of $I$ is equal to the valuation of the conductor of $\mathbb{Z}[\pi, \pi]$.

$(\ell, \ell)$-isogenies preserving $O_0$ are a composition of a $\varphi_1$-isogeny with a $\varphi_2$-isogeny.
Changing the real multiplication

Cyclic isogenies (that preserve principal polarisations) preserve real multiplication; so we need to look at \((\ell, \ell)\)-isogenies.

**Example**

- Let \(O_{\ell}\) be the order of conductor \(\ell\) inside \(O_{K_0}\). \((\ell, \ell)\)-isogenies going from \(O_{\ell}\) to \(O_{K_0}\) are of the form

\[
\mathbb{C}^g/(O_{\ell} \oplus O_{\ell}\tau) \rightarrow \mathbb{C}^g/(O_{K_0} \oplus O_{K_0}\tau).
\]

- Indeed we have an action of

\[
\text{Sl}_2(O_{K_0})/\text{Sl}_2(O_{\ell}) \cong \text{Sl}_2(O_{K_0}/\ell O_{K_0})/\text{Sl}_2(O_{\ell}/\ell O_{\ell}) \cong \text{SL}_2(\mathbb{F}_{\ell}^2)/\text{Sl}_2(\mathbb{F}_{\ell}) \cong \text{Sl}_2(\mathbb{F}_{\ell})
\]

on such isogenies, so we find \(\ell^3 - \ell\) \((\ell, \ell)\)-isogenies changing the real multiplication. On the other end there is \((\ell + 1)^2\) \((\ell, \ell)\)-isogenies preserving the real multiplication and in total we find all \(\ell^3 + \ell^2 + \ell + 1\) \((\ell, \ell)\)-isogenies.
In Mumford coordinate (using the canonical divisor as base point), the restriction of an isogeny $f : \text{Jac}(C_1) \to \text{Jac}(C_2)$ to $C_1$ is of the form $(u,v) \mapsto (X^2 + XR_1(u) + R_0(u), XvR_2(u) + vR_3(u))$, where the $R_i$ are rational functions;

$\text{Jac}(C_2)$ is birationally equivalent to the symmetric product $C_2 \times C_2$. A basis of section of $\Omega^1_{C_1}$ is given by $(du/v, udu/v)$ and a basis of $\Omega^2_{C_2}$ is given by $(dx_1/y_1 + dx_2/y_2, x_1dx_1/y_1 + x_2dx_2/y_2)$. The pullback $f^* : \Gamma(\Omega^1_{C_2}) \to \Gamma(\Omega^1_{C_1})$ is given by a matrix $\begin{pmatrix} m_{1,1} & m_{1,2} \\ m_{2,1} & m_{2,2} \end{pmatrix}$;

If $f(u,v) = Q_1 + Q_2 - K_{C_2}$, then one can recover the rational functions $R_i$ by solving the differential equations (in the formal completion)

$$
\frac{\dot{x}_1}{y_1} + \frac{\dot{x}_2}{y_2} = \frac{(m_{1,1} + m_{2,1}u)\dot{u}}{v}
$$

$$
\frac{x_1\dot{x}_1}{y_1} + \frac{x_2\dot{x}_2}{y_2} = \frac{(m_{1,2} + m_{2,2}u)\dot{u}}{v}
$$

where $Q_i = (x_i, y_i)$ and $m_{i,j}$.
Modular polynomials in dimension 2

- Modular polynomials for \((\ell, \ell)\)-isogenies can be computed via an evaluation-interpolation approach using the action of \(\Gamma/\Gamma_0(\ell)\) where \(\Gamma = \text{Sp}_{2g}(\mathbb{Z})\);

- A quasi-linear algorithm exists [Mil14] which uses a generalized version of the AGM to compute theta functions in quasi-linear time in the precision. They are very big: once the invariant of the abelian variety are plugged in, we have a polynomial of total degree \(\ell^3 + \ell^2 + \ell + 1\);

- If we fix the real multiplication \(O_{K_0}\), one can also define modular polynomial for cyclic isogenies by working on symmetric invariants for the Hilbert surface \(\mathcal{H}^1\);

- We use an evaluation-interpolation approach via the action of \(\text{Sl}_2(O_{K_0})/\Gamma_0(\varphi_i)\) (by symmetry, to get a rational polynomial we need to take the product of the polynomial computed via the action of \(\varphi_1\) and the one obtained via the action of \(\varphi_2\));

- They are much smaller (the total degree is \(2(\ell + 1)\) once the invariants are plugged in), but for now we need a precomputation for each \(K_0\).
AVIsogenies [Bisson, Cosset, R.]

- AVIsogenies: Magma code written by Bisson, Cosset and R.
  http://avisogenies.gforge.inria.fr
- Released under LGPL 2+.
- Implement isogeny computation (and applications thereof) for abelian varieties using theta functions.
- Current release 0.6.
- Cyclic isogenies coming “soon”!
Bibliography


A. Enge and A. Sutherland. “Class invariants by the CRT method, ANTS IX: Proceedings of the Algorithmic Number Theory 9th International Symposium”. In: Lecture Notes in Computer Science 6197 (July 2010), pp. 142–156 (cit. on p. 6).


