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

Complex elliptic curve

- Over $\mathbb{C}$: an elliptic curve is a torus $E = \mathbb{C}/\Lambda$, where Λ is a lattice $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$ ($\tau \in \mathfrak{H}_1$).
- Let $\wp(z,\Lambda) = \sum_{w\in\Lambda\setminus\{0_E\}}\left(\frac{1}{(z-w)^2} - \frac{1}{w^2}\right)$ be the Weierstrass $\wp$-function and $E_{2k}(\Lambda) = \lambda_k \sum_{w\in\Lambda\setminus\{0_E\}} \frac{1}{w^{2k}}$ 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 $f : E_1 \to E_2$ 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].

Constructive cryptographic applications

- One can recover informations on the elliptic curve E modulo ℓ by working over the ℓ-torsion.
- But by computing isogenies, one can work over a cyclic subgroup of cardinal ℓ instead.
- Since thus a subgroup is of degree ℓ, whereas the full ℓ-torsion is of degree ℓ^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 $f\colon E_1 \to E_2$ 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 $\operatorname{char} k > 3$ 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 $w_E = dx/2y$ be the canonical differential. Then $f^* w_{E'} = c w_E$, 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

$$X(P) = x(P) + \sum_{Q \in G \setminus \{0_E\}} \left(x(P+Q) - x(Q)\right)$$

$$Y(P) = y(P) + \sum_{Q \in G \setminus \{0_E\}} \left(y(P+Q) - y(Q)\right).$$

  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

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

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

where σ 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.

Modular polynomials

Here $k = \overline{k}$.

Definition (Modular polynomial)

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

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

Finding an isogeny between two isogenous elliptic curves

- Let E_1 and E_2 be ℓ-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 $A = -\frac{1}{48}\frac{J^2}{j_{E_2}(j_{E_2}-1728)}$, $B = -\frac{1}{864}\frac{J^3}{j_{E_2}^2(j_{E_2}-1728)}$ and $J = -\frac{18}{\ell}\frac{b}{a}\frac{{\varphi'}_\ell^{(X)}(j_{E_1}, j_{E_2})}{{\varphi'}_\ell^{(Y)}(j_{E_1}, j_{E_2})} j_{E_1}$.

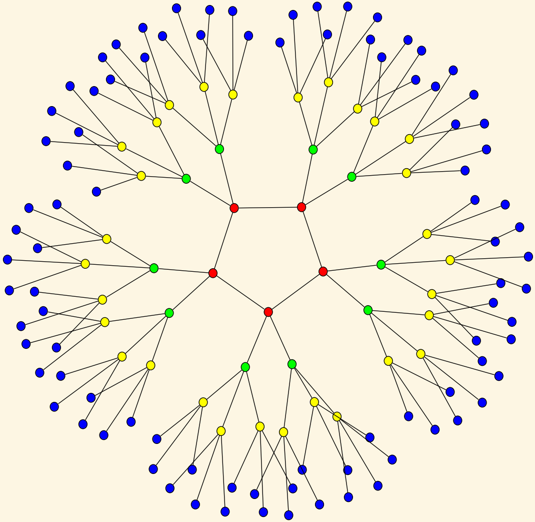
Remark

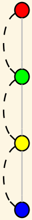
$E_2(\tau)$ is the differential logarithm of the discriminant. Similar methods allow to recover $E_2(\ell\tau)$, and from it $\sigma = \sum_{P \in K \setminus \{0_E\}} x(K)$.

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 ($\widetilde{O}(\ell)$).
- Knowing σ 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/Λ with

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

such that there exists an Hermitian form H on V with $E(\Lambda,\Lambda) \subset \mathbb{Z}$ where $E = \operatorname{Im} H$ 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 $E = \operatorname{Im} H$.
- Over a symplectic basis of Λ, E is of the form.

$$\begin{pmatrix} 0 & D_\delta \\ -D_\delta & 0 \end{pmatrix}$$

  where D_δ is a diagonal positive integer matrix $\delta = (\delta_1, \delta_2, \ldots, \delta_g)$, with $\delta_1 \mid \delta_2 | \cdots \mid \delta_g$.
- 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 $E_0((x_1,x_2),(y_1,y_2)) = {}^t x_1 \cdot y_2 - {}^t y_1 \cdot x_2$;
- 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 Ω;
- In particular $E(\Omega x_1 + x_2, \Omega y_1 + y_2) = {}^t x_1 \cdot y_2 - {}^t y_1 \cdot x_2$;
- The matrix Ω is in $\mathfrak{H}_g$, the Siegel space of symmetric matrices Ω with $\operatorname{Im}\Omega$ positive definite;
- In this basis, $\Lambda = \Omega\mathbb{Z}^g + \mathbb{Z}^g$ and H is given by the matrix $(\operatorname{Im}\Omega)^{-1}$.

Isogenies

Let $A = V/\Lambda$ and $B = V'/\Lambda'$.

Definition

An isogeny $f : A \to B$ is a bijective linear map $f : V \to V'$ 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 $f : A \to B$ (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 $\widehat{A} = \mathrm{Hom}_{\overline{\mathbb{C}}}(V, \mathbb{C})/\Lambda^*$. Here $\mathrm{Hom}_{\overline{\mathbb{C}}}(V, \mathbb{C})$ is the space of anti-linear forms and $\Lambda^* = \{f \mid f(\Lambda) \subset \mathbb{Z}\}$ is the orthogonal of Λ.

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

$$x \mapsto H(x, \cdot)$$

  of degree $\deg H$. We note $K(H)$ its kernel.
- If $f : A \to B$ is an isogeny, then its dual is an isogeny $\widehat{f} : \widehat{B} \to \widehat{A}$ of the same degree.

Remark

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

$$(x, f) \mapsto f(x).$$

Isogenies and polarisations

Definition

- 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 ℓ-isogeny between principally polarised abelian varieties if H_1 and H_2 are principal and $f^*H_2 = \ell H_1$.

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

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\Phi_{H_1}"] & B \arrow[d, "\Phi_{H_2}"] \\ \widehat{A} & \widehat{B} \arrow[l, "\widehat{f}"] \end{tikzcd}$$

Isogenies and polarisations

Definition

- An isogeny $f\colon (A,H_1) \to (B,H_2)$ 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 ℓ-isogeny between principally polarised abelian varieties if H_1 and H_2 are principal and $f^*H_2 = \ell H_1$.

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

$$\begin{tikzcd}
& A \arrow[r, "f"] \arrow[dl, "{[\ell]}"'] \arrow[d, "\Phi_{\ell H_1}"] & B \arrow[d, "\Phi_{H_2}"] \\
A \arrow[r, "\Phi_{H_1}"'] & \widehat{A} & \widehat{B} \arrow[l, "\widehat{f}"]
\end{tikzcd}$$

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 Λ;
- 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)

$\operatorname{Jac} C$ 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 $\operatorname{Jac} C \simeq \operatorname{Jac} H$ as non polarised abelian varieties!

Theta functions

- Let (A, H_0) be a principally polarised abelian variety over $\mathbb{C}$: $A = \mathbb{C}^g / (\Omega\mathbb{Z}^g + \mathbb{Z}^g)$ with $\Omega \in \mathfrak{H}_g$.
- Theta functions with characteristics $a, b \in \mathbb{Q}^g$:

$$\vartheta \begin{bmatrix} a \\ b \end{bmatrix} (z, \Omega) = \sum_{n \in \mathbb{Z}^g} e^{\pi i \, {}^t(n+a)\Omega(n+a) + 2\pi i \, {}^t(n+a)(z+b)} \qquad a, b \in \mathbb{Q}^g$$

- Define $\vartheta_i = \vartheta \left[\begin{smallmatrix} 0 \\ \frac{i}{n} \end{smallmatrix} \right] (., \frac{\Omega}{n})$ for $i \in Z(\overline{n}) = \mathbb{Z}^g / n\mathbb{Z}^g$
- $(\vartheta_i)_{i \in Z(\overline{n})} = \begin{cases} \text{coordinates system} & n \geqslant 3 \\ \text{coordinates on the Kummer variety } A/\pm 1 & n = 2 \end{cases}$

The isogeny theorem

Theorem

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

$$(\vartheta_i^B(x))_{i \in Z(\overline{n})} = (\vartheta_{\varphi(i)}^A(x))_{i \in Z(\overline{n})}$$

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.

Changing level

Theorem (Koizumi–Kempf)

Let F be a matrix of rank r such that ${}^tFF = \ell \operatorname{Id}_r$. 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

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

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

- If $\ell = a^2 + b^2$, we take $F = \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$, 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

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

$$\vartheta_b^B := \vartheta\left[\begin{smallmatrix} 0 \\ \frac{b}{n} \end{smallmatrix}\right]\left(\cdot, \frac{\Omega}{n}\right), \quad \vartheta_b^A := \vartheta\left[\begin{smallmatrix} 0 \\ \frac{b}{n} \end{smallmatrix}\right]\left(\cdot, \frac{\ell\Omega}{n}\right)$$

Proposition

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

$$\vartheta_{i_1}^A(\ell z)\dots\vartheta_{i_r}^A(0) = \sum_{\substack{t_1,\dots,t_r \in \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g \\ F(t_1,\dots,t_r)=(0,\dots,0)}} \vartheta_{j_1}^B(X_1 + t_1)\dots\vartheta_{j_r}^B(X_r + t_r),$$

Corollary

$$\vartheta_k^A(0)\vartheta_0^A(0)\dots\vartheta_0^A(0) = \sum_{\substack{t_1,\dots,t_r \in K \\ (t_1,\dots,t_r)F=(0,\dots,0)}} \vartheta_{j_1}^B(t_1)\dots\vartheta_{j_r}^B(t_r), \quad (j = (k, 0, \dots, 0)F^{-1} \in Z(\overline{n}))$$

The Algorithm [Cosset, R.]

$$\begin{tikzcd}
 & x \in (A, \ell H_1) \arrow[r, dashed] \arrow[dl, "f"'] \arrow[dd, "{[\ell]}"] & (x, 0, \dots, 0) \in (A^r, \ell H_1 \star \cdots \star \ell H_1) \arrow[d, "{}^t F"] \\
y \in (B, H_2) \arrow[dr, "\widetilde{f}"'] & & {}^t F(x, 0, \dots, 0) \in (A^r, \ell H_1 \star \cdots \star \ell H_1) \arrow[d, "F"] \\
 & \widetilde{f}(y) \in (A, H_1) & F \circ {}^t F(x, 0, \dots, 0) \in (A^r, H_1 \star \cdots \star H_1) \arrow[l, dashed]
\end{tikzcd}$$

Theorem ([Lubicz, R.])

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 $\widetilde{O}(\ell^g)$ or $\widetilde{O}(\ell^{2g})$ operations in $\mathbb{F}_q$ according to whether $\ell \cong 1$ 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:

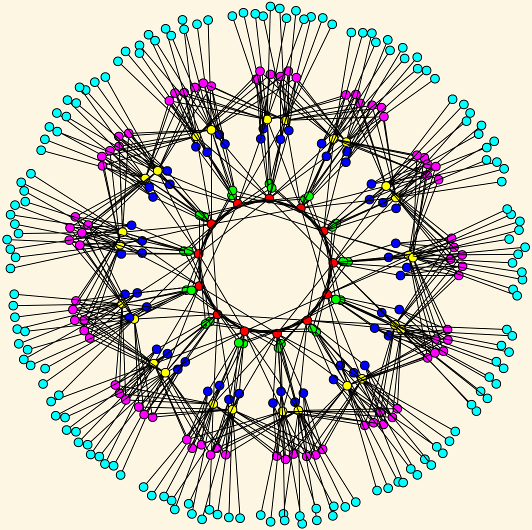
$$P_1(X_0, X_1) = 0$$

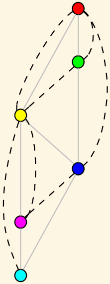
$$\dots$$

$$X_n X_0^d = P_n(X_0, X_1)$$

- By setting $X_0 = 1$ we can work with affine coordinates. The projective solutions can be written $(x_0, x_0 x_1, \dots, x_0 x_n)$ so X_0 can be seen as the normalization factor.
- We work in the algebra $\mathfrak{A} = k[X_1]/(P_1(X_1))$; each operation takes $\widetilde{O}(\ell^g)$ 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 η, compute $c.\eta$ and then $R := \vartheta_{j_1}^A(\eta)\vartheta_{j_2}^A(c.\eta) \in \mathfrak{A}$.
- 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 (ℓ,ℓ)-isogeny graph in dimension 2 [Bisson, Cosset, R.]





Non principal polarisations

- Let $f:(A,H_1)\rightarrow(B,H_2)$ be an isogeny between principally polarised abelian varieties;
- When $\mathrm{Ker} f$ is not maximal isotropic in $A[\ell]$ then f^*H_2 is not of the form ℓH_1;
- How can we go from the principal polarisation H_1 to f^*H_1?

Non principal polarisations

Theorem (Birkenhake-Lange, Th. 5.2.4)

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

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

Then

- *$\mathrm{NS}(A)$ is a torsor under the action of O_0;*
- *This induces a bijection between polarisations of degree d in $\mathrm{NS}(A)$ and totally positive symmetric endomorphisms of norm d in O_0;*
- *The isomorphic class of a polarisation $\mathscr{L}_f \in \mathrm{NS}(A)$ 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 ℓ;
- There exists φ such that the following diagram commutes:

$$
\begin{tikzcd}
 & A \arrow[r, "f"] \arrow[dl, "\varphi"'] \arrow[d, "\Phi_{f^*H_2}"] & B \arrow[d, "\Phi_{H_2}"] \\
A \arrow[r, "\Phi_{H_1}"'] & \widehat{A} & \widehat{B} \arrow[l, "\widehat{f}"]
\end{tikzcd}
$$

- φ is an $(\ell,0,\dots,\ell,0,\dots)$-isogeny whose kernel is not isotropic for the H_1-Weil pairing on $A[\ell]$!
- φ commutes with the Rosatti involution so is a real endomorphism (φ is H_1-symmetric). Since H_1 is Hermitian, φ is totally positive.
- $\operatorname{Ker} f$ is maximal isotropic for φH_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 φ

- The isogeny f induces a compatible isogeny between $\varphi H_1 = f^* H_2$ and H_2 where φH_1 is given by the following diagram

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[dr, "\Phi_{\varphi H_1}"'] & A \arrow[d, "\Phi_{H_1}"] \\ & \widehat{A} \end{tikzcd}$$

- φ plays the same role as $[\ell]$ for ℓ-isogenies;
- We then define the φ-contragredient isogeny $\widetilde{f}$ as the isogeny making the following diagram commute

$$\begin{tikzcd} & x \in (A, \varphi^* H_1) \arrow[dl, "f"'] \arrow[d, "\varphi"] \\ y \in (B, \varphi H_2) \arrow[r, "\widetilde{f}"] & \widetilde{f}(y) \in (A, H_1) \end{tikzcd}$$

φ-change of level

- 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)?
- φH_1 fits in the following diagram:

$$\begin{tikzcd}
A \arrow[r, "\varphi"] \arrow[d, "\Phi_{\varphi^* H_1}"'] \arrow[dr, "\Phi_{\varphi H_1}"] & A \arrow[d, "\Phi_{H_1}"] \\
\widehat{A} & \widehat{A} \arrow[l, "\hat{\varphi}"]
\end{tikzcd}$$

- Applying the isogeny theorem on φ allows to find relations between $\varphi^* H_1$ and H_1 but we want φH_1.

φ-change of level

- φ is a totally positive element of a totally positive order O_0;
- A theorem of Siegel show that φ is a sum of m squares in $K_0 = O_0 \otimes \mathbb{Q}$;
- Clifford's algebras give a matrix $F \in \mathrm{Mat}_r(K_0)$ such that $\mathrm{diag}(\varphi) = F^* F$;
- 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)

$$\vartheta\left[\begin{smallmatrix}0\\ i_1\end{smallmatrix}\right](Y_1, \frac{\Omega}{n}) \ldots \vartheta\left[\begin{smallmatrix}0\\ i_r\end{smallmatrix}\right](Y_r, \frac{\Omega}{n}) = \sum_{\substack{t_1,\ldots,t_r \in K(\varphi H_1) \\ F(t_1,\ldots,t_r)=(0,\ldots,0)}} \vartheta\left[\begin{smallmatrix}0\\ j_1\end{smallmatrix}\right](X_1 + t_1, \frac{\varphi^{-1}\Omega}{n}) \ldots \vartheta\left[\begin{smallmatrix}0\\ j_r\end{smallmatrix}\right](X_r + t_r, \frac{\varphi^{-1}\Omega}{n}),$$

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.]

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

Theorem

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

$$\vartheta_{i_1}^A(Y_1)\ldots\vartheta_{i_r}^A(Y_r) = \sum_{\substack{t_1,\ldots,t_r \in K(\varphi H_2) \\ (t_1,\ldots,t_r)F = (0,\ldots,0)}} \vartheta_{j_1}^B(X_1+t_1)\ldots\vartheta_{j_r}^B(X_r+t_r),$$

$$\begin{tikzcd}
 & x \in (A, \varphi H_1) \arrow[dl, "f"'] \arrow[dd, "\varphi"] \arrow[r, dashed] & (x,0,\ldots,0) \in (A^r, \varphi H_1 \star \cdots \star \varphi H_1) \arrow[d, "{}^tF"] \\
y \in (B, H_2) \arrow[dr, "\widetilde{f}"'] & & {}^tF(x,0,\ldots,0) \in (A^r, \varphi H_1 \star \cdots \star \varphi H_1) \arrow[d, "F"] \\
 & \widetilde{f}(y) \in (A, H_1) & F \circ {}^tF(x,0,\ldots,0) \in (A^r, H_1 \star \cdots \star H_1) \arrow[l, dashed]
\end{tikzcd}$$

Hidden details

- 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 Λ_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

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

  for a totally positive element $\lambda \in K_0^{++}$. In other words if $x_i, y_i \in K_0$, then $E(x_1 + y_1\tau, x_2 + y_2\tau) = \mathrm{Tr}_{K_0/\mathbb{Q}}(\lambda(x_2 y_1 - x_1 y_2))$.
- An abelian variety with CM by K is of the form $\mathbb{C}^g/\Phi(\Lambda)$ where Λ is a lattice in K and Φ is a CM-type.
- Furthermore, the polarisations are of the form

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

  for a totally imaginary element $\xi \in K$. The polarisation is principal iff $\xi \overline{\Lambda} = \Lambda^\star$ where $\Lambda^\star$ is the dual of Λ for the trace.

Cyclic isogenies in dimension 2 [IT14]

- 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 ℓ correspond to kernels inside $A[\varphi]$ for an endomorphism $\varphi \in O_0^{++}$ of degree ℓ. 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 φ_i is totally positive). Then $A[\ell] = A[\varphi_1] \oplus A[\varphi_2]$. We have two kind of cyclic isogenies: the φ_1-isogenies and the φ_2-isogenies.
- When we look only at φ_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 φ_1, we have 2, 1, or 0 horizontal-isogenies according to whether φ_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 φ_1 we have one ascending isogeny (to $O_0 + I/\varphi_1 O_K$) and ℓ descending ones;
  - We are at the bottom when the φ_1-valuation of I is equal to the valuation of the conductor of $\mathbb{Z}[\pi, \overline{\pi}]$.
- (ℓ, ℓ)-isogenies preserving O_0 are a composition of a φ_1-isogeny with a φ_2-isogeny.

Changing the real multiplication

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

Example

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

$$\mathbb{C}^g/(O_\ell \oplus O_\ell \tau) \to \mathbb{C}^g/(O_{K_0} \oplus O_{K_0}\tau).$$

- Indeed we have an action of $\mathrm{Sl}_2(O_{K_0})/\mathrm{Sl}_2(O_\ell) \simeq \mathrm{Sl}_2(O_{K_0}/\ell O_{K_0})/\mathrm{Sl}_2(O_\ell/\ell O_\ell) \simeq \mathrm{SL}_2(\mathbb{F}_l^2)/\mathrm{Sl}_2(\mathbb{F}_l) \simeq \mathrm{Sl}_2(\mathbb{F}_l)$ on such isogenies, so we find $\ell^3-\ell$ (ℓ,ℓ)-isogenies changing the real multiplication. On the other end there is $(\ell+1)^2$ (ℓ,ℓ)-isogenies preserving the real multiplication and in total we find all $\ell^3+\ell^2+\ell+1$ (ℓ,ℓ)-isogenies.

Isogenies between Jacobians of hyperelliptic curves of genus 2 [CE14]

- In Mumford coordinate (using the canonical divisor as base point), the restriction of an isogeny $f:\mathrm{Jac}(C_1)\to\mathrm{Jac}(C_2)$ 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;
- $\mathrm{Jac}(C_2)$ 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 $\Omega^2_{J_{C_2}}$ is given by $(dx_1/y_1+dx_2/y_2, x_1dx_1/y_1+x_2dx_2/y_2)$. The pullback $f^*:\Gamma(\Omega^1_{J_{C_2}})\to\Gamma(\Omega^1_{C_1})$ is given by a matrix $\left(\begin{smallmatrix} m_{1,1} & m_{1,2}\\ m_{2,1} & m_{2,2}\end{smallmatrix}\right)$;
- 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)

$$\frac{\dot{x}_1}{y_1}+\frac{\dot{x}_2}{y_2}=\frac{(m_{1,1}+m_{2,1}u)\dot{u}}{v}$$
$$\frac{x_1\dot{x}_1}{y_1}+\frac{x_2\dot{x}_2}{y_2}=\frac{(m_{1,2}+m_{2,2}u)\dot{u}}{v}$$
$$(x_1,y_1)\in C_2, (x_2,y_2)\in C_2$$

where $Q_i=(x_i,y_i)$ and $m_{i,j}$.

Modular polynomials in dimension 2

- Modular polynomials for (ℓ,ℓ)-isogenies can be computed via an evaluation-interpolation approach using the action of $\Gamma/\Gamma_0(\ell)$ where $\Gamma = \mathrm{Sp}_{2g}(\mathbb{Z})$;
- 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 $\mathfrak{H}^1$;
- We use an evaluation-interpolation approach via the action of $\mathrm{Sl}_2(O_{K_0})/\Gamma_0(\varphi_i)$ (by symmetry, to get a rational polynomial we need to take the product of the polynomial computed via the action of φ_1 and the one obtained via the action of φ_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

R. Bröker, K. Lauter, and A. Sutherland. "Modular polynomials via isogeny volcanoes". In: *Mathematics of Computation* 81.278 (2012), pp. 1201–1231. arXiv: 1001.0402 (cit. on p. 6).

D. Charles, K. Lauter, and E. Goren. "Cryptographic hash functions from expander graphs". In: *Journal of Cryptology* 22.1 (2009), pp. 93–113. ISSN: 0933-2790 (cit. on p. 7).

J.-M. Couveignes and T. Ezome. "Computing functions on Jacobians and their quotients". In: *arXiv preprint arXiv:1409.0481* (2014) (cit. on p. 40).

J. Couveignes and R. Lercier. "Galois invariant smoothness basis". In: *Algebraic geometry and its applications* (2008) (cit. on p. 7).

J. Couveignes and R. Lercier. "Elliptic periods for finite fields". In: *Finite fields and their applications* 15.1 (2009), pp. 1–22 (cit. on p. 7).

C. Doche, T. Icart, and D. Kohel. "Efficient scalar multiplication by isogeny decompositions". In: *Public Key Cryptography-PKC 2006* (2006), pp. 191–206 (cit. on p. 7).

N. Elkies. "Elliptic and modular curves over finite fields and related computational issues". In: *Computational perspectives on number theory: proceedings of a conference in honor of AOL Atkin, September 1995, University of Illinois at Chicago*. Vol. 7. Amer Mathematical Society. 1997, p. 21 (cit. on p. 6).

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).

S. Galbraith, F. Hess, and N. Smart. "Extending the GHS Weil descent attack". In: *Advances in Cryptology—EUROCRYPT 2002*. Springer. 2002, pp. 29–44 (cit. on p. 5).

P. Gaudry. “Fast genus 2 arithmetic based on Theta functions”. In: *Journal of Mathematical Cryptology* 1.3 (2007), pp. 243–265 (cit. on p. 7).

S. Ionica and E. Thomé. “Isogeny graphs with maximal real multiplication.” In: *IACR Cryptology ePrint Archive* 2014 (2014), p. 230 (cit. on p. 38).

E. Milio. “A quasi-linear algorithm for computing modular polynomials in dimension 2”. In: *arXiv preprint arXiv:1411.0409* (2014) (cit. on p. 41).

F. Morain. “Calcul du nombre de points sur une courbe elliptique dans un corps fini: aspects algorithmiques”. In: *J. Théor. Nombres Bordeaux* 7 (1995), pp. 255–282 (cit. on p. 6).

A. Rostovtsev and A. Stolbunov. “Public-key cryptosystem based on isogenies”. In: *International Association for Cryptologic Research. Cryptology ePrint Archive* (2006). eprint: http://eprint.iacr.org/2006/145 (cit. on p. 7).

R. Schoof. “Counting points on elliptic curves over finite fields”. In: *J. Théor. Nombres Bordeaux* 7.1 (1995), pp. 219–254 (cit. on p. 6).

N. Smart. “An analysis of Goubin’s refined power analysis attack”. In: *Cryptographic Hardware and Embedded Systems-CHES 2003* (2003), pp. 281–290 (cit. on p. 7).

B. Smith. *Isogenies and the Discrete Logarithm Problem in Jacobians of Genus 3 Hyperelliptic Curves.* Feb. 2009. arXiv: 0806.2995 (cit. on p. 5).

A. Sutherland. “Computing Hilbert class polynomials with the Chinese remainder theorem”. In: *Mathematics of Computation* 80.273 (2011), pp. 501–538 (cit. on p. 6).

E. Teske. “An elliptic curve trapdoor system”. In: *Journal of cryptology* 19.1 (2006), pp. 115–133 (cit. on p. 7).