Isogenies between abelian varieties

DAMIEN ROBERT

Notes of a talk given for the Conference "Effective moduli spaces and applications to cryptography" — Rennes

Abstract. In this talk we give a brief panorama of the effective computation of isogenies between principally polarized abelian varieties and of modular equations.

Given a principally polarized abelian variety A, we want to compute the following:

- Given a kernel K, compute the isogeny $A \to B = A/K$;
- Given a degree ℓ, compute all isogenous abelian varieties B (where the isogeny is of degree ℓ^g);
- Given two abelian varieties A and B, test if they are isogenous (of a given degree). If so find the kernel K of the isogeny $A \to B$.

Note: We will restrict to perfect fields, separable isogenies and principally polarised abelian varieties. In particular we will deal with isotropic kernels.

Theorem 0.1. *Suppose that A/k, B/k are absolutely simple over a perfect field k. Suppose that $\mathrm{Hom}_k(A,B) \neq \{0\}$, $\mathrm{End}_k(A) = \mathrm{End}_{\overline{k}}(A)$. Then $\mathrm{Hom}_k(A,B) = \mathrm{Hom}_{\overline{k}}(A,B)$.*

1. Elliptic curves

1.1. Isogenies from the kernel.

Theorem 1.1 ([Vél71])**.** *Let $E : y^2 = f_1(x)$ be an elliptic curve and $K \subset E(k)$ a finite subgroup. Then E/K is given by $Y^2 = f_2(X)$ where*

$$X(P) = x(P) + \sum_{Q \in K \backslash \{0_E\}} (x(P+Q) - x(Q))$$
$$Y(P) = y(P) + \sum_{Q \in K \backslash \{0_E\}} (y(P+Q) - y(Q)).$$

If $f_1(x) = x^3 + ax + b$ then $f_2(x) = x^3 + (a - 5t)x + b - 7w$ where

$$t = \sum_{Q \in K \backslash \{0_E\}} f'(Q), \quad u = 2 \sum_{Q \in K \backslash \{0_E\}} f(Q), \quad w = \sum_{Q \in K \backslash \{0_E\}} x(Q) f'(Q).$$

Proof. Uses the fact that x and y are characterised in $k(E)$ by

$$\begin{aligned} v_{0_E}(x) &= -2 \qquad v_P(x) \geq 0 \quad \text{if } P \neq 0_E \\ v_{0_E}(y) &= -3 \qquad v_P(y) \geq 0 \quad \text{if } P \neq 0_E \\ y^2/x^3(0_E) &= 1 \end{aligned}$$

□

Theorem 1.2 ([Koh96])**.** *Let $h(x) = \prod_{Q \in K \backslash \{0_E\}} (x - x(Q))$ defining the subgroup K of the elliptic curve $E_1 : y^2 = f_1(x)$; then the isogeny $f : E_1 \to E_2$ is defined by*

$$f(x,y) = \left(\frac{g(x)}{h(x)}, y \left(\frac{g(x)}{h(x)} \right)' \right), \text{ with } \frac{g(x)}{h(x)} = \#K.x - \sigma - f'(x) \frac{h'(x)}{h(x)} - 2f(x) \left(\frac{h'(x)}{h(x)} \right)',$$

Date: June 10, 2014.

where σ is the first power sum of h (the sum of the x-coordinates of the points in the kernel). When $\#K$ is odd, $h(x)$ is a square, so we can replace it by its square root. The complexity of computing the isogeny is then $O(M(\#K))$ operations in k.

Proof. Let $w_{E_1} = dx/2y$ be the canonical differential. Then $f^* w_{E_2} = c w_{E_2}$, with c in k. Up to a normalisation we can assume that $c = 1$, so $f(x,y) = \left(\frac{g(x)}{h(x)}, y\left(\frac{g(x)}{h(x)}\right)'\right)$. Plugging the formulas from theorem 1.1 yields the result. □

To compute all rational isogenous elliptic curves starting from E_1 with an isogeny of degree ℓ, we can compute all rational cyclic subgroups of $E[\ell]$ and apply Vélu's formulas. These subgroups can be obtained as factors of the ℓ-division polynomial $\prod_{Q \in E[\ell]\setminus\{0_E\}}(x - x(Q))$. This division polynomial has degree $(\ell^2-1)/2$ (if ℓ odd), and factorizing it will cost $O(\ell^{3.63})$ (over a finite field).

1.2. **Modular polynomials.**

Definition 1.3. Modular polynomials The modular polynomial $\varphi_\ell(x_1, x_2) \in \mathbb{Z}[x_1, x_2]$ is a bivariate polynomial such that $\varphi_\ell(x_1, x_2) = 0 \Leftrightarrow x = j(E_1)$ and $y = j(E_2)$ with E_1 and E_2 ℓ-isogenous.

One can also see the modular polynomial as the polynomial describing the modular curve $X_0(\ell)$ inside $X(1) \times X(1) \simeq \mathbb{P}^2$ [Koh03].

Proposition 1.4. *φ_ℓ is a symmetric polynomial of degree $\ell+1$. The height of the coefficients of φ_ℓ grows as $O(\ell \log \ell)$.*

The roots of $\varphi_\ell(j(E_1), .)$ are exactly the elliptic curves ℓ-isogenous to E_1. There are $\ell + 1 = \#\mathbb{P}^1(\mathbb{F}_\ell)$ such roots if ℓ is prime.

Theorem 1.5 (Rational roots of modular polynomials)**.** *Let $E_1/\mathbb{F}_q$ be an ordinary elliptic curve, ℓ be a prime and j_2 be a root of $\varphi_\ell(j_{E_1}, \cdot)$ over $\mathbb{F}_{q^n}$. Then there exists a twist E_1' of E_1 and an elliptic curve E_2 with j-invariant j_2 such that there is an $\mathbb{F}_{q^n}$-rational ℓ-isogeny $E_1' \to E_2$. Furthermore, if j_{E_1} is not equal to 0 or 1728 then we can take $E_1' = E_1$.*

Theorem 1.6. *There is an algorithm that computes φ_ℓ in a time quasi linear in its size $\widetilde{O}(\ell^3)$. Over a finite field, finding the isogenous elliptic curves (of degree ℓ) is then quasi-cubic.*

Proof.

- The complex analytic method [Eng09]: if we see $\tau \mapsto j(\tau)$ and $\tau \mapsto j(\tau/\ell)$ as a modular functions on $\mathfrak{H}$; then $\varphi_\ell(\cdot, j)$ is the minimal polynomial of $j(\cdot/\ell)$ in $\mathbb{C}(j)$. One can then recover the polynomial by computing the Fourrier coefficients of j and $j(\cdot/\ell)$ with high precision. For a quasi-linear algorithm use an evaluation interpolation approach rather than linear algebra on the Fourrier coefficients.

  This approach use the fact that
  $$\varphi_\ell(j(\tau), Y) = \prod_{g \in \Gamma/\Gamma_0(\ell} (Y - j(\ell g.\tau) = \sum c_i(\tau) Y^i \quad \text{(evaluation)}$$
  and then interpolate the coefficients $c_i(\tau)$ (which are invariant under the action of Γ) as polynomials in j (interpolation).
- The CRT method [BLS09]: use Vélu's formulas to compute $\varphi_\ell \mod p$ for small p and use the CRT to recover the full modular polynomial.

□

1.3. **Finding an isogeny between two isogenous elliptic curves.** Suppose that E_1 and E_2 are ℓ-isogenous elliptic curves, we want to compute $f : E_1 \to E_2$. The explicit forms of f is given by Vélu's formula, which give a normalized isogeny (meaning that $f^* w_{E_2} = w_{E_1}$). We first need to normalize E_2. Over $\mathbb{C}$, the equation of the normalized curve E_2 is given by the Eisenstein series $\mathcal{E}_4(\ell\tau)$ and $\mathcal{E}_6(\ell\tau)$. We have $j'(\ell\tau)/j(\ell\tau) = -\mathcal{E}_6(\tau)/\mathcal{E}_4(\tau)$. By differencing the modular polynomial, we recover the differential logarithms.

Proposition 1.7. *From $E : y^2 = x^3 + ax + b$, a normalized model of j_{E_2} is given by the Weierstrass equation*

$$y^2 = x^3 + Ax + B$$

where $A = -\frac{1}{48}\frac{J^2}{j_{E'}(j_{E'}-1728)}$, $B = -\frac{1}{864}\frac{J^3}{j_{E'}^2(j_{E'}-1728)}$ *and* $J = -\frac{18}{\ell}\frac{b}{a}\frac{{\varphi'}_\ell^{(X)}(j_E,j_{E'})}{{\varphi'}_\ell^{(Y)}(j_E,j_{E'})} j_E$.

Remark 1.8. $\mathcal{E}_2(\tau)$ is the differential logarithm of the discriminant. Similar methods allow to recover $\mathcal{E}_2(\ell\tau)$, and from it $\sigma = \sum_{P \in K \setminus \{0_E\}} x(K)$.

Finding the isogeny between the normalized models (I: Stark'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. Over $\mathbb{C}$ the coordinates of the elliptic curve are given by the elliptic functions: $x = \wp(z)$ and $y = \wp'(z)$. We have to find I such that $\wp_{E_2}(z) = I \circ \wp_{E_1}(z)$. Stark's idea is to develop $\wp_{E_2}$ as a continuous fraction in $\wp_{E_1}$, and approximate I as p_n/q_n. This algorithm is quasi-quadratic ($\widetilde{O}(\ell^2)$).
Finding the isogeny between the normalized models (II: Elkie's method [Elk92]). 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.)

Algorithm 1.9. To summarize, we have the following algorithm to find an isogeny from E_1 in large characteristic [BMS+08] in time $\widetilde{O}(\ell^3 + \ell \log^2 q)$:

(1) Compute φ_ℓ (cost $\widetilde{O}(\ell^3)$)
(2) Specialize on j_E to obtain $\varphi_\ell(X, j_E)$ (cost $\widetilde{O}(\ell^2 \log q)$)
(3) Find a root $j_{E'}$ of $\varphi_\ell(X, j_E)$ to obtain the j-invariant of a ℓ-isogenous curve E' (cost $\widetilde{O}(\ell \log^2 q)$).
(4) Compute the normalized model for E' (cost $\widetilde{O}(\ell^2 \log q)$).
(5) Solve the differential equation (cost $\widetilde{O}(\ell \log q)$).

2. Abelian varieties

2.1. **Theta functions.** Let $A/\mathbb{C} = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$ be a principally polarised abelian variety, with $\Omega \in \mathfrak{H}_g$. Recall the definition of the theta functions with characteristics $a, b \in \mathbb{Q}^g$:

$$\vartheta \left[\begin{smallmatrix} a \\ b \end{smallmatrix} \right] (z, \Omega) = \sum_{n \in \mathbb{Z}^g} e^{\pi i \, {}^t(n+a) \cdot \Omega \cdot (n+a) + 2\pi i \, {}^t(n+a) \cdot (z+b)}.$$

If $\mathcal{L} = \mathcal{L}_0^n$ is the polarisation of level n associated to the principal symmetric line bundle $\mathcal{L}_0$ coming from Ω, we let

$$\vartheta_i^{\mathcal{L}}(z) = \vartheta \left[\begin{smallmatrix} 0 \\ i/n \end{smallmatrix} \right] (z, \Omega/n),$$

for $i \in Z(\overline{n}) = (\mathbb{Z}/n\mathbb{Z})^g$. This form a basis of the sections of $\mathcal{L}$, that is of functions f on $\mathbb{C}^g$ that satisfy the following automorphic conditions:

$$f(z + m) = f(z),$$
$$f(z + \Omega m) = e^{-\pi i n \, {}^t m \cdot \Omega \cdot m - 2\pi i n \, {}^t z \cdot m} f(z).$$

Furthermore, this is the unique basis (up to multiplication by a constant) such that translation by a point of n-torsion is given by

$$\vartheta_b(z + \frac{m_1}{n} + \frac{\Omega m_2}{n}) = e^{-\pi i \, {}^t m_2 \cdot \frac{\Omega}{n} \cdot m_2 - 2\pi i \, {}^t m_2 \cdot z} e^{-2\pi i \, {}^t b \cdot m_2} \vartheta_{b+m_1}(z),$$

for $m_1, m_2 \in \mathbb{Z}^g$ (for more details on the canonical choice of a basis of sections, see [Mum83; Mum66]).

Proposition 2.1 (Lefschetz)**.**

- *If $n \geq 3$ we get an embedding of A into projective space;*
- *If $n = 2$ and $\mathcal{L}_0$ is indecomposable, we get an embedding of the Kummer variety $A/\pm 1$;*

- *$(A, \mathcal{L}, A[n])$ is entirely determined by the theta null point $(\vartheta_i(0))_{i \in Z(\overline{n})}$ when $2 \mid n$ and $n \geq 4$. (In fact the theta null point determines a symmetric theta structure of level n on A).*

We now suppose that $2 \mid n$, so $\mathcal{L}$ is totally symmetric.

Theorem 2.2 (Riemann relations)**.** *Let $x_1, y_1, u_1, v_1, z \in \mathbb{C}^g$, such that $2z = x_1 + y_1 + u_1 + v_1$ and let $x_2 = z - x_1$, $y_2 = z - y_1$, $u_2 = z - u_1$, $v_2 = z - v_1$. Then for all characters $\chi \in \hat{Z}(\overline{2})$ and all $i, j, k, l, m \in Z(\overline{n})$ such that $i + j + k + l = 2m$, if $i' = m - i$, $j' = m - j$, $k' = m - k$ and $l' = m - l$, then*

$$\big(\sum_{t \in Z(\overline{2})} \chi(t)\vartheta_{i+t}(x_1)\vartheta_{j+t}(y_1)\big).\big(\sum_{t \in Z(\overline{2})} \chi(t)\vartheta_{k+t}(u_1)\vartheta_{l+t}(v_1)\big) =$$
$$\big(\sum_{t \in Z(\overline{2})} \chi(t)\vartheta_{i'+t}(x_2)\vartheta_{j'+t}(y_2)\big).\big(\sum_{t \in Z(\overline{2})} \chi(t)\vartheta_{k'+t}(u_2)\vartheta_{l'+t}(v_2)\big).$$

In particular, we have the addition formulae for $z_1, z_2 \in \mathbb{C}^g$ (with χ, i, j, k, l like before):

$$\big(\sum_{t \in Z(\overline{2})} \chi(t)\vartheta_{i+t}(z_1 + z_2)\vartheta_{j+t}(z_1 - z_2)\big).\big(\sum_{t \in Z(\overline{2})} \chi(t)\vartheta_{k+t}(0)\vartheta_{l+t}(0)\big) =$$
$$\big(\sum_{t \in Z(\overline{2})} \chi(t)\vartheta_{-i'+t}(z_2)\vartheta_{j'+t}(z_2)\big).\big(\sum_{t \in Z(\overline{2})} \chi(t)\vartheta_{k'+t}(z_1)\vartheta_{l'+t}(z_1)\big).$$

Theorem 2.3 (Moduli space)**.**

- *If $n \geq 4$, then the homogeneous equations determining the locus of the embedding of A into projective spaces are generated by Riemann relations.*
- *If $n > 4$ then the moduli space $\mathcal{A}_{g,n}$ of abelian varieties with a level n symmetric theta structure form an open set inside the locus determined by Riemann relations on theta null points.*

Proof. [Mum66; Mum67a; Mum67b; Kem89]. □

2.2. Isogeny from the kernel.

Theorem 2.4 (Isogeny theorem)**.** *Let $f : A = \mathbb{C}^g/(\mathbb{Z}^g \oplus \Omega\mathbb{Z}^g) \to B = \mathbb{C}^g/(\mathbb{Z}^g \oplus \frac{1}{\ell}\Omega\mathbb{Z}^g) : z \mapsto z$ be the canonical isogeny with kernel $K = \frac{1}{\ell}\Omega\mathbb{Z}^g/\Omega\mathbb{Z}^g$. Then if we use the basis with level ℓn for A and the basis with level n for B, we get that*

$$f^*\left(\vartheta\left[\begin{smallmatrix}0\\ b/n\end{smallmatrix}\right](z, \frac{1}{n}(\frac{\Omega}{\ell}))\right) = \vartheta\left[\begin{smallmatrix}0\\ b\ell/n\ell\end{smallmatrix}\right](z, \frac{\Omega}{n\ell})$$

ie $f^*\vartheta_i^B = \vartheta_{\varphi(i)}^A$ where $\varphi : Z(\overline{n}) \to Z(\overline{\ell n})$ is the canonical injection.

Theorem 2.5 (Koizumi)**.** *Let $(\gamma_1, \dots, \gamma_r) \in \mathbb{Q}^r$, $(\delta_1, \dots, \delta_r) \in \mathbb{Q}^r$ and $F \in \mathrm{Gl}_r(\mathbb{Q})$ be such that*

$${}^tF \begin{pmatrix} \gamma_1 & & 0 \\ & \ddots & \\ 0 & & \gamma_r \end{pmatrix} F = \begin{pmatrix} \delta_1 & & 0 \\ & \ddots & \\ 0 & & \delta_r \end{pmatrix}.$$

Let $(x_1, \dots, x_r) \in (\mathbb{C}^g)^r$, and $(y_1, \dots, y_r) = (x_1, \dots, x_r)F$. Let $(a_1, \dots, a_r)$ and $(b_1, \dots, b_r)$ be elements of $(\mathbb{C}^g)^r$, and note

$$(a'_1, \dots, a'_r) = (a_1, \dots, a_r)\,{}^tF^{-1},$$
$$(b'_1, \dots, b'_r) = (b_1, \dots, b_r)F.$$

Let d be the index $[\mathrm{Mat}_{g\times r}(\mathbb{Z}) + \mathrm{Mat}_{g\times r}(\mathbb{Z})\,{}^tF : \mathrm{Mat}_{g\times r}(\mathbb{Z})]$ We have:

$$(1) \quad d\,\vartheta\left[\begin{smallmatrix}a_1\\ b_1\end{smallmatrix}\right](x_1, \gamma_1\Omega) \times \cdots \times \vartheta\left[\begin{smallmatrix}a_r\\ b_r\end{smallmatrix}\right](x_r, \gamma_r\Omega)$$
$$= \sum \vartheta\left[\begin{smallmatrix}a'_1+\alpha_1\\ b'_1+\beta_1\end{smallmatrix}\right](y_1, \delta_1\Omega) \times \cdots \times \vartheta\left[\begin{smallmatrix}a'_r+\alpha_r\\ b'_r+\beta_r\end{smallmatrix}\right](y_r, \delta_r\Omega)$$

where the sum is over the elements α and β such that

$$\begin{aligned} \alpha &\in \mathrm{Mat}_{g\times r}(\mathbb{Z})\,{}^tF^{-1}/\left(\mathrm{Mat}_{g\times r}(\mathbb{Z})\bigcap \mathrm{Mat}_{g\times r}(\mathbb{Z})\,{}^tF^{-1}\right), \\ \beta &\in \mathrm{Mat}_{g\times r}(\mathbb{Z})F/\left(\mathrm{Mat}_{g\times r}(\mathbb{Z})\bigcap \mathrm{Mat}_{g\times r}(\mathbb{Z})F\right). \end{aligned}$$

Proof. See [Koi76; Kem89; Mum83; Mum91]. □

Corollary 2.6 (Changing level)**.** *Let $\ell = a^2+b^2$, and let $F = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ so that ${}^tFF = \ell\,\mathrm{Id}$. The link between the theta coordinates of level n on A and the ones of level ℓn is given by*

$$\vartheta^{\mathcal{L}}_{i_1}(x_1)\vartheta^{\mathcal{L}}_{i_2}(x_2) = \sum_{t\in\frac{1}{\ell}\Omega\mathbb{Z}^g/\Omega\mathbb{Z}^g} \vartheta^{\mathcal{L}^\ell}_{j_1}(y_1+at)\vartheta^{\mathcal{L}^\ell}_{j_2}(y_2+bt).$$

where $(x_1,x_2) = F(y_1,y_2)$, $(i_1,i_2) = F(j_1,j_2)$.

Theorem 2.7 (Isogeny computation)**.** *Combining the isogeny theorem and the change of level, we can compute the contragredient isogeny $\widetilde{f} : (B,\mathcal{M}) \to (A,\mathcal{L})$ with kernel K while staying in level n. Let $z \in \mathbb{C}^g$, $Y = (\ell z, 0, \ldots, 0)$ and $X = YF^{-1}$ (so that $X_1, \ldots, X_r$ are integral multiples of z), let $k \in Z(\overline{n})$ and $j = (k, 0, \ldots, 0)F^{-1}$.*

$$\vartheta^A_k(\ell z)\vartheta^A_0(0)\ldots\vartheta^A_0(0) = \sum_{\substack{t_1,\ldots,t_r\in K \\ (t_1,\ldots,t_r)F=(0,\ldots,0)}} \vartheta^B_{j_1}(X_1+t_1)\ldots\vartheta^B_{j_r}(X_r+t_r).$$

Proof. See [CR13] which uses the following diagram:

$$\begin{tikzcd}
& x \in (A,\mathcal{L}^\ell) \arrow[dl, "f"] \arrow[dd, "{[\ell]}"] \arrow[rr, dashed] & & (x,0,\ldots,0) \in (A^r, \mathcal{L}^\ell\star\cdots\star\mathcal{L}^\ell) \arrow[d, "{}^tF"] \\
y \in (B,\mathcal{M}) \arrow[dr, "\widetilde{f}"] & & & {}^tF(x,0,\ldots,0) \in (A^r, \mathcal{L}^\ell\star\cdots\star\mathcal{L}^\ell) \arrow[d, "F"] \\
& \widetilde{f}(y) \in (A,\mathcal{L}) & & F\circ{}^tF(x,0,\ldots,0) \in (A^r, \mathcal{L}\star\cdots\star\mathcal{L}) \arrow[ll, dashed]
\end{tikzcd}$$

□

Complexity Analysis 2.8. *Let $r = 1$ if ℓ is a sum of two squares, $r = 2$ otherwise. Let k be the field of definition of the kernel K, and k' the field where the geometric points of K lives.*

- *From equations (in a suitable form) of K, one can compute the corresponding isogeny in time $O(\ell^{gr})$ in k [LR];*
- *From a basis of K, one can compute the corresponding isogeny in time $O(\ell^g)$ operations in k' and $O(\ell^{gr})$ operations in k.*

Proof. Let k' be the extension where the geometric points of K live.

- The isogeny formula assumes that the points are in affine coordinates. In practice, given A/k we only have projective coordinates ⇒ we use differential additions to normalize the coordinates;
- Computing the normalization factors takes $O(\log\ell)$ operations in k';
- Computing the points of the kernel via differential additions take $O(\ell^g)$ operations in k';
- If $\ell \equiv 1 \pmod 4$, applying the isogeny formula take $O(\ell^g)$ operations in k';
- If $\ell \equiv 3 \pmod 4$, applying the isogeny formula take $O(\ell^{2g})$ operations in k';

Over $\mathbb{F}_q$ the geometric points of the kernel live in a extension of degree at most $\ell^g - 1$; the total cost is then $\widetilde{O}(\ell^{2g})$ or $\widetilde{O}(\ell^{3g})$ operations in $\mathbb{F}_q$.

The complexity is much worse over a number field because we need to work with extensions of much higher degree.

We can compute the isogeny directly given the equations (in a suitable form) of the kernel K of the isogeny, by working with "formal tuples" [LR]. When K is rational, this gives a complexity of $\widetilde{O}(\ell^g)$ or $\widetilde{O}(\ell^{2g})$ operations in $\mathbb{F}_q$. When given a basis of K, computing the equations of K costs $O(\ell^g)$ operations in k'. □

2.3. **Cyclic isogenies.** Let $f : A \to B$ be an isogeny with cyclic kernel, and assume that we have principal polarization $\mathcal{L}_0$ and $\mathcal{M}_0$ on A and B. Let $\mathcal{L} = \mathcal{L}_0^n$ and $\mathcal{M} = \mathcal{M}_0^n$.

Then there exist φ such that the following diagram commutes:

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "\varphi_{f^*\mathcal{M}}"] \arrow[dd, bend right, "\varphi"'] & B \arrow[d, "\varphi_{\mathcal{M}}"] \\
\widehat{A}_k \arrow[d, "\varphi_{\mathcal{L}}^{-1}"] & \widehat{B}_k \arrow[l, "\widehat{f}"'] \\
A &
\end{tikzcd}$$

By construction, φ commutes with the Rosatti involution, so it is a (totally positive) totally real element of $\operatorname{End}^0(A)$. We note $\mathcal{L}^\varphi = f^*\mathcal{M}$ so that we have the following diagram

$$\begin{tikzcd}
A \arrow[r, "\varphi"] \arrow[dr, "\varphi_{\mathcal{L}^\varphi}"'] & A \arrow[d, "\varphi_{\mathcal{L}}"] \\
& \widehat{A}_k
\end{tikzcd}$$

It is easy to see that $K = \operatorname{Ker} f$ is isotropic under the commutator pairing of $\mathcal{L}^\varphi$.

Assume that we can find a matrix $F \in \operatorname{Mat}_r(\operatorname{End}^+(A))$ such that $\varphi \operatorname{Id} = {}^tFF$. Then we can compute the φ-contragredient isogey $\widetilde{f}$ as follow.

Proposition 2.9. *Let $(B, \mathcal{M}_0)$ be a ppav with a symmetric theta structure on $G(\mathcal{M})$ where $\mathcal{M} = \mathcal{M}_0^n$ is of level n even. Let $K' \subset B[\ell]$ be a maximal isotropic subgroup for $\mathcal{M}^\varphi$ and $\widetilde{f} : B \to A = B/K'$ be the associated isogeny. Assume that ℓ is prime to $2n$; then the theta structure on $G(\mathcal{M})$ induces a unique polarization $\mathcal{L}$ of level n on A and a unique compatible symmetric theta structure on $G(\mathcal{L})$. Let $F \in \operatorname{Mat}_r(O_{K_0})$ be such that ${}^tFF = \varphi \operatorname{Id}$.*

Let $i \in K_1(\mathcal{L})$ and $(j_1, \dots, j_r) \in K_1(\mathcal{M})^r$ be the unique preimage of $(i, 0, \dots, 0)$ by F. Let y be a geometric point of B and let $Y = {}^tF(y, 0, \dots, 0) \in B^r$. Then (up to a constant λ that may depend on y this time)

$$\vartheta_i^{\mathcal{L}}(\widetilde{f}(y)) \cdot \dots \cdot \vartheta_0^{\mathcal{L}}(0) = \lambda \sum_{\substack{(t_1,\dots,t_r) \in K'^r \\ F(t_1,\dots,t_r) = (0,\dots,0)}} \vartheta_{j_1}^{\mathcal{M}}(Y_1 + t_1) \cdot \dots \cdot \vartheta_{j_r}^{\mathcal{M}}(Y_r + t_r). \tag{2}$$

Proof. This is a work in progress with Dimitar Jetchev and Alina Dudeanu. We have the following diagram describing the steps of the isogeny computation

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

The full picture is summarized by:

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "\varphi_{\mathcal{L}}"] \arrow[dd, bend right, "\varphi_{f^*\mathcal{M}}"'] & B \arrow[r, "\widetilde{f}"] \arrow[d, "\varphi_{\mathcal{M}}"] \arrow[dd, bend right, "\varphi_{f^*\mathcal{L}}"'] & A \arrow[d, "\varphi_{\mathcal{L}}"] \\
\widehat{A}_k \arrow[d, "\widehat{\varphi}"] & \widehat{B}_k \arrow[d, "\widehat{\varphi}"] \arrow[dl, "\widehat{f}"] & \widehat{A}_k \arrow[dl, "\widehat{\widetilde{f}}"] \\
\widehat{A}_k & \widehat{B}_k &
\end{tikzcd}$$

□

Remark 2.10. In dimension 2, if ℓ splits completely into principal ideals as $\ell = \ell_1 \ell_2$ inside the real class field, then there are two types of cyclic isogenies according to whether the kernel is inside $A[\varphi_1]$ or $A[\varphi_2]$ where we note φ_i a generator of the ideal ℓ_i.

2.4. Moduli spaces.

Theorem 2.11 (Duplication formulae). *For all $\chi \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g$,*

$$\vartheta\left[\begin{smallmatrix}\chi\\0\end{smallmatrix}\right](0, 2\frac{\Omega}{n})^2 = \frac{1}{2^g} \sum_{t \in \frac{1}{2}\mathbb{Z}^g/\mathbb{Z}^g} e^{-2i\pi 2\, {}^t\chi \cdot t} \vartheta\left[\begin{smallmatrix}0\\t\end{smallmatrix}\right](0, \frac{\Omega}{n})^2$$

$$\vartheta\left[\begin{smallmatrix}0\\i/2\end{smallmatrix}\right](0, 2\Omega)^2 = \frac{1}{2^g} \sum_{i_1 + i_2 = 0 \pmod 2} \vartheta\left[\begin{smallmatrix}0\\i_1/2\end{smallmatrix}\right](0, \Omega) \vartheta\left[\begin{smallmatrix}0\\i_2/2\end{smallmatrix}\right](0, \Omega);$$

Example 2.12. In genus 1, via a simple change of variables, we recover the AGM:

$$\vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0, 2\Omega)^2 = \frac{\vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0, \Omega)^2 + \vartheta\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right](0, \Omega)^2}{2}$$

$$\vartheta\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right](0, 2\Omega)^2 = \sqrt{\vartheta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0, \Omega)^2 \vartheta\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right](0, \Omega)^2}$$

The duplication formulae allows, starting from the theta constants of level 2 of an abelian variety A_1 to compute the squares of the theta constants of level 2 of a 2-isogenous abelian variety A_2. Note that not all square roots correspond to valid theta constants, but a clever use of Riemann relations along with compatible additions from [LR13] allows to identify the "good" square roots from the "bad" ones (work in progress with David Lubicz).

Applications:

- Over $\mathbb{F}_{2^m}$, starting from an ordinary abelian variety $A = A_1$, (a subsequence of) the modular invariants of the abelian varieties A_i converge to the canonical lift $\widetilde{A}$;
- Over $\mathbb{Q}_{2^m}$, staring with $\widetilde{A}_1$, and applying the duplication formulae to get $\widetilde{A}_d$, then we get the same theta null point up to a constant u equal to the product of the eigenvalues of the Frobenius π inversible modulo 2 [Mes02].

- Over $\mathbb{C}$, we can recover the period matrix Ω (in a fundamental domain) from the theta null point when $g=1$ or $g=2$. Plugging a Newton iteration allows to compute theta constants in quasi-linear time from the period matrix [Dup06].

For modular correspondances, we can look at this diagram:

$$\begin{tikzcd}
 & \mathcal{A}_{g,\ell n} \arrow[d] \arrow[ddl, "\pi"'] \\
 & \mathcal{A}_{g,\ell n}/\mathfrak{H}_2 \simeq \mathcal{A}^1_{g,n}(\ell) \arrow[d] \\
\mathcal{A}_{g,n} & \mathcal{A}_{g,\ell n}/\mathfrak{H} \simeq \mathcal{A}^0_{g,n}(\ell) \arrow[l] \arrow[d, "\text{forget}"] \\
 & \mathcal{A}_{g,n}
\end{tikzcd}$$

Assume for simplicity that n is prime to ℓ, and look at the projection map coming from the isogeny theorem $\pi: \mathcal{A}_{g,\ell n} \to \mathcal{A}_{g,n}$, $(a_i)_{i \in Z(\overline{\ell n})} \mapsto (a_i)_{i \in Z(\overline{n})}$. From a theta null point $(B, \mathcal{M}, (b_i)_{i \in Z(\overline{n})}) \in \mathcal{A}_{g,n}$, the (non degenerate) fibers in $\pi^*((b_i)_{i \in Z(\overline{n})})$ corresponds to theta null points (of level ℓn) of abelian varieties ℓ-isogenous to B with a compatible theta structure.

Theorem 2.13. *Let $\mathfrak{H}$ be the subgroup of symmetric automorphisms of the Heisenberg group of level ℓn that fix the subgroup of level n. The group $\mathfrak{H}$ is a semidirect product $\mathfrak{H}_2 \times \overline{\mathfrak{H}_1}$ which acts on the fibers as follow:*

- *$\mathfrak{H}_1$ is generated by the actions*
$$(a_i)_{i \in Z(\overline{\ell n})} \mapsto (a_{\psi(i)})_{i \in Z(\overline{\ell n})}$$
for an automorphism $\psi: Z(\overline{\ell n}) \to Z(\overline{\ell n})$ fixing $Z(\overline{n})$.
- *$\mathfrak{H}_2$ is generated by the actions*
$$(a_i)_{i \in Z(\overline{\ell n})} \mapsto (e_{\overline{\ell n}}(\psi(i), i) a_i)_{i \in Z(\overline{\ell n})}$$
where ψ is a symmetric morphism $Z(\overline{\ell n}) \to \hat{Z}(\bar{\ell})$, coming from a symmetric morphism $\psi_2 : Z(\bar{\ell}) \to \hat{Z}(\bar{\ell})$. (Where symmetric means that $\psi_2(x)(y) = \psi_2(y)(x)$.)

The fiber is reduced of dimension 0. Furthermore the action of $\mathfrak{H}$ on the geometric points in the fibers has the following properties

- *A geometric point $(a_i)_{i \in Z(\overline{\ell n})}$ in the fiber $\pi^*((b_i)_{i \in Z(\overline{n})})$ is degenerate if and only if the action of $\mathfrak{H}$ on it is non free.*
- *Two valid theta null points in the fiber correspond to the same isogenous abelian variety (with a different theta structure) if and only if they are in the same orbit under the action of $\mathfrak{H}$.*

In particular, $\mathcal{A}_{g,\ell n}/\mathfrak{H}_2$ is isomorphic to $\mathcal{A}^1_{g,n}(\ell)$, the moduli spaces classifying abelian varieties $(B, \mathcal{M})$ with a level n symmetric theta structure and a basis of a maximal isotropic kernel K in the ℓ-torsion; and In particular, $\mathcal{A}_{g,\ell n}/\mathfrak{H}_2$ is isomorphic to $\mathcal{A}^0_{g,n}(\ell)$, the moduli spaces classifying abelian varieties $(B, \mathcal{M})$ with a level n symmetric theta structure and a maximal isotropic kernel K in the ℓ-torsion.

Proof. See [FLR11], where we also give a method to construct all degenerate points in the fiber. In dimension 2, $\pi^*((b_i)_{i \in Z(\overline{n})})/\mathfrak{H}$ is of size $\ell^3 + \ell^2 + \ell + 1$ (the number of ℓ-isogenies starting from B). The size of $\mathfrak{H}_1$ is $(\ell^2 - 1)(\ell^2 - \ell)$ while the size of $\mathfrak{H}_2$ is ℓ^3, so the number of valid theta null points in the fiber is $\ell^{10} - \ell^8 - \ell^6 + \ell^4$. In dimension g we get a bound of $O(\ell^{2g^2+g})$. □

While combining Riemann relations with Koizumi's like relations allows to give equations for the moduli space $\mathcal{A}^1_{g,n}(\ell)$ (ongoing work with David Lubicz), for isogenies computations we want equations of the moduli space $\mathcal{A}^0_{g,n}(\ell)$, or more precisely in its projection inside $\mathcal{A}_{g,n} \times \mathcal{A}_{g,n}$. Furthermore, for practical applications we want these equations to be in lexicographical Grőbner basis.

Remark 2.14. The equations for $\mathcal{A}^1_{g,n}(\ell)$ that we have allow, starting from two isogenous abelian varieties to recover the basis of the corresponding kernel by solving a Grőbner system. (Because when we have a point in this intermediate fiber, it is straightforward to recover a geometric point in the fiber $\pi^*((b_i)_{i \in Z(\overline{n})})$ and from it a basis of the kernel).

Theorem 2.15. *In dimension* 2*, let* $(b_i)_{i \in \{1,2,3\}}$ *be modular invariants on* $\mathcal{A}_2$ *(the moduli space of principally polarized abelian surfaces).*

Then an evaluation-interpolation algorithm can compute (in time quasi-linear in the output) the modular polynomials

$$\begin{aligned} \varphi_1(b_1, b_2, b_3, b_1') &= 0 \\ b_2' \varphi_1(b_1, b_2, b_3, b_1') &= \psi_2(b_1, b_2, b_3, b_1') \\ b_3' \varphi_1(b_1, b_2, b_3, b_1') &= \psi_3(b_1, b_2, b_3, b_1') \end{aligned}$$

classifying the couple of invariants $(b_i), (b_i')$ *of* ℓ*-isogenous abelian surfaces.*

Here the modular polynomials are actually rational functions, where the denominator lies in $\mathbb{Q}(b_1, b_2, b_3)$ *and comes from the Humber surface of discriminant* ℓ^2 *that classify abelian surfaces* ℓ*-isogenous to a product of elliptic curves (with the product polarisation).*

Proof. See [Dup06] which uses Igusa invariants and computed the modular polynomials of level 2. This work was extended by Milio which used invariants from Streng's phd thesis and computed the modular polynomials of level 3.

Instead of Igusa invariants, using quotient of level 2 theta constant allows to get much smaller polynomials with lots of symmetries. In this case we can prove that the denominator is of total degree $\ell^3 - \ell$. For more details we refer to an upcoming article by Milio. Milio also computed these polynomials up to level 7.

For instance in the evaluation we have that

$$\varphi_1(b_i(\tau)), Y) = \prod_{g \in \Gamma_{2,4}/\Gamma_{2,4} \bigcap \Gamma_0(\ell)} (Y - b_i(\ell g.\tau)),$$

where $b_i(\tau) = \vartheta_i(\tau)/\vartheta_0(\tau)$. For the evaluation we use the fact that theta constant of levels 2 generate the field of modular functions (of weight 0) invariant under $\Gamma_{2,4}$. □

References

[BMS+08] A. Bostan, F. Morain, B. Salvy, and E. Schost. "Fast algorithms for computing isogenies between elliptic curves". In: *Mathematics of Computation* 77.263 (2008), pp. 1755–1778 (cit. on p. 3).

[BLS09] R. Bröker, K. Lauter, and A. Sutherland. *Modular polynomials via isogeny volcanoes.* 2009. arXiv: 1001.0402 (cit. on p. 2).

[CR13] R. Cosset and D. Robert. "An algorithm for computing (ℓ, ℓ)-isogenies in polynomial time on Jacobians of hyperelliptic curves of genus 2". Accepted for publication at Mathematics of computation. Oct. 2013. URL: http://www.normalesup.org/~robert/pro/publications/articles/niveau.pdf. HAL: hal-00578991, eprint: 2011/143 (cit. on p. 5).

[Dup06] R. Dupont. "Moyenne arithmetico-geometrique, suites de Borchardt et applications". In: *These de doctorat, Ecole polytechnique, Palaiseau* (2006) (cit. on pp. 8, 9).

[Elk92] N. Elkies. "Explicit isogenies". In: *manuscript, Boston MA* (1992) (cit. on p. 3).

[Eng09] A. Enge. "Computing modular polynomials in quasi-linear time". In: *Math. Comp* 78.267 (2009), pp. 1809–1824 (cit. on p. 2).

[FLR11] J.-C. Faugère, D. Lubicz, and D. Robert. "Computing modular correspondences for abelian varieties". In: *Journal of Algebra* 343.1 (Oct. 2011), pp. 248–277. DOI: 10.1016/j.jalgebra.2011.06.031. arXiv: 0910.4668 [cs.SC]. URL: http://www.normalesup.org/~robert/pro/publications/articles/modular.pdf. HAL: hal-00426338 (cit. on p. 8).

[Kem89] G. Kempf. "Linear systems on abelian varieties". In: *American Journal of Mathematics* 111.1 (1989), pp. 65–94 (cit. on pp. 4, 5).

[Koh96] D. Kohel. "Endomorphism rings of elliptic curves over finite fields". PhD thesis. University of California, 1996 (cit. on p. 1).

[Koh03] D. Kohel. "The AGM-$X_0(N)$ Heegner point lifting algorithm and elliptic curve point counting". In: *Advances in cryptology—ASIACRYPT 2003*. Vol. 2894. Lecture Notes in Comput. Sci. Berlin: Springer, 2003, pp. 124–136 (cit. on p. 2).

[Koi76] S. Koizumi. "Theta relations and projective normality of abelian varieties". In: *American Journal of Mathematics* (1976), pp. 865–889 (cit. on p. 5).

[LR] D. Lubicz and D. Robert. "Computing separable isogenies in quasi-optimal time" (cit. on pp. 5, 6).

[LR13] D. Lubicz and D. Robert. "A generalisation of Miller's algorithm and applications to pairing computations on abelian varieties". Mar. 2013. URL: http://www.normalesup.org/~robert/pro/publications/articles/optimal.pdf. HAL: hal-00806923, eprint: 2013/192 (cit. on p. 7).

[Mes02] J.-F. Mestre. *Notes of a talk given at the Cryptography Seminar Rennes*. 2002. URL: http://www.math.univ-rennes1.fr/crypto/2001-02/mestre.ps (cit. on p. 7).

[Mum66] D. Mumford. "On the equations defining abelian varieties. I". In: *Invent. Math.* 1 (1966), pp. 287–354 (cit. on pp. 3, 4).

[Mum67a] D. Mumford. "On the equations defining abelian varieties. II". In: *Invent. Math.* 3 (1967), pp. 75–135 (cit. on p. 4).

[Mum67b] D. Mumford. "On the equations defining abelian varieties. III". In: *Invent. Math.* 3 (1967), pp. 215–244 (cit. on p. 4).

[Mum83] D. Mumford. *Tata lectures on theta I*. Vol. 28. Progress in Mathematics. With the assistance of C. Musili, M. Nori, E. Previato and M. Stillman. Boston, MA: Birkhäuser Boston Inc., 1983, pp. xiii+235. ISBN: 3-7643-3109-7 (cit. on pp. 3, 5).

[Mum91] D. Mumford. *Tata lectures on theta III*. Vol. 97. Progress in Mathematics. With the collaboration of Madhav Nori and Peter Norman. Boston, MA: Birkhäuser Boston Inc., 1991, pp. viii+202. ISBN: 0-8176-3440-1 (cit. on p. 5).

[Vél71] J. Vélu. "Isogénies entre courbes elliptiques". In: *Compte Rendu Académie Sciences Paris Série A-B* 273 (1971), A238–A241 (cit. on p. 1).

INRIA Bordeaux–Sud-Ouest, 200 avenue de la Vieille Tour, 33405 Talence Cedex FRANCE
E-mail address: damien.robert@inria.fr
URL: http://www.normalesup.org/~robert/