On isogenies and polarisations
2013/11/12 — Lfant seminar — Bordeaux

Gaëtan Bisson, Romain Cosset, Alina Dudeanu, Dimitar Jetchev, David Lubicz, Damien Robert
Outline

1. Abelian varieties and polarisations
2. Theta functions
3. Maximal isotropic isogenies
4. Cyclic isogenies
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.
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 $H_g$, 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 $(\text{Im} \Omega)^{-1}$. 
Action of the symplectic group

- Every principal symplectic form (hence symplectic basis) on $\mathbb{Z}^{2g}$ comes from the action of $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{Sp}_{2g}(\mathbb{Z})$ on $(\mathbb{Z}^{2g}, E_0)$;
- This action gives a new equivariant bijection $j_M : \mathbb{Z}^{2g} \to \Lambda$ via $j_M((x_1, x_2)) = (A\Omega x_1 + Bx_2, C\Omega x_1 + Dx_2)$;
- Normalizing this embedding via the action of $(C\Omega + D)^{-1}$ on $\mathbb{C}^g$, we get that $j_M((x_1, x_2)) = \Omega_M x_1 + x_2$ with $\Omega_M = (A\Omega + B)(C\Omega + D)^{-1} \in \mathfrak{H}_g$;
- The moduli space of principally polarised abelian varieties is then isomorphic to $\mathfrak{H}_g / \text{Sp}_{2g}(\mathbb{Z})$. 
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.

**Remark**

*Up to a renormalization, we can always assume that $V = V' = \mathbb{C}^g$, $f = \text{Id}$ and the isogeny is simply $\mathbb{C}^g/\Lambda \to \mathbb{C}^g/\Lambda'$ for $\Lambda \subset \Lambda'$.*
**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 \( \Lambda^* = \{ f \mid f(\Lambda) \subset \mathbb{Z} \} \) 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 \( \deg H \). 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):*

\[
(x, f) \mapsto f(x).
\]
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:

\[
\begin{array}{ccc}
A & \xrightarrow{f} & B \\
\downarrow \Phi_{H_1} & & \downarrow \Phi_{H_2} \\
\widehat{A} & \xleftarrow{\widehat{f}} & \widehat{B}
\end{array}
\]
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 $f^* H_2 = \ell H_1$.

$f : (A, H_1) \rightarrow (B, H_2)$ is an $\ell$-isogeny between principally polarised abelian varieties iff the following diagram commutes
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 $\Lambda \cong H^1(C, \mathbb{Z}) \subset V$ 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)**

$\text{Jac } C$ 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 $\text{Jac } C \cong \text{Jac } H$ as non polarised abelian varieties!
Proposition

Let $\Phi: A = V / \Lambda \rightarrow \mathbb{P}^{m-1}$ be a projective embedding. Then the linear functions $f$ associated to this embedding are $\Lambda$-automorphics:

$$f(x + \lambda) = a(\lambda, x)f(x) \quad x \in V, \lambda \in \Lambda;$$

for a fixed automorphy factor $a$:

$$a(\lambda + \lambda', x) = a(\lambda, x + \lambda')a(\lambda', x).$$

Theorem (Appell-Humbert)

All automorphy factors are of the form

$$a(\lambda, x) = \pm e^{\pi \theta(x, \lambda) + \frac{1}{2} H(\lambda, \lambda)}$$

for a polarisation $H$ on $A$. 
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 $\Omega \in \mathfrak{h}_g$.

All automorphic forms corresponding to a multiple of $H_0$ come from the theta functions with characteristics:

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

Automorphic property:

\[ \vartheta \left[ \begin{array}{c} a \\ b \end{array} \right] (z + m_1 \Omega + m_2, \Omega) = e^{2\pi i t (a \cdot m_2 - b \cdot m_1) - \pi i t m_1 \cdot m_1 - 2\pi i t m_1 \cdot z} \vartheta \left[ \begin{array}{c} a \\ b \end{array} \right] (z, \Omega). \]
Theta functions of level $n$

- Define $\vartheta_i = \vartheta \left[ \frac{0}{i}, \frac{\Omega}{n} \right]$ for $i \in \mathbb{Z}(n) = \mathbb{Z}^g / n\mathbb{Z}^g$ and
- This is a basis of the automorphic functions for $H = nH_0$ (theta functions of level $n$);
- This is the unique basis such that in the projective coordinates:
  
  $$
  A \rightarrow \mathbb{P}^{n^g - 1}_C
  $$
  
  $$
  z \rightarrow (\vartheta_i(z))_{i \in \mathbb{Z}(n)}
  $$

  the translation by a point of $n$-torsion is normalized by

  $$
  \vartheta_i(z + \frac{m_1}{n} \Omega + \frac{m_2}{n}) = e^{-\frac{2\pi i t}{n}} i^{m_1} \vartheta_{i+m_2}(z).
  $$

- $(\vartheta_i)_{i \in \mathbb{Z}(n)} = \begin{cases} \text{coordinates system} & n \geq 3 \\ \text{coordinates on the Kummer variety } A/\pm 1 & n = 2 \end{cases}$
- $(\vartheta_i)_{i \in \mathbb{Z}(n)}$: basis of the theta functions of level $n$
- Theta null point: $\vartheta_i(0)_{i \in \mathbb{Z}(n)} = \text{modular invariant}$. 
The differential addition law \((k = \mathbb{C})\)

\[
\left( \sum_{t \in \hat{Z}(2)} \chi(t) \theta_{i+t}(x + y) \theta_{j+t}(x - y) \right) \cdot \left( \sum_{t \in \hat{Z}(2)} \chi(t) \theta_{k+t}(0) \theta_{l+t}(0) \right) = \\
\left( \sum_{t \in \hat{Z}(2)} \chi(t) \theta_{-i'+t}(y) \theta_{j'+t}(y) \right) \cdot \left( \sum_{t \in \hat{Z}(2)} \chi(t) \theta_{k'+t}(x) \theta_{l'+t}(x) \right).
\]

where \(\chi \in \hat{Z}(2), i, j, k, l \in Z(n)\)

\((i', j', k', l') = A(i, j, k, l)\)

\[
A = \frac{1}{2} \begin{pmatrix}
1 & 1 & 1 & 1 \\
1 & 1 & -1 & -1 \\
1 & -1 & 1 & -1 \\
1 & -1 & -1 & 1 \\
\end{pmatrix}
\]
Cryptographic usage of isogenies

- Transfer the Discrete Logarithm Problem from one Abelian variety to another;
- Point counting algorithms ($\ell$-adic or $p$-adic) ⇒ Verify an abelian variety is secure;
- Compute the class field polynomials (CM-method) ⇒ Construct a secure abelian variety;
- Compute the modular polynomials ⇒ Compute isogenies;
- Determine $\text{End}(A)$ ⇒ CRT method for class field polynomials;
- Speed up the arithmetic;
- Hash functions and cryptosystems based on isogeny graphs.
The isogeny theorem

**Theorem**

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

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

**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.
An example with $g = 1$, $n = 2$, $\ell = 3$

$$z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n$$

$[\ell]$$

$$\ell z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n$$

$\tilde{f}$

$\mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g), \text{ level } n$
An example with $g = 1$, $n = 2$, $\ell = 3$

\[ z \in \mathbb{C}^g / (\mathbb{Z}^g + \ell \Omega \mathbb{Z}^g), \text{ level } \ell n \]

\[ \Rightarrow \quad \ell z \in \mathbb{C}^g / (\mathbb{Z}^g + \ell \Omega \mathbb{Z}^g), \text{ level } \ell n \]

Diagram:

\[ \begin{array}{ccc}
0 & 1 & 2 \\
\Omega & & 3\Omega \\
\end{array} \]

Points marked with $x$ and $y$ correspond to the example conditions.
An example with $g = 1$, $n = 2$, $\ell = 3$

$$z \in \mathbb{C}^g / (\mathbb{Z}^g + \ell \Omega \mathbb{Z}^g), \text{ level } \ell n \quad \xrightarrow{[\ell]} \quad \ell z \in \mathbb{C}^g / (\mathbb{Z}^g + \ell \Omega \mathbb{Z}^g), \text{ level } \ell n$$

$$f \quad \xrightarrow{\sim} \quad \tilde{f}$$

$$z \in \mathbb{C}^g / (\mathbb{Z}^g + \Omega \mathbb{Z}^g), \text{ level } n$$
An example with $g = 1$, $n = 2$, $\ell = 3$
An example with $g = 1$, $n = 2$, $\ell = 3$

$$z \in \mathbb{C}^g / (\mathbb{Z}^g + \ell \Omega \mathbb{Z}^g), \text{ level } \ell n \quad \xrightarrow{[\ell]} \quad \ell z \in \mathbb{C}^g / (\mathbb{Z}^g + \ell \Omega \mathbb{Z}^g), \text{ level } \ell n$$

$$z \in \mathbb{C}^g / (\mathbb{Z}^g + \Omega \mathbb{Z}^g), \text{ level } n$$

Diagram:

- $1$
- $R_2$
- $R_1$
- $R_0$
- $\Omega$
- $3\Omega$
An example with $g = 1$, $n = 2$, $\ell = 3$

$z \in \mathbb{C}^g / (\mathbb{Z}^g + \ell \Omega \mathbb{Z}^g)$, level $\ell n$ 

$[\ell] \quad \rightarrow \quad \ell z \in \mathbb{C}^g / (\mathbb{Z}^g + \ell \Omega \mathbb{Z}^g)$, level $\ell n$

$f \quad \rightarrow \quad \tilde{f}$

$z \in \mathbb{C}^g / (\mathbb{Z}^g + \Omega \mathbb{Z}^g)$, level $n$
An example with $g = 1$, $n = 2$, $\ell = 3$

$z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell \Omega \mathbb{Z}^g)$, level $\ell n$

$f$

$\ell z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell \Omega \mathbb{Z}^g)$, level $\ell n$

$\tilde{f}$

$z \in \mathbb{C}^g/(\mathbb{Z}^g + \Omega \mathbb{Z}^g)$, level $n$
Theorem (Koizumi–Kempf)

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

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

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

- 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 $r = 4$. 
Abelian varieties and polarisations

Theta functions

Maximal isotropic isogenies

Cyclic isogenies

The isogeny formula

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

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

**Proposition**

Let \( F \) be a matrix of rank \( r \) such that \( ^t F F = \ell \operatorname{Id}_r \). Let \( X \in (\mathbb{C}^g)^r \) and \( Y = X F^{-1} \in (\mathbb{C}^g)^r \). Let \( i \in (Z(n))^r \) and \( j = i F^{-1} \). Then we have

\[ \vartheta^A_{i_1}(Y_1) \cdots \vartheta^A_{i_r}(Y_r) = \sum_{t_1, \ldots, t_r \in \frac{1}{\ell} \mathbb{Z}^g / \mathbb{Z}^g} \vartheta^B_{j_1}(X_1 + t_1) \cdots \vartheta^B_{j_r}(X_r + t_r), \]

\( t_1, \ldots, t_r \in \mathbb{Z}^g / \mathbb{Z}^g \)

\( (t_1, \ldots, t_r) F = (0, \ldots, 0) \)

**Corollary**

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

\( t_1, \ldots, t_r \in K \)

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

\[ x \in (A, \ell H_1) \quad \Rightarrow \quad (x, 0, \ldots, 0) \in (A^r, \ell H_1 \star \ldots \star \ell H_1) \]

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

\[ \tilde{f}\]

\[ f \]

\[ \ell \]

\[ {}^t F (x, 0, \ldots, 0) \in (A^r, \ell H_1 \star \ldots \star \ell H_1) \]

\[ F \circ {}^t F (x, 0, \ldots, 0) \in (A^r, H_1 \star \ldots \star H_1) \]
The geometric points of the kernel live in an extension $k'$ of degree at most $\ell^g - 1$ over $k = \mathbb{F}_q$.

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 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 takes $O(\ell^g)$ operations in $k'$;

If $\ell \equiv 3 \pmod{4}$, applying the isogeny formula takes $O(\ell^{2g})$ operations in $k'$;

$\Rightarrow$ The total cost is $\widetilde{O}(\ell^{2g})$ or $\widetilde{O}(\ell^{3g})$ operations in $\mathbb{F}_q$.

**Remark**

The complexity is much worse over a number field because we need to work with extensions of much higher degree.
The geometric points of the kernel live in an extension $k'$ of degree at most $\ell^g - 1$ over $k = \mathbb{F}_q$;

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 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 $k'$;

$\Rightarrow$ The total cost is $\widetilde{O}(\ell^{2g})$ or $\widetilde{O}(\ell^{3g})$ operations in $\mathbb{F}_q$.

**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 $\mathbb{F}_q$.***
An $(\ell, \ell)$-isogeny graph in dimension 2 [Bisson, Cosset, R.]
An $(\ell,\ell)$-isogeny graph in dimension 2 [Bisson, Cosset, R.]
An \((\ell,\ell)\)-isogeny graph in dimension 2 [Bisson, Cosset, R.]
An \((\ell, \ell)\)-isogeny graph in dimension 2 [Bisson, Cosset, R.]
An \((\ell, \ell)\)-isogeny graph in dimension 2 [Bisson, Cosset, R.]
An \((\ell, \ell)\)-isogeny graph in dimension 2 [Bisson, Cosset, R.]
Let $f : (A, H_1) \to (B, H_2)$ 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 $O_0 = \text{End}(A)^s$ 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 $A$. 
Let \( f : (A, H_1) \rightarrow (B, H_2) \) be an isogeny between principally polarised abelian varieties with cyclic kernel of degree \( \ell \);

There exists \( \varphi \) such that the following diagram commutes:

\[
\begin{array}{ccc}
A & \xrightarrow{f} & B \\
\varphi \downarrow & & \downarrow \Phi_{H_2} \\
\Phi_{H_1} & \xleftarrow{\hat{f}} & \hat{B} \\
\end{array}
\]

- \( \varphi \) 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);
- \( \varphi \) is totally positive.
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

  ![Diagram](image)

- $\varphi$ 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

  ![Diagram](image)
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:

\[
\begin{array}{ccc}
A & \xrightarrow{\varphi} & A \\
\downarrow{\Phi_{\varphi^*H_1}} & & \downarrow{\Phi_{\varphi H_1}} \\
\hat{A} & \xleftarrow{\hat{\varphi}} & \hat{A}
\end{array}
\]

Applying the isogeny theorem on $\varphi$ allows to find relations between $\varphi^*H_1$ and $H_1$ but we want $\varphi H_1$. 
**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 $F \in \text{Mat}_r(K_0)$ 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

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

**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.]

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

\[
\vartheta^B_b := \vartheta \left[ \frac{0}{b/n} \right] \left( \cdot, \frac{\Omega}{n} \right), \quad \vartheta^A_b := \vartheta \left[ \frac{0}{b/n} \right] \left( \cdot, \frac{\varphi \Omega}{n} \right)
\]

**Theorem**

Let \( X \) in \((\mathbb{C}^g)^r\) and \( Y = XF^{-1} \in (\mathbb{C}^g)^r\). Let \( i \in (\mathbb{Z}(n))^r \) and \( j = iF^{-1} \).

\[
\vartheta^A_{i_1}(Y_1) \ldots \vartheta^A_{i_r}(Y_r) = \sum_{t_1, \ldots, t_r \in K(\varphi H_2)} \vartheta^B_{j_1}(X_1 + t_1) \ldots \vartheta^B_{j_r}(X_r + t_r),
\]

.. image:: image.png

\[x \in (A, \varphi H_1) \quad \Downarrow \quad (x, 0, \ldots, 0) \in (A^r, \varphi H_1 \star \cdots \star H_1)\]

\[y \in (B, H_2) \quad \Downarrow \quad \varphi \quad \Downarrow \quad \vartheta^A_{i_1}(Y_1) \quad \Downarrow \quad \vartheta^A_{i_r}(Y_r)
\]

\[\tilde{f}(y) \in (A, H_1) \quad \Downarrow \quad F \circ \vartheta^A_{i_1}(Y_1) \quad \Downarrow \quad F \circ \vartheta^A_{i_r}(Y_r)
\]

\[\tilde{f}(y) \in (A, H_1) \quad \Downarrow \quad F \circ \vartheta^A_{i_1}(Y_1) \quad \Downarrow \quad F \circ \vartheta^A_{i_r}(Y_r)
\]

\[\vartheta^A_{i_1}(Y_1) \ldots \vartheta^A_{i_r}(Y_r) = \sum_{t_1, \ldots, t_r \in K(\varphi H_2)} \vartheta^B_{j_1}(X_1 + t_1) \ldots \vartheta^B_{j_r}(X_r + t_r),
\]

\[\vartheta^A_{i_1}(Y_1) \ldots \vartheta^A_{i_r}(Y_r) = \sum_{t_1, \ldots, t_r \in K(\varphi H_2)} \vartheta^B_{j_1}(X_1 + t_1) \ldots \vartheta^B_{j_r}(X_r + t_r),
\]
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 \( \sqrt{d} \).

**Remark**

*Computing the action of \( \sqrt{d} \) directly may be expensive if \( d \) is big.*
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”!