Generalizing Vélu's formulas and some applications

ECC 2010

Romain Cosset[1], David Lubicz[2,3], **Damien Robert**[4]

[1]Nancy Université, CNRS, Inria Nancy Grand Est

[2]CÉLAR

[3]IRMAR, Université de Rennes 1

[4]Inria Bordeaux Sud-Ouest

21/10/2010 (Redmond)

Outline

Abelian varieties

Definition

An Abelian variety is a complete connected group variety over a base field k.

- (Polarised) abelian varieties = higher dimensional equivalent of elliptic curves.
- If C is a curve of genus g, it's Jacobian is a (principally polarised) abelian variety of dimension g.
- For $C : y^2 = f(x)$ ($\deg f = 2g-1$) hyperelliptic curve, Mumford coordinates:

$$\begin{aligned} D &= \sum_{i=1}^{k} (P_i - P_\infty) \qquad k \leqslant g, \quad -P_i \neq P_j \\ &= (u, v) \text{ with } u = \prod (x - x_i), v(x_i) = y_i. \end{aligned}$$

Isogenies

Definition

A (separable) isogeny is a finite surjective (separable) morphism between two Abelian varieties.

- Isogenies $\Leftrightarrow$ Finite subgroups.

$$(f : A \to B) \mapsto \operatorname{Ker} f$$
$$(A \to A/H) \leftarrow H$$

- The kernel of the dual isogeny $\widehat{f}$ is the Cartier dual of the kernel of $f \Rightarrow$ pairings!
- We want isogenies compatible with the polarizations $\Rightarrow$ isotropic kernels.

Cryptographic usage of isogenies

- Transfer the DLP from one Abelian variety to another.
- Point counting algorithms (ℓ-adic or p-adic) $\Rightarrow$ Verify a curve is secure.
- Compute the class field polynomials (CM-method) $\Rightarrow$ Construct a secure curve.
- Compute the modular polynomials $\Rightarrow$ Compute isogenies.
- Determine $\mathrm{End}(A)$ $\Rightarrow$ CRT method for class field polynomials.

Explicit isogeny computation

- Given an isotropic subgroup $K \subset A(\overline{k})$ compute the isogeny $A \mapsto A/K$. (Vélu's formula.)
- Given an abelian variety compute all the isogeneous varieties. (Modular polynomials.)
- Given two isogeneous abelian variety A and B find the isogeny $A \mapsto B$. ("Inverse Vélu's formula" $\Rightarrow$ SEA algorithm).

Explicit isogeny computation

- Given an isotropic subgroup $K \subset A(\overline{k})$ compute the isogeny $A \mapsto A/K$. (Vélu's formula.)
- Given an abelian variety compute all the isogeneous varieties. (Modular polynomials.)
- Given two isogeneous abelian variety A and B find the isogeny $A \mapsto B$. ("Inverse Vélu's formula" $\Rightarrow$ SEA algorithm).

Explicit isogeny computation

- Given an isotropic subgroup $K \subset A(\overline{k})$ compute the isogeny $A \mapsto A/K$. (Vélu's formula.)
- Given an abelian variety compute all the isogeneous varieties. (Modular polynomials.)
- Given two isogeneous abelian variety A and B find the isogeny $A \mapsto B$. ("Inverse Vélu's formula" $\Rightarrow$ SEA algorithm).

Explicit isogeny computation

- Given an isotropic subgroup $K \subset A(\overline{k})$ compute the isogeny $A \mapsto A/K$. (Vélu's formula.)
- Given an abelian variety compute all the isogeneous varieties. (Modular polynomials.)
- Given two isogeneous abelian variety A and B find the isogeny $A \mapsto B$. ("Inverse Vélu's formula" $\Rightarrow$ SEA algorithm).

Vélu's formula

Theorem

Let $E : y^2 = f(x)$ be an elliptic curve and $G \subset E(k)$ a finite subgroup. Then E/G is given by $Y^2 = g(X)$ where

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

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

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

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

- No such characterisation in genus $g \geqslant 2$ for Mumford coordinates.

The modular polynomial

Definition

- Modular polynomial $\phi_n(x,y) \in \mathbb{Z}[x,y]$: $\phi_n(x,y) = 0 \Leftrightarrow x = j(E)$ and $y = j(E')$ with E and E' n-isogeneous.
- If $E : y^2 = x^3 + ax + b$ is an elliptic curve, the j-invariant is

$$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}$$

- Roots of $\phi_n(j(E), .) \Leftrightarrow$ elliptic curves n-isogeneous to E.
- In genus 2, modular polynomials use Igusa invariants. The height explodes.

$\Rightarrow$ Genus 2: $(2,2)$-isogenies [Richelot]. Genus 3: $(2,2,2)$-isogenies [Smi09].

$\Rightarrow$ Moduli space given by invariants with more structure.

$\Rightarrow$ Fix the form of the isogeny and look for compatible coordinates.

The modular polynomial

Definition

- Modular polynomial $\phi_n(x,y) \in \mathbb{Z}[x,y]$: $\phi_n(x,y) = 0 \Leftrightarrow x = j(E)$ and $y = j(E')$ with E and E' n-isogeneous.
- If $E : y^2 = x^3 + ax + b$ is an elliptic curve, the j-invariant is

$$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}$$

- Roots of $\phi_n(j(E), .) \Leftrightarrow$ elliptic curves n-isogeneous to E.
- In genus 2, modular polynomials use Igusa invariants. The height explodes.

$\Rightarrow$ Genus 2: $(2,2)$-isogenies [Richelot]. Genus 3: $(2,2,2)$-isogenies [Smi09].

$\Rightarrow$ Moduli space given by invariants with more structure.

$\Rightarrow$ Fix the form of the isogeny and look for compatible coordinates.

Complex abelian varieties and theta functions of level n

- $(\vartheta_i)_{i\in Z(\overline{n})}$: basis of the theta functions of level n. $(Z(\overline{n}) := \mathbb{Z}^g/n\mathbb{Z}^g)$
  $\Leftrightarrow A[n] = A_1[n] \oplus A_2[n]$: symplectic decomposition.
- $(\vartheta_i)_{i\in Z(\overline{n})} = \begin{cases} \text{coordinates system} & n \geqslant 3 \\ \text{coordinates on the Kummer variety } A/\pm 1 & n = 2 \end{cases}$
- Theta null point: $\vartheta_i(0)_{i\in Z(\overline{n})}$ = modular invariant.

Example ($k = \mathbb{C}$)

Abelian variety over $\mathbb{C}$: $A = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$; $\Omega \in \mathcal{H}_g(\mathbb{C})$ the Siegel upper half space (Ω symmetric, $\operatorname{Im}\Omega$ positive definite).

$$\vartheta_i := \Theta\left[\begin{smallmatrix} 0 \\ i/n \end{smallmatrix}\right](z, \Omega/n).$$

The differential addition law ($k = \mathbb{C}$)

$$\Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{i+t}(x+y)\vartheta_{j+t}(x-y)\Big).\Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{k+t}(0)\vartheta_{l+t}(0)\Big) =$$

$$\Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{-i'+t}(y)\vartheta_{j'+t}(y)\Big).\Big(\sum_{t\in Z(\overline{2})} \chi(t)\vartheta_{k'+t}(x)\vartheta_{l'+t}(x)\Big).$$

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

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

$$A = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

The isogeny theorem

Theorem

- *Let $\ell \wedge n = 1$, and $\phi : Z(\overline{n}) \to Z(\overline{\ell n}), x \mapsto \ell.x$ be the canonical embedding. Let $K_0 = A[\ell]_2 \subset A[\ell n]_2$.*
- *Let $(\vartheta_i^A)_{i \in Z(\overline{\ell n})}$ be the theta functions of level ℓn on $A = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$.*
- *Let $(\vartheta_i^B)_{i \in Z(\overline{n})}$ be the theta functions of level n of $B = A/K_0 = \mathbb{C}^g/(\mathbb{Z}^g + \frac{\Omega}{\ell}\mathbb{Z}^g)$.*
- *We have:*

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

Example

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

The modular space of theta null points of level n ($\operatorname{car} k \nmid n$)

Definition

The modular space $\mathcal{M}_{\overline{n}}$ of theta null points is:

$$\sum_{t \in Z(\overline{2})} a_{x+t} a_{y+t} \sum_{t \in Z(\overline{2})} a_{u+t} a_{v+t} = \sum_{t \in Z(\overline{2})} a_{x'+t} a_{y'+t} \sum_{t \in Z(\overline{2})} a_{u'+t} a_{v'+t},$$

with the relations of symmetry $a_x = a_{-x}$.

- Abelian varieties with a n-structure = open locus of $\mathcal{M}_{\overline{n}}$.

Isogenies and modular correspondence [FLR09]

$$\begin{tikzcd}
A_k, A_k[\ell n] = A_k[\ell n]_1 \oplus A_k[\ell n]_2 \arrow[d, shift left, "\pi"] & & (a_i)_{i \in Z(\overline{\ell n})} \in \mathcal{M}_{\overline{\ell n}}(k) \arrow[ll, dotted, "\text{determines}"'] \arrow[d, "\phi_1"] \\
B_k, B_k[n] = B_k[n]_1 \oplus B_k[n]_2 \arrow[u, shift left, "\widehat{\pi}"] & & (b_i)_{i \in Z(\overline{n})} \in \mathcal{M}_{\overline{n}}(k) \arrow[ll, dotted]
\end{tikzcd}$$

- Every isogeny (with isotropic kernel K) comes from a modular solution.
- We can detect degenerate solutions.

Isogenies and modular correspondence [FLR09]

$$\begin{tikzcd}
A_k, A_k[\ell n] = A_k[\ell n]_1 \oplus A_k[\ell n]_2 \arrow[d, shift left, "\pi"] & & (a_i)_{i \in Z(\overline{\ell n})} \in \mathcal{M}_{\overline{\ell n}}(k) \arrow[ll, dotted, "\text{determines}"'] \arrow[d, "\phi_1"] \\
B_k, B_k[n] = B_k[n]_1 \oplus B_k[n]_2 \arrow[u, shift left, "\widehat{\pi}"] & & (b_i)_{i \in Z(\overline{n})} \in \mathcal{M}_{\overline{n}}(k) \arrow[ll, dotted]
\end{tikzcd}$$

- Every isogeny (with isotropic kernel K) comes from a modular solution.
- We can detect degenerate solutions.

Isogenies and modular correspondence [FLR09]

$$\begin{tikzcd}
A_k, A_k[\ell n] = A_k[\ell n]_1 \oplus A_k[\ell n]_2 \arrow[d, shift left, "\pi"] & & (a_i)_{i \in Z(\overline{\ell n})} \in \mathcal{M}_{\overline{\ell n}}(k) \arrow[ll, dotted, "\text{determines}"'] \arrow[d, "\phi_1"] \\
B_k, B_k[n] = B_k[n]_1 \oplus B_k[n]_2 \arrow[u, shift left, "\widehat{\pi}"] & & (b_i)_{i \in Z(\overline{n})} \in \mathcal{M}_{\overline{n}}(k) \arrow[ll, dotted]
\end{tikzcd}$$

- Every isogeny (with isotropic kernel K) comes from a modular solution.
- We can detect degenerate solutions.

The contragredient isogeny [LR10a]

$$\begin{tikzcd} x \in A \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & z \in A \\ & y \in B \arrow[ur, "\widehat{\pi}"'] & \end{tikzcd}$$

Let $\pi : A \to B$ be the isogeny associated to $(a_i)_{i \in Z(\overline{\ell n})}$. Let $y \in B$ and $x \in A$ be one of the ℓ^g antecedents. Then

$$\widehat{\pi}(y) = \ell . x$$

The contragredient isogeny [LR10a]

$$\begin{tikzcd} x \in A \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & z \in A \\ & y \in B \arrow[ur, "\widehat{\pi}"'] & \end{tikzcd}$$

Let $\pi : A \to B$ be the isogeny associated to $(a_i)_{i \in Z(\overline{\ell n})}$. Let $y \in B$ and $x \in A$ be one of the ℓ^g antecedents. Then

$$\widehat{\pi}(y) = \ell . x$$

The contragredient isogeny [LR10a]

$$\begin{tikzcd}
x \in A \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & z \in A \\
& y \in B \arrow[ur, "\widehat{\pi}"'] &
\end{tikzcd}$$

Let $\pi : A \to B$ be the isogeny associated to $(a_i)_{i \in Z(\overline{\ell n})}$. Let $y \in B$ and $x \in A$ be one of the ℓ^g antecedents. Then

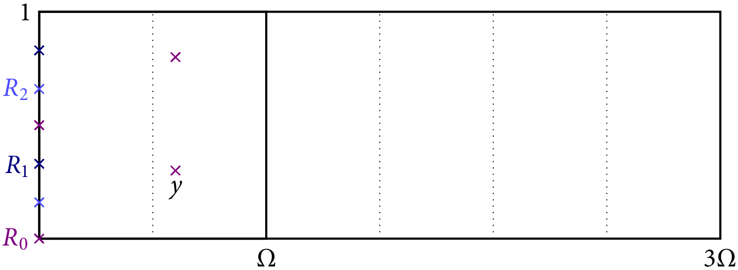
$$\widehat{\pi}(y) = \ell . x$$

The contragredient isogeny [LR10a]

$$\begin{tikzcd}
x \in A \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & z \in A \\
& y \in B \arrow[ur, "\widehat{\pi}"'] &
\end{tikzcd}$$

Let $\pi : A \to B$ be the isogeny associated to $(a_i)_{i \in Z(\overline{\ell n})}$. Let $y \in B$ and $x \in A$ be one of the ℓ^g antecedents. Then

$$\widehat{\pi}(y) = \ell.x$$

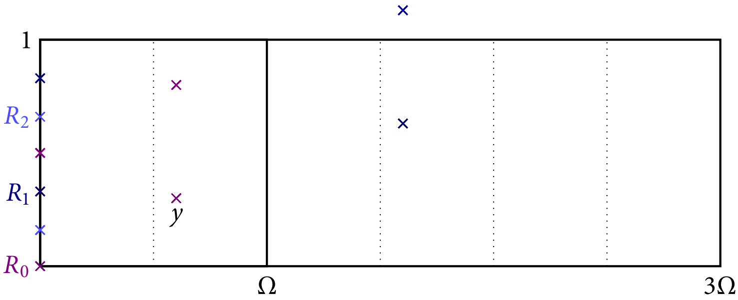


The contragredient isogeny [LR10a]

$$\begin{tikzcd}
x \in A \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & z \in A \\
& y \in B \arrow[ur, "\widehat{\pi}"'] &
\end{tikzcd}$$

Let $\pi : A \to B$ be the isogeny associated to $(a_i)_{i \in Z(\overline{\ell n})}$. Let $y \in B$ and $x \in A$ be one of the ℓ^g antecedents. Then

$$\widehat{\pi}(y) = \ell . x$$

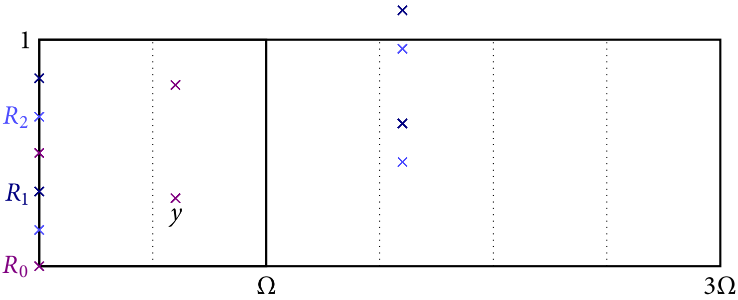


The contragredient isogeny [LR10a]

$$\begin{tikzcd}
x \in A \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & z \in A \\
& y \in B \arrow[ur, "\widehat{\pi}"'] &
\end{tikzcd}$$

Let $\pi : A \to B$ be the isogeny associated to $(a_i)_{i \in Z(\overline{\ell n})}$. Let $y \in B$ and $x \in A$ be one of the ℓ^g antecedents. Then

$$\widehat{\pi}(y) = \ell . x$$

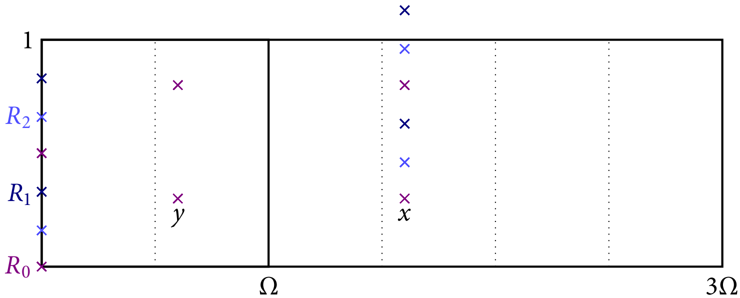


The contragredient isogeny [LR10a]

$$\begin{tikzcd}
x \in A \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & z \in A \\
& y \in B \arrow[ur, "\widehat{\pi}"'] &
\end{tikzcd}$$

Let $\pi : A \to B$ be the isogeny associated to $(a_i)_{i \in Z(\overline{\ell n})}$. Let $y \in B$ and $x \in A$ be one of the ℓ^g antecedents. Then

$$\widehat{\pi}(y) = \ell . x$$



The contragredient isogeny [LR10a]

$$\begin{tikzcd}
x \in A \arrow[rr, "{[\ell]}"] \arrow[dr, "\pi"'] & & z \in A \\
& y \in B \arrow[ur, "\widehat{\pi}"'] &
\end{tikzcd}$$

Let $\pi : A \to B$ be the isogeny associated to $(a_i)_{i \in Z(\overline{\ell n})}$. Let $y \in B$ and $x \in A$ be one of the ℓ^g antecedents. Then

$$\widehat{\pi}(y) = \ell . x$$

Explicit isogenies algorithm

- (Compressed) modular point from K: $g(g+1)/2$ ℓ^{th}-roots and $g(g+1)/2 \cdot O(\log(\ell))$ chain additions.

$\Rightarrow$ (Compressed) isogeny: $g \cdot O(\log(\ell))$ chain additions.

Example

- B: elliptic curve $y^2 = x^3 + 23x + 3$ over $k = \mathbb{F}_{31}$

  $\Rightarrow$ Theta null point of level 4: $(3:1:18:1) \in \mathcal{M}_4(\mathbb{F}_{31})$.

- $K = \{(3:1:18:1), (22:15:4:1), (18:29:23:1)\} \Rightarrow$ modular solution:

  $(3, \eta^{14233}, \eta^{2317}, 1, \eta^{1324}, \eta^{5296}, 18, \eta^{5296}, \eta^{1324}, 1, \eta^{2317}, \eta^{14233})$
  $(\eta^3 + \eta + 28 = 0)$.

- $y = (\eta^{19406}, \eta^{19805}, \eta^{10720}, 1)$; $\quad \widehat{\pi}(y)$?

Example

$$R_1 = (\eta^{1324}, \eta^{5296}, \eta^{2317}, \eta^{14233}) \quad y = (\eta^{19406}, \eta^{19805}, \eta^{10720}, 1)$$

$$y \oplus R_1 = \lambda_1(\eta^{2722}, \eta^{28681}, \eta^{26466}, \eta^{2096})$$

Example

$$R_1 = (\eta^{1324}, \eta^{5296}, \eta^{2317}, \eta^{14233}) \quad y = (\eta^{19406}, \eta^{19805}, \eta^{10720}, 1)$$

$$y \oplus R_1 = \lambda_1(\eta^{2722}, \eta^{28681}, \eta^{26466}, \eta^{2096})$$

$$y + 2R_1 = \lambda_1^2(\eta^{28758}, \eta^{11337}, \eta^{27602}, \eta^{22972})$$

$$y + 3R_1 = \lambda_1^3(\eta^{18374}, \eta^{18773}, \eta^{9688}, \eta^{28758}) = y/\eta^{1032} \quad \text{so } \lambda_1^3 = \eta^{28758}$$

Example

$$R_1 = (\eta^{1324}, \eta^{5296}, \eta^{2317}, \eta^{14233}) \quad y = (\eta^{19406}, \eta^{19805}, \eta^{10720}, 1)$$

$$y \oplus R_1 = \lambda_1(\eta^{2722}, \eta^{28681}, \eta^{26466}, \eta^{2096})$$

$$y + 2R_1 = \lambda_1^2(\eta^{28758}, \eta^{11337}, \eta^{27602}, \eta^{22972})$$

$$y + 3R_1 = \lambda_1^3(\eta^{18374}, \eta^{18773}, \eta^{9688}, \eta^{28758}) = y/\eta^{1032} \quad \text{so } \lambda_1^3 = \eta^{28758}$$

$$2y + R_1 = \lambda_1^2(\eta^{17786}, \eta^{12000}, \eta^{16630}, \eta^{365})$$

$$3y + R_1 = \lambda_1^3(\eta^{7096}, \eta^{11068}, \eta^{8089}, \eta^{20005}) = \eta^{5772} R_1$$

Example

$$R_1 = (\eta^{1324}, \eta^{5296}, \eta^{2317}, \eta^{14233}) \quad y = (\eta^{19406}, \eta^{19805}, \eta^{10720}, 1)$$

$$y \oplus R_1 = \lambda_1(\eta^{2722}, \eta^{28681}, \eta^{26466}, \eta^{2096})$$

$$y + 2R_1 = \lambda_1^2(\eta^{28758}, \eta^{11337}, \eta^{27602}, \eta^{22972})$$

$$y + 3R_1 = \lambda_1^3(\eta^{18374}, \eta^{18773}, \eta^{9688}, \eta^{28758}) = y/\eta^{1032} \quad \text{so } \lambda_1^3 = \eta^{28758}$$

$$2y + R_1 = \lambda_1^2(\eta^{17786}, \eta^{12000}, \eta^{16630}, \eta^{365})$$

$$3y + R_1 = \lambda_1^3(\eta^{7096}, \eta^{11068}, \eta^{8089}, \eta^{20005}) = \eta^{5772} R_1$$

$$\widehat{\pi}(y) = (3, \eta^{21037}, \eta^{15925}, 1, \eta^{8128}, \eta^{18904}, 18, \eta^{12100}, \eta^{14932}, 1, \eta^{9121}, \eta^{27841})$$

Changing level by taking an isogeny

$$
\begin{tikzcd}
B \arrow[dd, "{[\ell]}"'] \arrow[dr, "\widehat{\pi}"] & & \\
& A, A[\ell] = A[\ell]_1 \oplus A[\ell]_2 \arrow[dl, "\pi"] \arrow[d, equal] \arrow[dr, "\pi_2"] & \\
B = A/A[\ell]_2 & A & C = A/A[\ell]_1
\end{tikzcd}
$$

- $\pi_2 \circ \widehat{\pi}$: ℓ^2 isogeny in level n.
- Modular points (corresponding to K) $\Leftrightarrow A[\ell] = A[\ell]_1 \oplus \widehat{\pi}(B[\ell])$
  $\Leftrightarrow \ell^2$-isogenies $B \to C$.

Changing level by taking an isogeny

$$
\begin{tikzcd}
B \arrow[dr, "\widehat{\pi}"] \arrow[dd, "{[\ell]}"'] & & \\
& A, A[\ell] = A[\ell]_1 \oplus A[\ell]_2 \arrow[dl, "\pi"'] \arrow[d, equal] \arrow[dr, "\pi_2"] & \\
B = A/A[\ell]_2 & A & C = A/A[\ell]_1
\end{tikzcd}
$$

- $\pi_2 \circ \widehat{\pi}$: ℓ^2 isogeny in level n.
- Modular points (corresponding to K) $\Leftrightarrow A[\ell] = A[\ell]_1 \oplus \widehat{\pi}(B[\ell])$
  $\Leftrightarrow \ell^2$-isogenies $B \to C$.

Changing level without taking isogenies

Theorem (Koizumi-Kempf)

- *Let $\mathcal{L}$ be the space of theta functions of level ℓn and $\mathcal{L}'$ the space of theta functions of level n.*
- *Let $F \in \mathrm{M}_r(\mathbb{Z})$ be such that ${}^t F F = \ell \,\mathrm{Id}$, and $f : A^r \to A^r$ the corresponding isogeny.*

We have $\mathcal{L} = f^* \mathcal{L}'$ and the isogeny f is given by

$$f^*(\vartheta_{i_1}^{\mathcal{L}'} \star \ldots \star \vartheta_{i_r}^{\mathcal{L}'}) = \lambda \sum_{\substack{(j_1,\ldots,j_r) \in K_1(\mathcal{L}') \times \ldots \times K_1(\mathcal{L}') \\ f(j_1,\ldots,j_r) = (i_1,\ldots,i_r)}} \vartheta_{j_1}^{\mathcal{L}} \star \ldots \star \vartheta_{j_r}^{\mathcal{L}}$$

- $F = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ gives the Riemann relations. (For general ℓ, use the quaternions.)

$\Rightarrow$ Go up and down in level without taking isogenies [Cosset+R].

A complete generalisation of Vélu's algorithm [Cosset+R]

- Compute the isogeny $B \to A$ while staying in level n.
- No need of ℓ-roots. Need only $O(\#K)$ differential additions in B + $O(\ell^g)$ or $O(\ell^{2g})$ multiplications $\Rightarrow$ fast.
- The formulas are rational if the kernel K is rational.

- Blocking part: compute $K \Rightarrow$ compute all the ℓ-torsion on B. $g = 2$: ℓ-torsion, $\widetilde{O}(\ell^6)$ vs $O(\ell^2)$ or $O(\ell^4)$ for the isogeny.

$\Rightarrow$ Work in level 2.

$\Rightarrow$ Convert back and forth to Mumford coordinates:

$$\begin{tikzcd}
B \arrow[r, "\widehat{\pi}"] \arrow[d, equal] & A \arrow[d, equal] \\
\mathrm{Jac}(C_1) \arrow[r, dotted] & \mathrm{Jac}(C_2)
\end{tikzcd}$$

Avisogenies

- Avisogenies: Magma code written by Bisson, Cosset and R.
- Released under LGPL 2+.
- Implement isogeny computation (and applications thereof) for abelian varieties using theta functions.
- Current alpha release: isogenies in genus 2.

Implementation

H hyperelliptic curve of genus 2 over $k = \mathbb{F}_q$, $J = \mathrm{Jac}(H)$, ℓ odd prime, $2\ell \wedge \mathrm{car}\, k = 1$. Compute all rational (ℓ, ℓ)-isogenies $J \mapsto \mathrm{Jac}(H')$ (we suppose the zeta function known):

1. Compute the extension $\mathbb{F}_{q^n}$ where the geometric points of the maximal isotropic kernel of $J[\ell]$ lives.
2. Compute a "symplectic" basis of $J[\ell](\mathbb{F}_{q^n})$.
3. Find the rational maximal isotropic kernels K.
4. For each kernel K, convert its basis from Mumford to theta coordinates of level 2. (Rosenhain then Thomae).
5. Compute the other points in K in theta coordinates using differential additions.
6. Apply the change level formula to recover the theta null point of J/K.
7. Compute the Igusa invariants of J/K ("Inverse Thomae").
8. Distinguish between the isogeneous curve and its twist.

Implementation

H hyperelliptic curve of genus 2 over $k = \mathbb{F}_q$, $J = \mathrm{Jac}(H)$, ℓ odd prime, $2\ell \wedge \mathrm{car}\, k = 1$. Compute all rational (ℓ, ℓ)-isogenies $J \mapsto \mathrm{Jac}(H')$ (we suppose the zeta function known):

1. Compute the extension $\mathbb{F}_{q^n}$ where the geometric points of the maximal isotropic kernel of $J[\ell]$ lives.
2. Compute a "symplectic" basis of $J[\ell](\mathbb{F}_{q^n})$.
3. Find the rational maximal isotropic kernels K.
4. For each kernel K, convert its basis from Mumford to theta coordinates of level 2. (Rosenhain then Thomae).
5. Compute the other points in K in theta coordinates using differential additions.
6. Apply the change level formula to recover the theta null point of J/K.
7. Compute the Igusa invariants of J/K ("Inverse Thomae").
8. Distinguish between the isogeneous curve and its twist.

Implementation

H hyperelliptic curve of genus 2 over $k = \mathbb{F}_q$, $J = \mathrm{Jac}(H)$, ℓ odd prime, $2\ell \wedge \operatorname{car} k = 1$. Compute all rational (ℓ,ℓ)-isogenies $J \mapsto \mathrm{Jac}(H')$ (we suppose the zeta function known):

1. Compute the extension $\mathbb{F}_{q^n}$ where the geometric points of the maximal isotropic kernel of $J[\ell]$ lives.
2. Compute a "symplectic" basis of $J[\ell](\mathbb{F}_{q^n})$.
3. Find the rational maximal isotropic kernels K.
4. For each kernel K, convert its basis from Mumford to theta coordinates of level 2. (Rosenhain then Thomae).
5. Compute the other points in K in theta coordinates using differential additions.
6. Apply the change level formula to recover the theta null point of J/K.
7. Compute the Igusa invariants of J/K ("Inverse Thomae").
8. Distinguish between the isogeneous curve and its twist.

Implementation

H hyperelliptic curve of genus 2 over $k = \mathbb{F}_q$, $J = \mathrm{Jac}(H)$, ℓ odd prime, $2\ell \wedge \operatorname{car} k = 1$. Compute all rational (ℓ, ℓ)-isogenies $J \mapsto \mathrm{Jac}(H')$ (we suppose the zeta function known):

1. Compute the extension $\mathbb{F}_{q^n}$ where the geometric points of the maximal isotropic kernel of $J[\ell]$ lives.
2. Compute a ‘‘symplectic’’ basis of $J[\ell](\mathbb{F}_{q^n})$.
3. Find the rational maximal isotropic kernels K.
4. For each kernel K, convert its basis from Mumford to theta coordinates of level 2. (Rosenhain then Thomae).
5. Compute the other points in K in theta coordinates using differential additions.
6. Apply the change level formula to recover the theta null point of J/K.
7. Compute the Igusa invariants of J/K (‘‘Inverse Thomae’’).
8. Distinguish between the isogeneous curve and its twist.

Implementation

H hyperelliptic curve of genus 2 over $k = \mathbb{F}_q$, $J = \mathrm{Jac}(H)$, ℓ odd prime, $2\ell \wedge \mathrm{car}\, k = 1$. Compute all rational (ℓ, ℓ)-isogenies $J \mapsto \mathrm{Jac}(H')$ (we suppose the zeta function known):

1. Compute the extension $\mathbb{F}_{q^n}$ where the geometric points of the maximal isotropic kernel of $J[\ell]$ lives.
2. Compute a "symplectic" basis of $J[\ell](\mathbb{F}_{q^n})$.
3. Find the rational maximal isotropic kernels K.
4. For each kernel K, convert its basis from Mumford to theta coordinates of level 2. (Rosenhain then Thomae).
5. Compute the other points in K in theta coordinates using differential additions.
6. Apply the change level formula to recover the theta null point of J/K.
7. Compute the Igusa invariants of J/K ("Inverse Thomae").
8. Distinguish between the isogeneous curve and its twist.

Implementation

H hyperelliptic curve of genus 2 over $k = \mathbb{F}_q$, $J = \mathrm{Jac}(H)$, ℓ odd prime, $2\ell \wedge \operatorname{car} k = 1$. Compute all rational (ℓ, ℓ)-isogenies $J \mapsto \mathrm{Jac}(H')$ (we suppose the zeta function known):

1. Compute the extension $\mathbb{F}_{q^n}$ where the geometric points of the maximal isotropic kernel of $J[\ell]$ lives.
2. Compute a "symplectic" basis of $J[\ell](\mathbb{F}_{q^n})$.
3. Find the rational maximal isotropic kernels K.
4. For each kernel K, convert its basis from Mumford to theta coordinates of level 2. (Rosenhain then Thomae).
5. Compute the other points in K in theta coordinates using differential additions.
6. Apply the change level formula to recover the theta null point of J/K.
7. Compute the Igusa invariants of J/K ("Inverse Thomae").
8. Distinguish between the isogeneous curve and its twist.

Implementation

H hyperelliptic curve of genus 2 over $k = \mathbb{F}_q$, $J = \mathrm{Jac}(H)$, ℓ odd prime, $2\ell \wedge \mathrm{car}\, k = 1$. Compute all rational (ℓ, ℓ)-isogenies $J \mapsto \mathrm{Jac}(H')$ (we suppose the zeta function known):

1. Compute the extension $\mathbb{F}_{q^n}$ where the geometric points of the maximal isotropic kernel of $J[\ell]$ lives.
2. Compute a "symplectic" basis of $J[\ell](\mathbb{F}_{q^n})$.
3. Find the rational maximal isotropic kernels K.
4. For each kernel K, convert its basis from Mumford to theta coordinates of level 2. (Rosenhain then Thomae).
5. Compute the other points in K in theta coordinates using differential additions.
6. Apply the change level formula to recover the theta null point of J/K.
7. Compute the Igusa invariants of J/K ("Inverse Thomae").
8. Distinguish between the isogeneous curve and its twist.

Implementation

H hyperelliptic curve of genus 2 over $k = \mathbb{F}_q$, $J = \mathrm{Jac}(H)$, ℓ odd prime, $2\ell \wedge \operatorname{car} k = 1$. Compute all rational (ℓ, ℓ)-isogenies $J \mapsto \mathrm{Jac}(H')$ (we suppose the zeta function known):

1. Compute the extension $\mathbb{F}_{q^n}$ where the geometric points of the maximal isotropic kernel of $J[\ell]$ lives.
2. Compute a "symplectic" basis of $J[\ell](\mathbb{F}_{q^n})$.
3. Find the rational maximal isotropic kernels K.
4. For each kernel K, convert its basis from Mumford to theta coordinates of level 2. (Rosenhain then Thomae).
5. Compute the other points in K in theta coordinates using differential additions.
6. Apply the change level formula to recover the theta null point of J/K.
7. Compute the Igusa invariants of J/K ("Inverse Thomae").
8. Distinguish between the isogeneous curve and its twist.

Implementation

H hyperelliptic curve of genus 2 over $k = \mathbb{F}_q$, $J = \mathrm{Jac}(H)$, ℓ odd prime, $2\ell \wedge \mathrm{car}\, k = 1$. Compute all rational (ℓ, ℓ)-isogenies $J \mapsto \mathrm{Jac}(H')$ (we suppose the zeta function known):

1. Compute the extension $\mathbb{F}_{q^n}$ where the geometric points of the maximal isotropic kernel of $J[\ell]$ lives.
2. Compute a "symplectic" basis of $J[\ell](\mathbb{F}_{q^n})$.
3. Find the rational maximal isotropic kernels K.
4. For each kernel K, convert its basis from Mumford to theta coordinates of level 2. (Rosenhain then Thomae).
5. Compute the other points in K in theta coordinates using differential additions.
6. Apply the change level formula to recover the theta null point of J/K.
7. Compute the Igusa invariants of J/K ("Inverse Thomae").
8. Distinguish between the isogeneous curve and its twist.

Computing the right extension

- $J = \mathrm{Jac}(H)$ abelian variety of dimension 2. $\chi(X)$ the corresponding zeta function.
- Degree of a point of ℓ-torsion | the order of X in $\mathbb{F}_\ell[X]/\chi(X)$.
- If K rational, $K(\overline{k}) \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$, the degree of a point in K | the LCM of orders of X in $\mathbb{F}_\ell[X]/P(X)$ for $P \mid \chi$ of degree two.
- Since we are looking to K maximal isotropic, $J[\ell] \simeq K \oplus K'$ and we know that $P \mid \chi$ is such that $\chi(X) \equiv P(X)P(\overline{X}) \mod \ell$ where $\overline{X} = q/X$ represents the Verschiebung.

Remark

The degree n is $\leqslant \ell^2 - 1$. If ℓ is totally split in $\mathbb{Z}[\pi, \overline{\pi}]$ then $n \mid \ell - 1$.

Computing the ℓ-torsion

- We want to compute $J(\mathbb{F}_{q^n})[\ell]$.
- From the zeta function $\chi(X)$ we can compute random points in $J(\mathbb{F}_{q^n})[\ell^\infty]$ uniformly.
- If P is in $J(\mathbb{F}_{q^n})[\ell^\infty]$, $\ell^m P \in J(\mathbb{F}_{q^n})[\ell]$ for a suitable m. This does not give uniform points of ℓ-torsion but we can correct the points obtained.

Example

- Suppose $J(\mathbb{F}_{q^n})[\ell^\infty] =< P_1, P_2 >$ with P_1 of order ℓ^2 and P_2 of order ℓ.
- First random point $Q_1 = P_1 \Rightarrow$ we recover the point of ℓ-torsion: $\ell.P_1$.
- Second random point $Q_2 = \alpha P_1 + \beta P_2$. If $\alpha \neq 0$ we recover the point of ℓ-torsion $\alpha \ell P_1$ which is not a new generator.
- We correct the original point: $Q_2' = Q_2 - \alpha Q_1 = \beta P_2$.

Weil pairing

- Used to decompose a point $P \in J[\ell]$ in term of a basis of the ℓ-torsion (and to construct a symplectic basis).
- The magma implementation is **extremely** slow in genus 2 for non degenerate divisors.
- But since we convert the points in theta coordinates we can use the pairing in theta coordinates [LR10b].

Timings for isogenies computations ($\ell = 7$)

```
Jacobian of Hyperelliptic Curve defined by y^2 = t^254*x^6 + t^223*x^5 +
  t^255*x^4 + t^318*x^3 + t^668*x^2 + t^543*x + t^538 over GF(3^6)
> time RationallyIsogenousCurvesG2(J,7);
** Computing  7 -rationnal isotropic subgroups
  -- Computing the 7 -torsion over extension of deg 4
  !! Basis: 2 points in Finite field of size 3^24
  -- Listing subgroups
  1 subgroups over Finite field of size 3^24
  -- Convert the subgroups to theta coordinates
  Time: 0.060
Computing the 1 7 -isogenies
  ** Precomputations for l= 7 Time: 0.180
  ** Computing the 7 -isogeny
    Computing the l-torsion Time: 0.030
    Changing level Time: 0.210
  Time: 0.430
Time: 0.490
[ <[ t^620, t^691, t^477 ], Jacobian of Hyperelliptic Curve defined by
y^2 = t^615*x^6 + t^224*x^5 + t^37*x^4 + t^303*x^3 + t^715*x^2 + t^128*x
```

Timings for isogenies computations $(\ell = 5)$

```
Jacobian of Hyperelliptic Curve defined by y^2 = 39*x^6 + 4*x^5 + 82*x^4
  + 10*x^3 + 31*x^2 + 39*x + 2 over GF(83)
> time RationallyIsogenousCurvesG2(J,5);
** Computing  5 -rationnal isotropic subgroups
  -- Computing the 5 -torsion over extension of deg 24
  Time: 0.940
  !! Basis: 4 points in Finite field of size 83^24
  -- Listing subgroups
  Time: 1.170
  6 subgroups over Finite field of size 83^24
  -- Convert the subgroups to theta coordinates
  Time: 0.360
Time: 2.630
Computing the 6 5 -isogenies
Time: 0.820
Time: 3.460
 [ <[ 36, 69, 38 ], Jacobian of Hyperelliptic Curve defined by
 y^2 = 27*x^6 + 63*x^5 + 5*x^4 + 24*x^3 + 34*x^2 + 6*x + 76 over GF(83)>,
   ...]
```

Timings for isogeny graphs $(\ell = 3)$

```
Jacobian of Hyperelliptic Curve defined by y^2 = 41*x^6 + 131*x^5 +
  55*x^4 + 57*x^3 + 233*x^2 + 225*x + 51 over GF(271)
time isograph,jacobians:=IsoGraphG2(J,{3}: save_mem:=-1);
Computed 540 isogenies and found 135 curves.
Time: 14.410
```

- Core 2 with 4BG of RAM.
- Computing kernels: $\approx 5s$.
- Computing isogenies: $\approx 7s$ (Torsion: $\approx 2s$, Changing level: $\approx 3.5s$.)

Going further $(\ell = 53)$

```
Jacobian of Hyperelliptic Curve defined by y^2 = 97*x^6 + 77*x^5 +
  62*x^4 + 14*x^3 + 33*x^2 + 18*x + 40 over GF(113)
> time RationallyIsogenousCurvesG2(J,53);
** Computing  53 -rationnal isotropic subgroups
  -- Computing the 53 -torsion over extension of deg 52 Time: 8.610
  !! Basis: 3 points in Finite field of size 113^52
  -- Listing subgroups Time: 1.210
  2 subgroups over Finite field of size 113^52
  -- Convert the subgroups to theta coordinates Time: 0.100
  Time: 9.980
Computing the 2 53 -isogenies
  ** Precomputations for l= 53 Time: 0.240
  ** Computing the 53 -isogeny
    Computing the l-torsion Time: 7.570
    Changing level Time: 1.170
  Time: 8.840
  ** Computing the 53 -isogeny
  Time: 8.850
Time: 27.950
```

Going further $(\ell = 19)$

```
Jacobian of Hyperelliptic Curve defined by y^2 = 194*x^6 + 554*x^5 +
606*x^4 + 523*x^3 + 642*x^2 + 566*x + 112 over GF(859)
> time RationallyIsogenousCurvesG2(J,19);
** Computing  19 -rationnal isotropic subgroups (extension degree 18)
Time: 0.760
Computing the 2 19 -isogenies
  ** Precomputations for l= 19 Time: 11.160
  ** Computing the 19 -isogeny
    Computing the l-torsion Time: 0.250
    Changing level Time: 18.590
  Time: 18.850
  ** Computing the 19 -isogeny
    Computing the l-torsion Time: 0.250
    Changing level Time: 18.640
  Time: 18.900
Time: 51.060
[ <[ 341, 740, 389 ], Jacobian of Hyperelliptic Curve defined by y^2 = 72
    680*x^5 + 538*x^4 + 613*x^3 + 557*x^2 + 856*x + 628 over GF(859)>,
  ... ]
```

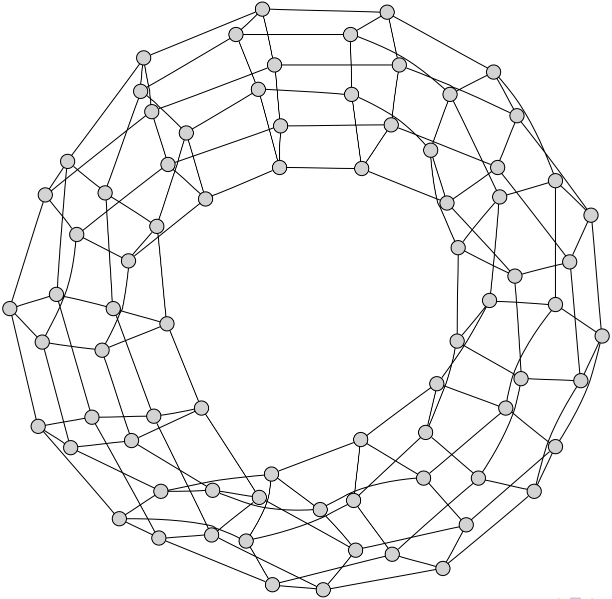
A record isogeny computation! ($\ell = 1321$)

- J Jacobian of $y^2 = x^5 + 41691x^4 + 24583x^3 + 2509x^2 + 15574x$ over $\mathbb{F}_{42179}$.
- $\#J = 2^{10} 1321^2$.

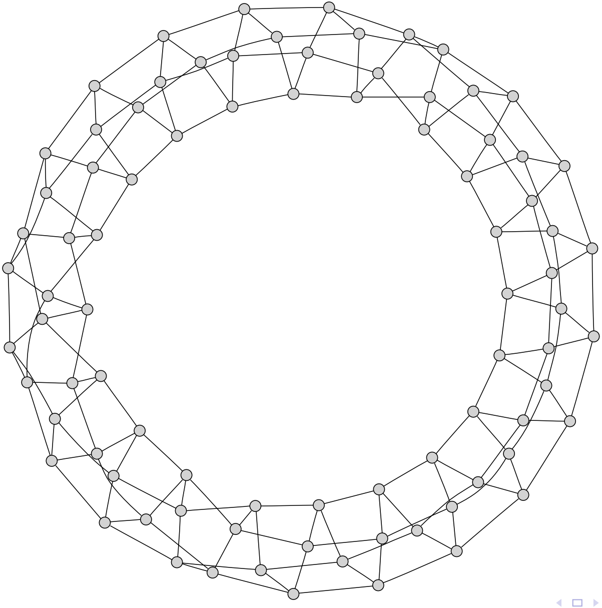
```
> time RationallyIsogenousCurvesG2(J,1321:ext_degree:=1);
** Computing  1321 -rationnal isotropic subgroups
Time: 0.350
Computing the 1 1321 -isogenies
  ** Precomputations for l= 1321
  Time: 1276.950
  ** Computing the 1321 -isogeny
    Computing the l-torsion
    Time: 1200.270
    Changing level
    Time: 1398.780
  Time: 5727.250
Time: 7004.240
Time: 7332.650
[ <[ 9448, 15263, 31602 ], Jacobian of Hyperelliptic Curve defined by
  y^2 = 33266*x^6 + 20155*x^5 + 31203*x^4 + 9732*x^3 +
  4204*x^2 + 18026*x + 29732 over GF(42179)> ]
```

- Core 2 with 32GB of RAM

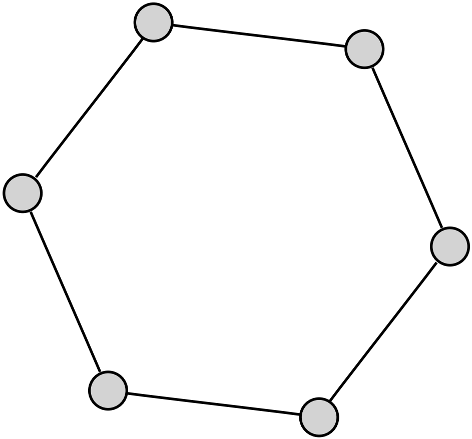
Isogeny graphs: $\ell = q_1 q_2 = \mathfrak{Q}_1\overline{\mathfrak{Q}_1}\mathfrak{Q}_2\overline{\mathfrak{Q}_2}$ $(\mathbb{Q} \mapsto K_0 \mapsto K)$



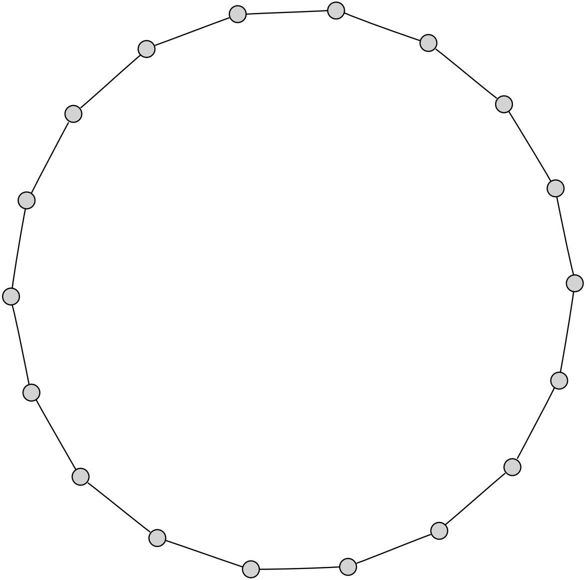
Isogeny graphs: $\ell = q_1 q_2 = Q_1 \overline{Q_1} Q_2 \overline{Q_2}$ $(\mathbb{Q} \mapsto K_0 \mapsto K)$



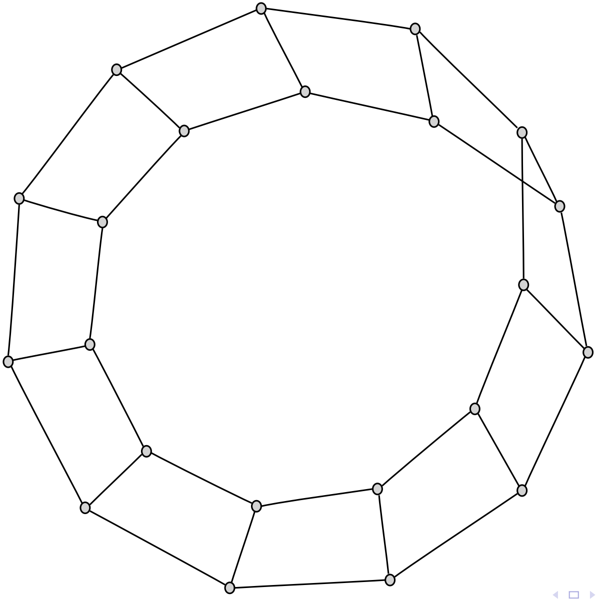
Isogeny graphs: $\ell = q = \mathfrak{Q}\overline{\mathfrak{Q}}$ $(\mathbb{Q} \mapsto K_0 \mapsto K)$



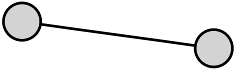
Isogeny graphs: $\ell = q_1 q_2 = Q_1 \overline{Q}_1 Q_2^2$ $(\mathbb{Q} \mapsto K_0 \mapsto K)$



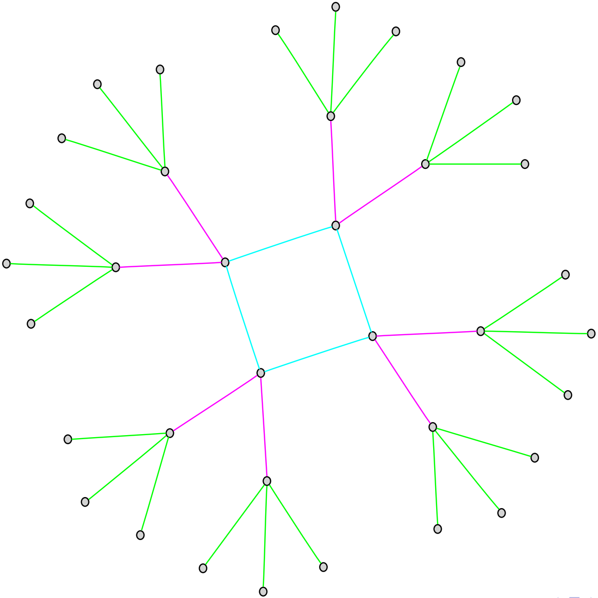
Isogeny graphs: $\ell = q^2 = Q^2\overline{Q}^2$ $(\mathbb{Q} \mapsto K_0 \mapsto K)$



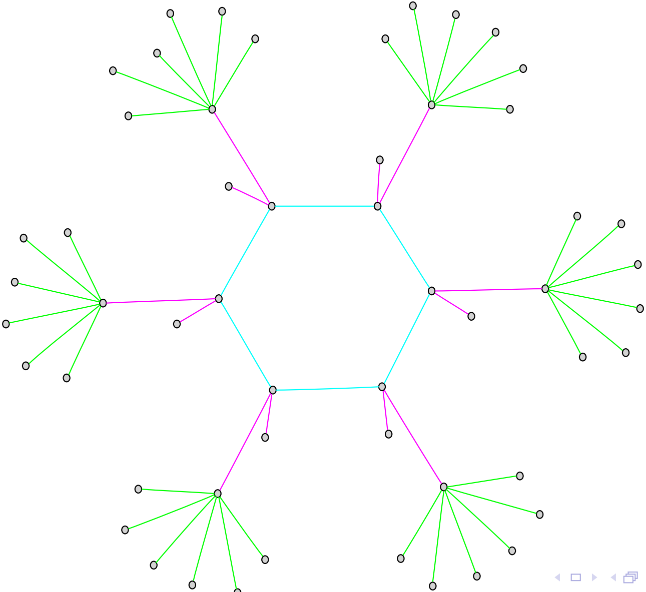
Isogeny graphs: $\ell = q^2 = Q^4$ $(\mathbb{Q} \mapsto K_0 \mapsto K)$

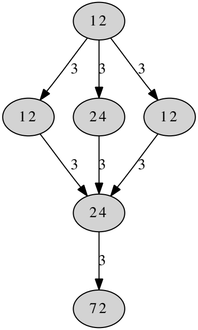


Non maximal isogeny graphs ($\ell = q = Q\overline{Q}$)

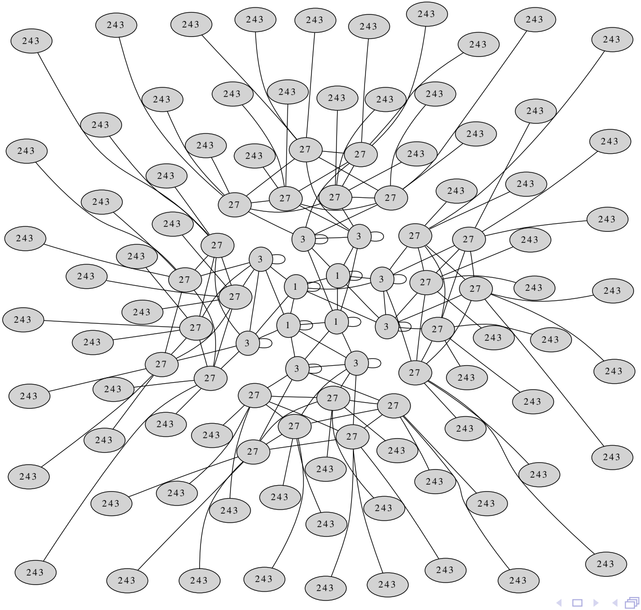


Non maximal isogeny graphs ($\ell = q = Q\overline{Q}$)

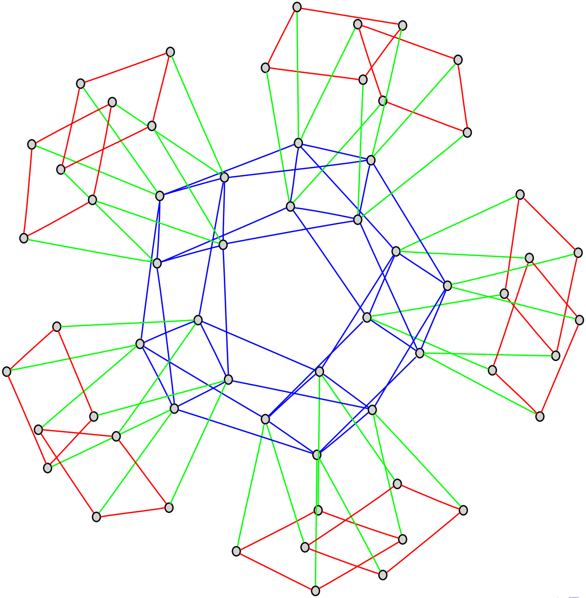




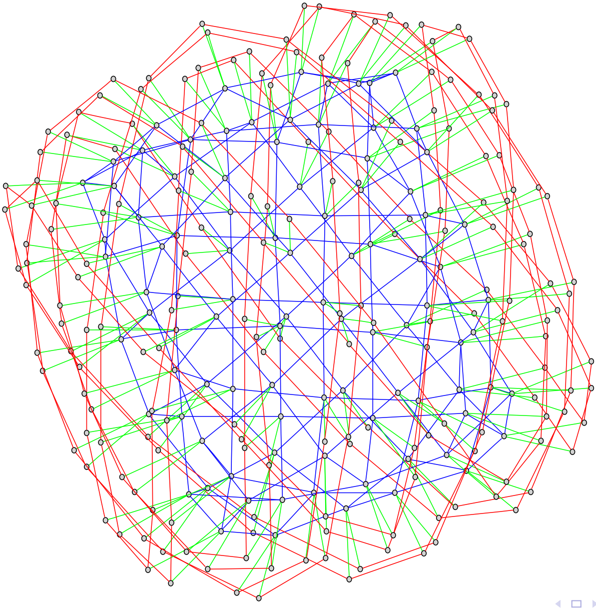
Non maximal isogeny graphs ($\ell = q = Q\overline{Q}$)



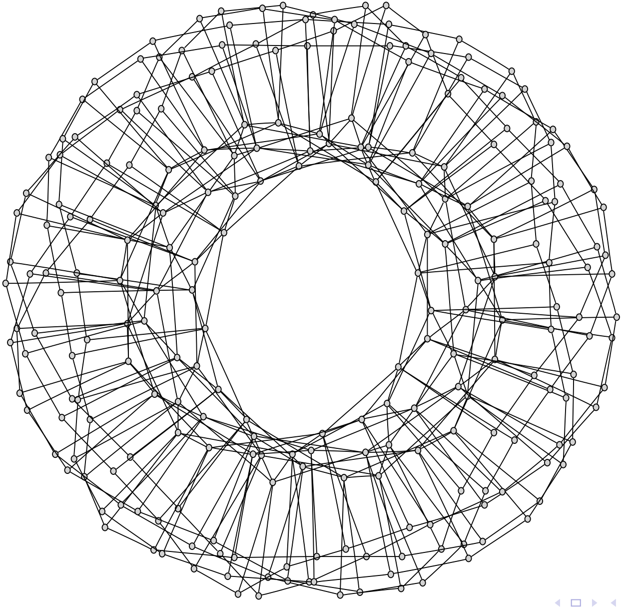
Non maximal isogeny graphs ($\ell = q_1 q_2 = Q_1\overline{Q_1}Q_2\overline{Q_2}$)



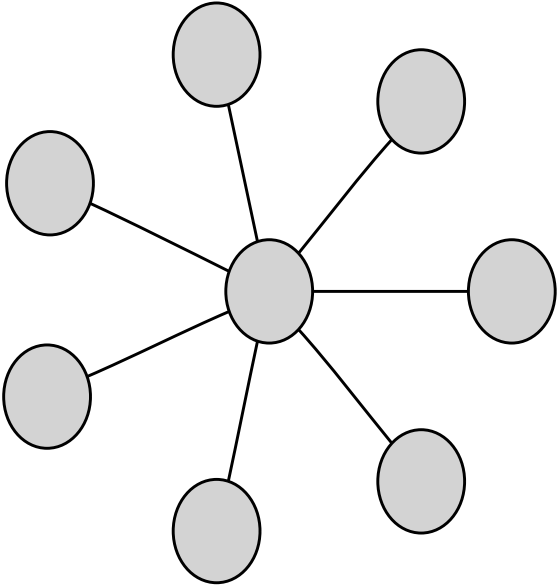
Non maximal isogeny graphs ($\ell = q_1 q_2 = Q_1\overline{Q_1}Q_2\overline{Q_2}$)



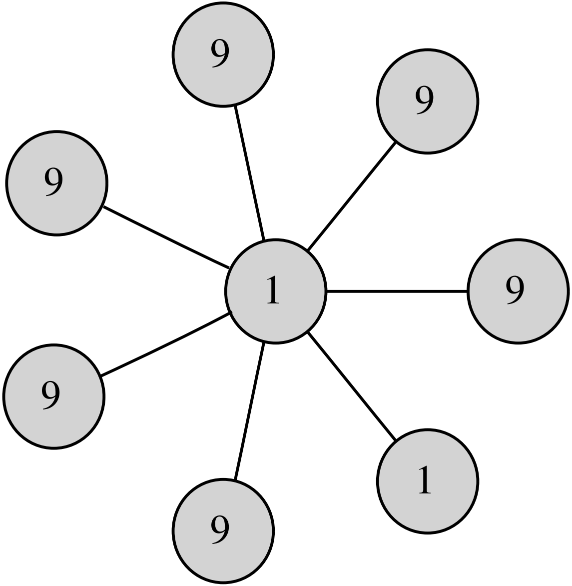
Non maximal isogeny graphs ($\ell = q_1 q_2 = Q_1\overline{Q_1}Q_2\overline{Q_2}$)



Non maximal isogeny graphs ($\ell = q = Q^2$)



Non maximal isogeny graphs ($\ell = q = Q^2$)



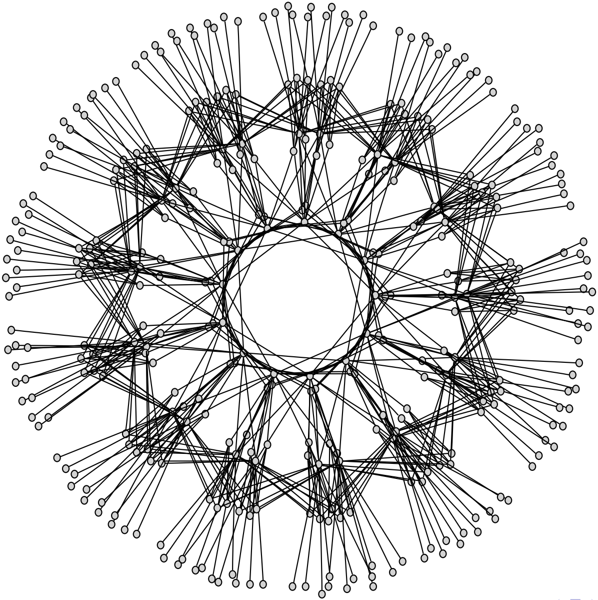
Applications of isogenies to higher genus

- Computing endomorphism ring. Generalize [BS09] to higher genus, work by Bisson.
- Class polynomials in genus 2 using the CRT. If K is a CM field and $J/\mathbb{F}_p$ is such that $\mathrm{End}(J) \otimes_{\mathbb{Z}} \mathbb{Q} = K$, use isogenies to find the Jacobians whose endomorphism ring is O_K. Work by Lauter+R.
- Modular polynomials in genus 2 using theta null points: computed by Gruenewald using analytic methods for $\ell = 3$.

Question

How to compute $(\ell, 1)$-isogenies in genus 2?

Thank you for your attention!



Bibliography

[BS09] G. Bisson and A.V. Sutherland. "Computing the endomorphism ring of an ordinary elliptic curve over a finite field". In: *Journal of Number Theory* (2009). (Cit. on p. 70).

[FLR09] Jean-Charles Faugère, David Lubicz, and Damien Robert. *Computing modular correspondences for abelian varieties*. May 2009. arXiv: 0910.4668. (Cit. on pp. 17–19).

[LR10a] David Lubicz and Damien Robert. *Computing isogenies between abelian varieties*. Jan. 2010. arXiv: 1001.2016. (Cit. on pp. 20–27).

[LR10b] David Lubicz and Damien Robert. *Efficient pairing computation with theta functions*. Ed. by Guillaume Hanrot, François Morain, and Emmanuel Thomé. 9th International Symposium, Nancy, France, ANTS-IX, July 19-23, 2010, Proceedings. Jan. 2010. URL: http://www.normalesup.org/~robert/pro/publications/articles/pairings.pdf. (Cit. on p. 49).

[Smi09] Benjamin Smith. *Isogenies and the Discrete Logarithm Problem in Jacobians of Genus 3 Hyperelliptic Curves*. Feb. 2009. arXiv: 0806.2995. (Cit. on pp. 11, 12).