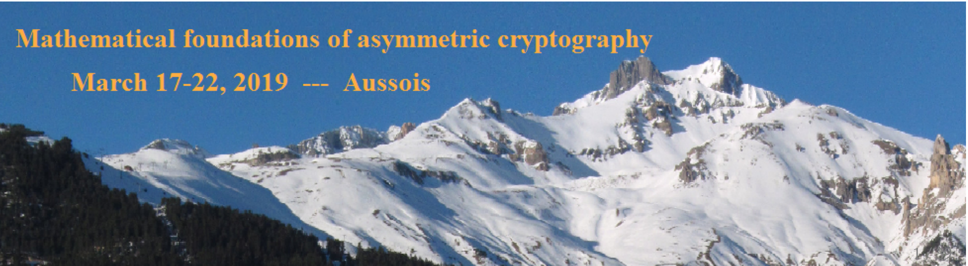
Cryptographic applications of isogeny graphs of genus 2 and 3 curves

Chloe Martindale
www.martindale.info
Eindhoven University of Technology



Raising the dimension: abelian varieties

- Elliptic curves are one-dimensional principally polarised[1] abelian varieties with a point (given by the group identity).

[1] Read: has equations + more later.
[2] DLPs = Discrete Logarithm Problems

Raising the dimension: abelian varieties

- Elliptic curves are one-dimensional principally polarised[1] abelian varieties with a point (given by the group identity).
- To any algebraic curve C we can associate an principally polarised abelian variety called the Jacobian $\mathrm{Jac}(C)$ of C.

[1] Read: has equations + more later.

[2] DLPs = Discrete Logarithm Problems

Raising the dimension: abelian varieties

- Elliptic curves are one-dimensional principally polarised[1] abelian varieties with a point (given by the group identity).
- To any algebraic curve C we can associate an principally polarised abelian variety called the Jacobian $\mathrm{Jac}(C)$ of C.
- There exists a group law on an abelian variety.
  $\rightsquigarrow$ can study DLPs[2] on the group of points.

---

[1] Read: has equations + more later.
[2] DLPs = Discrete Logarithm Problems

Raising the dimension: abelian varieties

- Elliptic curves are one-dimensional principally polarised[1] abelian varieties with a point (given by the group identity).
- To any algebraic curve C we can associate an principally polarised abelian variety called the Jacobian $\mathrm{Jac}(C)$ of C.
- There exists a group law on an abelian variety.
  $\rightsquigarrow$ can study DLPs[2] on the group of points.
- Dimension 1, 2, and 3 principally polarised abelian varieties are all given by Jacobians of curves.

[1] Read: has equations + more later.
[2] DLPs = Discrete Logarithm Problems

Raising the dimension: abelian varieties

Dimension 1, 2, and 3 principally polarised abelian varieties are all given by Jacobians of curves $\mathrm{Jac}(C)$.

Dimension one :

$$C/k : y^2 = f(x),$$

where $f(x) \in k[x]$ and $\deg(f) = 3$.

Raising the dimension: abelian varieties

Dimension 1, 2, and 3 principally polarised abelian varieties are all given by Jacobians of curves $\mathrm{Jac}(C)$.

Dimension one (if $\mathrm{char}(k) \neq 2$):

$$C/k : y^2 = f(x),$$

where $f(x) \in k[x]$ and $\deg(f) = 3$.

Raising the dimension: abelian varieties

Dimension 1, 2, and 3 principally polarised abelian varieties are all given by Jacobians of curves $\mathrm{Jac}(C)$.

Dimension two (if $\mathrm{char}(k) \neq 2$):

$$C/k : y^2 = f(x),$$

where $f(x) \in k[x]$ and $\deg(f) = 5$ or 6.

Raising the dimension: abelian varieties

Dimension 1, 2, and 3 principally polarised abelian varieties are all given by Jacobians of curves $\mathrm{Jac}(C)$.

Dimension three (if $\mathrm{char}(k) \neq 2$):

$$C/k : y^2 = f(x),$$

where $f(x) \in k[x]$ and $\deg(f) = 7$ or 8.

Raising the dimension: abelian varieties

Dimension 1, 2, and 3 principally polarised abelian varieties are all given by Jacobians of curves $\mathrm{Jac}(C)$.

Dimension three (if $\mathrm{char}(k) \neq 2$):

$$C/k : y^2 = f(x),$$

where $f(x) \in k[x]$ and $\deg(f) = 7$ or 8.

OR

$$C/k : f(x, y) = 0,$$

where $f(x, y) \in k[x, y]$ and $\deg(f) = 4$.

Raising the dimension: abelian varieties

Dimension 1, 2, and 3 principally polarised abelian varieties are all given by Jacobians of curves $\mathrm{Jac}(C)$.

Dimension three (if $\mathrm{char}(k) \neq 2$):

$$C/k : y^2 = f(x), \qquad \text{'hyperelliptic'}$$

where $f(x) \in k[x]$ and $\deg(f) = 7$ or 8.

OR

$$C/k : f(x, y) = 0,$$

where $f(x, y) \in k[x, y]$ and $\deg(f) = 4$.

Raising the dimension: abelian varieties

Dimension 1, 2, and 3 principally polarised abelian varieties are all given by Jacobians of curves $\mathrm{Jac}(C)$.

Dimension three (if $\mathrm{char}(k) \neq 2$):

$$C/k : y^2 = f(x), \qquad \text{'hyperelliptic'}$$

where $f(x) \in k[x]$ and $\deg(f) = 7$ or 8.

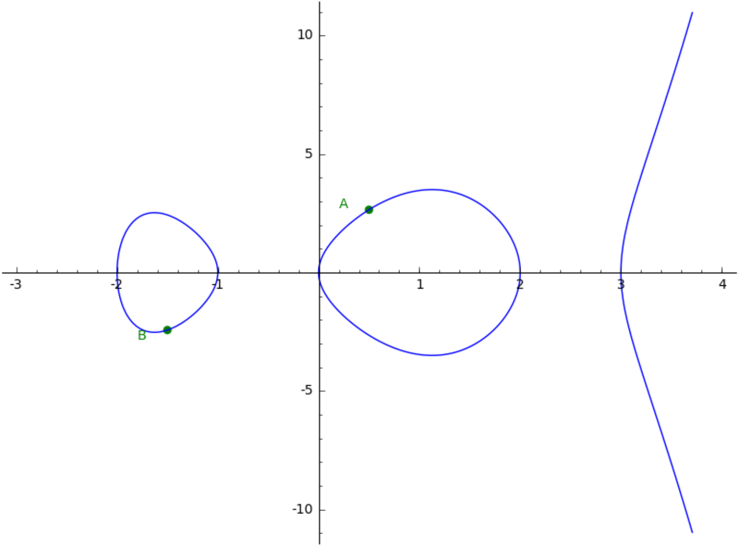
OR

$$C/k : f(x,y) = 0, \qquad \text{'plane quartic'}$$

where $f(x,y) \in k[x,y]$ and $\deg(f) = 4$.

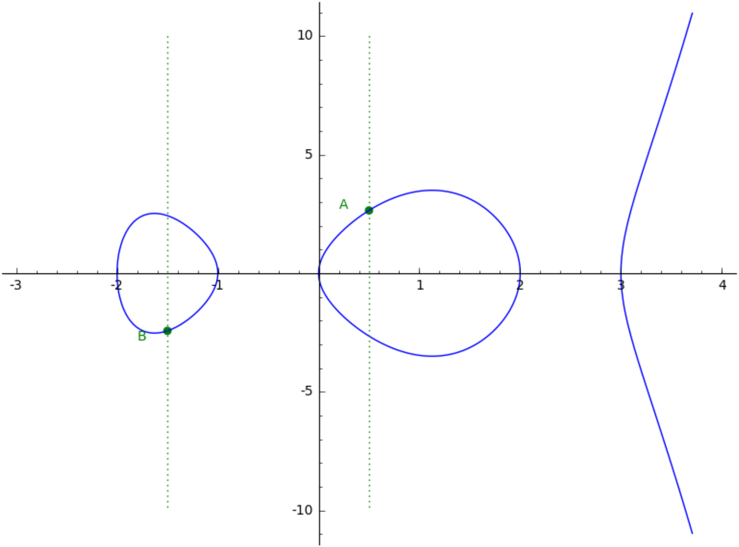
Example: group law in dimension 2

We define a group law on Jacobians of genus 2 curves with pairs of points on the curves.



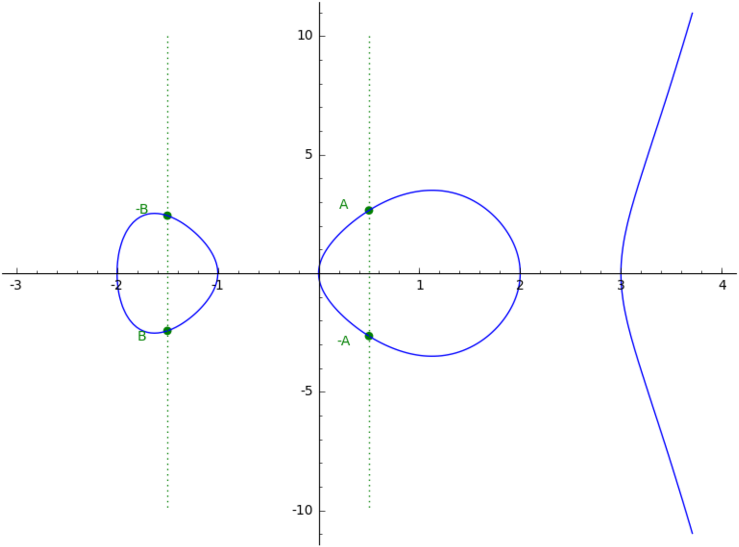
Example: group law in dimension 2

First we define the inverse of $\{A, B\}$:



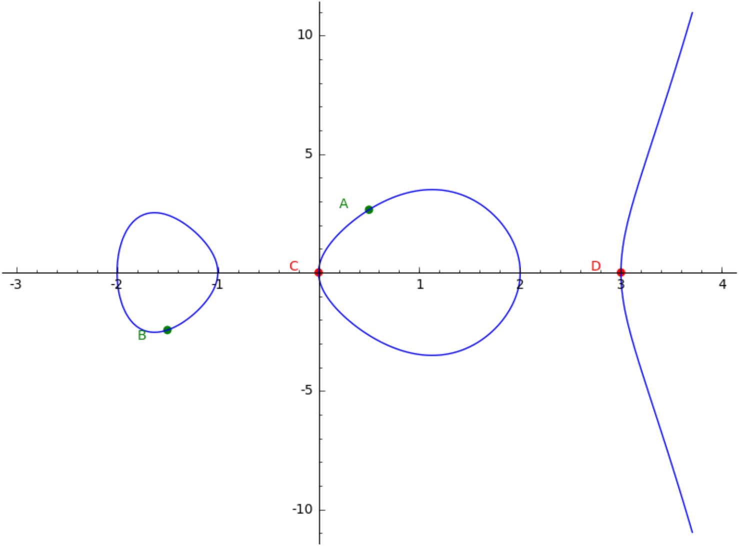
Example: group law in dimension 2

First we define the inverse of $\{A, B\}$: $-\{A, B\} = \{-A, -B\}$



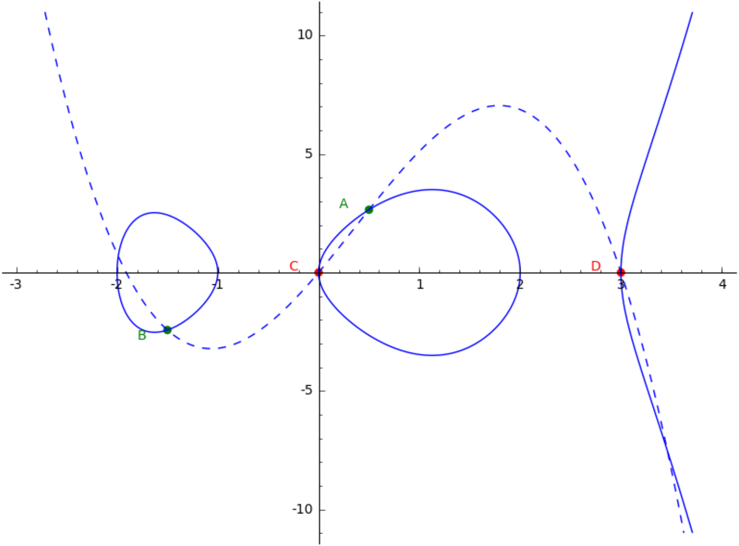
Example: group law in dimension 2

Suppose we have another pair of points $\{C, D\}$:



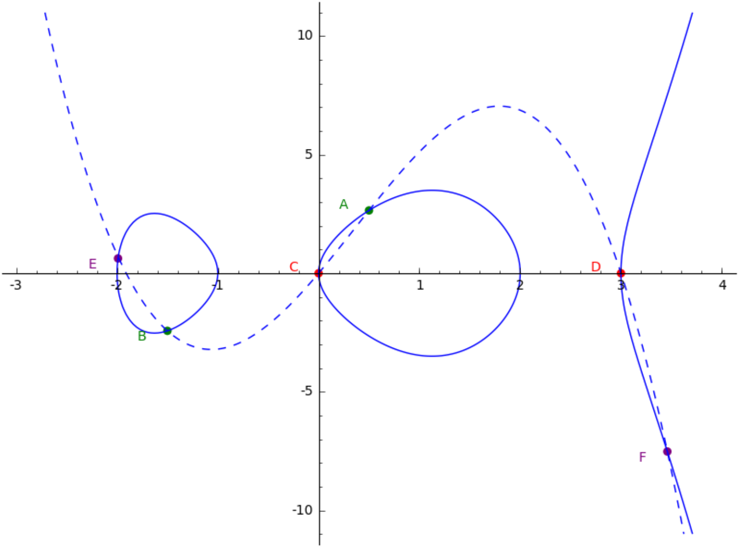
Example: group law in dimension 2

Draw the unique cubic passing through A, B, C, D:



Example: group law in dimension 2

We define $\{A, B\} + \{C, D\} + \{E, F\} = 0$.



Raising the dimension: isogenies

Recall:

Definition

E/k and E'/k elliptic curves. An isogeny

$$f : E \to E'$$

is a surjective morphism with finite kernel that sends the identity to the identity.

Raising the dimension: isogenies

Definition
A/k and A'/k abelian varieties. An isogeny

$$f : A \to A'$$

is a surjective morphism with finite kernel that sends the identity to the identity.

Raising the dimension: isogenies

Recall:

Definition

$f : E \to E'$ an isogeny of elliptic curves $/k$.
This induces an injective morphism of function fields

$$\bar{k}(E') \to \bar{k}(E).$$

The degree of f is

$$\deg(f) = [\bar{k}(E) : \bar{k}(E')].$$

If f is separable then

$$\deg(f) = \#\ker(f).$$

If $\deg(f) = \ell$, we call f an ℓ-isogeny.

Raising the dimension: isogenies

Definition

$f : A \to A'$ an isogeny of abelian varieties $/k$.
This induces an injective morphism of function fields

$$\bar{k}(A') \to \bar{k}(A).$$

The degree of f is

$$\deg(f) = [\bar{k}(A) : \bar{k}(A')].$$

If f is separable then

$$\deg(f) = \#\ker(f).$$

If $\deg(f) = \ell$, we almost call f an ℓ-isogeny. (Need more. . .)

Raising the dimension: isogenies

Recall:

An ℓ-isogeny $f : E \to E'$ has a dual ℓ-isogeny $f^\vee : E' \to E$ such that

$$f \circ f^\vee = f^\vee \circ f = [\ell].^\dagger$$

† $[\ell] : P \to \ell P$ is just multiplication by ℓ

Raising the dimension: isogenies

An ℓ-isogeny $f : E \to E'$ has a dual ℓ-isogeny $f^\vee : E' \to E$ such that

$$f \circ f^\vee = f^\vee \circ f = [\ell].^\dagger$$

We are using: for any elliptic curve E, there is an isomorphism $E \cong E^\vee$ to its dual.

† $[\ell] : P \to \ell P$ is just multiplication by ℓ

Raising the dimension: isogenies

An ℓ-isogeny $f : E \to E'$ has a dual ℓ-isogeny $f^\vee : E' \to E$ such that

$$f \circ f^\vee = f^\vee \circ f = [\ell].^\dagger$$

We are using: for any elliptic curve E, there is an isomorphism $E \cong E^\vee$ to its dual.

This isomorphism comes from a principal polarisation.

† $[\ell] : P \to \ell P$ is just multiplication by ℓ

Raising the dimension: isogenies

An ℓ-isogeny $f : E \to E'$ has a dual ℓ-isogeny $f^\vee : E' \to E$ such that

$$f \circ f^\vee = f^\vee \circ f = [\ell].^\dagger$$

We are using: for any elliptic curve E, there is an isomorphism $E \cong E^\vee$ to its dual.

This isomorphism comes from a principal polarisation.

If an abelian variety A is principally polarised, then

† $[\ell] : P \to \ell P$ is just multiplication by ℓ

Raising the dimension: isogenies

An ℓ-isogeny $f : E \to E'$ has a dual ℓ-isogeny $f^\vee : E' \to E$ such that

$$f \circ f^\vee = f^\vee \circ f = [\ell].^\dagger$$

We are using: for any elliptic curve E, there is an isomorphism $E \cong E^\vee$ to its dual.

This isomorphism comes from a principal polarisation.

If an abelian variety A is principally polarised, then

- A can be embedded in projective space so has equations.

† $[\ell] : P \to \ell P$ is just multiplication by ℓ

Raising the dimension: isogenies

An ℓ-isogeny $f : E \to E'$ has a dual ℓ-isogeny $f^\vee : E' \to E$ such that

$$f \circ f^\vee = f^\vee \circ f = [\ell].^\dagger$$

We are using: for any elliptic curve E, there is an isomorphism $E \cong E^\vee$ to its dual.

This isomorphism comes from a principal polarisation.

If an abelian variety A is principally polarised, then

- A can be embedded in projective space so has equations.
- The polarisation defines an isomorphism $A \cong A^\vee$ from A to the dual $A^\vee$ of A.

(and much more stuff, out of the scope of this talk).

† $[\ell] : P \to \ell P$ is just multiplication by ℓ

Raising dimensions: isogenies

Recall:

Definition

$f : E \to E'$ an isogeny of elliptic curves $/\mathbb{F}_q$.

Let ℓ be a prime $\neq p$ (q is a power of p).

If $\#\ker(f) = \ell$, we call f an ℓ-isogeny.

If f an ℓ-isogeny, then $f^\vee \circ f = [\ell]$.

Raising dimensions: isogenies

Definition

$f : E \to E'$ an isogeny of elliptic curves $/\mathbb{F}_q$.

Let ℓ be a prime $\neq p$ (q is a power of p).

If $\ker(f) \cong \mathbb{Z}/\ell\mathbb{Z}$, we call f an ℓ-isogeny.

If f an ℓ-isogeny, then $f^\vee \circ f = [\ell]$.

Raising dimensions: isogenies

Definition

$f : A \to A'$ an isogeny of d-dimensional abelian varieties $/\mathbb{F}_q$.

Let ℓ be a prime $\neq p$ (q is a power of p).

If $\ker(f) \cong \underbrace{\mathbb{Z}/\ell\mathbb{Z} \times \cdots \times \mathbb{Z}/\ell\mathbb{Z}}_{d \text{ times}}$ and $f^\vee \circ f = [\ell]$ (up to polarisation-isomorphisms) we call f an $\underbrace{(\ell, \ldots, \ell)}_{d \text{ times}}$-isogeny.

Raising dimensions: isogenies

Definition

$f : A \to A'$ an isogeny of d-dimensional abelian varieties $/\mathbb{F}_q$.

Let ℓ be a prime $\neq p$ (q is a power of p).

If $\ker(f) \cong \underbrace{\mathbb{Z}/\ell\mathbb{Z} \times \cdots \times \mathbb{Z}/\ell\mathbb{Z}}_{d \text{ times}}$ and $f^\vee \circ f = [\ell]$ (up to polarisation-isomorphisms) we call f an $(\underbrace{\ell, \ldots, \ell}_{d \text{ times}})$-isogeny.

Natural question: Are there any isogenies of degree ℓ when $d > 1$?

(Isogenies with cyclic kernel are important in cryptographic algorithms).

Raising dimensions: cyclic isogenies

Question: Are there prime degree isogenies of higher dimensional principally polarised abelian varieties?

Raising dimensions: cyclic isogenies

Question: Are there prime degree isogenies of higher dimensional principally polarised abelian varieties?

Answer: Yes.

Raising dimensions: cyclic isogenies

Recall:

Definition

E/k an elliptic curve. An endomorphism of E is a morphism $E \to E$.

Example

- For $n \in \mathbb{Z}$, the multiplication-by-n map $[n] : P \to nP$.
- If $k = \mathbb{F}_q$, the q-power Frobenius map $\mathrm{Frob}_q : (x, y) \to (x^q, y^q)$.

$\rightsquigarrow$ if $k = \mathbb{F}_q$, then $\mathbb{Z}[\mathrm{Frob}_q] \subseteq \mathrm{End}(E)$, the endomorphism ring of E.

Raising dimensions: cyclic isogenies

Definition

A/k an abelian variety. An endomorphism of A is a morphism $A \to A$.

Example

- For $n \in \mathbb{Z}$, the multiplication-by-n map $[n] : P \to nP$.
- If $k = \mathbb{F}_q$, the q-power Frobenius map $\mathrm{Frob}_q : (x_1, \dots, x_n) \to (x_1^q, \dots, x_n^q)$

$\rightsquigarrow$ if $k = \mathbb{F}_q$, then $\mathbb{Z}[\mathrm{Frob}_q, \overline{\mathrm{Frob}_q}] \subseteq \mathrm{End}(A)$, the endomorphism ring of A.

Raising dimensions: cyclic isogenies

Definition

A/k an abelian variety. An endomorphism of A is a morphism $A \to A$.

Example

- For $n \in \mathbb{Z}$, the multiplication-by-n map $[n] : P \to nP$.
- If $k = \mathbb{F}_q$, the q-power Frobenius map $\mathrm{Frob}_q : (x_1, \ldots, x_n) \to (x_1^q, \ldots, x_n^q)$

$\rightsquigarrow$ if $k = \mathbb{F}_q$, then $\mathbb{Z}[\mathrm{Frob}_q, \overline{\mathrm{Frob}_q}] \subseteq \mathrm{End}(A)$, the endomorphism ring of A.

Example

Let $C/\mathbb{F}_{17} : y^2 = x^6 + 2x + 1$. Then the Jacobian $\mathrm{Jac}(C)$ of C is a two-dimensional principally polarised abelian variety

Raising dimensions: cyclic isogenies

Definition

A/k an abelian variety. An endomorphism of A is a morphism $A \to A$.

Example

- For $n \in \mathbb{Z}$, the multiplication-by-n map $[n] : P \to nP$.
- If $k = \mathbb{F}_q$, the q-power Frobenius map $\mathrm{Frob}_q : (x_1, \ldots, x_n) \to (x_1^q, \ldots, x_n^q)$

$\rightsquigarrow$ if $k = \mathbb{F}_q$, then $\mathbb{Z}[\mathrm{Frob}_q, \overline{\mathrm{Frob}_q}] \subseteq \mathrm{End}(A)$, the endomorphism ring of A.

Example

Let $C/\mathbb{F}_{17} : y^2 = x^6 + 2x + 1$. Then the Jacobian $\mathrm{Jac}(C)$ of C is a two-dimensional principally polarised abelian variety with endomorphism algebra $\mathrm{End}(\mathrm{Jac}(C)) \otimes \mathbb{Q} = \mathbb{Q}(\mathrm{Frob}_{17})$.

Raising dimensions: cyclic isogenies

Let $C/\mathbb{F}_{17} : y^2 = x^6 + 2x + 1$. Then the Jacobian $\mathrm{Jac}(C)$ of C is a two-dimensional principally polarised abelian variety with endomorphism algebra $\mathrm{End}(\mathrm{Jac}(C)) \otimes \mathbb{Q} = \mathbb{Q}(\mathrm{Frob}_{17})$.

Raising dimensions: cyclic isogenies

Let $C/\mathbb{F}_{17} : y^2 = x^6 + 2x + 1$. Then the Jacobian $\mathrm{Jac}(C)$ of C is a two-dimensional principally polarised abelian variety with endomorphism algebra $\mathrm{End}(\mathrm{Jac}(C)) \otimes \mathbb{Q} = \mathbb{Q}(\mathrm{Frob}_{17})$.

The characteristic polynomial of Frob_{17} is

$$\chi(t) = t^4 + 3t^3 + 25t^2 + 51t + 289,$$

Raising dimensions: cyclic isogenies

Let $C/\mathbb{F}_{17} : y^2 = x^6 + 2x + 1$. Then the Jacobian $\mathrm{Jac}(C)$ of C is a two-dimensional principally polarised abelian variety with endomorphism algebra $\mathrm{End}(\mathrm{Jac}(C)) \otimes \mathbb{Q} = \mathbb{Q}(\mathrm{Frob}_{17})$.

The characteristic polynomial of Frob_{17} is

$$\chi(t) = t^4 + 3t^3 + 25t^2 + 51t + 289,$$

so

$$\mathrm{End}(\mathrm{Jac}(C)) \otimes \mathbb{Q} = \mathbb{Q}[t]/\chi(t)$$

is a degree four number field K.

Raising dimensions: cyclic isogenies

Let $C/\mathbb{F}_{17} : y^2 = x^6 + 2x + 1$. Then the Jacobian $\mathrm{Jac}(C)$ of C is a two-dimensional principally polarised abelian variety with endomorphism algebra $\mathrm{End}(\mathrm{Jac}(C)) \otimes \mathbb{Q} = \mathbb{Q}(\mathrm{Frob}_{17})$.

The characteristic polynomial of Frob_{17} is

$$\chi(t) = t^4 + 3t^3 + 25t^2 + 51t + 289,$$

so

$$\mathrm{End}(\mathrm{Jac}(C)) \otimes \mathbb{Q} = \mathbb{Q}[t]/\chi(t)$$

is a degree four number field K.
This has a real quadratic subfield $K_0 = \mathbb{Q}(\sqrt{5})$.

Raising dimensions: cyclic isogenies

Let $C/\mathbb{F}_{17} : y^2 = x^6 + 2x + 1$. Then the Jacobian $\mathrm{Jac}(C)$ of C is a two-dimensional principally polarised abelian variety with endomorphism algebra $\mathrm{End}(\mathrm{Jac}(C)) \otimes \mathbb{Q} = \mathbb{Q}(\mathrm{Frob}_{17})$.

The characteristic polynomial of Frob_{17} is

$$\chi(t) = t^4 + 3t^3 + 25t^2 + 51t + 289,$$

so

$$\mathrm{End}(\mathrm{Jac}(C)) \otimes \mathbb{Q} = \mathbb{Q}[t]/\chi(t)$$

is a degree four number field K.
This has a real quadratic subfield $K_0 = \mathbb{Q}(\sqrt{5})$.
Our example has an endomorphism of norm 5^2:

$$\mu = \frac{5 + \sqrt{5}}{2}.$$

Raising dimensions: cyclic isogenies

Example: The Jacobian $\mathrm{Jac}(C)$ of $C/\mathbb{F}_{17} : y^2 = x^6 + 2x + 1$.
$\mu = \frac{5+\sqrt{5}}{2} \in \mathrm{End}(\mathrm{Jac}(C))$.

Raising dimensions: cyclic isogenies

Example: The Jacobian $\mathrm{Jac}(C)$ of $C/\mathbb{F}_{17} : y^2 = x^6 + 2x + 1$.
$\mu = \frac{5+\sqrt{5}}{2} \in \mathrm{End}(\mathrm{Jac}(C))$.

- The kernel of a $(5, 5)$-isogeny from $\mathrm{Jac}(C)$ is isomorphic to $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ and is generated by

$$P \in \mathrm{Jac}(C)[5] \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

Raising dimensions: cyclic isogenies

Example: The Jacobian $\mathrm{Jac}(C)$ of $C/\mathbb{F}_{17} : y^2 = x^6 + 2x + 1$.
$\mu = \frac{5+\sqrt{5}}{2} \in \mathrm{End}(\mathrm{Jac}(C))$.

- The kernel of a $(5,5)$-isogeny from $\mathrm{Jac}(C)$ is isomorphic to $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ and is generated by

$$P \in \mathrm{Jac}(C)[5] \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

- The kernel of a cyclic μ-isogeny f from $\mathrm{Jac}(C)$ is isomorphic to $\mathbb{Z}/5\mathbb{Z}$ (hence is cyclic!) and is generated by

$$P \in \mathrm{Jac}(C)[\mu] \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

- This isogeny satisfies $f^\vee \circ f = [\mu]$ (up to polarisation-isomorphisms).

Raising dimensions: cyclic isogenies

Example: The Jacobian $\mathrm{Jac}(C)$ of $C/\mathbb{F}_{17} : y^2 = x^6 + 2x + 1$.
$\mu = \frac{5+\sqrt{5}}{2} \in \mathrm{End}(\mathrm{Jac}(C))$.

- The kernel of a $(5,5)$-isogeny from $\mathrm{Jac}(C)$ is isomorphic to $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ and is generated by

$$P \in \mathrm{Jac}(C)[5] \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

- The kernel of a cyclic μ-isogeny f from $\mathrm{Jac}(C)$ is isomorphic to $\mathbb{Z}/5\mathbb{Z}$ (hence is cyclic!) and is generated by

$$P \in \mathrm{Jac}(C)[\mu] \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

- This isogeny satisfies $f^\vee \circ f = [\mu]$ (up to polarisation-isomorphisms).

Do these isogenies always exist?

Raising dimensions: cyclic isogenies

- Let $A/\mathbb{F}_q$ be a d-dimensional principally polarised abelian variety for which $\mathrm{End}(A) \otimes \mathbb{Q} = \mathbb{Q}(\mathrm{Frob}_q)$ and is a degree $2d$ CM-field K

Raising dimensions: cyclic isogenies

- Let $A/\mathbb{F}_q$ be a d-dimensional principally polarised abelian variety for which $\mathrm{End}(A) \otimes \mathbb{Q} = \mathbb{Q}(\mathrm{Frob}_q)$ and is a degree $2d$ CM-field K

  (an imaginary quadratic extension of a totally real number field K_0).

Raising dimensions: cyclic isogenies

- Let $A/\mathbb{F}_q$ be a d-dimensional principally polarised abelian variety for which $\mathrm{End}(A) \otimes \mathbb{Q} = \mathbb{Q}(\mathrm{Frob}_q)$ and is a degree $2d$ CM-field K

  (an imaginary quadratic extension of a totally real number field K_0).

- Write $\mathcal{O}_{K_0}$ for the ring of integers of K_0. If:
  1. $\mu \in \mathcal{O}_{K_0}$ is a prime element and is totally positive (all embeddings are positive), $\mathrm{Norm}_{K_0/\mathbb{Q}}(\mu) = \ell$, and

Raising dimensions: cyclic isogenies

- Let $A/\mathbb{F}_q$ be a d-dimensional principally polarised abelian variety for which $\mathrm{End}(A) \otimes \mathbb{Q} = \mathbb{Q}(\mathrm{Frob}_q)$ and is a degree $2d$ CM-field K

  (an imaginary quadratic extension of a totally real number field K_0).

- Write $\mathcal{O}_{K_0}$ for the ring of integers of K_0. If:
  1. $\mu \in \mathcal{O}_{K_0}$ is a prime element and is totally positive (all embeddings are positive), $\mathrm{Norm}_{K_0/\mathbb{Q}}(\mu) = \ell$, and
  2. $\mathcal{O}_{K_0} \subseteq \mathrm{End}(A)$,

Raising dimensions: cyclic isogenies

- Let $A/\mathbb{F}_q$ be a d-dimensional principally polarised abelian variety for which $\mathrm{End}(A) \otimes \mathbb{Q} = \mathbb{Q}(\mathrm{Frob}_q)$ and is a degree $2d$ CM-field K

  (an imaginary quadratic extension of a totally real number field K_0).

- Write $\mathcal{O}_{K_0}$ for the ring of integers of K_0. If:
  1. $\mu \in \mathcal{O}_{K_0}$ is a prime element and is totally positive (all embeddings are positive), $\mathrm{Norm}_{K_0/\mathbb{Q}}(\mu) = \ell$, and
  2. $\mathcal{O}_{K_0} \subseteq \mathrm{End}(A)$,

  then $P \in A[\mu]$ of order ℓ will generate the kernel of a degree-ℓ cyclic isogeny f that satisfies $f^\vee \circ f = [\mu]$ (up to polarisation-isomorphisms).

Raising dimensions: cyclic isogenies

- Let $A/\mathbb{F}_q$ be a d-dimensional principally polarised abelian variety for which $\mathrm{End}(A) \otimes \mathbb{Q} = \mathbb{Q}(\mathrm{Frob}_q)$ and is a degree $2d$ CM-field K

  (an imaginary quadratic extension of a totally real number field K_0).

- Write $\mathcal{O}_{K_0}$ for the ring of integers of K_0. If:
  1. $\mu \in \mathcal{O}_{K_0}$ is a prime element and is totally positive (all embeddings are positive), $\mathrm{Norm}_{K_0/\mathbb{Q}}(\mu) = \ell$, and
  2. $\mathcal{O}_{K_0} \subseteq \mathrm{End}(A)$,

  then $P \in A[\mu]$ of order ℓ will generate the kernel of a degree-ℓ cyclic isogeny f that satisfies $f^\vee \circ f = [\mu]$ (up to polarisation-isomorphisms).

Open(?) question: what conditions on $A/\mathbb{F}_q$ are necessary for cyclic isogenies to exist?

Recap so far

- We focus on d-dimensional principally polarised abelian varieties A.

Recap so far

- We focus on d-dimensional principally polarised abelian varieties A.
  1. $d = 2$: $A = \mathrm{Jac}(C)$, where
     - $C : y^2 = f(x)$ is hyperelliptic, $\deg(f) = 5, 6$.
  2. $d = 3$: $A = \mathrm{Jac}(C)$, where
     - $C : y^2 = f(x)$ is hyperelliptic, $\deg(f) = 7, 8$, or
     - $C : f(x, y) = 0$ is plane quartic, $\deg(f) = 4$.
- There are two types of polarisation-preserving isogeny (ℓ prime):

Recap so far

- We focus on d-dimensional principally polarised abelian varieties A.
  1. $d = 2$: $A = \mathrm{Jac}(C)$, where
     - $C : y^2 = f(x)$ is hyperelliptic, $\deg(f) = 5, 6$.
  2. $d = 3$: $A = \mathrm{Jac}(C)$, where
     - $C : y^2 = f(x)$ is hyperelliptic, $\deg(f) = 7, 8$, or
     - $C : f(x, y) = 0$ is plane quartic, $\deg(f) = 4$.
- There are two types of polarisation-preserving isogeny (ℓ prime):
  1. $\underbrace{(\ell, \ldots, \ell)}_{d \text{ times}}$-isogenies f.

Recap so far

- We focus on d-dimensional principally polarised abelian varieties A.
  1. $d = 2$: $A = \mathrm{Jac}(C)$, where
     - $C : y^2 = f(x)$ is hyperelliptic, $\deg(f) = 5, 6$.
  2. $d = 3$: $A = \mathrm{Jac}(C)$, where
     - $C : y^2 = f(x)$ is hyperelliptic, $\deg(f) = 7, 8$, or
     - $C : f(x, y) = 0$ is plane quartic, $\deg(f) = 4$.
- There are two types of polarisation-preserving isogeny (ℓ prime):
  1. $\underbrace{(\ell, \ldots, \ell)}_{d \text{ times}}$-isogenies f.
     - Degree: ℓ^d.
     - Kernel generated by ℓ-torsion point.
     - Satisfies $f^\vee \circ f = [\ell]$ up to polarisation-isomorphisms.

Recap so far

- We focus on d-dimensional principally polarised abelian varieties A.
  1. $d = 2$: $A = \mathrm{Jac}(C)$, where
     - $C : y^2 = f(x)$ is hyperelliptic, $\deg(f) = 5, 6$.
  2. $d = 3$: $A = \mathrm{Jac}(C)$, where
     - $C : y^2 = f(x)$ is hyperelliptic, $\deg(f) = 7, 8$, or
     - $C : f(x, y) = 0$ is plane quartic, $\deg(f) = 4$.
- There are two types of polarisation-preserving isogeny (ℓ prime):
  1. $\underbrace{(\ell, \ldots, \ell)}_{d \text{ times}}$-isogenies f.
     - Degree: ℓ^d.
     - Kernel generated by ℓ-torsion point.
     - Satisfies $f^\vee \circ f = [\ell]$ up to polarisation-isomorphisms.
  2. Cyclic μ-isogenies f; μ is an endomorphism of norm ℓ^2 (and more).

Recap so far

- We focus on d-dimensional principally polarised abelian varieties A.
  1. $d = 2$: $A = \mathrm{Jac}(C)$, where
     - $C : y^2 = f(x)$ is hyperelliptic, $\deg(f) = 5, 6$.
  2. $d = 3$: $A = \mathrm{Jac}(C)$, where
     - $C : y^2 = f(x)$ is hyperelliptic, $\deg(f) = 7, 8$, or
     - $C : f(x, y) = 0$ is plane quartic, $\deg(f) = 4$.
- There are two types of polarisation-preserving isogeny (ℓ prime):
  1. $\underbrace{(\ell, \ldots, \ell)}_{d \text{ times}}$-isogenies f.
     - Degree: ℓ^d.
     - Kernel generated by ℓ-torsion point.
     - Satisfies $f^\vee \circ f = [\ell]$ up to polarisation-isomorphisms.
  2. Cyclic μ-isogenies f; μ is an endomorphism of norm ℓ^2 (and more).
     - Degree: ℓ.
     - Kernel generated by μ-torsion point.
     - Satisfies $f^\vee \circ f = [\mu]$ up to polarisation-isomorphisms.

Brief[3] history of genus 2 and 3 curves in crypto

pre-2006 Pollard rho is best algorithm for attacking DLP on small dimensional $A/\mathbb{F}_p$, complexity $O(p^{d/2})$.
Theoretical efficiency of crypto with n-bit security roughly the same for $d = 1, 2, 3$.

2006 Diem [D06] publishes index-calculus method to solve DLP on plane quartic genus 3 curves $/\mathbb{F}_q$, complexity $O(q)$.

2008 Smith [S08] finds method of efficiently constructing a $(2,2,2)$-isogeny to a plane quartic genus 3 curve from 18.57% of all hyperelliptic genus 3 curves $/\mathbb{F}_q$.
(Thus solving DLP in time $O(q)$ on these curves).

2010 Joux and Vitse [JV10] compute efficient 'covering map' $E/\mathbb{F}_{q^3} \to \mathrm{Jac}(C)/\mathbb{F}_q$, where C is a plane quartic genus 3 curve (for some elliptic curves).
(Thus solving DLP in time $O(q) < O(q^{3/2})$ on E).

---

[3] Definitely not comprehensive

Brief history of genus 2 and 3 curves in crypto (contd.)

2010 Bisson, Cosset, and Robert [BCR10] release MAGMA package 'AVIsogenies' for computing (ℓ, ℓ)-isogenies.

2017 Renes and Smith [RS17] show that genus 2 arithmetic is as fast as and less memory intensive than elliptic curve arithmetic (for the same security level).

2017 Dudeanu, Jetchev, Robert, and Vuille [DJRV17] publish article on efficient computation of cyclic isogenies (in the case we covered).

2018 Costello [C18] introduces new methods for efficient computation of $(2, 2)$-isogenies.

2019 Flynn and Ti [FT19] introduce a genus-2 version of SIDH using $(2, 2)$- and $(3, 3)$-isogeny graphs.

2020? Applications of isogeny graphs of abelian varieties?

Raising dimensions: isogeny graphs

Luca showed some nice applications of isogeny graphs of elliptic curves.

Natural question 1: What is the structure of isogeny graphs of abelian varieties?

Natural question 2: Are there (different) cryptographic applications of isogeny graphs of abelian varieties?

Q1: Structure of isogeny graphs of abelian varieties?

Recall:
An ℓ-isogeny graph of elliptic curves $/k$ has:

- Vertices: Elliptic curves E/k with the same number of rational points (up to isomorphism).
- Edges: An edge $E - E'$ represents an ℓ-isogeny $E \to E'$ and its dual (up to isomorphism).

Q1: Structure of isogeny graphs of abelian varieties?

An $(\ell, \ldots, \ell)$-isogeny (resp. cyclic μ-isogeny) graph of abelian varieties $/k$ satisfying property P [4] has:

- Vertices: Abelian varieties A/k satisying P with the same number of rational points (up to P-preserving-isomorphism).
- Edges: An edge $A - A'$ represents an P-preserving $(\ell, \ldots, \ell)$-isogeny (resp. cyclic μ-isogeny) $A \to A'$ and its dual (up to P-preserving-isomorphism).

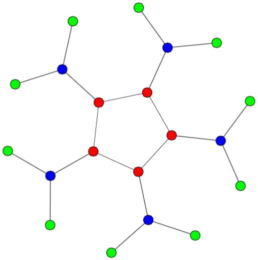
[4] This property should include that abelian varieties are isomorphic to their duals

Q1: Structure of isogeny graphs of abelian varieties?

Recall:

Theorem ([K96])

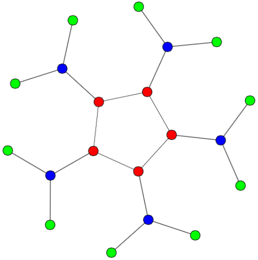
Let $E/\mathbb{F}_q$ be an ordinary elliptic curve such that $j(E) \neq 0, 1728$, and let $\ell \in \mathbb{Z}$ be a prime. Then the connected component of the ℓ-isogeny graph containing E is a volcano.



Q1: Structure of isogeny graphs of abelian varieties?

Theorem ([BJW17]/[M18])

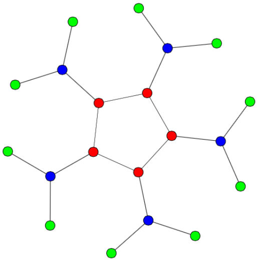
Let $A/\mathbb{F}_q$ be a principally polarised abelian variety with $\mathrm{End}(A) \otimes \mathbb{Q} = K$ a CM-field with maximal totally real subfield K_0 such that $j(E) \neq 0, 1728$, and let $\ell \in \mathbb{Z}$ be a prime. Then the connected component of the ℓ-isogeny graph containing E is a volcano.



Q1: Structure of isogeny graphs of abelian varieties?

Theorem ([BJW17]/[M18])

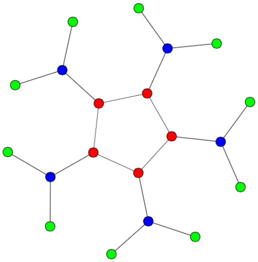
Let $A/\mathbb{F}_q$ be a principally polarised abelian variety with $\mathrm{End}(A) \otimes \mathbb{Q} = K$ a CM-field with maximal totally real subfield K_0 such that the only roots of unity in K are ± 1, and let $\ell \in \mathbb{Z}$ be a prime. Then the connected component of the ℓ-isogeny graph containing E is a volcano.



Q1: Structure of isogeny graphs of abelian varieties?

Theorem ([BJW17]/[M18])

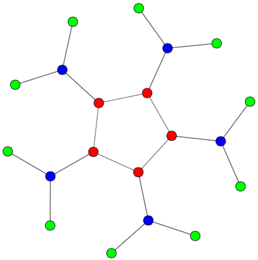
Let $A/\mathbb{F}_q$ be a principally polarised abelian variety with $\mathrm{End}(A) \otimes \mathbb{Q} = K$ a CM-field with maximal totally real subfield K_0 such that the only roots of unity in K are ± 1, and let μ be a totally positive prime element in $\mathcal{O}_{K_0}$. Then the connected component of the ℓ-isogeny graph containing E is a volcano.



Q1: Structure of isogeny graphs of abelian varieties?

Theorem ([BJW17]/[M18])

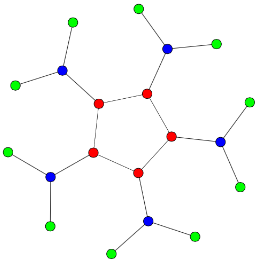
Let $A/\mathbb{F}_q$ be a principally polarised abelian variety with $\mathrm{End}(A) \otimes \mathbb{Q} = K$ a CM-field with maximal totally real subfield K_0 such that the only roots of unity in K are ± 1, and let μ be a totally positive prime element in $\mathcal{O}_{K_0}$. If $\mathcal{O}_{K_0} \subseteq \mathrm{End}(A)$, then the connected component of the cyclic μ-isogeny graph containing A is a volcano.



Q1: Structure of isogeny graphs of abelian varieties?

Theorem ([K96])

With notation as before, locally at ℓ, a vertex at depth d has endomorphism ring $\ell^d\mathcal{O}_K$.

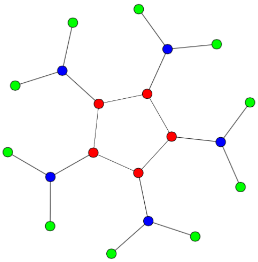


depth $= 0$ depth $= 1$ depth $= 2$

Q1: Structure of isogeny graphs of abelian varieties?

Theorem ([BJW17]/[M18])

With notation as before, locally at μ, a vertex at depth d has endomorphism ring $\mu^d \mathcal{O}_K$.



depth $= 0$ depth $= 1$ depth $= 2$

Q1: Structure of isogeny graphs of abelian varieties?

Theorem ([BJW17]/[M18])

With notation as before, locally at μ, a vertex at depth d has endomorphism ring $\mu^d \mathcal{O}_K$.

$\rightsquigarrow$ As

$$\mathbb{Z}[\mathrm{Frob}_q, \overline{\mathrm{Frob}_q}] \subseteq \mathrm{End}(A) \subseteq \mathcal{O}_K,$$

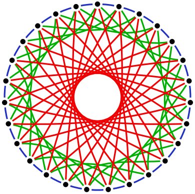
if

$$\ell \nmid \left[\mathcal{O}_K : \mathbb{Z}[\mathrm{Frob}_q, \overline{\mathrm{Frob}_q}]\right]$$

and $\mu \in \mathcal{O}_{K_0}$ a prime above ℓ, then the μ-isogeny graph containing A is a disjoint union of cycles.

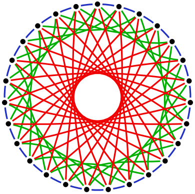
Q2: Applications of these isogeny graphs?

Application 1: Random sampling on the Schreier graph (idea in this context due to [JW17]).



Q2: Applications of these isogeny graphs?

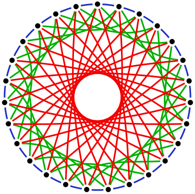
Application 1: Random sampling on the Schreier graph (idea in this context due to [JW17]).



Nodes: (A subset of all the) simple, ordinary, principally polarised abelian varieties with $\mathrm{End}(A) \otimes \mathbb{Q} = K$, as above.

Q2: Applications of these isogeny graphs?

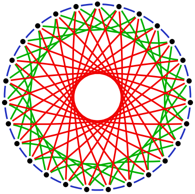
Application 1: Random sampling on the Schreier graph (idea in this context due to [JW17]).



Nodes: (A subset of all the) simple, ordinary, principally polarised abelian varieties with $\mathrm{End}(A) \otimes \mathbb{Q} = K$, as above.
Edges: cyclic μ_1-, μ_2-, and μ_3-isogenies of norms ℓ_1, ℓ_2, and ℓ_3 not dividing $\left[\mathcal{O}_K : \mathbb{Z}[\mathrm{Frob}_q, \overline{\mathrm{Frob}_q}]\right]$.

Q2: Applications of these isogeny graphs?

Application 1: Random sampling on the Schreier graph (idea in this context due to [JW17]).



Nodes: (A subset of all the) simple, ordinary, principally polarised abelian varieties with $\mathrm{End}(A) \otimes \mathbb{Q} = K$, as above.
Edges: cyclic μ_1-, μ_2-, and μ_3-isogenies of norms ℓ_1, ℓ_2, and ℓ_3 not dividing $\left[\mathcal{O}_K : \mathbb{Z}[\mathrm{Frob}_q, \overline{\mathrm{Frob}_q}]\right]$.

Main challenge: efficient computation of cyclic μ-isogenies (computing neighbours in graph).

Q2: Applications of these graphs?

Idea: use random sampling to get a probabilistic algorithm to compute an isogeny from any hyperelliptic genus 3 curve to a plane quartic genus 3 curve (where DLP is weaker). [a]

[a] Idea due to [BJW17]. Solution and most of the rest of this talk is ongoing work with Jetchev-Martindale-Milio-Vuille-Wesolowski

This can only work if a 'random' three-dimensional principally polarised abelian variety is plane quartic.

Q2: Applications of these graphs?

Idea: use random sampling to get a probabilistic algorithm to compute an isogeny from any hyperelliptic genus 3 curve to a plane quartic genus 3 curve (where DLP is weaker). [a]

[a] Idea due to [BJW17]. Solution and most of the rest of this talk is ongoing work with Jetchev-Martindale-Milio-Vuille-Wesolowski

This can only work if a 'random' three-dimensional principally polarised abelian variety is plane quartic.
What does this mean?

Q2: Applications of these graphs?

Definition

We define an isogeny graph G of principally polarised abelian varieties of dimension 3 over $\mathbb{F}_q$ to be good if there exists a constant $0 < c < 1$ such that

$$\#\{\text{non-hyp vertices}\} \geq c\#\{\text{hyperelliptic vertices}\},$$

and the non-hyperelliptic vertices are ‘sufficiently randomly distributed’ in each of the connected components of G.

Q2: Applications of these graphs?

Definition

We define an isogeny graph G of principally polarised abelian varieties of dimension 3 over $\mathbb{F}_q$ to be good if there exists a constant $0 < c < 1$ such that

$$\#\{\text{non-hyp vertices}\} \geq c\#\{\text{hyperelliptic vertices}\},$$

and the non-hyperelliptic vertices are 'sufficiently randomly distributed' in each of the connected components of G.

Heuristic H: there exists a constant $c > 0$, independent of q, such that a randomly chosen ordinary isogeny class† over $\mathbb{F}_q$ is good with probability 1.

† An ordinary isogeny class is a set of abelian varieties that are all isogenous and all ordinary (have full p-torsion). (They also all have the same CM-field as an endomorphism algebra - our K).

Q2: Applications of these graphs?

Application 2: Assuming Heuristic H, use random sampling to get a probabilistic algorithm to compute an isogeny from any hyperelliptic genus 3 curve to a plane quartic genus 3 curve (where DLP is weaker).

Problem: nodes in this Schreier graph are very special– what happens when $\mathcal{O}_{K_0} \not\subseteq \mathrm{End}(A)$ (not even locally)?

Q2: Applications of these graphs?

Application 2: Assuming Heuristic H, use random sampling to get a probabilistic algorithm to compute an isogeny from any hyperelliptic genus 3 curve to a plane quartic genus 3 curve (where DLP is weaker).

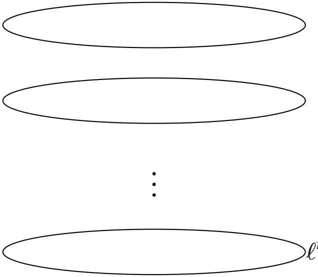
Problem: nodes in this Schreier graph are very special– what happens when $\mathcal{O}_{K_0} \not\subseteq \mathrm{End}(A)$ (not even locally)?

- There are no cyclic polarisation-preserving degree-ℓ isogenies from A.
- But there could be $(\ell, \ldots, \ell)$-isogenies.
  $\rightsquigarrow$ Also need to look at the $(\ell, \ldots, \ell)$-isogeny graph.

Q1: Structure of isogeny graphs of abelian varieties?

Connected component of $(\ell, \ldots, \ell)$-isogeny graph of a simple and ordinary principally polarised abelian variety over $\mathbb{F}_q$:

$\mathrm{End}^{\mathbb{R}}(A)$ is the real part of $\mathrm{End}(A)$.



$$\mathcal{O}_{K_0} \subseteq \mathrm{End}^{\mathbb{R}}(A)$$

$$\ell\mathcal{O}_{K_0} \subseteq \mathrm{End}^{\mathbb{R}}(A) \not\subseteq \mathcal{O}_{K_0}$$

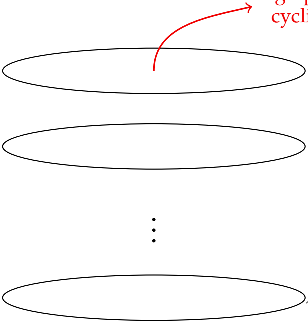
$$\vdots$$

$$\ell^n\mathcal{O}_{K_0} \subseteq \mathrm{End}^{\mathbb{R}}(A) \not\subseteq \ell^{n-1}\mathcal{O}_{K_0}$$

Q1: Structure of isogeny graphs of abelian varieties?

Connected component of $(\ell, \ldots, \ell)$-isogeny graph of a simple and ordinary principally polarised abelian variety over $\mathbb{F}_q$:

$\mathrm{End}^{\mathbb{R}}(A)$ is the real part of $\mathrm{End}(A)$.



graph deduced from cyclic isogeny graphs

$\mathcal{O}_{K_0} \subseteq \mathrm{End}^{\mathbb{R}}(A)$

$\ell\mathcal{O}_{K_0} \subseteq \mathrm{End}^{\mathbb{R}}(A) \not\subseteq \mathcal{O}_{K_0}$

$\vdots$

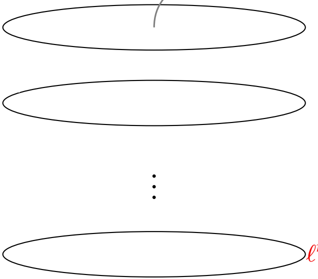
$\ell^n\mathcal{O}_{K_0} \subseteq \mathrm{End}^{\mathbb{R}}(A) \not\subseteq \ell^{n-1}\mathcal{O}_{K_0}$

Q1: Structure of isogeny graphs of abelian varieties?

Connected component of $(\ell, \ldots, \ell)$-isogeny graph of a simple and ordinary principally polarised abelian variety over $\mathbb{F}_q$:

$\mathrm{End}^{\mathbb{R}}(A)$ is the real part of $\mathrm{End}(A)$.

graph deduced from cyclic isogeny graphs



$\mathcal{O}_{K_0} \subseteq \mathrm{End}^{\mathbb{R}}(A)$

$\ell\mathcal{O}_{K_0} \subseteq \mathrm{End}^{\mathbb{R}}(A) \not\subseteq \mathcal{O}_{K_0}$

$\vdots$

$\ell^n\mathcal{O}_{K_0} \subseteq \mathrm{End}^{\mathbb{R}}(A) \not\subseteq \ell^{n-1}\mathcal{O}_{K_0}$

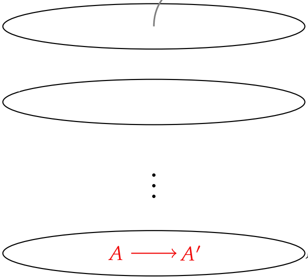
n is max s.t. ℓ^n divides $\left[\mathcal{O}_{K_0} : \mathbb{Z}[\mathrm{Frob}_q + \overline{\mathrm{Frob}_q}]\right]$

Q1: Structure of isogeny graphs of abelian varieties?

Connected component of $(\ell, \ldots, \ell)$-isogeny graph of a simple and ordinary principally polarised abelian variety over $\mathbb{F}_q$:

$\mathrm{End}^{\mathbb{R}}(A)$ is the real part of $\mathrm{End}(A)$.

graph deduced from cyclic isogeny graphs



$\mathcal{O}_{K_0} \subseteq \mathrm{End}^{\mathbb{R}}(A)$

$\ell\mathcal{O}_{K_0} \subseteq \mathrm{End}^{\mathbb{R}}(A) \not\subseteq \mathcal{O}_{K_0}$

$\vdots$

Isogenies within layers are ‘RM-horizontal’

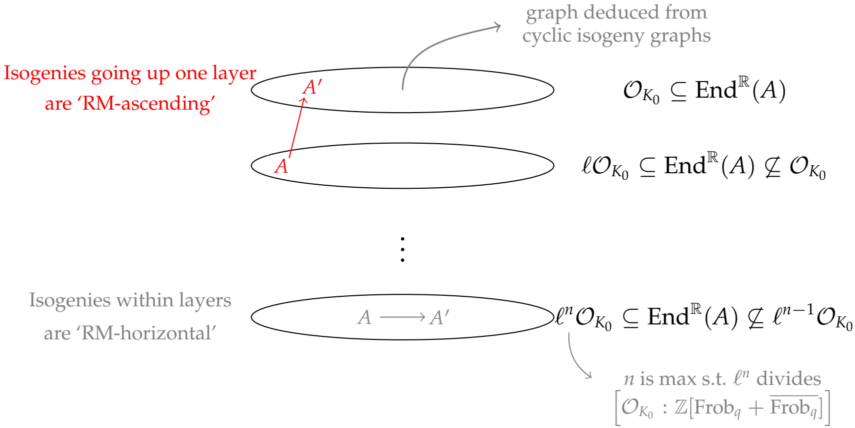
$\ell^n\mathcal{O}_{K_0} \subseteq \mathrm{End}^{\mathbb{R}}(A) \not\subseteq \ell^{n-1}\mathcal{O}_{K_0}$

n is max s.t. ℓ^n divides $\left[\mathcal{O}_{K_0} : \mathbb{Z}[\mathrm{Frob}_q + \overline{\mathrm{Frob}_q}]\right]$

Q1: Structure of isogeny graphs of abelian varieties?

Connected component of $(\ell, \ldots, \ell)$-isogeny graph of a simple and ordinary principally polarised abelian variety over $\mathbb{F}_q$:

$\mathrm{End}^{\mathbb{R}}(A)$ is the real part of $\mathrm{End}(A)$.



Q1: Structure of isogeny graphs of abelian varieties?

Connected component of $(\ell, \ldots, \ell)$-isogeny graph of a simple and ordinary principally polarised abelian variety over $\mathbb{F}_q$:

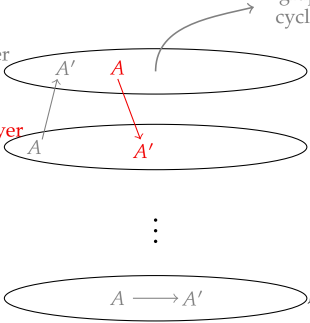
$\mathrm{End}^{\mathbb{R}}(A)$ is the real part of $\mathrm{End}(A)$.

graph deduced from cyclic isogeny graphs

Isogenies going up one layer are ‘RM-ascending’

Isogenies going down one layer are ‘RM-descending’

Isogenies within layers are ‘RM-horizontal’



$\mathcal{O}_{K_0} \subseteq \mathrm{End}^{\mathbb{R}}(A)$

$\ell\mathcal{O}_{K_0} \subseteq \mathrm{End}^{\mathbb{R}}(A) \not\subseteq \mathcal{O}_{K_0}$

$\ell^n\mathcal{O}_{K_0} \subseteq \mathrm{End}^{\mathbb{R}}(A) \not\subseteq \ell^{n-1}\mathcal{O}_{K_0}$

n is max s.t. ℓ^n divides $\left[\mathcal{O}_{K_0} : \mathbb{Z}[\mathrm{Frob}_q + \overline{\mathrm{Frob}_q}]\right]$

Q1: Structure of isogeny graphs of abelian varieties?

Connected component of $(\ell, \ldots, \ell)$-isogeny graph of a simple and ordinary principally polarised abelian variety over $\mathbb{F}_q$:

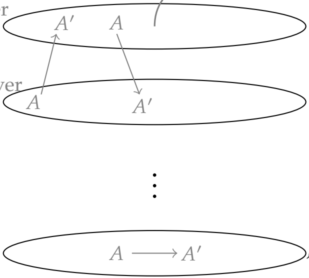
$\mathrm{End}^{\mathbb{R}}(A)$ is the real part of $\mathrm{End}(A)$.

graph deduced from cyclic isogeny graphs

Isogenies going up one layer are 'RM-ascending'

Isogenies going down one layer are 'RM-descending'

Isogenies within layers are 'RM-horizontal'



$\mathcal{O}_{K_0} \subseteq \mathrm{End}^{\mathbb{R}}(A)$

$\ell\mathcal{O}_{K_0} \subseteq \mathrm{End}^{\mathbb{R}}(A) \not\subseteq \mathcal{O}_{K_0}$

$\ell^n\mathcal{O}_{K_0} \subseteq \mathrm{End}^{\mathbb{R}}(A) \not\subseteq \ell^{n-1}\mathcal{O}_{K_0}$

n is max s.t. ℓ^n divides $\left[\mathcal{O}_{K_0} : \mathbb{Z}[\mathrm{Frob}_q + \overline{\mathrm{Frob}_q}]\right]$

There is a unique RM-ascending $(\ell, \ldots, \ell)$-isogeny from every vertex not on the top layer.

Q1: Structure of isogeny graphs of abelian varieties?

Connected component of $(\ell, \ldots, \ell)$-isogeny graph of a simple and ordinary principally polarised abelian variety over $\mathbb{F}_q$:

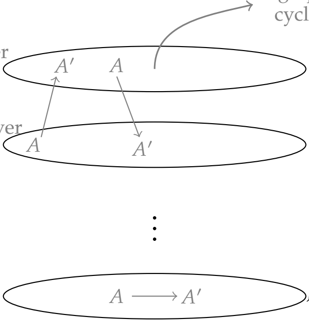
$\mathrm{End}^{\mathbb{R}}(A)$ is the real part of $\mathrm{End}(A)$.

graph deduced from cyclic isogeny graphs

Isogenies going up one layer are 'RM-ascending'

Isogenies going down one layer are 'RM-descending'

Isogenies within layers are 'RM-horizontal'



$\mathcal{O}_{K_0} \subseteq \mathrm{End}^{\mathbb{R}}(A)$

$\ell\mathcal{O}_{K_0} \subseteq \mathrm{End}^{\mathbb{R}}(A) \not\subseteq \mathcal{O}_{K_0}$

$\ell^n\mathcal{O}_{K_0} \subseteq \mathrm{End}^{\mathbb{R}}(A) \not\subseteq \ell^{n-1}\mathcal{O}_{K_0}$

n is max s.t. ℓ^n divides $\left[\mathcal{O}_{K_0} : \mathbb{Z}[\mathrm{Frob}_q + \overline{\mathrm{Frob}_q}]\right]$

There is a unique RM-ascending $(\ell, \ldots, \ell)$-isogeny from every vertex not on the top layer.

Q2: Applications of these graphs?

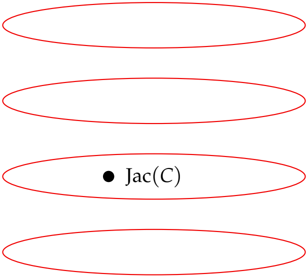
Reminder–Application 2: under Heuristic H, construct an isogeny from (almost) any hyperelliptic genus 3 Jacobian $\mathrm{Jac}(C)/\mathbb{F}_q$ to a plane quartic genus 3 Jacobian $\mathrm{Jac}(C')/\mathbb{F}_q$, thus attacking DLP on $\mathrm{Jac}(C)$ in time $O(q)$ (next-best-option Pollard-rho is $O(q^{3/2})$). [a]

[a] Disclaimer: given a sufficiently efficient method of computing isogenies.

Constructing an isogeny from a hyperelliptic to a plane quartic (simplified)

Example

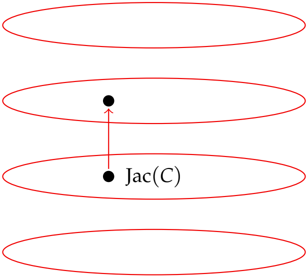
- Suppose $\left[\mathcal{O}_{K_0} : \mathbb{Z}[\mathrm{Frob}_q + \overline{\mathrm{Frob}_q}]\right] = \ell_1^4 \ell_2$.
- Ascend the (ℓ_1, ℓ_1, ℓ_1)-isogeny graph.



Constructing an isogeny from a hyperelliptic to a plane quartic (simplified)

Example

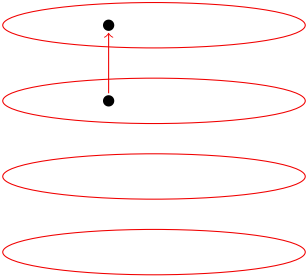
- Suppose $\left[\mathcal{O}_{K_0} : \mathbb{Z}[\mathrm{Frob}_q + \overline{\mathrm{Frob}_q}]\right] = \ell_1^4 \ell_2$.
- Ascend the (ℓ_1, ℓ_1, ℓ_1)-isogeny graph.



Constructing an isogeny from a hyperelliptic to a plane quartic (simplified)

Example

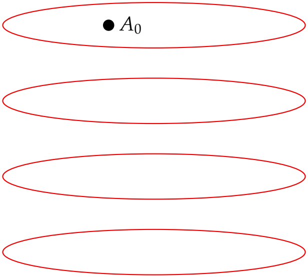
- Suppose $\left[\mathcal{O}_{K_0} : \mathbb{Z}[\mathrm{Frob}_q + \overline{\mathrm{Frob}_q}]\right] = \ell_1^4 \ell_2$.
- Ascend the (ℓ_1, ℓ_1, ℓ_1)-isogeny graph.



Constructing an isogeny from a hyperelliptic to a plane quartic (simplified)

Example

- Suppose $\left[\mathcal{O}_{K_0} : \mathbb{Z}[\mathrm{Frob}_q + \overline{\mathrm{Frob}_q}]\right] = \ell_1^4 \ell_2$.
- Ascend the (ℓ_1, ℓ_1, ℓ_1)-isogeny graph.

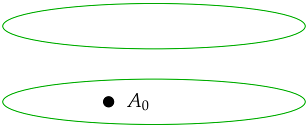


- Locally at ℓ_1, $\mathcal{O}_{K_0} \subseteq \mathrm{End}(A_0)$.

Constructing an isogeny from a hyperelliptic to a plane quartic (simplified)

Example

- Suppose $\left[\mathcal{O}_{K_0} : \mathbb{Z}[\mathrm{Frob}_q + \overline{\mathrm{Frob}_q}]\right] = \ell_1^4 \ell_2$.
- Ascend the (ℓ_1, ℓ_1, ℓ_1)-isogeny graph.
- Ascend the (ℓ_2, ℓ_2, ℓ_2)-isogeny graph.

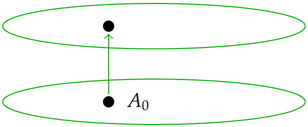


- Locally at ℓ_1, $\mathcal{O}_{K_0} \subseteq \mathrm{End}(A_0)$.

Constructing an isogeny from a hyperelliptic to a plane quartic (simplified)

Example

- Suppose $\left[\mathcal{O}_{K_0} : \mathbb{Z}[\mathrm{Frob}_q + \overline{\mathrm{Frob}_q}]\right] = \ell_1^4 \ell_2$.
- Ascend the (ℓ_1, ℓ_1, ℓ_1)-isogeny graph.
- Ascend the (ℓ_2, ℓ_2, ℓ_2)-isogeny graph.

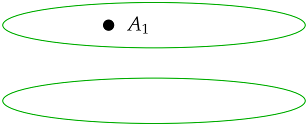


- Locally at ℓ_1, $\mathcal{O}_{K_0} \subseteq \mathrm{End}(A_0)$.

Constructing an isogeny from a hyperelliptic to a plane quartic (simplified)

Example

- Suppose $\left[\mathcal{O}_{K_0} : \mathbb{Z}[\mathrm{Frob}_q + \overline{\mathrm{Frob}_q}]\right] = \ell_1^4 \ell_2$.
- Ascend the (ℓ_1, ℓ_1, ℓ_1)-isogeny graph.
- Ascend the (ℓ_2, ℓ_2, ℓ_2)-isogeny graph.



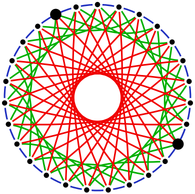
- Locally at ℓ_1, $\mathcal{O}_{K_0} \subseteq \mathrm{End}(A_0)$.
- $\mathcal{O}_{K_0} \subseteq \mathrm{End}(A_1)$.

Constructing an isogeny from a hyperelliptic to a plane quartic (simplified)

- $\mathcal{O}_{K_0} \subseteq \operatorname{End}(A_1)$.
- Suppose $\left[\mathcal{O}_K : \mathcal{O}_{K_0}[\mathrm{Frob}_q, \overline{\mathrm{Frob}_q}]\right] = 1$. Then do not need to ascend any cyclic-isogeny graphs as $\operatorname{End}(A') = \mathcal{O}_K$.

Constructing an isogeny from a hyperelliptic to a plane quartic (simplified)

- $\mathcal{O}_{K_0} \subseteq \mathrm{End}(A_1)$.
- Suppose $\left[\mathcal{O}_K : \mathcal{O}_{K_0}[\mathrm{Frob}_q, \overline{\mathrm{Frob}_q}]\right] = 1$. Then do not need to ascend any cyclic-isogeny graphs as $\mathrm{End}(A') = \mathcal{O}_K$.
- Do a random walk on the union of several cyclic-μ-isogeny graphs. (With our conditions, these graphs are disjoint unions of cycles).



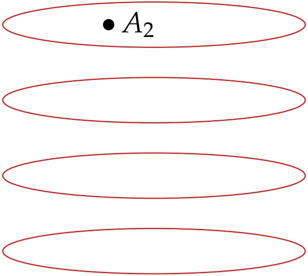
- The resulting abelian variety A_2 is uniformly random within the top layer of all (ℓ, ℓ, ℓ)-isogeny graphs.

Constructing an isogeny from a hyperelliptic to a plane quartic (simplified)

- A_2 is uniformly random within the top layer of sufficiently many (ℓ, ℓ, ℓ)-isogeny graphs.
- Vast majority of abelian varieties are in the bottom layer.

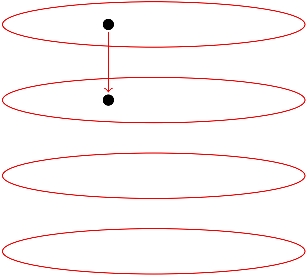
Constructing an isogeny from a hyperelliptic to a plane quartic (simplified)

- A_2 is uniformly random within the top layer of sufficiently many (ℓ, ℓ, ℓ)-isogeny graphs.
- Vast majority of abelian varieties are in the bottom layer.
- Descend the (ℓ_1, ℓ_1, ℓ_1)-isogeny graph.



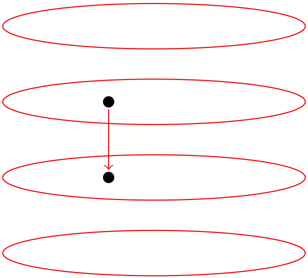
Constructing an isogeny from a hyperelliptic to a plane quartic (simplified)

- A_2 is uniformly random within the top layer of sufficiently many (ℓ, ℓ, ℓ)-isogeny graphs.
- Vast majority of abelian varieties are in the bottom layer.
- Descend the (ℓ_1, ℓ_1, ℓ_1)-isogeny graph.



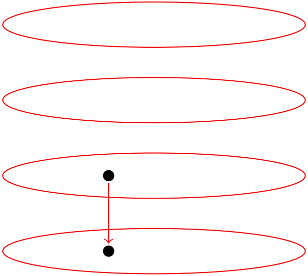
Constructing an isogeny from a hyperelliptic to a plane quartic (simplified)

- A_2 is uniformly random within the top layer of sufficiently many (ℓ, ℓ, ℓ)-isogeny graphs.
- Vast majority of abelian varieties are in the bottom layer.
- Descend the (ℓ_1, ℓ_1, ℓ_1)-isogeny graph.



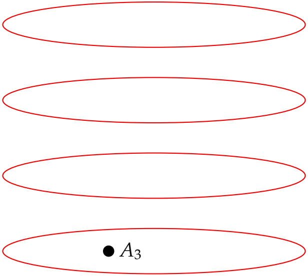
Constructing an isogeny from a hyperelliptic to a plane quartic (simplified)

- A_2 is uniformly random within the top layer of sufficiently many (ℓ, ℓ, ℓ)-isogeny graphs.
- Vast majority of abelian varieties are in the bottom layer.
- Descend the (ℓ_1, ℓ_1, ℓ_1)-isogeny graph.



Constructing an isogeny from a hyperelliptic to a plane quartic (simplified)

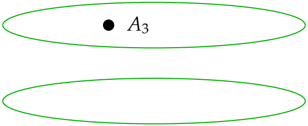
- A_2 is uniformly random within the top layer of sufficiently many (ℓ, ℓ, ℓ)-isogeny graphs.
- Vast majority of abelian varieties are in the bottom layer.
- Descend the (ℓ_1, ℓ_1, ℓ_1)-isogeny graph.



- Locally at ℓ_1, $\mathrm{End}^{\mathbb{R}}(A_3) = \mathbb{Z}[\mathrm{Frob}_q + \overline{\mathrm{Frob}_q}]$.

Constructing an isogeny from a hyperelliptic to a plane quartic (simplified)

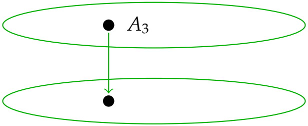
- A_2 is uniformly random within the top layer of sufficiently many (ℓ, ℓ, ℓ)-isogeny graphs.
- Vast majority of abelian varieties are in the bottom layer.
- Descend the (ℓ_1, ℓ_1, ℓ_1)-isogeny graph.
- Descend the (ℓ_2, ℓ_2, ℓ_2)-isogeny graph.



- Locally at ℓ_1, $\mathrm{End}^{\mathbb{R}}(A_3) = \mathbb{Z}[\mathrm{Frob}_q + \overline{\mathrm{Frob}_q}]$.

Constructing an isogeny from a hyperelliptic to a plane quartic (simplified)

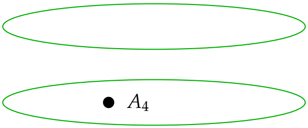
- A_2 is uniformly random within the top layer of sufficiently many (ℓ, ℓ, ℓ)-isogeny graphs.
- Vast majority of abelian varieties are in the bottom layer.
- Descend the (ℓ_1, ℓ_1, ℓ_1)-isogeny graph.
- Descend the (ℓ_2, ℓ_2, ℓ_2)-isogeny graph.



- Locally at ℓ_1, $\mathrm{End}^{\mathbb{R}}(A_3) = \mathbb{Z}[\mathrm{Frob}_q + \overline{\mathrm{Frob}_q}]$.

Constructing an isogeny from a hyperelliptic to a plane quartic (simplified)

- A_2 is uniformly random within the top layer of sufficiently many (ℓ, ℓ, ℓ)-isogeny graphs.
- Vast majority of abelian varieties are in the bottom layer.
- Descend the (ℓ_1, ℓ_1, ℓ_1)-isogeny graph.
- Descend the (ℓ_2, ℓ_2, ℓ_2)-isogeny graph.



- Locally at ℓ_1, $\mathrm{End}^{\mathbb{R}}(A_3) = \mathbb{Z}[\mathrm{Frob}_q + \overline{\mathrm{Frob}_q}]$.
- A_4 is a sufficiently random node; it is plane quartic with high probability.

(modulo many details.)

Known applications of isogeny graphs of abelian varieties

- We can use random sampling on isogeny graphs to attack DLP for a high percentage of hyperelliptic genus 3 curves under Heuristic H.

Known applications of isogeny graphs of abelian varieties

- We can use random sampling on isogeny graphs to attack DLP for a high percentage of hyperelliptic genus 3 curves under Heuristic H.
- Flynn and Ti [FT19] recently showed that an SIDH-style algorithm can theoretically be carried out with $(2,2)$- and $(3,3)$-isogeny graphs of supersingular two-dimensional abelian varieties over $\mathbb{F}_q$.

Known applications of isogeny graphs of abelian varieties

- We can use random sampling on isogeny graphs to attack DLP for a high percentage of hyperelliptic genus 3 curves under Heuristic H.
- Flynn and Ti [FT19] recently showed that an SIDH-style algorithm can theoretically be carried out with $(2, 2)$- and $(3, 3)$-isogeny graphs of supersingular two-dimensional abelian varieties over $\mathbb{F}_q$.

Both of these applications still need efficient implementations of isogenies of abelian varieties.

What don't we know?

- Efficient implementations of both cyclic isogenies and (ℓ, ℓ) or (ℓ, ℓ, ℓ)-isogenies are needed.

What don't we know?

- Efficient implementations of both cyclic isogenies and (ℓ, ℓ) or (ℓ, ℓ, ℓ)-isogenies are needed.
- Proof and/or more precise statement of Heuristic H is also needed.

What don't we know?

- Efficient implementations of both cyclic isogenies and (ℓ, ℓ) or (ℓ, ℓ, ℓ)-isogenies are needed.
- Proof and/or more precise statement of Heuristic H is also needed.
- Given that genus 2 arithmetic is less memory heavy and as efficient as elliptic curve arithmetic, computing isogenies may follow the same pattern?

What don't we know?

- Efficient implementations of both cyclic isogenies and (ℓ, ℓ) or (ℓ, ℓ, ℓ)-isogenies are needed.
- Proof and/or more precise statement of Heuristic H is also needed.
- Given that genus 2 arithmetic is less memory heavy and as efficient as elliptic curve arithmetic, computing isogenies may follow the same pattern?
- We only covered some cases of structure theorems for abelian varieties: much more to understand!

What don't we know?

- Efficient implementations of both cyclic isogenies and (ℓ, ℓ) or (ℓ, ℓ, ℓ)-isogenies are needed.
- Proof and/or more precise statement of Heuristic H is also needed.
- Given that genus 2 arithmetic is less memory heavy and as efficient as elliptic curve arithmetic, computing isogenies may follow the same pattern?
- We only covered some cases of structure theorems for abelian varieties: much more to understand!
- There are more options for creating useful graphs with more choices of abelian variety
  $\rightsquigarrow$ new (maybe post-quantum) applications?

Further reading

Background on (hyper)elliptic curves:

- Silverman, *The Arithmetic of Elliptic Curves*
  https://www.springer.com/gp/book/9780387094939
- Cassels and Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*
  https://doi.org/10.1017/CBO9780511526084
- Avanzi, Cohen, Doche, Frey, Lange, Nguyen, and Vercauteren, *Handbook of Hyperelliptic Curve Cryptography*
  https://www.hyperelliptic.org/HEHCC/
- Sutherland, *Isogeny volcanoes*
  https://arxiv.org/abs/1208.5370

Further reading

Mentioned in this presentation:

BCR10 Bisson, Cosset, and Robert, *AVIsogenies* (2010)
http://avisogenies.gforge.inria.fr/

BJW17 Brooks, Jetchev, and Wesolowski, *Isogeny graphs of ordinary abelian varieties* (2017)
https://arxiv.org/abs/1609.09793

C18 Costello, *Computing supersingular isogenies on Kummer surfaces* (2018)
https://eprint.iacr.org/2018/850

D06 Diem, *An Index Calculus Algorithm for Plane Curves of Small Degree* (2006)
https://link.springer.com/chapter/10.1007/11792086_38

DJRV17 Dudeanu, Jetchev, Robert, and Vuille, *Cyclic Isogenies for Abelian Varieties with Real Multiplication* (2017)
https://arxiv.org/abs/1710.05147

FT19 Flynn and Ti, *Genus Two Isogeny Cryptography* (2019)
https://eprint.iacr.org/2019/177

Further reading

Mentioned in this presentation (contd.):

JW17 Jetchev and Wesolowski, *Horizontal isogeny graphs of ordinary abelian varieties and the discrete logarithm problem* (2017)
https://arxiv.org/abs/1506.00522

JV10 Joux and Vitse, *Cover and Decomposition Index Calculus on Elliptic Curves made practical* (2010)
https://eprint.iacr.org/2011/020.pdf

K96 Kohel, *Endomorphism rings of elliptic curves over finite fields* (PhD thesis) (1996)
http://iml.univ-mrs.fr/~kohel/pub/thesis.pdf

M18 Martindale, *Isogeny graphs, modular polynomials, and applications* (PhD thesis) (2018)
http://www.martindale.info/research/Thesis.pdf

RS17 Renes and Smith, *qDSA: Small and Secure Digital Signatures with Curve-based Diffie-Hellman Key Pairs* (2017)
https://eprint.iacr.org/2017/518

S08 Smith, *Isogenies and the Discrete Logarithm Problem in Jacobians of Genus 3 Hyperelliptic Curves* (2008)
https://arxiv.org/abs/0806.2995