Connecting Kani's Lemma and the Bruhat-Tits tree to compute endomorphism rings of supersingular elliptic curves

Gabrielle Scullard (Penn State)
joint with Kirsten Eisenträger (Penn State)

March 26, 2024

Endomorphism ring problem

- **Problem:** Given a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, compute its endomorphism ring $\mathrm{End}(E)$.

Endomorphism ring problem

- **Problem:** Given a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, compute its endomorphism ring $\mathrm{End}(E)$.
  - Means: compute a basis for $\mathrm{End}(E)$.

Endomorphism ring problem

- **Problem:** Given a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, compute its endomorphism ring $\mathrm{End}(E)$.
  - Means: compute a basis for $\mathrm{End}(E)$.
- Usually two steps:

Endomorphism ring problem

- **Problem:** Given a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, compute its endomorphism ring $\mathrm{End}(E)$.
  - Means: compute a basis for $\mathrm{End}(E)$.
- Usually two steps:
  - Step 1: Compute a basis for a full-rank subring $\mathcal{O}_0 \subset \mathrm{End}(E)$.

Endomorphism ring problem

- **Problem:** Given a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, compute its endomorphism ring $\mathrm{End}(E)$.
  - Means: compute a basis for $\mathrm{End}(E)$.
- Usually two steps:
  - Step 1: Compute a basis for a full-rank subring $\mathcal{O}_0 \subset \mathrm{End}(E)$.
  - Step 2: From a full-rank subring $\mathcal{O}_0 \subset \mathrm{End}(E)$, compute $\mathrm{End}(E)$.

Endomorphism ring problem

- **Problem:** Given a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, compute its endomorphism ring $\mathrm{End}(E)$.
  - Means: compute a basis for $\mathrm{End}(E)$.
- Usually two steps:
  - Step 1: Compute a basis for a full-rank subring $\mathcal{O}_0 \subset \mathrm{End}(E)$.
  - Step 2: From a full-rank subring $\mathcal{O}_0 \subset \mathrm{End}(E)$, compute $\mathrm{End}(E)$.
- Our work gives a polynomial-time algorithm for Step 2, using repeated applications of Kani's lemma to compute $\mathrm{End}(E)$ locally on the Bruhat-Tits tree.

Endomorphism ring problem

- **Problem:** Given a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, compute its endomorphism ring $\mathrm{End}(E)$.
  - Means: compute a basis for $\mathrm{End}(E)$.
- Usually two steps:
  - Step 1: Compute a basis for a full-rank subring $\mathcal{O}_0 \subset \mathrm{End}(E)$.
  - Step 2: From a full-rank subring $\mathcal{O}_0 \subset \mathrm{End}(E)$, compute $\mathrm{End}(E)$.
- Our work gives a polynomial-time algorithm for Step 2, using repeated applications of Kani's lemma to compute $\mathrm{End}(E)$ locally on the Bruhat-Tits tree.

Outline

1. Kani's Lemma
2. Quaternion algebras and the Bruhat-Tits tree
3. Describe the algorithm (simplest case)

Kani's Lemma

A, A_1, A_2, B are elliptic curves

for abelian varieties

Kani's Lemma ([Kan97]; [Rob23a])

d_1 - isogeny

Let $f = f_1' \circ f_1 = f_2' \circ f_2$ such that $\cancel{\deg(f_1) = \deg(f_2') = d_1}$, $\underline{\deg(f_2) = \deg(f_1') = d_2}$, and $(d_1, d_2) = 1$.

f_2, f_1' d_2 - isogeny

$$\begin{tikzcd} A \arrow[r, "f_1"'] \arrow[d, "f_2"'] & A_1 \arrow[d, "f_1'"'] \\ A_2 \arrow[r, "f_2'"'] & B \end{tikzcd}$$

Then $F = \begin{pmatrix} f_1 & \tilde{f}_1' \\ -f_2 & f_2' \end{pmatrix}$ is d-isogeny $F : A \times B \to A_1 \times A_2$ with $d = d_1 + d_2$ and kernel $\operatorname{Ker} F = \{(\tilde{f}_1(P), f_1'(P)) : P \in A_1[d]\}$.

Application

detailed proof
and analysis

Algorithm 1 ([Rob23b]; [HLMW23])

Input: $\beta \in \mathrm{End}(E)$, $n \in \mathbb{Z}$
Output: TRUE if $\frac{\beta}{n} \in \mathrm{End}(E)$, FALSE if $\frac{\beta}{n} \notin \mathrm{End}(E)$

- Algorithm 1 runs in polynomial time (see Theorem 4.16 of [HLMW23] for more details)
- Uses Kani's Lemma with the following diagram, where α is an a-isogeny such that $\deg(\beta)/n^2 + a$ is powersmooth and coprime to $\deg(\beta)$.

$$\begin{tikzcd} E^4 \arrow[r, "\frac{\beta}{n}\cdot \mathrm{Id}_4"'] \arrow[d, "\alpha"'] & E^4 \arrow[d, "\alpha"'] \\ E^4 \arrow[r, "\frac{\beta}{n}\cdot \mathrm{Id}_4"'] & E^4 \end{tikzcd}$$

Applications of Algorithm 1

- Robert ([Rob23b]) first described Algorithm 1 to compute endomorphism rings of ordinary elliptic curves.

Applications of Algorithm 1

- Robert ([Rob23b]) first described Algorithm 1 to compute endomorphism rings of ordinary elliptic curves.
- Also used in work relating endomorphism ring computation and knowledge of a single non-scalar endomorphism ([HLMW23] [PW23])

  Compute End(E)

Containment Testing

- **Global test:** Given $\mathcal{O} \subset \mathrm{End}(E) \otimes \mathbb{Q}$ (specified by basis elements of the form $\frac{\beta}{n}$ with $\beta \in \mathrm{End}(E)$), we can efficiently determine if $\mathcal{O} \subset \mathrm{End}(E)$.

Containment Testing

- **Global test:** Given $\mathcal{O} \subset \mathrm{End}(E) \otimes \mathbb{Q}$ (specified by basis elements of the form $\frac{\beta}{n}$ with $\beta \in \mathrm{End}(E)$), we can efficiently determine if $\mathcal{O} \subset \mathrm{End}(E)$.
  - Test each basis element.

Containment Testing

- **Global test:** Given $\mathcal{O} \subset \mathrm{End}(E) \otimes \mathbb{Q}$ (specified by basis elements of the form $\frac{\beta}{n}$ with $\beta \in \mathrm{End}(E)$), we can efficiently determine if $\mathcal{O} \subset \mathrm{End}(E)$.
  - Test each basis element.
- **Local test:** Let q be prime. Given $\Lambda \subset \mathrm{End}(E) \otimes \mathbb{Q}_q$, we can efficiently determine if $\Lambda \subset \mathrm{End}(E) \otimes \mathbb{Z}_q$.

Containment Testing

$\left\{ \frac{\beta_1}{q_1^{e_1}}, \frac{\beta_2}{q_2^{e_2}}, \frac{\beta_3}{q_3^{e_3}}, \frac{\beta_4}{q_4^{e_4}} \right\}$

- **Global test:** Given $\mathcal{O} \subset \mathrm{End}(E) \otimes \mathbb{Q}$ (specified by basis elements of the form $\frac{\beta}{n}$ with $\beta \in \mathrm{End}(E)$), we can efficiently determine if $\mathcal{O} \subset \mathrm{End}(E)$.
  - Test each basis element.
- **Local test:** Let q be prime. Given $\Lambda \subset \mathrm{End}(E) \otimes \mathbb{Q}_q$, we can efficiently determine if $\Lambda \subset \mathrm{End}(E) \otimes \mathbb{Z}_q$.
  - Use global test for an appropriate global order.

Global Notation

We set some notation:

- $B_{p,\infty}$ = the quaternion algebra over $\mathbb{Q}$ ramified at p and ∞

Global Notation

We set some notation:

- $B_{p,\infty}$ = the quaternion algebra over $\mathbb{Q}$ ramified at p and ∞
    - Noncommutative rank 4 algebra over $\mathbb{Q}$

Global Notation

We set some notation:

- $B_{p,\infty}$ = the quaternion algebra over $\mathbb{Q}$ ramified at p and ∞
  - Noncommutative rank 4 algebra over $\mathbb{Q}$
- From now on, assume we are given:

Global Notation

We set some notation:

- $B_{p,\infty}$ = the quaternion algebra over $\mathbb{Q}$ ramified at p and ∞
  - Noncommutative rank 4 algebra over $\mathbb{Q}$
- From now on, assume we are given:
  - $\mathcal{O}_0 \subset \mathrm{End}(E)$

Global Notation

We set some notation:

- $B_{p,\infty}$ = the quaternion algebra over $\mathbb{Q}$ ramified at p and ∞
  - Noncommutative rank 4 algebra over $\mathbb{Q}$
- From now on, assume we are given:
  - $\mathcal{O}_0 \subset \mathrm{End}(E)$
  - a factorization for the quantity $D = \mathrm{discrd}(\mathcal{O}_0)$ (this can be computed from the basis)

Structure of the endomorphism ring

- End(E) is isomorphic to a maximal order in $B_{p,\infty}$

Structure of the endomorphism ring

- $\mathrm{End}(E)$ is isomorphic to a maximal order in $B_{p,\infty}$
- $\mathrm{End}(E)$ is equal to a maximal order in $\mathcal{O}_0 \otimes \mathbb{Q}$ which also contains $\mathcal{O}_0$.

Structure of the endomorphism ring

- End(E) is isomorphic to a maximal order in $B_{p,\infty}$
- End(E) is equal to a maximal order in $\mathcal{O}_0 \otimes \mathbb{Q}$ which also contains $\mathcal{O}_0$.
- [EHL+20]: Compute End(E) by computing all maximal orders containing $\mathcal{O}_0$ and testing each one
  - But they require some restrictions on $\mathcal{O}_0$ so that there are not exponentially many orders to test.

→ Computed all local maximal orders containing $\mathcal{O}_0$

Local-global principle

- **Local-global principle**: A global order $\mathcal{O}$ in a quaternion algebra is determined by its completions $\mathcal{O} \otimes \mathbb{Z}_q$ at each prime q.

Local-global principle

- **Local-global principle**: A global order $\mathcal{O}$ in a quaternion algebra is determined by its completions $\mathcal{O} \otimes \mathbb{Z}_q$ at each prime q.
- To compute $\mathrm{End}(E)$, we compute $\mathrm{End}(E) \otimes \mathbb{Z}_q$ for each prime q.

Local-global principle

- **Local-global principle**: A global order $\mathcal{O}$ in a quaternion algebra is determined by its completions $\mathcal{O} \otimes \mathbb{Z}_q$ at each prime q.
- To compute $\mathrm{End}(E)$, we compute $\mathrm{End}(E) \otimes \mathbb{Z}_q$ for each prime q.
- Maximality is a local property: For every prime q, $\mathrm{End}(E) \otimes \mathbb{Z}_q$ is a maximal order containing $\mathcal{O}_0 \otimes \mathbb{Z}_q$.

Local-global principle

- **Local-global principle**: A global order $\mathcal{O}$ in a quaternion algebra is determined by its completions $\mathcal{O} \otimes \mathbb{Z}_q$ at each prime q.
- To compute $\mathrm{End}(E)$, we compute $\mathrm{End}(E) \otimes \mathbb{Z}_q$ for each prime q.
- Maximality is a local property: For every prime q, $\mathrm{End}(E) \otimes \mathbb{Z}_q$ is a maximal order containing $\mathcal{O}_0 \otimes \mathbb{Z}_q$.
  - $\mathcal{O}_0 \otimes \mathbb{Z}_q$ is already maximal at all primes except those dividing D/p.

Local-global principle

- **Local-global principle**: A global order $\mathcal{O}$ in a quaternion algebra is determined by its completions $\mathcal{O} \otimes \mathbb{Z}_q$ at each prime q.
- To compute $\mathrm{End}(E)$, we compute $\mathrm{End}(E) \otimes \mathbb{Z}_q$ for each prime q.
- Maximality is a local property: For every prime q, $\mathrm{End}(E) \otimes \mathbb{Z}_q$ is a maximal order containing $\mathcal{O}_0 \otimes \mathbb{Z}_q$.
  - $\mathcal{O}_0 \otimes \mathbb{Z}_q$ is already maximal at all primes except those dividing D/p.
  - There is only one maximal order in $B_{p,\infty} \otimes \mathbb{Q}_p$.

Local-global principle

- **Local-global principle**: A global order $\mathcal{O}$ in a quaternion algebra is determined by its completions $\mathcal{O} \otimes \mathbb{Z}_q$ at each prime q.
- To compute $\mathrm{End}(E)$, we compute $\mathrm{End}(E) \otimes \mathbb{Z}_q$ for each prime q.
- Maximality is a local property: For every prime q, $\mathrm{End}(E) \otimes \mathbb{Z}_q$ is a maximal order containing $\mathcal{O}_0 \otimes \mathbb{Z}_q$.
  - $\mathcal{O}_0 \otimes \mathbb{Z}_q$ is already maximal at all primes except those dividing D/p.
  - There is only one maximal order in $B_{p,\infty} \otimes \mathbb{Q}_p$.
  - Interesting case: $q \neq p$

Switch to Local

Assume $q \neq p$.

- **Fact:** $B_{p,\infty} \otimes \mathbb{Q}_q \cong M_2(\mathbb{Q}_q)$.

Switch to Local

Assume $q \neq p$.

- **Fact:** $B_{p,\infty} \otimes \mathbb{Q}_q \cong M_2(\mathbb{Q}_q)$.
- **Fact:** All maximal orders of $M_2(\mathbb{Q}_q)$ are conjugate to $M_2(\mathbb{Z}_q)$.

Switch to Local

Assume $q \neq p$.

- **Fact:** $B_{p,\infty} \otimes \mathbb{Q}_q \cong M_2(\mathbb{Q}_q)$.
- **Fact:** All maximal orders of $M_2(\mathbb{Q}_q)$ are conjugate to $M_2(\mathbb{Z}_q)$.
- From now on, assume we have computed an isomorphism $f : \mathcal{O}_0 \otimes \mathbb{Q}_q \to M_2(\mathbb{Q}_q)$ such that $f(\mathcal{O}_0) \subset M_2(\mathbb{Z}_q)$

$\mathrm{End}(E) \otimes \mathbb{Q}_q \to$ matrices

Switch to Local

Assume $q \neq p$.

- **Fact:** $B_{p,\infty} \otimes \mathbb{Q}_q \cong M_2(\mathbb{Q}_q)$.
- **Fact:** All maximal orders of $M_2(\mathbb{Q}_q)$ are conjugate to $M_2(\mathbb{Z}_q)$.
- From now on, assume we have computed an isomorphism $f : \mathcal{O}_0 \otimes \mathbb{Q}_q \to M_2(\mathbb{Q}_q)$ such that $f(\mathcal{O}_0) \subset M_2(\mathbb{Z}_q)$
  - $\Lambda_0 := f(\mathcal{O}_0 \otimes \mathbb{Z}_q)$

Switch to Local

Assume $q \neq p$.

- **Fact:** $B_{p,\infty} \otimes \mathbb{Q}_q \cong M_2(\mathbb{Q}_q)$.
- **Fact:** All maximal orders of $M_2(\mathbb{Q}_q)$ are conjugate to $M_2(\mathbb{Z}_q)$.
- From now on, assume we have computed an isomorphism $f : \mathcal{O}_0 \otimes \mathbb{Q}_q \to M_2(\mathbb{Q}_q)$ such that $f(\mathcal{O}_0) \subset M_2(\mathbb{Z}_q)$
  - $\Lambda_0 := f(\mathcal{O}_0 \otimes \mathbb{Z}_q)$
  - $\Lambda_E := f(\mathrm{End}(E) \otimes \mathbb{Z}_q)$

Switch to Local

Assume $q \neq p$.

- **Fact:** $B_{p,\infty} \otimes \mathbb{Q}_q \cong M_2(\mathbb{Q}_q)$.
- **Fact:** All maximal orders of $M_2(\mathbb{Q}_q)$ are conjugate to $M_2(\mathbb{Z}_q)$.
- From now on, assume we have computed an isomorphism $f : \mathcal{O}_0 \otimes \mathbb{Q}_q \to M_2(\mathbb{Q}_q)$ such that $f(\mathcal{O}_0) \subset M_2(\mathbb{Z}_q)$
  - $\Lambda_0 := f(\mathcal{O}_0 \otimes \mathbb{Z}_q)$
  - $\Lambda_E := f(\mathrm{End}(E) \otimes \mathbb{Z}_q)$
  - Any orders we refer to will be orders in $M_2(\mathbb{Q}_q)$

Goal: Find Λ_E among $\overset{\text{maximal}}{\text{orders}}$ containing Λ_0

Bruhat-Tits tree

The Bruhat-Tits tree is a graph which organizes the maximal orders of $M_2(\mathbb{Q}_q)$.

Bruhat-Tits tree

The Bruhat-Tits tree is a graph which organizes the maximal orders of $M_2(\mathbb{Q}_q)$.

- Vertices $= \{\text{maximal orders } \Lambda \subset M_2(\mathbb{Q}_q)\}$
- Edges $= \{(\Lambda, \Lambda') | [\Lambda : \Lambda \cap \Lambda'] = q\}$

$$\begin{array}{c} \parallel \\ [\Lambda' : \Lambda \cap \Lambda'] \end{array}$$

Properties of the Bruhat-Tits tree

- $(q+1)$-regular tree

Properties of the Bruhat-Tits tree

- $(q+1)$-regular tree
- The **distance** between Λ and Λ' is the length of the unique path between them, denoted $d(\Lambda, \Lambda')$

Properties of the Bruhat-Tits tree

- $(q+1)$-regular tree
- The **distance** between Λ and Λ' is the length of the unique path between them, denoted $d(\Lambda, \Lambda')$
- Every maximal order Λ can be written as $\gamma^{-1} M_2(\mathbb{Z}_q)\gamma$, where γ is a product of matrices which encodes the steps of the path between the vertices $M_2(\mathbb{Z}_q)$ and Λ.

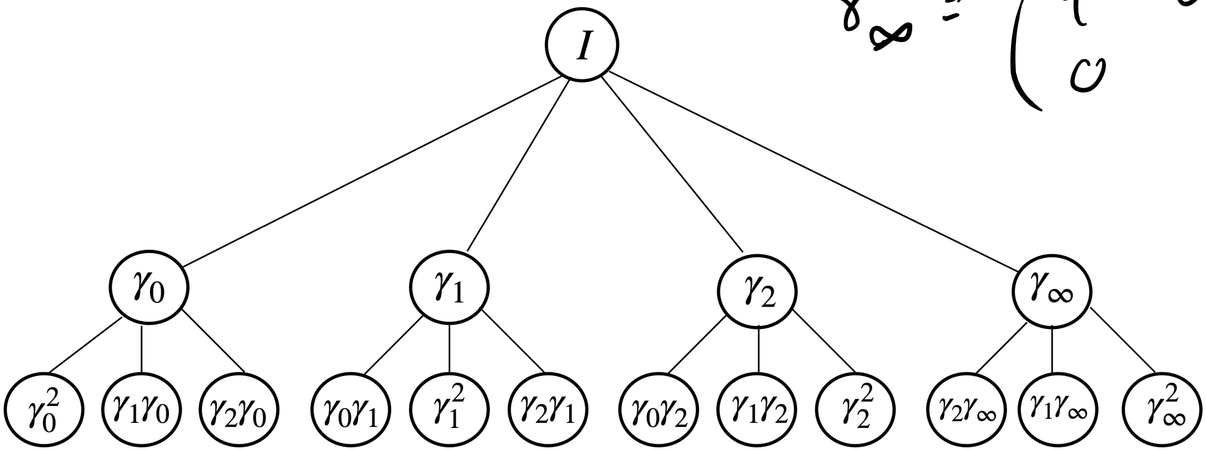
Properties of the Bruhat-Tits tree

- $(q+1)$-regular tree
- The **distance** between Λ and Λ' is the length of the unique path between them, denoted $d(\Lambda, \Lambda')$
- Every maximal order Λ can be written as $\gamma^{-1} M_2(\mathbb{Z}_q)\gamma$, where γ is a product of matrices which encodes the steps of the path between the vertices $M_2(\mathbb{Z}_q)$ and Λ.
- The set of maximal orders containing a (full-rank) order is a (finite) subtree.

Bruhat-Tits tree

$$\gamma_c = \begin{pmatrix} 1 & 0 \\ c & q \end{pmatrix}$$

$$\gamma_\infty = \begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}$$



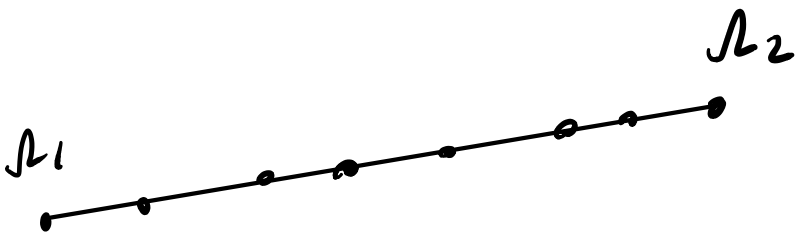
Truncated Bruhat-Tits tree for $q = 3$. The vertex labels are products of matrices $\gamma_0, \gamma_1, \gamma_2, \gamma_\infty$. The vertex labelled γ corresponds to the order $\gamma^{-1} M_2(\mathbb{Z}_q)\gamma$.

Moral: Maximal orders can be represented explicitly in terms of where they are located on the tree.

Intersections of two maximal orders

- If Λ_1, Λ_2, and Λ are maximal orders, then

$$\Lambda \supset \Lambda_1 \cap \Lambda_2 \iff \Lambda \text{ lies on the path between } \Lambda_1 \text{ and } \Lambda_2.$$



Intersection of three maximal orders

More complicated statement for intersections of three maximal orders.

Intersection of three maximal orders

More complicated statement for intersections of three maximal orders.

- Every finite intersection of maximal orders is an intersection of at most three maximal orders. ([Tu11])

Intersection of three maximal orders

More complicated statement for intersections of three maximal orders.

- Every finite intersection of maximal orders is an intersection of at most three maximal orders. ([Tu11])
- Corresponds to a neighborhood of a path (with respect to earlier-defined distance).

Special Case Algorithm

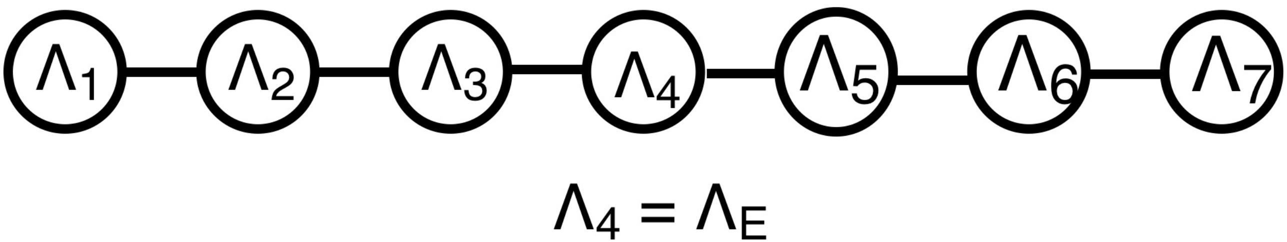
- If the subtree of orders containing Λ_0 is a path, generate a list of orders containing Λ_0 and perform a binary search to find Λ_E.
- Length of the path is at most $v_q(D) + 1$.

Special Case Algorithm

Example: The tree of maximal orders containing Λ_0 is the path between Λ_1 and Λ_7.
$\Rightarrow \Lambda_E$ is one of the Λ_i on this path.

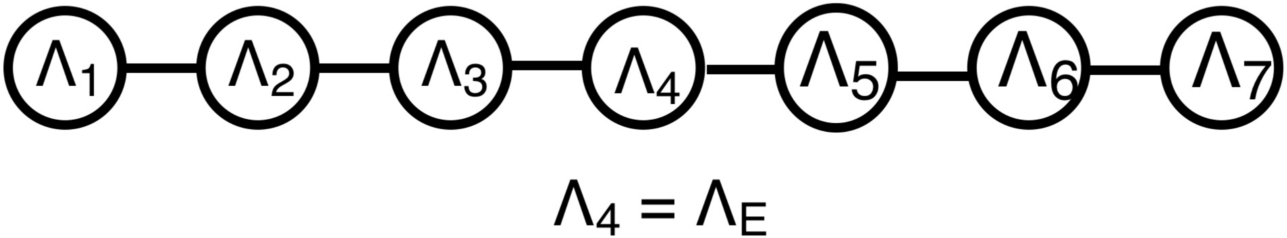
Special Case Algorithm

Example: The tree of maximal orders containing Λ_0 is the path between Λ_1 and Λ_7.
$\Rightarrow \Lambda_E$ is one of the Λ_i on this path.



Special Case Algorithm

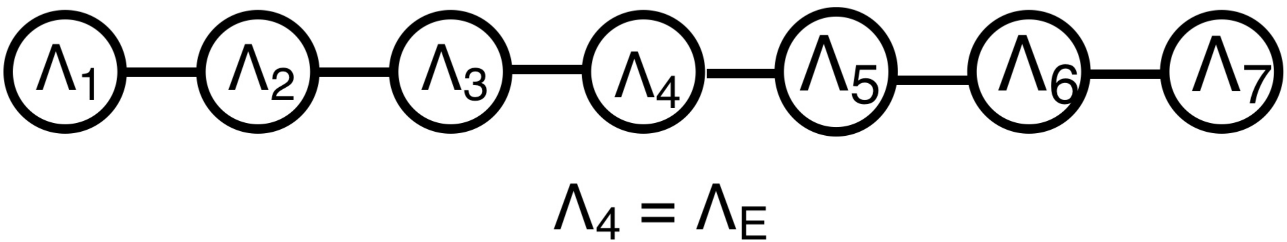
Example: The tree of maximal orders containing Λ_0 is the path between Λ_1 and Λ_7.
$\Rightarrow \Lambda_E$ is one of the Λ_i on this path.



Either $\Lambda_E \supset \Lambda_1 \cap \Lambda_4$ or $\Lambda_E \supset \Lambda_5 \cap \Lambda_7$.

Special Case Algorithm

Example: The tree of maximal orders containing Λ_0 is the path between Λ_1 and Λ_7.
$\Rightarrow \Lambda_E$ is one of the Λ_i on this path.



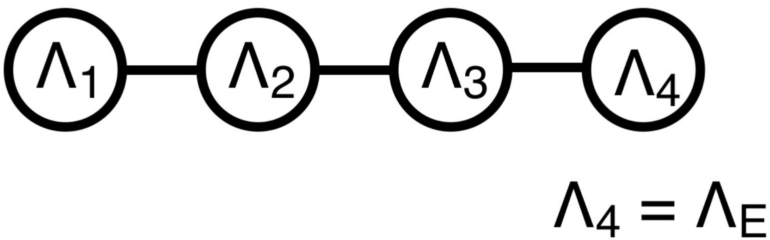
Either $\Lambda_E \supset \Lambda_1 \cap \Lambda_4$ or $\Lambda_E \supset \Lambda_5 \cap \Lambda_7$.
Local Test: $\Lambda_1 \cap \Lambda_4 \subset \Lambda_E$

Special Case Algorithm

$\Rightarrow \Lambda_E$ is one of $\Lambda_1, \Lambda_2, \Lambda_3, \Lambda_4$

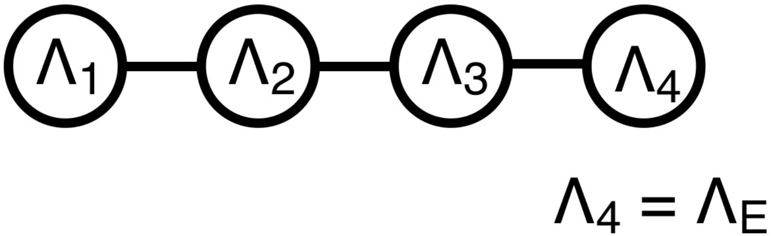
Special Case Algorithm

$\Rightarrow \Lambda_E$ is one of $\Lambda_1, \Lambda_2, \Lambda_3, \Lambda_4$



Special Case Algorithm

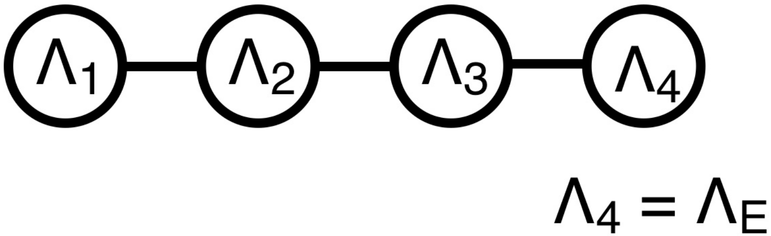
$\Rightarrow \Lambda_E$ is one of $\Lambda_1, \Lambda_2, \Lambda_3, \Lambda_4$



Either $\Lambda_E \supset \Lambda_1 \cap \Lambda_2$ or $\Lambda_E \supset \Lambda_3 \cap \Lambda_4$.

Special Case Algorithm

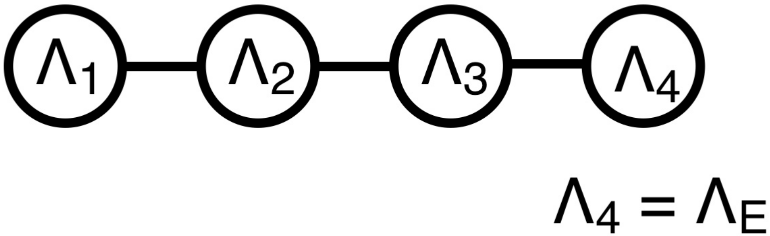
$\Rightarrow \Lambda_E$ is one of $\Lambda_1, \Lambda_2, \Lambda_3, \Lambda_4$



Either $\Lambda_E \supset \Lambda_1 \cap \Lambda_2$ or $\Lambda_E \supset \Lambda_3 \cap \Lambda_4$.
Local Test: $\Lambda_1 \cap \Lambda_2 \not\subset \Lambda_E$

Special Case Algorithm

$\Rightarrow \Lambda_E$ is one of $\Lambda_1, \Lambda_2, \Lambda_3, \Lambda_4$



Either $\Lambda_E \supset \Lambda_1 \cap \Lambda_2$ or $\Lambda_E \supset \Lambda_3 \cap \Lambda_4$.

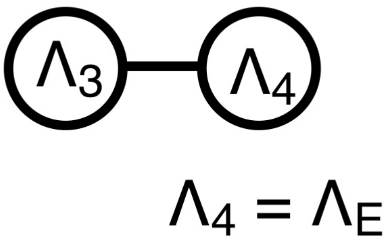
Local Test: $\Lambda_1 \cap \Lambda_2 \not\subset \Lambda_E$

Special Case Algorithm

$\Rightarrow \Lambda_E$ is one of Λ_3 or Λ_4

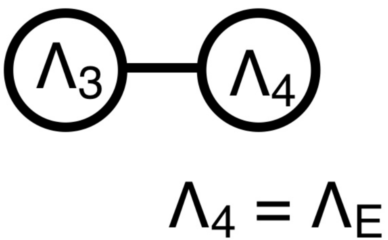
Special Case Algorithm

$\Rightarrow \Lambda_E$ is one of Λ_3 or Λ_4



Special Case Algorithm

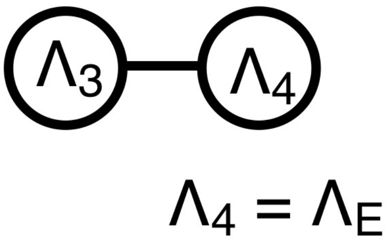
$\Rightarrow \Lambda_E$ is one of Λ_3 or Λ_4



Either $\Lambda_E \supset \Lambda_3$ or $\Lambda_E \supset \Lambda_4$.

Special Case Algorithm

$\Rightarrow \Lambda_E$ is one of Λ_3 or Λ_4



Either $\Lambda_E \supset \Lambda_3$ or $\Lambda_E \supset \Lambda_4$.

Local Test: $\Lambda_3 \not\subset \Lambda_E \Rightarrow \boxed{\Lambda_E = \Lambda_4}$

General case

- In general, not efficient to generate a list of all orders containing Λ_0.

General case

- In general, not efficient to generate a list of all orders containing Λ_0.
  - But Λ_E is at most $v_q(D)$ steps from $M_2(\mathbb{Z}_q)$.

General case

- In general, not efficient to generate a list of all orders containing Λ_0.
  - But Λ_E is at most $v_q(D)$ steps from $M_2(\mathbb{Z}_q)$.
- Use local containment testing for specially-chosen orders to deduce information about Λ_E.

General case

- In general, not efficient to generate a list of all orders containing Λ_0.
  - But Λ_E is at most $v_q(D)$ steps from $M_2(\mathbb{Z}_q)$.
- Use local containment testing for specially-chosen orders to deduce information about Λ_E.
  - Replaces intersections of two orders in the special case with intersections of three orders.

General case

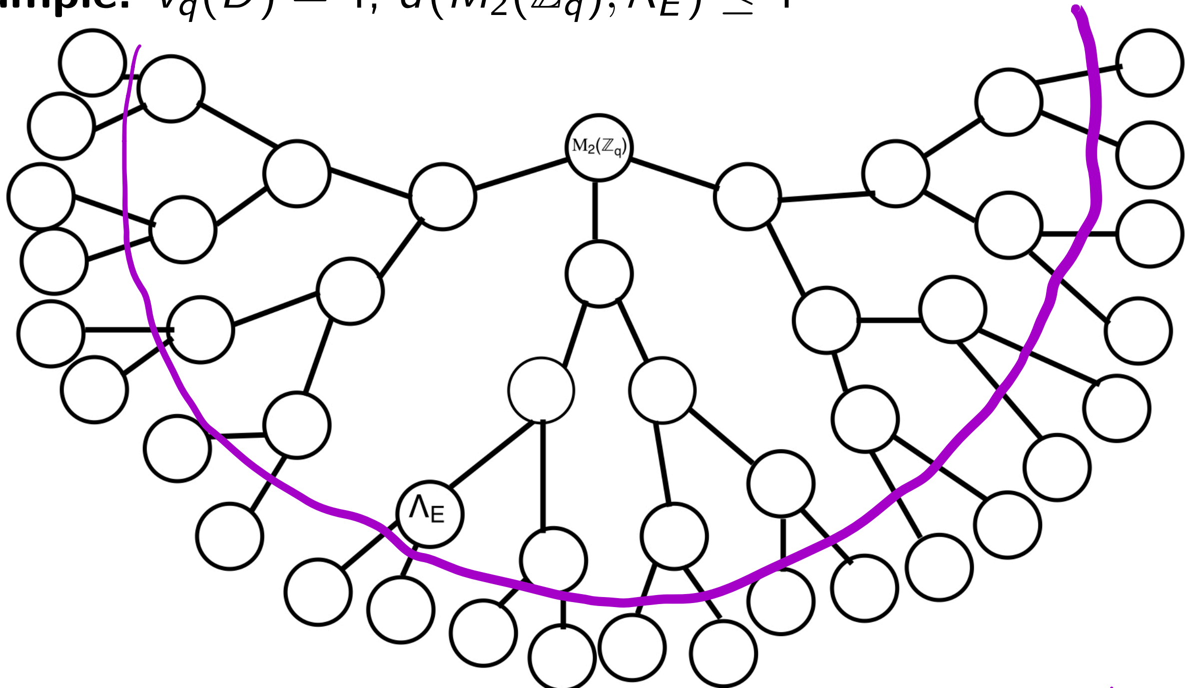
- In general, not efficient to generate a list of all orders containing Λ_0.
  - But Λ_E is at most $v_q(D)$ steps from $M_2(\mathbb{Z}_q)$.
- Use local containment testing for specially-chosen orders to deduce information about Λ_E.
  - Replaces intersections of two orders in the special case with intersections of three orders.
  - Many more details in the paper! [ES24]

General case

- Step 1: Compute the distance between $M_2(\mathbb{Z}_q)$ and Λ_E.
  - At most $v_q(D)$ orders for local containment testing.
- Step 2: Construct the path from $M_2(\mathbb{Z}_q)$ to Λ_E, one step at a time. (More costly)
  - There are $q+1$ choices for the first step: we can test each choice until we find the correct one.
  - There are q choices for all subsequent steps.

General case

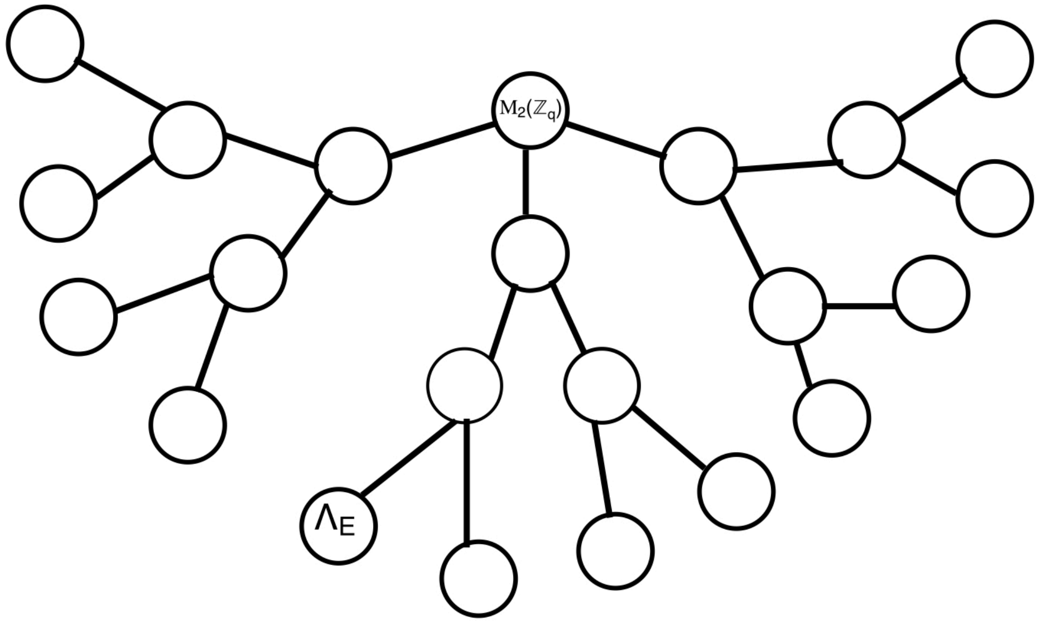
Example: $v_q(D) = 4,\ d(M_2(\mathbb{Z}_q), \Lambda_E) \leq 4$



Λ_E is above the purple curve

Local containment test: $d(M_2(\mathbb{Z}_q), \Lambda_E) \leq 3$

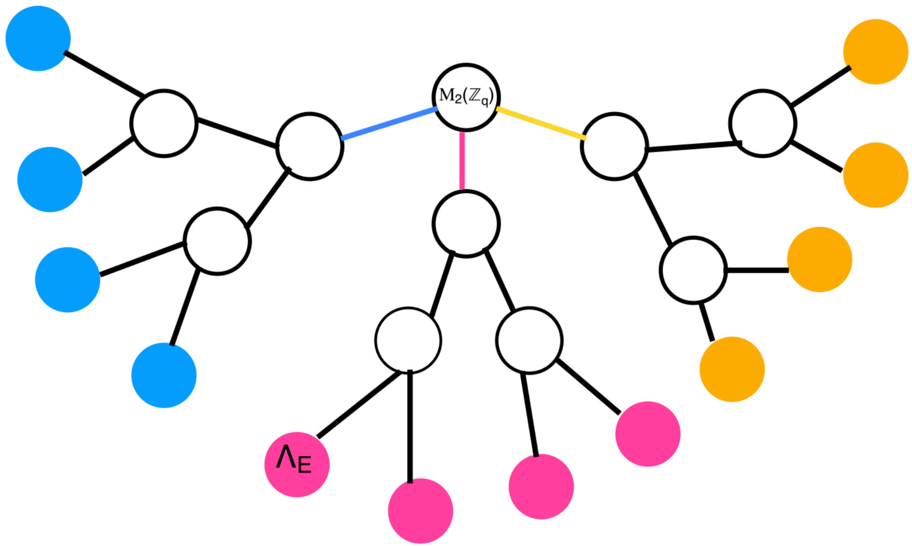
General case



Local containment test: $d(M_2(\mathbb{Z}_q), \Lambda_E) > 2 \Rightarrow d(M_2(\mathbb{Z}_q), \Lambda_E) = 3$

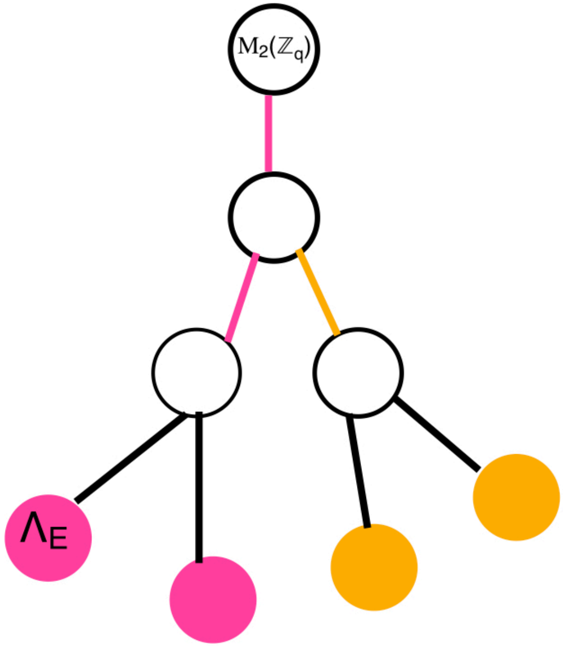
General case

$\Rightarrow \Lambda_E$ is one of the blue, pink, or yellow orders.



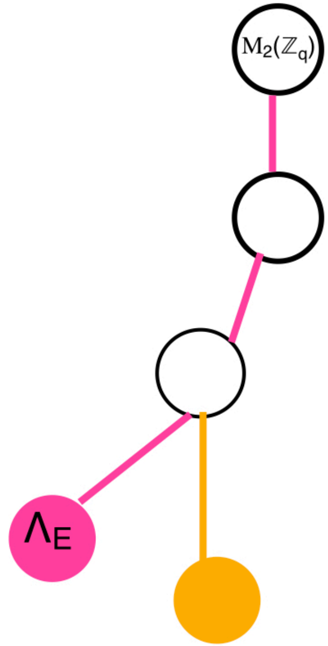
Check $q+1$ possibilities: $\Rightarrow \Lambda_E$ is one of the pink orders (determines the first step in the path).

General case



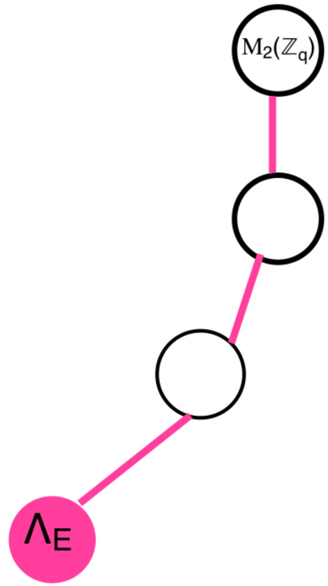
Check q possibilities: determines the next step in the path.

General case



Check q possibilities: determines the next step in the path.

General case



$\gamma^{-1} M_2(\mathbb{Z}_q)\, \gamma$

$=$

Found Λ_E!

Conclusion

- Kani's lemma can be used to test containment of local orders in the local endomorphism ring Λ_E
- Local containment testing can be used to find Λ_E
  - $\approx v_q(D)q$ steps to rule out exponentially many orders

Questions?

$$\frac{\beta}{n} \in \mathrm{End}(E)$$

$$\beta\big|_{E[n]} = 0$$

:)

References I

- Kirsten Eisenträger, Sean Hallgren, Chris Leonardi, Travis Morrison, and Jennifer Park, *Computing endomorphism rings of supersingular elliptic curves and connections to path-finding in isogeny graphs*, ANTS XIV—Proceedings of the Fourteenth Algorithmic Number Theory Symposium, Open Book Ser., vol. 4, Math. Sci. Publ., Berkeley, CA, 2020, pp. 215–232. MR 4235115
- Kirsten Eisentraeger and Gabrielle Scullard, *Connecting kani's lemma and path-finding in the bruhat-tits tree to compute supersingular endomorphism rings*, 2024, `https://arxiv.org/pdf/2402.05059.pdf`.
- Arthur Herlédan Le Merdy and Benjamin Wesolowski, *The supersingular endomorphism ring problem given one endomorphism*, Cryptology ePrint Archive, Paper 2023/1448, 2023, `https://eprint.iacr.org/2023/1448`.

References II

Ernst Kani, *The number of curves of genus two with elliptic differentials*, J. Reine Angew. Math. **485** (1997), 93–121. MR 1442190

Aurel Page and Benjamin Wesolowski, *The supersingular endomorphism ring and one endomorphism problems are equivalent*, Cryptology ePrint Archive, Paper 2023/1399, 2023, https://eprint.iacr.org/2023/1399.

Damien Robert, *Breaking SIDH in polynomial time*, Advances in cryptology—EUROCRYPT 2023. Part V, Lecture Notes in Comput. Sci., vol. 14008, Springer, Cham, [2023] ©2023, pp. 472–503. MR 4591005

Damien Robert, *Some applications of higher dimensional isogenies to elliptic curves*, Preprint, 2023, https://www.normalesup.org/~robert/pro/publications/articles/isogenies_applications.pdf.

References III

Fang-Ting Tu, *On orders of $M(2, K)$ over a non-Archimedean local field*, Int. J. Number Theory **7** (2011), no. 5, 1137–1149. MR 2825964