Orientations and Isogeny Graphs

Sarah Arpin
Universiteit Leiden

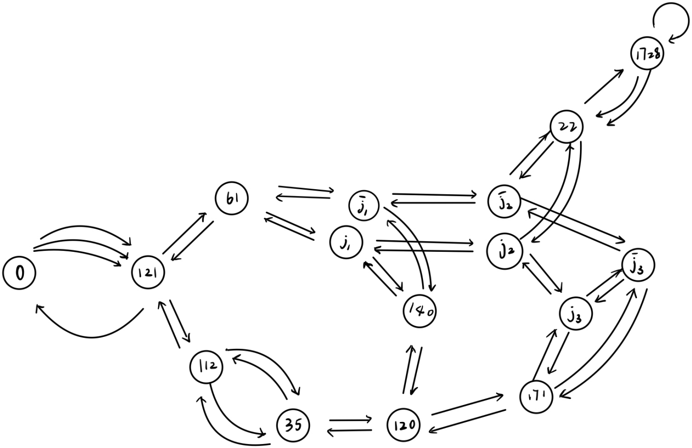
Women in Numbers 5 (WIN5)
Joint work with M. Chen, K. Lauter, R. Scheidler, K. Stange, and H. Tran

Isogeny Club

31 January 2023

Overview

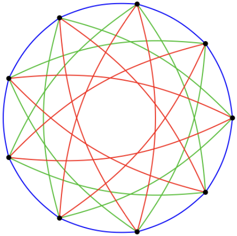
Our Favorite Graphs, I

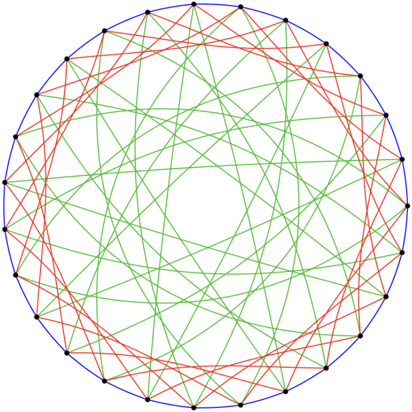


WIN5 II, `https://arxiv.org/pdf/2205.03976.pdf`

$p = 179, \ell = 2$

Our Favorite Graphs, II



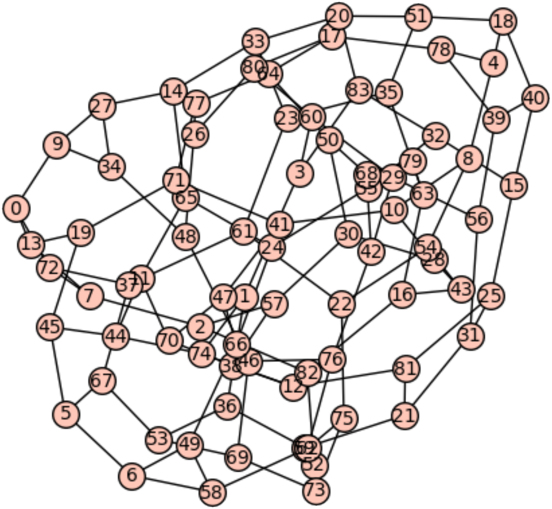


CSIDH, `https://eprint.iacr.org/2018/383.pdf`

$p = 419$, $\ell = 3, 5, 7$

Hard Problems

$p = 1009, \ell = 2$



[EHLMP, 2018]: **Pathfinding** in the ℓ-isogeny graph is equivalent to computing the endomorphism ring via **cycles** in the ℓ-isogeny graph

Motivating Questions

How do these hard problems change when we add orientations to our supersingular elliptic curves?

- Can we use the existence of oriented ℓ-isogeny volcanoes for **pathfinding** in the supersingular ℓ-isogeny graph?
  WIN5 I, 2022 “Orienteering with one endomorphism”.

- The rims of oriented ℓ-isogeny volcanoes form cycles. How do these cycles relate to **cycles** in the supersingular ℓ-isogeny graph?:
  WIN5 II, 2022 “Orientations and cycles in supersingular isogeny graphs”.

Class Group Action: CSIDH and $\mathbb{F}_p$-curves

For CSIDH conditions on p:

$$X := \{E : y^2 = x^3 + Ax^2 + x : A \in \mathbb{F}_p,\ E \text{ supersingular}\}.$$

X covers all of the $\mathbb{F}_p$-isomorphism classes of SECs with

$$\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}[\sqrt{-p}].$$

$\mathcal{C}\ell(\mathbb{Z}[\sqrt{-p}])$ acts on X as follows:
Take an integral ideal $\mathfrak{l} \in [\mathfrak{l}] \in \mathcal{C}\ell(\mathbb{Z}[\sqrt{-p}])$.

$$E[\mathfrak{l}] := \cap_{\alpha \in \mathfrak{l}} \ker(\alpha)$$

$$[\mathfrak{l}] * E := E/E[\mathfrak{l}]$$

To compute $\cap_{\alpha \in \mathfrak{l}} \ker(\alpha)$ when $\mathfrak{l} = (\ell, \pi_p - 1)$, it suffices to compute $\ker(\ell) \cap \ker(\pi_p - 1)$.
This action of $\mathcal{C}\ell(\mathbb{Z}[\sqrt{-p}])$ is **free** and **transitive** on X.

Class Group Action: Generally

Supersingular elliptic curve $E/\overline{\mathbb{F}_p} \Rightarrow \mathrm{End}(E) \cong M$, a maximal order of the quaternion algebra $B_{p,\infty}$.
Take $\mathcal{O} \subset B_{p,\infty}$, quadratic imaginary subring and define:

$SS_{\mathcal{O}} := \{E/\overline{\mathbb{F}_p}$ supersingular with $\mathcal{O} \subset \mathrm{End}(E)\}/\overline{\mathbb{F}_p}$-isomorphism

$\mathcal{C}\ell(\mathcal{O})$ acts on $SS_{\mathcal{O}}$ as follows:
Take an integral ideal $\mathfrak{l} \in [\mathfrak{l}] \in \mathcal{C}\ell(\mathbb{Z}[\sqrt{-p}])$.

$$E[\mathfrak{l}] := \cap_{\alpha\in\mathfrak{l}} \ker(\alpha)$$

$$[\mathfrak{l}] * E := E/E[\mathfrak{l}]$$

We want to refine this action to a subset of $SS_{\mathcal{O}}$, so we will put this on hold for a moment...

Orientations: Partial End(E) Information

K: imaginary quadratic field; E: supersingular elliptic curve.

Definition ((Primitive) Orientation)

A **K-orientation** on E is an embedding
$\iota : K \hookrightarrow \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} =: \mathrm{End}^0(E) \cong B_{p,\infty}$.
A K-orientation is an **$\mathcal{O}$-orientation** if $\iota(\mathcal{O}) \subseteq \mathrm{End}(E)$, and it is a **primitive $\mathcal{O}$-orientation** if $\iota(\mathcal{O}) = \mathrm{End}(E) \cap \iota(K)$.

Example

$p = 179$, $\mathrm{End}(E_{22}) \cong \mathbb{Z}\left\langle 1, 2i, \frac{1}{2} + \frac{3}{4}i + \frac{1}{4}ij, \frac{1}{2} + i - \frac{1}{2}j \right\rangle$.
$\iota : \mathbb{Q}(i) \hookrightarrow \mathrm{End}^0(E_{22})$ given via $i \mapsto i$.
ι is not a $\mathbb{Z}[i]$-orientation. It is a primitive $\mathbb{Z}[2i]$ orientation.

Definition (Conjugate)

Let ι be a $(K := \mathbb{Q}(\omega))$-orientation and define: $\bar{\iota}(\overline{\omega}) := \iota(\omega)$

Colo-Kohel 2020: https://arxiv.org/abs/2012.10803
Onuki 2020: https://arxiv.org/abs/2002.09894

Oriented isogenies

Let (E, ι) be a K-oriented supersingular elliptic curve.
An isogeny $\varphi : E \to E'$ induces an isogeny $\varphi : (E, \iota) \to (E', \varphi_* \iota)$, where we define:

$$(\varphi_* \iota) : K \to \mathrm{End}^0(E')$$

$$(\varphi_* \iota)(\alpha) := \frac{1}{[\deg \varphi]} \varphi \circ \iota(\alpha) \circ \hat{\varphi}.$$

If (E, ι) is a primitively $\mathcal{O}$-oriented supersingular elliptic curve, then $(E', \varphi_* \iota)$ is primitively $\mathcal{O}'$-oriented and one of the following is true:

- $\mathcal{O}' = \mathcal{O}$ (φ is horizontal),
- $\mathcal{O}' \subsetneq \mathcal{O}$ (φ is descending),
- $\mathcal{O}' \supsetneq \mathcal{O}$ (φ is ascending).

(E, ι) and (E', ι) are **K-isomorphic** if there exists an isomorphism $\eta : E \to E'$ such that $\eta_* \iota = \iota'$.

Oriented isogeny volcanoes

$p = 179, \ell = 2$

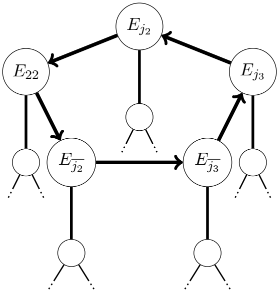
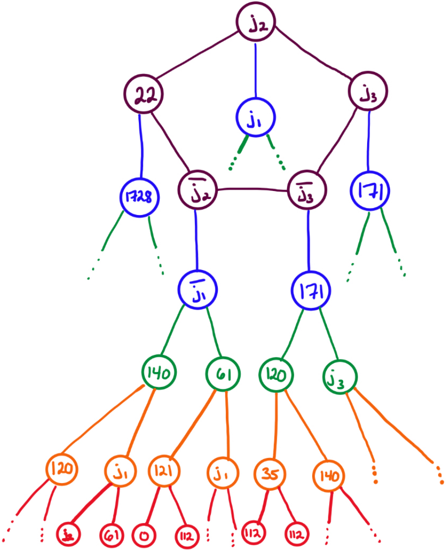
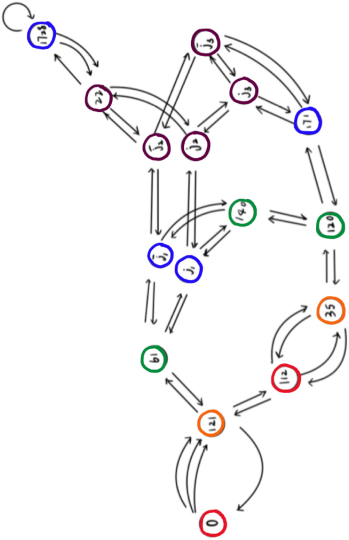


Figure: The $\mathbb{Q}(\sqrt{-47})$-oriented 2-isogeny volcano. Rim vertices are primitively oriented by $\mathcal{O} = \mathbb{Z}\left[\frac{1+\sqrt{-47}}{2}\right]$. Vertices on the altitude below the rim are primitively $\mathbb{Z}[\sqrt{-47}]$-oriented.

Each oriented isogeny volcano covers the ℓ-isogeny graph:





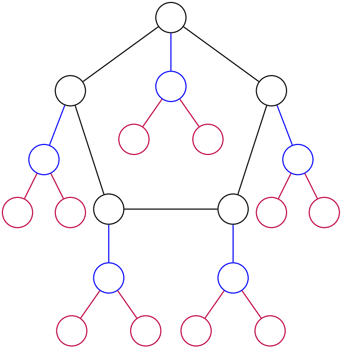
OSIG: Graph Structure (Our Favorite Graphs, III)

$\varphi : E \to F$, $\deg \varphi = \ell$, K-orientation $\iota : K \hookrightarrow \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$

The vertices on the **rim** of the volcano have a primitive $\mathcal{O}$-orientation, where $\mathcal{O}$ is an order in K of conductor f, $(f, \ell) = 1$.

The vertices on **altitude 1** of the volcano have a primitive $(\mathbb{Z} + \ell\mathcal{O})$-orientation.

The vertices on **altitude 2** of the volcano have a primitive $(\mathbb{Z} + \ell^2\mathcal{O})$-orientation.



There can be multiple volcanoes of $\mathcal{O}$-oriented curves.
The collection of volcanoes is called a **cordillera**.

The Technical Bit: $SS_{\mathcal{O}}^{pr}$ and $\mathcal{E}\ell\ell(\mathcal{O})$

Fix p, K, $\mathcal{O}$. Fix L'/K in which $\exists$ prime $\mathfrak{p}$ above p such that every EC with CM by $\mathcal{O}$ has a rep. over L' with good reduction at $\mathfrak{p}$ [AEC].

Definition ($SS_{\mathcal{O}}^{pr}$, $\mathcal{E}\ell\ell(\mathcal{O})$)

$SS_{\mathcal{O}}^{pr} :=$ {primitively $\mathcal{O}$-oriented supersingular EC's}$/K$-isom.
$\mathcal{E}\ell\ell(\mathcal{O}) := \{E/L' : \mathrm{End}(E) \cong \mathcal{O}$ with good red. at $\mathfrak{p}\}/$isom.

- $|\mathcal{E}\ell\ell(\mathcal{O})| = h(\mathcal{O})$.
- Normalizing wrt the invariant differential, $\exists!$ choice of primitive $\mathcal{O}$-orientation ι for $E \in \mathcal{E}\ell\ell(\mathcal{O})$.

Define $\rho : \mathcal{E}\ell\ell(\mathcal{O}) \to SS_{\mathcal{O}}^{pr}$ by $\rho(E) := (\widetilde{E}, \iota)$.

- ρ is injective.
- If p is ramified in $\mathcal{O}$, $\rho(\mathcal{E}\ell\ell(\mathcal{O})) = SS_{\mathcal{O}}^{pr}$.
- For $(E, \iota) \in SS_{\mathcal{O}}^{pr}$, (E, ι) or $(E^{(p)}, (\pi_p)_*\iota)$ is in $\rho(\mathcal{E}\ell\ell(\mathcal{O}))$.

Class group action: Walking the rim cycles

$(E, \iota) \in SS_{\mathcal{O}}^{pr}$.
$\mathfrak{a}$: an ideal of $\mathcal{O}$ coprime to p.

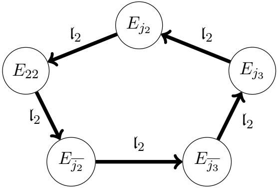
Define a subgroup:
$E[\iota(\mathfrak{a})] := \bigcap_{\alpha \in \iota(\mathfrak{a})} \ker(\alpha)$
and isogeny with this kernel:
$\varphi_{\mathfrak{a}} : E \to E/E[\iota(\mathfrak{a})]$.

The action of $Cl(\mathcal{O})$ on $SS_{\mathcal{O}}^{pr}$ is:
$\mathfrak{a} * (E, \iota) := (\varphi_{\mathfrak{a}}(E), (\varphi_{\mathfrak{a}})_* \iota)$.

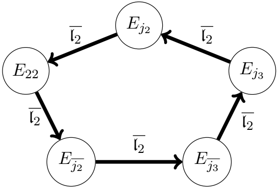
Theorem (Onuki, 2021)

The action of $Cl(\mathcal{O})$ is free and transitive on $\rho(\mathcal{E}\ell\ell(\mathcal{O}))$.

$p = 179, \ell = 2, K = \mathbb{Q}(\sqrt{-47})$,
$\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-47}}{2}\right]$, $(2)\mathcal{O}_K = \mathfrak{l}_2\overline{\mathfrak{l}_2}$

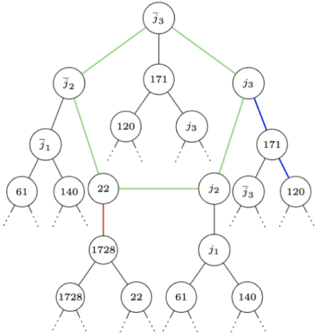


Conjugate vertex orientations:

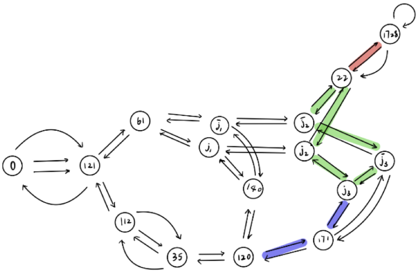


Cycles in ℓ-isogeny graphs

$p = 179, \ell = 2, \mathcal{O} = \mathbb{Z}[\sqrt{-47}]$



$\Longrightarrow$



Green rim corresponds to green cycle.

Isogeny cycles

How do we find cycles in the supersingular ℓ-isogeny graph?

- Wandering the graph and hoping to find collisions is inefficient. We can navigate the graph by finding paths to curves with known endomorphism rings (like E_{1728}).
- WIN5 I (2022) "Orienteering with one endomorphism" provides explicit algorithms.
- WIN5 II (2022) "Orientations and cycles in supersingular isogeny graphs" count cycles in $\mathcal{G}_\ell$ of a given length.

WIN5 I: `https://arxiv.org/abs/2201.11079`, WIN5 II: `https://arxiv.org/abs/2205.03976`

Definition (Isogeny cycle)

An isogeny cycle is a closed walk, forgetting basepoint, in $\mathcal{G}_\ell$ containing no backtracking (no consecutive edges compose to multiplication-by-ℓ) which is not a power of another closed walk (i.e., not equal to another closed walk repeated more than once).

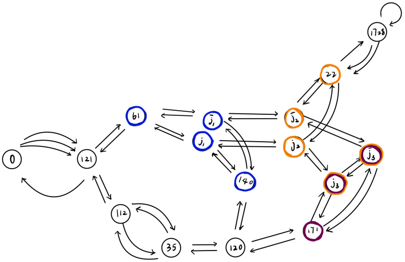
Bijection

Theorem (WIN5 II)

*The **isogeny-cycles of length** r in $\mathcal{G}_\ell$ are in bijection with the directed **rims of length** r of the union of all oriented supersingular ℓ-isogeny volcanoes over $\overline{\mathbb{F}}_p$, up to conjugation of the orientations.*

- The map from volcano rims to isogeny cycles is simply forgetting the orientation.
- The map from isogeny cycles to volcano rims consists of obtaining orientations from the endomorphisms defined by walking around the cycle.
- Vertices with extra automorphisms provide difficulties in cycle counting. In particular: isogenies with $j = 0, 1728$ as codomain. We make a careful choice for each such isogeny.

Example



isogeny cycle	length	endomorphism	$\mathcal{O}$	$h(\mathcal{O})$
$(j_3, \overline{j_3}, 171)$	3	$\frac{\pm 1 \pm \sqrt{-31}}{2}$	$\mathbb{Z}\left[\frac{1+\sqrt{-31}}{2}\right]$	3
$(61, j_1, 140, \overline{j_1})$	4	$\frac{\pm 5 \pm \sqrt{-39}}{2}$	$\mathbb{Z}\left[\frac{1+\sqrt{-39}}{2}\right]$	4
$(22, \overline{j_2}, \overline{j_3}, j_3, j_2)$	5	$\frac{\pm 9 \pm \sqrt{-47}}{2}$	$\mathbb{Z}\left[\frac{1+\sqrt{-47}}{2}\right]$	5

Table: Cycles of lengths 3, 4, and 5 in $\mathcal{G}_2$ with $p = 179$, with the associated endomorphisms to which the cycles compose.

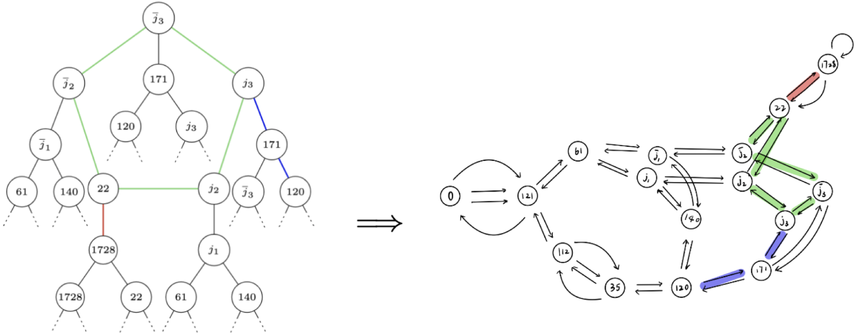
Example

isogeny cycle	length	endomorphism	$\mathcal{O}$	$h(\mathcal{O})$
$(22, \overline{j_2}, \overline{j_1}, 140, j_1, j_2)$	6	$\frac{\pm 13 \pm \sqrt{-87}}{2}$	$\mathbb{Z}\left[\frac{1+\sqrt{-87}}{2}\right]$	6
$(140, j_1, j_2, j_3, 171, 120)$ $(140, \overline{j_1}, \overline{j_2}, \overline{j_3}, 171, 120)$	6	$\frac{\pm 5 \pm \sqrt{-231}}{2}$	$\mathbb{Z}\left[\frac{1+\sqrt{-231}}{2}\right]$	12
$(0, 121, 112, 35, 112, 121)^*$	6	$\frac{\pm 3 \pm \sqrt{-247}}{2}$	$\mathbb{Z}\left[\frac{1+\sqrt{-247}}{2}\right]$	6
$(22, j_2, j_3, 171, \bar{j}_3, \bar{j}_2)$ $(0, 121, 112, 35, 112, 121)^*$	6	$\frac{\pm 1 \pm \sqrt{-255}}{2}$	$\mathbb{Z}\left[\frac{1+\sqrt{-255}}{2}\right]$	12
$(61, j_1, j_2, 22, \overline{j_2}, \overline{j_1})$	6	$\frac{\pm 11 \pm 3\sqrt{-15}}{2}$	$\mathbb{Z}\left[3\left(\frac{1+\sqrt{-15}}{2}\right)\right]$	6

Table: Isogeny cycles of length six, with the associated endomorphisms to which the cycles compose. *The two starred cycles are not uniquely determined by their j-invariants. The bijection between these two cycles and the two associated endomorphisms is not canonical, but we choose an arbitrary assignment and make a non-canonical bijection.

Path-finding

$p = 179, \ell = 2, \mathcal{O} = \mathbb{Z}[\sqrt{-47}]$



Combining the blue, green, and red paths in the oriented volcano, we find a path from E_{120} to E_{1728} in the supersingular 2-isogeny graph.

Walking to the rim

E: supersingular elliptic curve over $\overline{\mathbb{F}_p}$ with primitive $\mathcal{O}$-orientation ι. Let $\mathcal{O} = \langle \alpha \rangle \subseteq K$ and set $\theta := \iota(\alpha)$.

Task: Find a path of ℓ-isogenies from (E, ι) to the rim of a K-oriented ℓ-isogeny volcano.

- The number of steps to the rim is the number of times ℓ^2 divides the discriminant of θ. Call this number k.
- Translate θ to an ℓ-suitable translation (so that division-by-$[\ell]$ is possible for $\varphi_* \iota$ when φ is ascending)
- Any non-trivial $P \in \ker(\theta) \cap E[\ell]$ generates the kernel of an **ascending** ℓ-isogeny φ.
- Compute the resulting $(E', \varphi_* \iota)$
- Repeat steps (2) through (3) until the resulting oriented curve is on the rim.

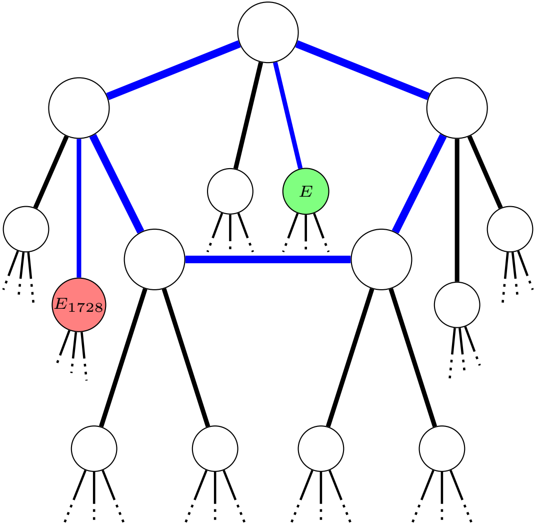
Explicit code: `https://github.com/SarahArpin/WIN5`

Explicit Classical Path-Finding Algorithm

Theorem (WIN5 I)

Given a supersingular elliptic curve $E/\overline{\mathbb{F}}_p$ and an endomorphism θ, we provide a classical algorithm for ℓ-isogeny path-finding that is subexponential in $\log p$ times a class number relating to θ.

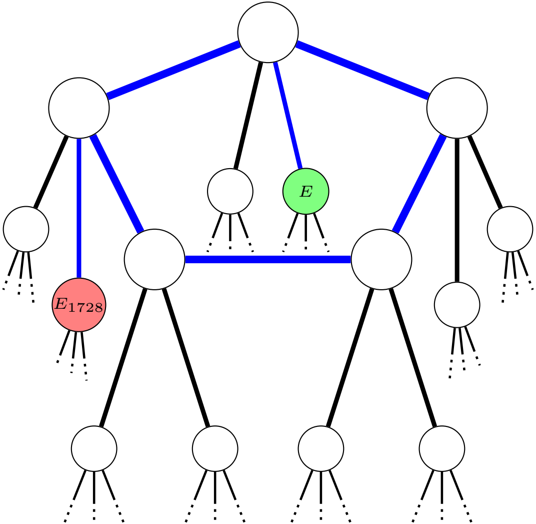
This algorithm is polynomial time in some cases.



Explicit Quantum Path-Finding Algorithm

Theorem (WIN5 I)

Given a supersingular elliptic curve $E/\overline{\mathbb{F}}_p$ and an endomorphism θ, we provide a quantum algorithm for finding a smooth isogeny to E_{1728} that runs in subexponential time in $\operatorname{disc}(\theta)$*, plus factors depending on θ's evaluation time.*



Conclusion

- Cycles in supersingular ℓ-isogeny graphs enable endomorphism ring computation.
- Oriented supersingular ℓ-isogeny graphs cover the supersingular ℓ-isogeny graph $\mathcal{G}_\ell$.
- The isogeny cycles in $\mathcal{G}_\ell$ are rims of oriented supersingular isogeny volcanoes.
- The behavior of primes above ℓ in the class groups of imaginary quadratic orders determines the number of isogeny cycles of a fixed length.
- Leaking information about small endomorphisms and certain classes of large endomorphisms leads to a subexponential path-finding algorithm on the supersingular ℓ-isogeny graph.

Thank you.

Any questions?