Adventures in Supersingularland: An Exploration of Supersingular Elliptic Curve Isogeny Graphs

Sarah Arpin
University of Colorado Boulder
Joint Mathematics Meeting - January 9th, 2021

Joint work with Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Travis Scholl, Jana Sotáková. [ACL^{+}19]

Overview

Motivation

Post-Quantum Cryptography

- NIST: 2015 call for proposals of post-quantum safe cryptography protocols
- Supersingular Isogeny Graph Cryptograhy: $\sim$ 15 years old: original hash function by Charles-Goren-Lauter [CGL06]; SIKE key exchange [Jao]

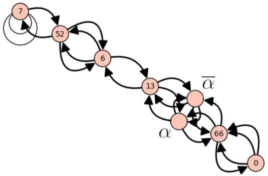
Hard Problems

- Path-finding in supersingular ℓ-isogeny graph
- Endomorphism ring computation [EHL$^+$18]

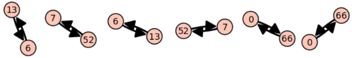
Three Graphs

- $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$:
  - Vertices: $\overline{\mathbb{F}}_p$-isomorphism classes of elliptic curves
  - Edges: ℓ-isogenies, up to equivalence
- $\mathcal{G}_\ell(\mathbb{F}_p)$:
  - Vertices: $\mathbb{F}_p$-isomorphism classes of elliptic curves
  - Edges: ℓ-isogenies, up to $\mathbb{F}_p$-equivalence
- Spine $\mathcal{S}$:
  - Subgraph of $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$
  - Vertices: $\overline{\mathbb{F}}_p$-isomorphism classes of curves with $j \in \mathbb{F}_p$
  - Edges: ℓ-isogenies up to $\overline{\mathbb{F}}_p$-equivalence

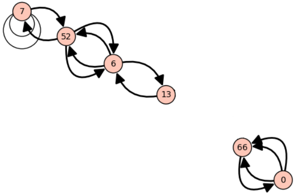
$\mathcal{G}_2(\overline{\mathbb{F}}_{89})$



$\mathcal{G}_2(\mathbb{F}_{89})$



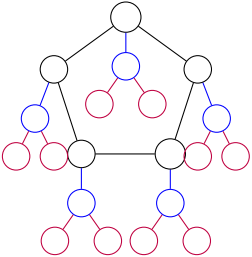
$\mathcal{S}$



Vertices labeled with j-invariants

$\mathcal{G}_\ell(\mathbb{F}_p)$: Volcanoes

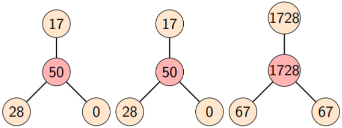
Ordinary ℓ-isogeny graphs



Kohel [Koh96];
Fouquet and Morain [FM02]

Supersingular ℓ-isogeny graphs $/\mathbb{F}_p$: p: a prime; E: supersingular elliptic curve over $\mathbb{F}_p$

$$\mathrm{End}_{\mathbb{F}_p}(E) \cong \begin{cases} \mathbb{Z}[\sqrt{-p}], & \text{floor} \\ \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right], & \text{surface} \end{cases}$$

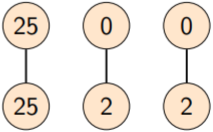


Structure of $\mathcal{G}_2(\mathbb{F}_p)$

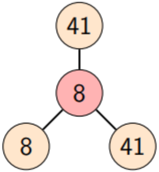
Delfs and Galbraith determined the structure of $\mathcal{G}_\ell(\mathbb{F}_p)$ [DG16].
For $\ell = 2$:

Theorem (Theorem 2.7 [DG16])

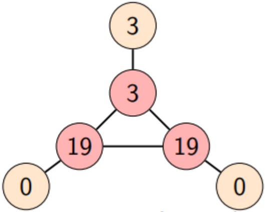
- $p \equiv 1 \pmod 4$*: Vertices paired together in isolated edges.*
- $p \equiv 3 \pmod 8$*: Vertices form volcanoes, each with four vertices: surface is one vertex connected to three vertices on the floor.*
- $p \equiv 7 \pmod 8$*: Vertices form a volcano; each surface vertex is connected 1:1 with the floor.*



$p = 29 \equiv 1 \pmod 4$



$p = 43 \equiv 3 \pmod 8$



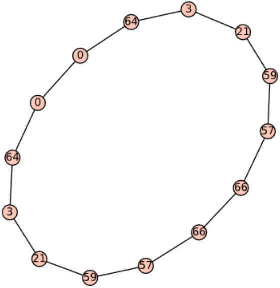
$p = 23 \equiv 7 \pmod 8$

Structure of $\mathcal{G}_\ell(\mathbb{F}_p)$

For $\ell > 2$:

Theorem (Theorem 2.7 [DG16])

- $\left(\frac{-p}{\ell}\right) = 1$: *two ℓ-isogenies*
- $\left(\frac{-p}{\ell}\right) = -1$: *no ℓ-isogenies*

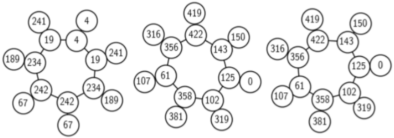


$p = 103$, $\ell = 3$

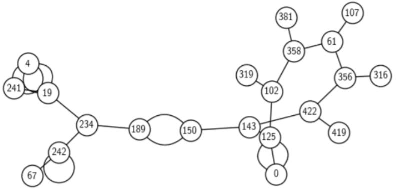
Possible changes, passing from $\mathcal{G}_\ell(\mathbb{F}_p)$ to $\overline{\mathbb{F}}_p$

Definition (3.13 ACL+19)

- If two distinct components of $\mathcal{G}_\ell(\mathbb{F}_p)$ have exactly the same set of vertices up to j-invariant, then they will **stack** over $\overline{\mathbb{F}}_p$.
- A component of $\mathcal{G}_\ell(\mathbb{F}_p)$ will **fold** if it contains both vertices corresponding to each j-invariant in its vertex set.
- Two distinct components of $\mathcal{G}_\ell(\mathbb{F}_p)$ will **attach with a new edge**.
- Two distinct components of $\mathcal{G}_\ell(\mathbb{F}_p)$ will **attach along a j-invariant** if one vertex of each share a j-invariant (only possible for $\ell > 2$).



(a) The $\mathcal{G}_2(\mathbb{F}_p)$ for $p = 431$



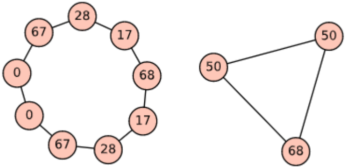
(b) The spine $\mathcal{S} \subset \mathcal{G}_2(\overline{\mathbb{F}}_p)$ for $p = 431$.

What actually happens for $\ell > 2$?

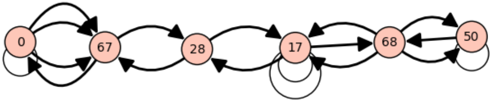
Theorem (Proposition 3.9 ACL+19)

Mapping $\mathcal{G}_\ell(\mathbb{F}_p)$ to $\mathcal{S}$, the only possible events are stacking, folding and n attachments by a new edge and m attachments along a j-invariant with $m + 2n \leq 2\ell(2\ell - 1)$.

$\mathcal{G}_3(\mathbb{F}_{83})$:



$\mathcal{S}$:

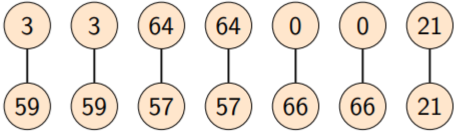


What actually happens for $\ell = 2$?

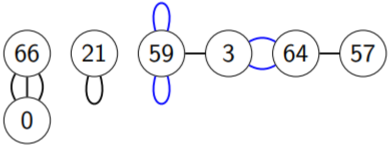
Theorem (Theorem 3.26 of ACL+19)

Mapping $\mathcal{G}_2(\mathbb{F}_p)$ to $\mathcal{S}$, only stacking, folding or at most one attachment by a new (double) edge are possible. No attachments by a j-invariant.

$\mathcal{G}_2(\mathbb{F}_{101})$:



$\mathcal{S}$:



Frobenius and Mirror Involution

$$E : y^2 = x^3 + ax + b \xrightarrow{Frob} E^{(p)} : y^2 = x^3 + a^p x + b^p$$
$$(x, y) \mapsto (x^p, y^p)$$
$$j(E) \mapsto j(E)^p$$

For $\alpha \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$, let $\overline{\alpha}$ denote the Frobenius conjugate of α.
If α is supersingular, so is $\overline{\alpha}$.

Definition (Mirror Involution on $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$)

If $\exists$ ℓ-isogeny $\phi : E(\alpha_1) \to E(\alpha_2)$ then $\exists$ ℓ-isogeny $\phi' : E(\overline{\alpha}_1) \to E(\overline{\alpha}_2)$.

Given a path in $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$:

$$\begin{tikzcd} \alpha \arrow[r, dash] & \beta \arrow[r, dash] & \gamma \end{tikzcd}$$

Mirror Involution gives another path:

$$\begin{tikzcd} \overline{\alpha} \arrow[r, dash] & \overline{\beta} \arrow[r, dash] & \overline{\gamma} \end{tikzcd}$$

Mirror Paths

When can we connect a path with its mirror involution?

- α_i: j-invariants in $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$
- a: j-invariant in $\mathbb{F}_p$

Option 1: Through an $\mathbb{F}_p$ vertex

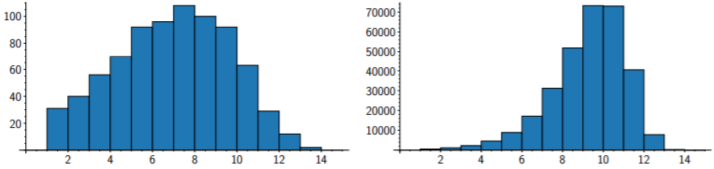
$$\alpha_0 \text{ --- } \alpha_1 \text{ --- } a \text{ --- } \overline{\alpha}_1 \text{ --- } \overline{\alpha}_0$$

Option 2: Through an ℓ-isogenous pair of conjugate vertices

$$\alpha_0 \text{ --- } \alpha_1 \text{ --- } \alpha_2 \text{ --- } \overline{\alpha}_2 \text{ --- } \overline{\alpha}_1 \text{ --- } \overline{\alpha}_0$$

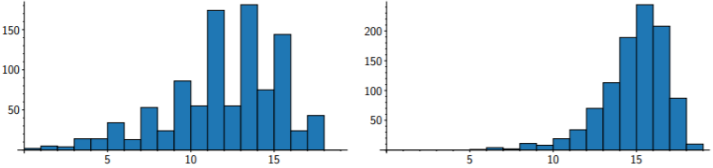
How often are paths of the first type? Second type?

How far are conjugate j-invariants in $\mathcal{G}_2(\overline{\mathbb{F}}_p)$?



(a) Distances between conjugate pairs. *(b) Distances between arbitrary pairs.*

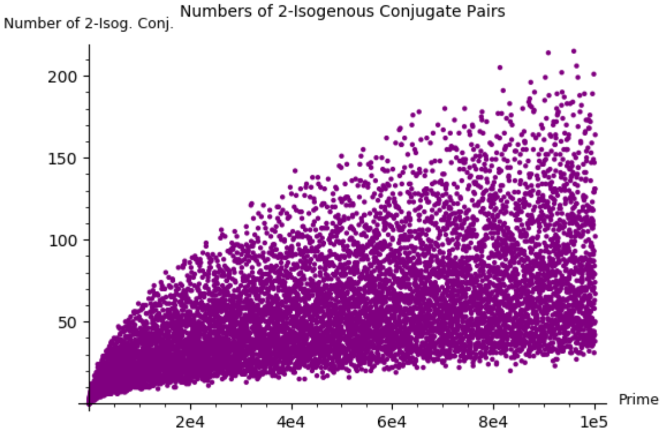
Figure 4.1: *Distances measured between conjugate pairs and arbitrary pairs of vertices not in $\mathbb{F}_p$ for the prime $p = 19489$.*



(a) Distances between conjugate pairs. *(b) Distances between arbitrary pairs.*

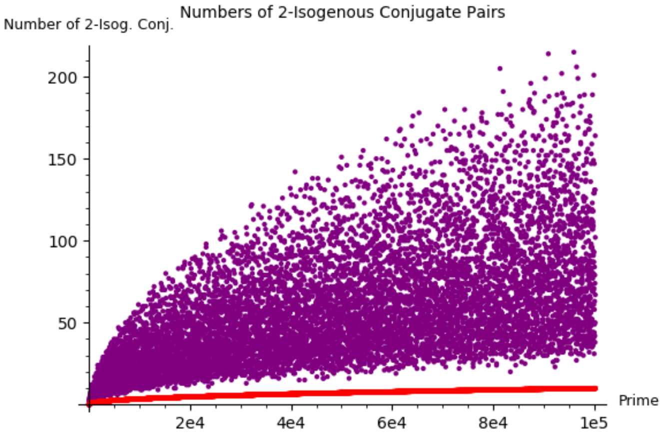
Figure 4.2: *Distances between 1000 randomly sampled pairs of arbitrary and conjugate vertices for the prime $p = 1000003$.*

How often are conjugate j-invariants 2-isogenous?



How often are conjugate j-invariants 2-isogenous?

[EHL+20]: Lower-bound on number of ℓ-isogenous conjugate j-invariants



Summary

- We understand completely how to map $\mathcal{G}_\ell(\mathbb{F}_p)$ into $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$.
- Mirror involution gives a new perspective on supersingular isogeny graph structure, further studied in [EHL$^+$20].
- Vertices which are conjugate appear to be closer than random vertices.
- Further heuristics on other interesting graph aspects can be found in our paper.

Thank you.

Sarah Arpin, Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Travis Scholl, and Jana Sotáková.
Adventures in Supersingularland.
submitted, 2019.
https://arxiv.org/abs/1909.07779.

Denis Charles, Eyal Goren, and Kristin Lauter.
Cryptographic hash functions from expander graphs.
Cryptology ePrint Archive, Report 2006/021, 2006.
https://eprint.iacr.org/2006/021.

C. Delfs and S. D. Galbraith.
Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$.
Des. Codes Cryptography, 78(2):425–440, 2016.
https://arxiv.org/pdf/1310.7789.pdf.

Kirsten Eisentraeger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit.
Supersingular isogeny graphs and endomorphism rings: reductions and solutions.
Eurocrypt 2018 Proceedings, 2018.

Kirsten Eisentraeger, Sean Hallgren, Chris Leonardi, Travis Morrison, and Jennifer Park.
Computing endomorphism rings of supersingular elliptic curves and connections to pathfinding in isogeny graphs, 2020.

Mireille Fouquet and François Morain.
Isogeny volcanoes and the sea algorithm.
ANTS 2002. Lecture Notes in Computer Science, vol 2369. Springer, Berlin, Heidelberg., 2002.

David Jao.
SIKE.
http://sike.org.
Accessed: 2019-11-13.

David Kohel.
Endomorphism rings of elliptic curves over finite fields.
Ph.D. thesis, University of California, Berkeley, 1996.