Superspecial Abelian Varieties

Lukas Zobernig

The University of Auckland

PAGEANT 2021

Introduction

- (Supersingular) Elliptic Curves
- Isogeny Graphs
- Polarisations
- Superspecial Abelian Varieties

(Supersingular) Elliptic Curves

Fix a prime p and consider a smooth projective curve E of genus 1 (an **elliptic curve**) over a finite field of characteristic p.

- Points on E form an abelian group under **addition**, with the **point at infinity** $O_E \in E$ serving as the identity element. This makes E an **abelian variety**. The **multiplication-by-**m map $[m] : E \to E$ acts as $[m]P = \underbrace{P + \cdots + P}_{m \text{ times}}$.
- Denote by $E[m]$ the kernel of $[m]$, i.e. $\{P \in E \mid [m]P = O_E\}$.
- For general m with $p \nmid m$ we have $E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$.
- We either have $E[p] \cong \mathbb{Z}/p\mathbb{Z}$ and E is called **ordinary**, or
- $E[p] \cong 0$ and E is called **supersingular**.
- The **endomorphism ring** $\mathrm{End}(E)$ in the ordinary case is an order in an imaginary quadratic field.
- In the supersingular case we have that $\mathrm{End}(E)$ is a maximal order $\mathcal{O}$ in the definite quaternion algebra $B_{p,\infty}$ ramified at p. Deuring showed a correspondence between the (finite number of) maximal orders of $B_{p,\infty}$ and supersingular elliptic curves.

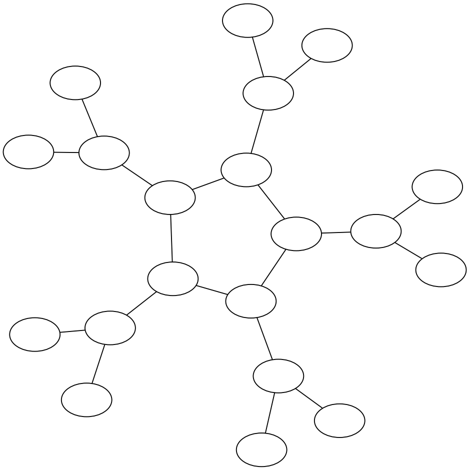
Isogeny Graphs

An isogeny $\phi : E_1 \to E_2$ is a surjective homomorphism with finite kernel between two elliptic curves E_1, E_2.

- Given a *separable* isogeny ϕ, its **degree** $\deg(\phi) = |\ker \phi|$ is the size of its kernel.
- For example, if $p \nmid m$ then $[m] : E \to E$ is a separable isogeny of degree m^2.
- Any finite subgroup G of E induces an isogeny $E \to E/G$. Vice versa, any isogeny $E \to E'$ determines a finite subgroup of E.
- Fixing a positive integer m, we can consider all outgoing degree-m isogenies of an elliptic curve E. Taking isomorphism classes of elliptic curves as vertices and degree-m isogenies as edges, this induces an m-**isogeny graph**.

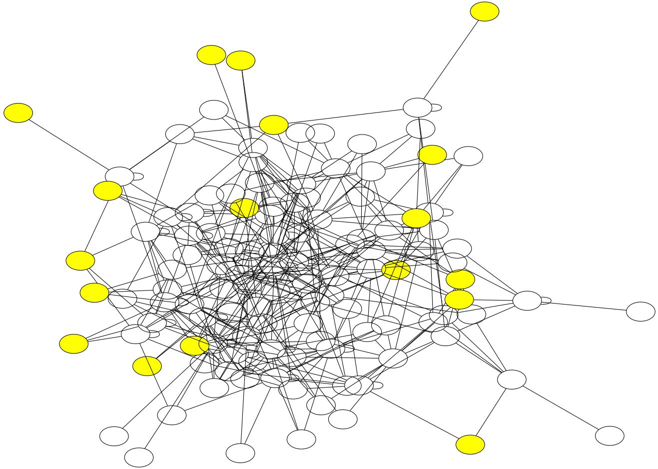
Ordinary Isogeny Graphs

These are so called **volcanos**: We find a circular **crater** which is connected to multiple descending **regular trees**. The length of the crater and depth of the trees is controlled by the endomorphism ring of the elliptic curves in the crater.



Supersingular Isogeny Graphs

Since there are only finitely many supersingular elliptic curves for each prime p, this is a finite graph. It is connected, regular, and an **optimal expander graph** (often called a **Ramanujan graph**).



Polarisations

Recall the point O_E acting as the identity for the group law on E. It essentially comes from a *canonical* **principal polarisation** on E. Formally, the situation for an abelian variety A is as follows:

- A polarisation $\mathcal{P}$ is certain data on A which induces an isogeny $\phi_{\mathcal{P}} : A \to A^\vee$ from A to its dual $A^\vee$.
- We call $\mathcal{P}$ **principal** if $\phi_{\mathcal{P}}$ is an isomorphism.

Example: (Elliptic) Curves

- Given a genus g curve C, we consider its **Picard group** $\mathrm{Pic}^0(C)$ (the group of degree-0 *Divisors* on C up to **rational equivalence**). The Picard group turns out to be an abelian variety.
- For an elliptic curve we have isomorphisms $\mathrm{Pic}^0(E) \cong (\mathrm{Pic}^0)^\vee(E) \cong E$. NB: The last isomorphism exists in genus 1, but not in genus 2 and higher.

Superspecial Abelian Varieties

Superspecial abelian varieties are one of the possible generalisations of supersingular elliptic curves to higher genus. We call an abelian variety A of genus $g \geq 2$ superspecial if $A \cong E^g$ for some supersingular elliptic curve E.

Theorem (Deligne, Ogus, Shioda, Oort)

Let A a superspecial abelian variety A of genus $g \geq 2$. Then

$$A \cong E_1 \times E_2 \times \cdots \times E_g$$

for any supersingular elliptic curves $E_1, \ldots, E_g$.

By the *Poincaré reducibility theorem* we have

$$\mathrm{End}(A) \cong M_g(\mathcal{O}),$$

i.e. the $g \times g$ matrices with entries in the maximal order $\mathcal{O}$ corresponding to the elliptic curve E.

A Finer Classification

We consider **principally polarised superspecial abelian varieties** instead, i.e. tuples $(A, \mathcal{L})$ of a superspecial abelian variety A and a principal polarisation $\mathcal{L}$.

An Embedding Into $\mathrm{End}(A)$

A polarisation $\mathcal{L}$ can be mapped to an element in $\mathrm{End}(A) \cong M_g(\mathcal{O})$ via $\mathcal{L} \mapsto \phi_{\mathcal{P}}^{-1} \circ \phi_{\mathcal{L}}$, where $\mathcal{P}$ is a fixed principal polarisation on the product E^g (recall that every polarisation $\mathcal{L}$ induces an isogeny $\phi_{\mathcal{L}} : A \to A^\vee$).

Theorem (Ibukiyama, Katsura, Oort)

The image of all principal polarisations in End(A) is

$$\left\{ H \in GL_g(\mathcal{O}) \,\middle|\, H^\dagger = H, H > 0 \right\},$$

i.e. the invertible, positive definite Hermitian matrices in $M_g(\mathcal{O})$.

Quaternion Hermitian Forms, Class Numbers, Isogenies

- We should really consider principally polarised abelian varieties **up to automorphism**.
- In matrix land for superspecial $(E^g, \mathcal{L})$ this corresponds to positive definite Hermitian matrices in $GL_g(\mathcal{O})$ **up to conjugation**.
- These can be counted via certain class numbers of quaternion Hermitian forms.
- Some explicit formulas are known, but are not very nice. For example, we find that the number of superspecial abelian surfaces is roughly p^3.
- Isogenies are very explicit: Let $A \cong E^g$ be a superspecial abelian variety, and let H and H' be the matrices corresponding to the principal polarisations $\mathcal{L}$ and $\mathcal{L}'$, respectively. Given an *admissible* isogeny $\phi : A \to A$ of degree ℓ^{gn}, we have $\phi^*\mathcal{L}' = \ell^n\mathcal{L}$ if and only if $M^\dagger H' M = \ell^n H$ for a matrix $M \in M_g(\mathcal{O})$ (which then corresponds to ϕ).

Superspecial $(2,2)$-isogeny Graph over $\mathbb{F}_{11^2}$