Lifted Isogeny Graphs

Honours Project

Shai Levin
Supervisor: Felipe Voloch

28 May 2021

Elliptic Curves and Isogenies

- **Elliptic Curves**. $y^2 = x^3 + ax + b$ Algebraic and geometric structure. Set of solutions over a field form a group.
- Morphisms of elliptic curves are called **isogenies**. Isogenies preserve group & geometric structure. Isogenies have a notion of degree (usually $\#$ kernel).
- These objects intersect algebraic geometry and number theory.
- But also combinatorics (as we shall see)!

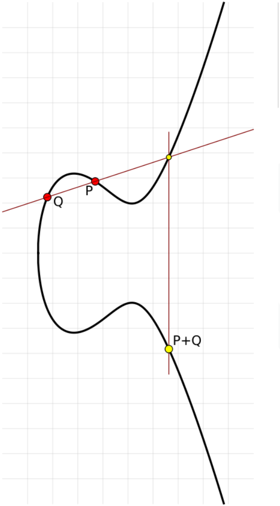

Figure 1: Group operation on $y^2 = x^3 - 4x + 7$

- Pick your favourite field K, and prime ℓ.
- Define a graph: **vertices** are all the elliptic curves over K, **edges** are isogenies between them of fixed degree ℓ.
- This graph has rich structure. Two classes of connected components.
- One **supersingular** component. The rest are called **ordinary** and form 'volcanoes' - finite if K is finite.
- Supersingular component of particular interest to cryptography. Finding paths on this graph is hard. Promising cryptographic primitive.

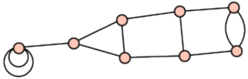

Figure 2: Supersingular component $K = \mathbb{F}_{97^2}$, $\ell = 2$

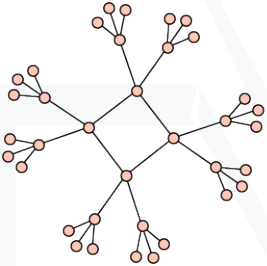

Figure 3: A volcano graph

Adding Γ Structure

- Same set up, take elliptic curves of a given component, and define a new graph. Fix another prime m.
- **Vertex** - (E, G): Elliptic curve E. From group structure of E a cyclic subgroup G of order m.
- **Edge** - $((E_1, G_1), (E_2, G_2))$: If isogeny $\phi : E_1 \to E_2$ such that $\phi(G_1) = G_2$.
- Forms *covering graphs* or *lifts* of the original isogeny graphs. 'Locally isomorphic' to base graph. Analogous to topological covering spaces.
- **Volcanoes:** Using this combinatorial result to prove that this 'lift' structure on a volcano yields a disjoint union of volcanoes.

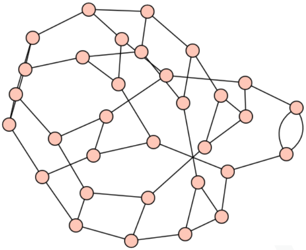

Figure 4: Γ structure applied to a supersingular component

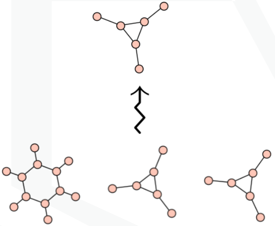

Figure 5: **Top**: an ordinary component, **Bottom**: corresponding Γ structure graph