Ш versus the volcano

Felipe Voloch

NTOC

June 2020

Abstract

We describe the structure of the Tate-Shafarevich group of constant elliptic curves over function fields by exploiting the volcano structure of isogeny graphs of elliptic curves over finite fields.

III vs the Volcano

Joint work with B. Creutz

Ш

$E/\mathbb{F}_q$ elliptic curve.

$C/\mathbb{F}_q$ curve and $K = \mathbb{F}_q(C)$ its function field.

Base change E/K constant elliptic curve.

$Ш(E/K) := \ker\left(\mathrm{H}^1(K,E) \to \bigoplus_v \mathrm{H}^1(K_v,E)\right)$

Theorem (Tate-Milne)

BSD holds for E/K and $Ш(E/K)$ is finite.

Isogeny graphs I

For k field and integer ℓ, the (undirected) ℓ-isogeny graph has vertices E/k, elliptic curves and edges representing ℓ-isogenies between them.

Many computational techniques on elliptic curves and some cryptographical constructions depend on navigating on this graph.

Isogeny graphs II

Theorem (Kohel)

Let $\phi : E \to E'$ be an isogeny of ordinary elliptic curves over k. Then $\mathrm{End}(E), \mathrm{End}(E')$ are isomorphic if and only if there exists an isogeny $E \to E'$ of degree relatively prime to $\deg \phi$

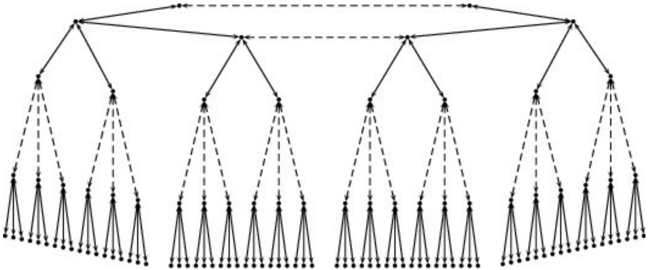
From this, Fouquet and Morain, obtained that that a component of the ℓ isogeny graph for a prime ℓ over a finite field k consisting of ordinary curves has the structure of a volcano.

Volcano graphs

A graph with vertex set V is an ℓ-volcano graph if there is a partition $V = V_1 \cup V_2 \cdots \cup V_m$, m is the height of the volcano, V_1 the base and V_m the crater or top. In addition, the induced graph on V_m is a cycle (the edges on this subgraph are called horizontal), the degree of all vertices not on V_1 is $\ell + 1$, the degree of the vertices in V_1 is 1, for each vertex on $V_i, i < m$, there is a unique edge from it to a vertex in V_{i+1} (these are called upward edges) and for each vertex on $V_i, i > 1$, the other edges go to vertices in V_{i-1} (these are called downward edges). The vertices in V_i are said to have height (or level) i.

Volcanos

Volcano with $\ell = 3$



Main results

E, E_1, F elliptic curves over k in the same component of the ℓ-isogeny graph, $K = k(F)$ and $h(E)$ is the level of E in the graph.

Theorem 1

Suppose $\phi : E \to E_1$ is an isogeny of prime degree ℓ. TFAE

1. $h(E_1) < h(E) \leq h(F)$;
2. $E_1(K)/\phi(E(K)) = E_1(k)/\phi(E(k))$;
3. $\text{Ш}(E/K)[\phi] = \text{Ш}(E/K)[\ell]$ *has rank* 2.

Main results II

Theorem 2

If $E, F/k$ are ordinary and isogenous then, as abelian groups,

$$Ш(E/k(F)) \simeq ((\mathrm{End}(E) \cap \mathrm{End}(F))/\mathbb{Z}[\pi])^2,$$

where $\pi \in \mathrm{End}(E), \mathrm{End}(F)$ is the k-Frobenius and the intersection is taken in $\mathbb{Q}(\pi)$.

Idea of proof

Descent sequence

$$0 \to E_1(K)/\phi(E(K)) \to \mathrm{Sel}^{\phi}(E_1/K) \to Ш(E/K)[\phi] \to 0$$

Suppose $h(E_1) < h(E) \leq h(F)$. Let $\alpha : F \to E_1$ isogeny. Factor α as $\alpha_\ell \circ \alpha'$ with $\alpha' : F \to F'$ of degree prime to ℓ and $\alpha_\ell : F' \to E_1$ of ℓ-primary degree. By Kohel's theorem $h(F) = h(F')$. So α_ℓ factors through ϕ using the structure of the ℓ-isogeny graph.

THANK YOU