18.783 Elliptic Curves
Lecture 22

Shiva Chidambaram

November 30, 2023

ℓ-isogeny graphs

Throughout this lecture, k is a field and $\ell \neq \mathrm{char}(k)$ is a prime.
Let E_1/k be an elliptic curve and let $j_1 := j(E_1)$. The k-rational roots of

$$\phi_\ell(Y) := \Phi_\ell(j_1, Y)$$

are precisely the j-invariants of the elliptic curves E_2/k that are ℓ-isogenous to E_1.

Definition

The ℓ-isogeny graph $G_\ell(k)$ is the directed graph with vertex set k and edges (j_1, j_2) present with multiplicity equal to the multiplicity of j_2 as a root of $\Phi_\ell(j_1, Y)$.

$G_\ell(k)$ may contain self-loops (ℓ-isogenies may be endomorphisms), and edges may occur with multiplicity (ℓ-isogenies $E_1 \to E_2$ may have distinct kernels).

If (j_1, j_2) is an edge in $G_\ell(k)$ then so is (j_2, j_1) (there is a dual isogeny).
For $j_1, j_2 \notin \{0, 1728\}$ these edges have the same multiplicity.

Horizontal and vertical ℓ-isogenies

Theorem

Let $\varphi\colon E \to E'$ be an ℓ-isogeny of elliptic curves over k. Then $\mathrm{End}^0(E') \simeq \mathrm{End}^0(E)$. If $\mathrm{End}^0(E) = K$ is an imaginary quadratic field then $\mathrm{End}(E) = \mathcal{O}$ and $\mathrm{End}(E') = \mathcal{O}'$ are orders in K such that one of the following holds:

$$\text{(i) } \mathcal{O} = \mathcal{O}', \qquad \text{(ii) } [\mathcal{O} : \mathcal{O}'] = \ell, \qquad \text{(iii) } [\mathcal{O}' : \mathcal{O}] = \ell.$$

Proof: To the board!

Definition

Let $\varphi\colon E \to E'$ be an ℓ-isogeny of with $\mathrm{End}(E) = \mathcal{O}$ and $\mathrm{End}(E') = \mathcal{O}'$ rank 2.

(i) When $\mathcal{O} = \mathcal{O}'$ we say that φ is horizontal;

(ii) When $[\mathcal{O} : \mathcal{O}'] = \ell$ we say that φ is descending;

(iii) When $[\mathcal{O}' : \mathcal{O}] = \ell$ we say that φ is ascending.

We collectively refer to ascending and descending isogenies as vertical isogenies.

ℓ-isogeny graphs over $\mathbb{C}$

Theorem

Let $E/\mathbb{C}$ be an elliptic curve with CM by an order $\mathcal{O}$ of discriminant D. If $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ then E admits $1 + \left(\frac{D}{\ell}\right)$ horizontal, $\ell - \left(\frac{D}{\ell}\right)$ descending, and no ascending ℓ-isogenies. Otherwise E admits no horizontal, ℓ descending, and one ascending ℓ-isogenies.

Proof: To the board!

Over the complex numbers ℓ-isogeny graphs are (countably) infinite: there are infinitely many connected components (there is at least one for each $\mathcal{O} \subseteq \mathcal{O}_K$ with $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$), and each component is infinite, since we can always keep descending.

Vertices corresponding to elliptic curves with $\ell | [\mathcal{O}_K : \mathcal{O}]$ all look the same: there is a single ascending edge and ℓ descending edges.

ℓ-isogeny graphs over finite fields

Lemma

Let $\mathcal{O}$ be an imaginary quadratic order of discriminant D and $q \perp D$ be a prime power. The set $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ is either empty or has cardinality $h(D)$. If $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ is nonempty, so is $\mathrm{Ell}'_{\mathcal{O}}(\mathbb{F}_q)$ for every imaginary quadratic order $\mathcal{O}'$ that contains $\mathcal{O}$.

Proof: To the board!

Corollary

Let $E/\mathbb{F}_q$ be an elliptic curve with CM by $\mathcal{O}$ of discriminant $D \perp q$ in an imaginary quadratic field K, and let $\ell \nmid q$ be prime. Then E admits $1 + (\frac{D}{\ell})$ horizontal ℓ-isogenies and one or zero ascending ℓ-isogenies, depending on whether $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ or not. The number of descending ℓ-isogenies admitted by E over $\mathbb{F}_q$ is either zero or $\ell - (\frac{D}{\ell})$, depending on whether $\mathrm{Ell}_{\mathcal{O}'}(\mathbb{F}_q)$ is empty or not, where $\mathcal{O}'$ is the order of index ℓ in $\mathcal{O}$.

The CM action over finite fields

If $E/\mathbb{F}_q$ is an elliptic curve with CM by an imaginary quadratic order $\mathcal{O}$ and $\mathfrak{a}$ is a proper $\mathcal{O}$-ideal, then we have an $\mathfrak{a}$-torsion subgroup

$$E[\mathfrak{a}] := \{P \in E(\overline{\mathbb{F}}_q) : \alpha(P) = 0 \text{ for all } \alpha \in \mathfrak{a}\}.$$

Provided the norm of $\mathfrak{a}$ is prime to q, there is a corresponding separable isogeny $\varphi_{\mathfrak{a}} \colon E \to E'$ with $\ker \varphi_{\mathfrak{a}} = E[\mathfrak{a}]$ and $\deg \varphi_{\mathfrak{a}} = \mathrm{N}\mathfrak{a}$ which is unique up to isomorphism.

Every ideal class contains infinitely many prime ideals, so we can always realize the CM action using horizontal ℓ-isogenies.

Corollary

Let $\mathcal{O}$ be an imaginary quadratic order of discriminant D and let $\mathbb{F}_q$ be a finite field with $q \perp D$. If the set $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ is nonempty then it is a $\mathrm{cl}(\mathcal{O})$-torsor in which the action of the ideal class of any proper $\mathcal{O}$-ideal of prime norm $\ell \nmid q$ is given by a horizontal ℓ-isogeny, and the inverse of this action is given by the dual isogeny.

Isogeny volcanoes

Definition

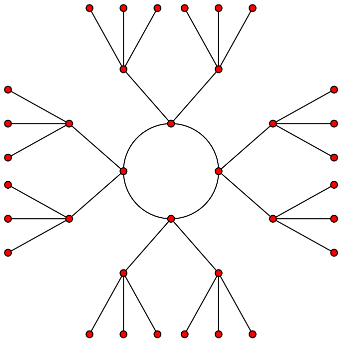
An ℓ-volcano V is a connected undirected graph whose vertices are partitioned into one or more levels $V_0, \ldots, V_d$ such that the following hold:

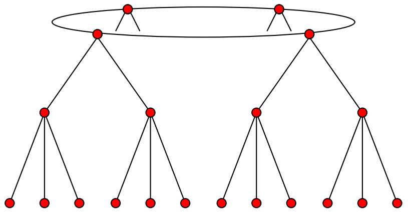
1. The subgraph on V_0 (the surface) is a regular graph of degree at most 2.
2. For $i > 0$, each vertex in V_i has exactly one neighbor in level V_{i-1}, and this accounts for every edge not on the surface.
3. For $i < d$, each vertex in V_i has degree $\ell + 1$.

Level V_d is called the floor of the volcano; the floor and surface coincide when $d = 0$.

Like $G_\ell(k)$, an ℓ-volcano may have multiple edges and self-loops, but it is an undirected graph. If the surface of an ℓ-volcano has more than two vertices, it must be a simple cycle. Two vertices may be connected by 1 or 2 edges, and a single vertex may have 0, 1, or 2 self-loops. The shape of an ℓ-volcano is determined by the integers ℓ, d, $|V_0|$.

Isogeny volcanoes





If we ignore components that contain the two exceptional j-invariants 0 and 1728, the ordinary components of $G_\ell(\mathbb{F}_p)$ are all ℓ-volcanoes. This was proved by David Kohel in his Ph.D., although the term "volcano" was coined later by Fouquet and Morain.

Isogeny volcanoes

Theorem (Kohel)

Let $\mathbb{F}_q$ be a finite field, let $\ell \nmid q$ be a prime, and let V be an ordinary component of $G_\ell(\mathbb{F}_q)$ that does not contain the j-invariants 0 or 1728. Then V is an ℓ-volcano and:

(i) *The vertices in level V_i all have the same endomorphism ring $\mathcal{O}_i$.*

(ii) *The subgraph on V_0 has degree $1 + (\frac{D_0}{\ell})$, where $D_0 = \operatorname{disc}(\mathcal{O}_0)$.*

(iii) *If $(\frac{D_0}{\ell}) \geq 0$, then $|V_0|$ is the order of $[\mathfrak{l}] \in \operatorname{cl}(\mathcal{O}_0)$, where $\ell\mathcal{O}_0 = \mathfrak{l}\bar{\mathfrak{l}}$, else $|V_0| = 1$.*

(iv) *V has depth d, where $4q = t^2 - \ell^{2d}v^2 D_0$ with $\ell \nmid v$, $t^2 = (\operatorname{tr}\pi_E)^2$, for $j(E) \in V$.*

(v) *$\ell \nmid [\mathcal{O}_K : \mathcal{O}_0]$ and $[\mathcal{O}_i : \mathcal{O}_{i+1}] = \ell$ for $0 \leq i < d$.*

Proof: To the board!

Remark

This theorem be extends to $0, 1728 \in V$ with minor modifications.

Finding the floor

The vertices that lie on the floor of an ℓ-volcano V are distinguished by their degree.

Lemma

Let v be a vertex in an ordinary component V of depth d in $G_\ell(\mathbb{F}_q)$.
Then either $\deg v \le 2$ and $v \in V_d$, or $\deg v = \ell + 1$ and $v \notin V_d$.

Algorithm (FindFloor)

Given an ordinary vertex $v_0 \in G_\ell(\mathbb{F}_q)$, find a vertex on the floor of its component.

1. If $\deg v_0 \le 2$ then output v_0 and terminate.
2. Pick a random neighbor v_1 of v_0 and set $s \leftarrow 1$.
3. While $\deg v_s > 1$: pick a random neighbor $v_{s+1} \ne v_{s-1}$ of v_s and increment s.
4. Output v_s.

Pro tip: rather than picking v_{s+1} as a root of $\phi(Y) = \Phi_\ell(v_s, Y)$ use $\phi(Y)/(Y - v_{s-1})^e$, where e is the multiplicity of v_{s-1} as a root of $\phi(Y)$.

Finding a shortest path to the floor

Algorithm (FindShortestPathToFloor)

Given an ordinary $v_0 \in G_\ell(\mathbb{F}_q)$, find a shortest path to the floor of its component.

1. Let $v_0 = j(E)$. If $\deg v_0 \leq 2$ then output v_0 and terminate.
2. Pick three neighbors of v_0 and extend paths from each of these neighbors in parallel, stopping as soon as any of them reaches the floor.[1]
3. Output a path that reached the floor.

If δ is the length of the shortest path to the floor V_d, then $j(E) \in V_{d-\delta}$.
This effectively gives us an "altimeter" $\delta(v)$ that we may use to navigate V. We can determine whether a given edge (v_1, v_2) is horizontal, ascending, or descending, by comparing $\delta(v_1)$ to $\delta(v_2)$, and we can determine the exact level of any vertex.

A more sophisticated approach uses the Weil pairing for large d (but this is rare).

[1] If v_0 does not have three distinct neighbors then just pick all of them.