23.1 Isogenies between elliptic curves with complex multiplication

Let E/k be an elliptic curve with CM by an order $\mathcal{O}$ of discriminant D in an imaginary quadratic field K, and let ℓ be a prime not equal to the characteristic of k. The roots of $\Phi_\ell(j(E), Y)$ correspond to $\ell+1$ distinct ℓ-isogenies from E to elliptic curves E', not all of which may be defined over k; this depends on whether the roots lie in k or a proper extension of k. Of these $\ell+1$ roots, 0, 1, or 2 may correspond to elliptic curves that also have CM by $\mathcal{O}$, depending on whether ℓ divides the conductor $[\mathcal{O}_K : \mathcal{O}]$ and whether ℓ is inert, ramified, or split in K, as you proved on Problem Set 10. We note that any such curves can be defined over k, since the set $\mathrm{Ell}_{\mathcal{O}}(k)$ is either empty or includes the j-invariant of every elliptic curve with CM by $\mathcal{O}$. This is clear in characteristic 0, since the ring class field for $\mathcal{O}$ is the splitting field of $H_D(X)$ over $\mathbb{Q}$ (and over K). For finite fields $\mathbb{F}_p$ it follows from Theorem 22.10, and in fact it holds for all fields of characteristic p.

But what about elliptic curves that that are ℓ-isogenous to E but don't have CM by $\mathcal{O}$? We know that over a suitable extension of k at least $\ell-1$ such curves exist. These elliptic curves have CM by a different imaginary quadratic order $\mathcal{O}'$ in the same field K, and $\mathcal{O}'$ either contains or is contained by $\mathcal{O}$, with index ℓ.

Theorem 23.1. *Let E/k be an elliptic curve with CM by an order $\mathcal{O}$ in an imaginary quadratic field K, and suppose that there exists an isogeny $\varphi\colon E \to E'$ of prime degree ℓ. Then E' has CM by an order $\mathcal{O}'$ in K, and 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. For any $\phi \in \mathrm{End}(E)$, the composition $\varphi \circ \tau \circ \hat{\varphi}$ lies in $\mathrm{End}(E')$, and conversely, for any $\phi' \in \mathrm{End}(E')$, the composition $\hat{\varphi} \circ \tau \circ \varphi$ lies in $\mathrm{End}(E)$. It follows that the endomorphism algebras $\mathrm{End}^0(E)$ and $\mathrm{End}^0(E')$ are the same, so E' has CM by an order $\mathcal{O}'$ in K. Furthermore, both $\ell\mathcal{O} \subseteq \mathcal{O}'$ and $\ell\mathcal{O} \subseteq \mathcal{O}'$ hold; since ℓ is prime, the theorem follows.[1] □

Definition 23.2. We use the following terminology to distinguish the three possibilities for the ℓ-isogeny φ of Theorem 23.1:

(i) when $\mathcal{O} = \mathcal{O}'$ we say that φ is a *horizontal*,

(ii) when $[\mathcal{O} : \mathcal{O}']$ we say that φ is *descending*,

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

In both of the last two cases, we also say that φ is a *vertical* isogeny.

Horizontal ℓ-isogenies correspond to the CM action of a proper $\mathcal{O}$-ideal of norm ℓ. You determined the number of horizontal ℓ-isogenies for an elliptic curve with CM by $\mathcal{O}$ in Problem Set 10.

Lemma 23.3. *Let E/k be an elliptic curve with CM by an order $\mathcal{O}$ in an imaginary quadratic field K. If ℓ divides $[\mathcal{O}_K : \mathcal{O}]$ then there are no horizontal isogenies from E, and otherwise the number of horizontal ℓ-isogenies is $1 + \left(\frac{D}{\ell}\right)$, where $D = \mathrm{disc}(\mathcal{O})$.*

[1] Note that $\mathcal{O}'$ is an order, hence a ring, so it contains 1. Thus if $\ell\mathcal{O} \subseteq \mathcal{O}'$ with $\mathcal{O} = [1, \tau]$, then the index-ℓ suborder $[1, \ell\tau]$ of $\mathcal{O}$ lies in $\mathcal{O}'$ (and vice versa).

Proof. See Problem 2.4 on Problem Set 10. □

Earlier we defined the set $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ of elliptic curves over $\mathbb{C}$ with CM by $\mathcal{O}$. We now extend this definition to arbitrary fields k

Definition 23.4. For any field k, the set $\mathrm{Ell}_{\mathcal{O}}(k)$ consists of the j-invariants of all elliptic curves defined over k whose endomorphism ring is isomorphic to $\mathcal{O}$.

Over a non-algebraically closed field k, the set $\mathrm{Ell}_{\mathcal{O}}(k)$ may be empty, but if it is non-empty then it is as large as possible.

Lemma 23.5. *The cardinality of* $\mathrm{Ell}_{\mathcal{O}}(k)$ *is either* 0 *or* $h(\mathcal{O})$.

Proof. In characteristic 0 the prime field of k is isomorphic to $\mathbb{Q}$, and the lemma follows from the fact that $\mathbb{Q}(j(E))$ is the splitting field of $H_D(X)$ over $\mathbb{Q}$. In characteristic p the lemma is implied by the Duering lifting theorem and related results (see Theorems 12-14 in Chapter 13 of [5]). Duering proved that in characteristic p not only does every elliptic curve with CM by $\mathcal{O}$ arise as the reduction of an elliptic curve over $\overline{\mathbb{Q}}$ with CM by $\mathcal{O}$, there is a one-to-one correspondence between j-invariants (in particular, their reductions are distinct). □

Remark 23.6. Lemma 23.5 does *not* imply that $H_D(X)$ must either be irreducible or split completely over k; it is possible for $H_D(X)$ to have some, but not all, of its roots in k. In this situation the roots of $H_D(X)$ do not correspond to elliptic curves with CM by $\mathcal{O}$. It is true that if $\sqrt{D} \in k$ and $H_D(X)$ splits completely, then its roots must be the set $\mathrm{Ell}_{\mathcal{O}}(k)$, this follows from Theorem 22.10 and the Duering lifting theorem.

We now wish to determine the number of ascending ℓ-isogenies that an elliptic curve with CM by an imaginary quadratic order may have. To set things up, let us suppose that $[\mathcal{O}\colon \mathcal{O}'] = \ell$, so that ℓ-isogenies from elliptic curves with CM by $\mathcal{O}'$ to elliptic curves with CM by $\mathcal{O}$ are ascending. There is a norm-preserving map ρ that sends each invertible $\mathcal{O}'$-ideal $\mathfrak{a}$ to the (necessarily invertible) $\mathcal{O}$-ideal $\mathfrak{a}\mathcal{O}$, and ρ induces a surjective group homomorphism from $\mathrm{cl}(\mathcal{O}')$ to $\mathrm{cl}(\mathcal{O})$. This is more or less obvious, but see [2, Prop. 7.20] for a proof when $\mathcal{O} = \mathcal{O}_K$, and see [1, §3] for the general case.

Theorem 23.7. *Let E'/k be an elliptic curve with CM by an imaginary quadratic order $\mathcal{O}'$ that is an index-ℓ suborder of $\mathcal{O}$, with* $\mathrm{disc}(\mathcal{O}) < -4$ *and* $\ell \neq \mathrm{char}(k)$ *prime. Up to isomorphism, there is a unique ℓ-isogeny from E to an elliptic curve E'/k with CM by $\mathcal{O}$.*

Proof. We first note that the existence of E'/k implies that $\mathrm{Ell}_{\mathcal{O}'}(k)$ is non-empty, and since $\mathcal{O}$ contains $\mathcal{O}'$, it follows that $\mathrm{Ell}_{\mathcal{O}}(k)$ is also non-empty.[2] Thus the cardinality of $\mathrm{Ell}_{\mathcal{O}}(k)$ is $h(\mathcal{O})$ and the cardinality of $\mathrm{Ell}_{\mathcal{O}'}(k)$ is $h(\mathcal{O}')$, by Lemma 23.5.

Suppose there exists an ascending ℓ-isogeny $\phi_1\colon E_1' \to E_1$, for some elliptic curve E_1' with CM by $\mathcal{O}'$. Twisting E_1 if necessary, we may choose an invertible $\mathcal{O}'$-ideal $\mathfrak{a}'$ so that the horizontal isogeny $\varphi_{\mathfrak{a}'}$ corresponding to the CM-action of $\mathfrak{a}'$ on E_1 maps E_1' to E'. If we now set $\mathfrak{a} = \rho(\mathfrak{a}')$ and let E be the image of $\varphi_{\mathfrak{a}} \circ \phi_1$, then E has CM by $\mathcal{O}$, and there is a unique isogeny $\phi\colon E' \to E$ such that $\phi \circ \varphi_{\mathfrak{a}'} = \varphi_{\mathfrak{a}} \circ \phi_1$, by [7, Cor. 4.11]. We have $\deg \phi = \deg \varphi_{\mathfrak{a}} \deg \phi_1 / \deg \varphi_{\mathfrak{a}'} = \ell$, thus ϕ is an ascending ℓ-isogeny. It follows that if any E_1'/k with CM by $\mathcal{O}'$ admits an ascending ℓ-isogeny, then so does every such elliptic curve.

[2] One way to see this is to note that k contains the roots of the Hilbert class polynomial for $\mathcal{O}'$, hence it must contain the roots of the Hilbert class polynomial for $\mathcal{O}$, since the ring class field of $\mathcal{O}'$ contains the ring class field of $\mathcal{O}$.

We now proceed by induction on $d = \nu_\ell([\mathcal{O}_K : \mathcal{O}])$, where $\mathcal{O}_K$ is the maximal order in the imaginary quadratic field K containing $\mathcal{O}$, and $\nu_\ell(n)$ is the ℓ-adic valuation (the largest e for which ℓ^e divides n). Let $D_K = \operatorname{disc}(\mathcal{O}_K)$. For $d = 0$, every elliptic curve E/k with CM by $\mathcal{O}$ admits $\ell + 1$ k-rational ℓ-isogenies, of which $1 + \left(\frac{D_K}{\ell}\right)$ are horizontal and none are ascending. The remaining $\ell - \left(\frac{D_K}{\ell}\right) > 0$ must be descending, and their duals are ascending ℓ-isogenies from elliptic curves with CM by $\mathcal{O}'$. It follows that there are a total of $(\ell - \left(\frac{D_K}{\ell}\right))h(\mathcal{O})$ ascending ℓ-isogenies from $\mathrm{Ell}_{\mathcal{O}'}(k)$ to $\mathrm{Ell}_{\mathcal{O}}(k)$. By Lemma 23.8 below, this is equal to the cardinality $h(\mathcal{O}')$ of $\mathrm{Ell}_{\mathcal{O}'}(k)$. Since there is at least one ascending ℓ-isogeny from each elliptic curve E'/k with CM by $\mathcal{O}'$, there must be exactly one in each case.

The argument for $d > 0$ is similar. By the inductive hypothesis, every elliptic curve E/k with CM by $\mathcal{O}$ admits exactly one ascending ℓ-isogeny, and since ℓ now divides $[\mathcal{O}_K : \mathcal{O}]$, there are no horizontal isogenies from E, and all ℓ of the remaining ℓ-isogenies from E must by descending. There are thus a total of $\ell h(\mathcal{O})$ ascending ℓ-isogenies from $\mathrm{Ell}_{\mathcal{O}'}(k)$, which equals the cardinality $h(\mathcal{O}')$ of $\mathrm{Ell}_{\mathcal{O}'}(k)$, again by Lemma 23.8. □

Lemma 23.8. *Let ℓ be a prime, let $\mathcal{O}'$ be an index-ℓ suborder of an imaginary quadratic order $\mathcal{O}$ of discriminant $D < -4$, and let $\mathcal{O}_K$ be the maximal order containing $\mathcal{O}$, with discriminant $\mathbb{D}_K$. If ℓ divides $[\mathcal{O}_K : \mathcal{O}]$, then $h(\mathcal{O}') = \ell h(\mathcal{O})$, and otherwise*

$$\frac{h(\mathcal{O}')}{h(\mathcal{O})} = \ell - \left(\frac{D_K}{\ell}\right).$$

Proof. This follows directly from the class number formula for non-maximal orders, a standard result that won't prove here; see [2, Thm. 7.24]. □

Remark 23.9. The reason for requiring $D < -4$ in Theorem 23.7 and Lemma lem:hcard is that the unit group of an imaginary quadratic order with discriminant less than -4 is $\{\pm 1\}$, but the orders $\mathbb{Z}[e^{2\pi/3}]$ and $\mathbb{Z}[i]$ with discriminants -3 and -4 have larger unit groups (of order 6 and 4, respectively), and these extra units correspond to extra automorphisms of the elliptic curves with j-invariants 0 and 1728 (respectively) that have CM by these orders.

If $\phi \in \mathrm{Aut}(E)$, then whenever we have an ℓ-isogeny $\lambda\colon E \to E'$, we also have the ℓ-isogeny $\lambda \circ \phi$. Now if $\phi = \pm 1$, then $\ker(\lambda \circ \phi) = \ker \lambda$ and we regard these two isogenies as equivalent, but if $\phi \neq \pm 1$, then $\ker(\lambda \circ \phi) \neq \ker \lambda$ and these really are inequivalent isogenies; the polynomial $\Phi_\ell(j(E), Y)$ will have $j(E')$ as a root with multiplicity equal to $|\mathrm{Aut}(E)|/2$. But the isogenies dual to λ and $\phi \circ \lambda$ *will* have the same kernel. Thus when considering isogenies up to equivalence, we do not have a 1-to-1 correspondence between isogenies and their duals when $j(E) \in \{0, 1728\}$, but otherwise we do. For this reason we will often exclude the j-invariants 0 and 1728 in what follows (the special cases 0 and 1728 can be handled by taking $\mathrm{Aut}(E)$ into account).

23.2 Isogeny volcanoes

We now define the ℓ-isogeny graph of the field k. As above $\ell \neq \mathrm{char}(k)$ is a prime.

Definition 23.10. 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 $\Phi_\ell(j_1, Y)$.

Note that $G_\ell(k)$ may contain multiple edges between the same pair of vertices, and it may contain self-loops (edges from a vertex to itself). The vertices of $G_\ell(k)$ correspond to j-invariants of elliptic curves, and its edges correspond to (isomorphism classes of) isogenies.

Edges (j_1, j_2) that are not incident to 0 or 1728 occur with the same multiplicity as (j_2, j_1) (the reverse edges correspond to dual isogenies). Thus the subgraph on $k\backslash\{0, 1728\}$ is bi-directed and we may regard it as an undirected graph. For any fixed k, the graphs $G_\ell(k)$ all have the same vertex set but different edge sets, depending on the prime ℓ. Given an elliptic curve E/k, we may view $j(E)$ as a vertex in any of these graphs.

If follows from Theorem 23.1 and its proof that the edges of $G_\ell(k)$ are always between (isomorphism classes of) elliptic curves with the same endomorphism algebra. When k is a finite field, this means that we can classify each component of $G_\ell(k)$ as ordinary or supersingular. In this lecture we will focus on the ordinary components; you will have a chance to explore the supersingular components on Problem Set 12.

Figure 1 depicts a typical ordinary component of an ℓ-isogeny graph.

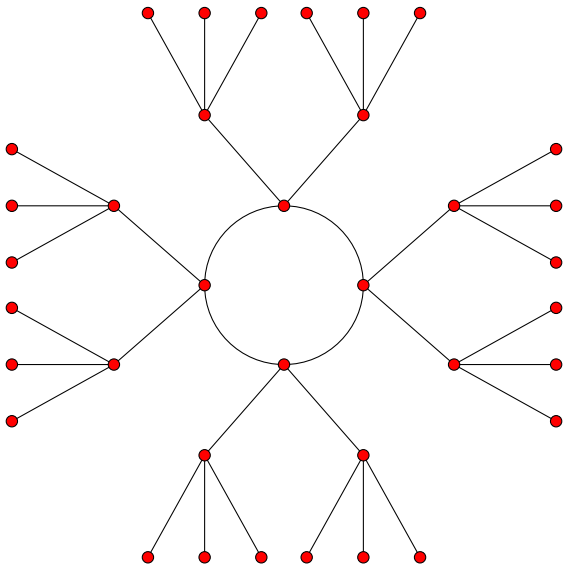

Figure 1: An ordinary component of $G_3(k)$.

Figure 2 shows the same graph from a different perspective. With a bit of imagination, one can see that the graph looks like a volcano: there is a crater formed by the cycle at the top, and the trees handing down from each edge form the sides of the volcano.

Definition 23.11. An *ℓ-volcano* V is a connected undirected graph whose vertices are partitioned into one or more *levels* $V_0, \dots, V_d$ 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 $d = 0$.

As with $G_\ell(K)$, we allow multiple edges and self-loops, but now we work with an undirected graph. Note that if the surface of an ℓ-volcano has more than two vertices, it must

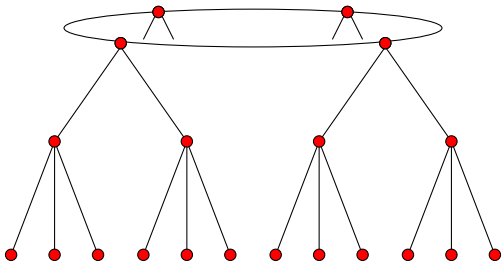

Figure 2: A 3-volcano of depth 2.

be a simple cycle. Two vertices may be connected by one or two edges, and a single vertex may have 0, 1, or 2 self-loops. Note that, as an abstract graph, an ℓ-volcano is completely determined by the integers ℓ, d, and $|V_0|$.

Remarkably, if we ignore exceptions at the j-invariants 0 and 1728, the ordinary components of $G_\ell(k)$ are all ℓ-volcanoes. This was proved by David Kohel in his 1996 PhD thesis.[3]

Theorem 23.12 (**Kohel**). *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 for which the following hold:*

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

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

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

(iv) *The depth of V is $d = \nu_\ell\left((t^2 - 4q)/D_0\right)/2$, where $t^2 = (\operatorname{tr}\pi_E)^2$ 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. The theorem follows easily from the results we have already proved. Let V be an ordinary component of $G_\ell(\mathbb{F}_q)$ that does not contain 0 or 1728. Then, as previously noted, V is bi-directed and can be viewed as an undirected graph. It follows from Theorem 22.1 that every vertex of V has the same endomorphism algebra, an imaginary quadratic field K, and that the orders $\mathcal{O}$ in K that arise as endomorphism rings of vertices in V differ only in the power of ℓ that divides their conductor. Furthermore, if ℓ^d is the largest power of ℓ that divides the conductor of any of the orders $\mathcal{O}$, then we may partition V into levels $V_0, \ldots, V_d$ corresponding to orders $\mathcal{O}_0, \ldots, \mathcal{O}_d$ for which $\nu_\ell([\mathcal{O}_K : \mathcal{O}_i]) = \ell$, This addresses (i) and (v).

Parts (ii) and (iii) follow from Lemma 23.3 and the CM action of $\operatorname{cl}(\mathcal{O}_0)$, and part (iv) follows from Theorem 22.10 (which can be generalized to prime powers q) and Lemma 23.5: if we have $4q = t^2 - v^2 D_0$ then the sets $\operatorname{Ell}_{\mathcal{O}_i}(k)$ are all non-empty but the set $\operatorname{Ell}_{\mathcal{O}_{d+1}}(k)$ must be empty since ℓ^{d+1} does not divide v.

Finally, Theorem 22.1 and Lemma 23.5 together imply that for $i > d$ every $v \in V_i$ must have degree $\ell + 1$, because the roots of $\Phi_\ell(v, Y)$ (which has degree $\ell + 1$) all lie in $\operatorname{Ell}_{O_i}(\mathbb{F}_q)$, $\operatorname{Ell}_{O_{i+1}}(\mathbb{F}_q)$, or, for $i > 0$, $\operatorname{Ell}_{O_{i-1}}(\mathbb{F}_q)$. This, together with (ii) and Theorem 22.1, proves that V is indeed an ℓ-volcano. □

[3]The term "volcano" was not used by Kohel, it was introduced by Fouquet and Morain in [3].

Remark 23.13. Theorem 23.12 is easily extended to the case where V contains 0 or 1728, via Remark 23.9 Parts (i)-(v) still hold, the only necessary modification is the claim that V is an ℓ-volcano. When V contains 0, if V_1 is non-empty then it contains $\frac{1}{3}\big(\ell - \big(\frac{-3}{\ell}\big)\big)$ vertices, and each vertex in V_1 has three incoming edges from 0 but only one outgoing edge to 0. When V contains 1728, if V_1 is non-empty then it contains $\frac{1}{2}\big(\ell - \big(\frac{-1}{\ell}\big)\big)$ vertices, and each vertex in V_1 has two incoming edges from 1728 but only one outgoing edge to 1728. This 3-to-1 (resp. 2-to-1) discrepancy arises from the action of $\mathrm{Aut}(E)$ on the cyclic subgroups of $E[\ell]$ when $j(E) = 0$ (resp. 1728). Otherwise, V satisfies all the requirements of an ℓ-volcano, and most of the algorithms designed for ℓ-volcanoes work just as well on ordinarycomponents of $G_\ell(\mathbb{F}_q)$ that contain 0 or 1728.

23.3 Finding the floor

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

Lemma 23.14. *Let v be a vertex in an ordinary component V of depth d in $G_\ell(\mathbb{F}_q)$. Either $\deg v \le 2$ and $v \in V_d$, or $\deg v = \ell + 1$ and $v \notin V_d$.*

Proof. If $d = 0$ then $V = V_0 = V_d$ is a regular graph of degree at most 2 and $v \in V_d$. Otherwise, either $v \in V_d$ and v has degree 1, or $v \notin V_d$ and v has degree $\ell + 1$. □

Given an arbitrary vertex $v \in V$, we would like to find a vertex on the floor of V. Our strategy is very simple: if $v_0 = j(E)$ is not already on the floor then we will construct a random path from v_0 to a vertex v_s on the floor. By a *path*, we mean a sequence of vertices $v_0, v_1, \ldots, v_s$ such that each pair (v_{i-1}, v_i) is an edge and $v_i \ne v_{i-2}$ (no backtracking is allowed).

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.

Remark 23.15 (Removing known roots). As a minor optimization, rather than picking v_{s+1} as a root of $\phi(Y) = \Phi_\ell(v_s, Y)$ in step 3 of the FindFloor algorithm, we may use $\phi(Y)/(Y - v_{s-1})^e$, where e is the multiplicity of v_{s-1} as a root of $\phi(Y)$. This is slightly faster and eliminates the need to check that $v_{s+1} \ne v_{s-1}$.

Notice that once FindFloor picks a descending edge (one leading closer to the floor), every subsequent edge must also be descending, because it is not allowed to backtrack along the single ascending edge and there are no horizontal edges below the surface. It follows that the expected length of the path chosen by FindFloor is $\delta + O(1)$, where δ is the distance from v_0 to the floor along a shortest path. With a bit more effort we can find a path of exactly length δ, a shortest path to the floor. The key to doing so is observe that all but at most two of the $\ell + 1$ edges incident to any vertex above the floor must be descending edges. Thus if we construct *three* random paths from v_0 that all start with a different initial

edge, then one of the initial edges must be a descending edge, which necessarily leads to 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.[4]
3. Output a path that reached the floor.

The main virtue of FindShortestPathToFloor is that it allows us to compute δ, which tells us the level $V_{d-\delta}$ of $j(E)$ relative to the floor V_d. It effectively gives us an "altimeter" $\delta(v)$ that we may be used 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.[5]

There are many practical applications of isogeny volcanoes, some of which you will explore on Problem Set 12. See the survey paper [8] for further details and references.

References

[1] Reinier Bröker, Kristin Lauter, and Andrew V. Sutherland, *Modular polynomials via isogeny volcanoes*, Mathematics of Computation **81**, 2012, 1201–1231.

[2] David A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, Wiley, 1989.

[3] Mireille Fouquet and Francois Morain, *Isogeny volcanoes and the SEA algorithm*, ANTS V, LNCS **2369**, Spring 2002, 276–291.

[4] Sorina Ionica and Antoine Joux, *Pairing the volcano*, Mathematics of Computation **82** (2013), 581–603.

[5] Serge Lang, *Elliptic functions*, second edition, Springer, 1987.

[6] David Kohel, *Endomorphism rings of elliptic curves over finite fields*, PhD thesis, University of California at Berkeley, 1996.

[7] Joseph H. Silveman, *The arithmetic of elliptic curves*, second edition, Springer, 2009.

[8] Andrew V. Sutherland, *Isogeny volcanoes*, ANTS X, arxiv.org/abs/1208.5370.

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

[5] An alternative approach based on pairings has recently been developed by Ionica and Joux [4, ?], which is more efficient when d is large.

18.783 Elliptic Curves
Spring 2013