Isogenizable discrete logs

Chloe Martindale

18th October, 2018

These notes are from a talk given in the spontaneous 'isogeny day' at KU Leuven. This talk includes results from my PhD thesis, supervised by Marco Streng, and joint work (in progress) with Dimitar Jetchev, Enea Milio, Marius Vuille, and Benjamin Wesolawski.

1 Isogeny graphs of elliptic curves

Definition. Suppose that E and E' are elliptic curves over a field k. An *isogeny* $\phi : E \to E'$ is a surjective morphism with finite kernel that sends the identity to the identity.

Definition. Suppose that $\phi : E \to E'$ is an isogeny of elliptic curves over a field k. This induces an injective morphism of function fields

$$\overline{k}(E') \longrightarrow \overline{k}(E).$$

We define the *degree* of ϕ to be

$$\deg(\phi) = [\overline{k}(E) : \overline{k}(E')].$$

If $\deg(\phi) = \ell$, then we call ϕ an *ℓ-isogeny.*

Remark. If $\phi : E \to E'$ is a separable isogeny (i.e. if the field extension is separable) then the degree of the isogeny is just the size of the kernel.

Remark. An ℓ-isogeny $\phi : E \to E'$ has a dual ℓ-isogeny $\phi^\vee : E' \to E'$ such that

$$\phi \circ \phi^\vee = \phi^\vee \circ \phi = [\ell],$$

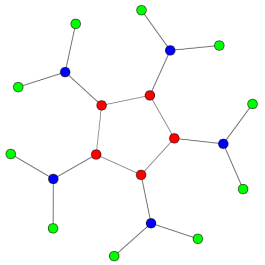
where $[\ell]$ denotes the multiplication-by-ℓ morphism.

Definition. An *ℓ-isogeny graph of elliptic curves* as an undirected graph for which each vertex represents a j-invariant (this is an isomorphism invariant) of an elliptic curve over a field k, and an edge between $j(E)$ and $j(E')$ represents an ℓ-isogeny $E \to E'$ defined over k and its dual isogeny $E' \to E$.

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

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

Example. Here is a 2-volcano with $d = 2$:



Theorem (Kohel '96)**.** *Let $\ell \in \mathbb{Z}$ be a prime, and let $E/\mathbb{F}_q$ be an ordinary elliptic curve with $j(E) \neq 0, 1728$. Then the connected component of the ℓ-isogeny graph containing $j(E)$ is a* ℓ-volcano*. Furthermore, locally at ℓ, the vertices occurring in level V_i have endomorphism ring $\ell^i \mathcal{O}_K$.*

Remark. The conditions in this theorem, namely 'ordinary' and $j(E) \neq 0, 1728$, are to have control on the endomorphisms and the automorphisms of E. Given an elliptic curve over any field, for every $n \in \mathbb{Z}$ there is and endomorphism of E defined by the multiplication-by-n map, so in a natural way we can identify $\mathbb{Z}$ with a subring of $\mathrm{End}(E)$. Furthermore, for every elliptic curve defined over a finite field $\mathbb{F}_q$, there exists the Frobenius morphism on E, and by looking at the characteristic polynomial of this morphism, under Kohel's conditions, we can identify the Frobenius morphism with an algebraic integer π for which $\mathbb{Q}(\pi)$ is an imaginary quadratic number field. In fact, the elliptic curve being ordinary tells us even more, that

$$\mathrm{End}(E) \otimes \mathbb{Q} = \mathbb{Q}(\pi).$$

Remark. From the above remark, we see that

$$\mathbb{Z}[\pi] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_{\mathbb{Q}(\pi)},$$

where π is the algebraic integer corresponding to the Frobenius morphism. Therefore, the depth is $\leq \max\{r \in \mathbb{Z} : \ell^r | [\mathcal{O}_K : \mathbb{Z}[\pi]]\}$, where π is the q-power Frobenius endomorphism of E and $K = \mathbb{Q}(\pi)$, and in fact this is attained. So the depth is as easy to compute as the Frobenius endomorphism. The structure of level V_0 and the number of connected components are also easy to compute.

Now with a simple path walking algorithm we can determine if $j(E)$ and $j(E')$ are in the same connected component of the isogeny graph, hence determine if they are isogenous, and if they are, determine the degree of the isogeny (or at least of one of the isogenies).

In fact, we can do even more, we can determine the endomorphism ring of an elliptic curve by using a path walking algorithm to determine its position in the ℓ-volcano. The conditions on the elliptic curve E ensure that $\mathrm{End}(E)$ is an order in an imaginary quadratic number field $\mathbb{Q}(\pi)$, where π is the q-power Frobenius morphism on E. As locally at ℓ, the vertices occurring in level V_i have endomorphism ring $\ell^i\mathcal{O}_K$, to determine the endomorphism ring of a given elliptic curve (satisfying the conditions of Kohel's theorem), we just have to determine the endomorphism algebra K, list the primes $\ell_1, \ldots, \ell_r$ dividing the index $[\mathcal{O}_K : \mathbb{Z}[\pi]]$, and do a path walking algorithm to determine the depth of the vertex in the $\ell_1, \ldots, \ell_r$-volcanoes.

2 Isogeny graphs of abelian varieties

We are able to define a discrete logarithm on elliptic curves and classify isogenies of elliptic curves using isogeny graphs largely due to one property: that there exists a group law. Recall that an elliptic curve (for odd characteristic) is defined by a polynomial

$$y^2 = f(x),$$

where $\deg(f) = 3$. One could ask, what happens if $\deg(f) > 3$? Or what about other algebraic curves? One of the reasons that we so often stick to such a special class of algebraic curves is because of the simple group law. But all is not lost for other algebraic curves: although there is no known group law on the curves themselves, to each algebraic curve C we can associate an *abelian variety* (on which there exists a group law), called the *Jacobian* of C, written $J(C)$, or $\mathrm{Jac}(C)$. In fact, we can do even better, we can assume that the Jacobian is a *principally polarised* abelian variety A - which for all purposes of this talk means that there exists a 'nice' isomorphism from A to its dual. Furthermore, if C is defined over k, then

$$C(k) \subseteq \mathrm{Jac}(C)(k),$$

so we can study the k-rational points of C by studying the points on the Jacobian, where we have a group law to help us.

Recall that the conditions on the elliptic curves to which Kohel's theorem can be applied ensured that the endomorphism algebra would be an imaginary quadratic field generated by the Frobenius. We will need a natural generalisation of this to abelian varieties.

Definition. A *CM-field* K is a totally imaginary quadratic extension of a totally real number field K_0.

Examples.

- $K = \mathbb{Q}(\sqrt{-2})$ is a CM-field with $K_0 = \mathbb{Q}$.
- $K = \mathbb{Q}(\sqrt{-3+\sqrt{2}})$ is a CM-field with $K_0 = \mathbb{Q}(\sqrt{2})$.

Definition. An abelian variety A of dimension g has *CM by a CM-field* K of degree $2g$ over $\mathbb{Q}$ if the endomorphism algebra $\mathrm{End(A)} \otimes \mathbb{Q} = K$. If K_0 is the maximal totally real subfield of K, we say that A *RM by* K_0.

A simple ordinary abelian variety defined over $\mathbb{F}_q$ is CM, i.e., there exists a CM-field K of degree $2g$ over $\mathbb{Q}$ such that A has CM by K. This is again a consequence of the existence Frobenius endomorphism π on A and its dual $\overline{\pi}$. From now on, unless stated otherwise, we will assume that A has CM by K, and that $\mathcal{O}_{K_0} \subseteq \mathrm{End}(\mathrm{A})$ (i.e. A has *maximal real multiplication by* K_0).

Definition. A morphism of abelian varieties is an *isogeny* if it preserves the identity, is surjective, and has finite kernel.

The generalisation of an ℓ-isogeny to higher dimension that we use is quite complicated, so we do not a precise definition. The interested reader can find the definition in the upcoming thesis of the author [Mar]. Recall that for elliptic curves, given an isogeny $E \to E'$, there was a dual isogeny $E' \to E$. What we did not mention in the case of elliptic curves was that, to observe that the dual isogeny is a morphism $E' \to E$, we used that an elliptic curve is isomorphic to its dual. For general abelian varieties this is not true, but abelian varieties that are Jacobians of curves are 'principally polarisable', which for all intents and purposes of this talk means that there exists a 'nice' isomorphism $\mathrm{A} \to \mathrm{A}^\vee$. We again associate a prime to the isogeny, but now a prime ideal in $\mathcal{O}_{K_0}$ - we study 'μ-isogenies' of principally polarised ordinary abelian varieties, where μ is a totally positive element of $\mathcal{O}_{K_0}$ which generates a prime ideal in K_0. A morphism $\phi : \mathrm{A} \to \mathrm{A}'$ of principally polarised ordinary abelian varieties is 'defined' to be a μ-isogeny if, up to the polarisations $\mathrm{A} \cong \mathrm{A}^\vee$ and $\mathrm{A}' \cong (\mathrm{A}')^\vee$, we have that

$$\phi^\vee \circ \phi = [\mu],$$

where $[\mu]$ denotes the multiplication-by-μ map on A, and ϕ preserves the RM structure. Note in particular that the degree of ϕ is $\mathrm{Norm}_{K_0/\mathbb{Q}}(\mu)$, hence if ϕ is separable and the norm of μ is prime, then ϕ has cyclic kernel, again mimicking the genus 1 case.

Definition. A μ-isogeny graph of principally polarised abelian varieties with maximal real multiplication is an undirected graph for which each vertex represents a principally polarised ordinary abelian variety with maximal real multiplication over a field $\mathbb{F}_q$ up to (polarisation and RM preserving) isomorphism, and an edge between A and A$'$ represents a μ-isogeny $\mathrm{A} \to \mathrm{A}'$ defined over $\mathbb{F}_q$ together with its dual isogeny $(A')^\vee \to A^\vee$ (again, up to isomorphism).

Let I be the graph with one vertex and no edges, let R_1 be a 1-cycle with one edge of weight $\frac{1}{2}$, let R_2 be 2 vertices joined by a single edge, and let C_n be a cycle of length n.

Theorem (M. '17)**.** *Let* $\mathrm{A}/\mathbb{F}_q$ *be a principally polarised ordinary abelian variety with maximal real multiplication by* K_0 *and suppose that the only roots of unity in* $\mathrm{End}(\mathrm{A}) \otimes \mathbb{Q}$ *are* ± 1*. Then the connected component of the* μ*-isogeny graph containing* A *is a* $\mathrm{Norm}_{K_0/\mathbb{Q}}(\mu)$*-volcano with* $V_0 \in \{I, R_1, R_2, C_n\}$*. Furthermore, locally at* μ*, the vertices occurring in level* V_i *have endomorphism ring* $\mu^i \mathcal{O}_K$*.*

Remark. Independently, Brooks, Jetchev, and Wesolowski proved a similar statement (for abelian varieties with primitive CM type) in [BJW].

Remark. As before, the existence of the Frobenius morphism on A tells us that there exists an algebraic integer π of degree $2g$ over $\mathbb{Q}$ for which $q = \pi\overline{\pi}$ and $\mathbb{Z}[\pi] \subseteq \mathrm{End(A)}$. Similarly, the Verschiebung morphism on A tells us that $\mathbb{Z}[\overline{\pi}] \subseteq \mathrm{End(A)}$ and by assumption we have that $\mathcal{O}_{K_0} \subseteq \mathrm{End(A)} \subseteq \mathcal{O}_K$. In particular, the endomorphism ring of A must be an order in K such that

$$\mathcal{O}_{K_0}[\pi, \overline{\pi}] \subseteq \mathrm{End(A)} \subseteq \mathcal{O}_K.$$

As before, we can conclude from this that the depth of the μ-volcano is

$$\leq \max_{r \in \mathbb{Z}} \{\mu^r \mathcal{O}_K \subseteq (\mathcal{O}_{K_0}[\pi, \overline{\pi}] : \mathcal{O}_K),$$

and again, this is realised. Note in particular that this formula for the depth shows that for all but finitely many μ, the depth is 0, that is, the connected component is exactly V_0. The structure of V_0 is also easy to compute, but we do not address that here for reasons of time.

In the following section, we drop the condition that $\mathcal{O}_{K_0} \subseteq \mathrm{End(A)}$.

3 The Discrete Logarithm Problem for Genus 3 Curves

Many cryptosystems are based on the *Diffie-Hellman key exchange*. Let G be a large commutative group, and suppose that Alice and Bob want to compute a shared secret element of this group. To do this, Alice chooses a secret integer $a \in \mathbb{Z}$ and Bob chooses a secret integer $b \in \mathbb{Z}$, and Alice (or Bob, or the NSA, or you) chooses and publishes an element g of G of large order. Alice then computes ag and sends it to Bob, and Bob computes bg and sends in to Alice. Alice and Bob can then both compute their shared secret abg.

The security of this cryptosystem relies on the hardness of the so-called *Discrete Logarithm Problem*: given ng and $g \in G$, compute $n \in \mathbb{Z}$. The groups used should be sufficiently large so that enumeration is not computationally feasible, but even then there are some deeper mathematical tricks that can be used on some groups to solve the problem in sub-exponential time. To get an idea of how hard the discrete logarithm problem is for some groups, consider the following examples:

Examples.

- Let $G = E(\mathbb{F}_q)$ be the group of $\mathbb{F}_q$-rational points on a 'sufficiently generic' elliptic curve defined over $\mathbb{F}_q$. The best known algorithm for the Discrete Logarithm Problem on G has complexity $O(\sqrt{q})$.
- Let $G = \mathcal{J}(C)(\mathbb{F}_q)$ be the group of $\mathbb{F}_q$-rational points on the Jacobian of a 'sufficiently generic' genus 2 curve defined over $\mathbb{F}_q$. The best known algorithm for the Discrete Logarithm Problem on G has complexity $O(q)$.

- Let $G = \mathcal{J}(C)(\mathbb{F}_q)$ be the group of $\mathbb{F}_q$-rational points on the Jacobian of a 'sufficiently generic' hyperelliptic genus 3 curve over $\mathbb{F}_q$. The best known algorithm for the Discrete Logarithm Problem on G has complexity $O(q^{3/2})$.
- Let $G = \mathcal{J}(C)(\mathbb{F}_q)$ be the group of $\mathbb{F}_q$-rational points on the Jacobian of a 'sufficienly generis' plane quartic genus 3 curve over $\mathbb{F}_q$. The best known algorithm, due to Diem and Smith, for the Discrete Logarithm on G has complexity $O(q)$. In this case 'the Discrete Logarithm Problem is broken', by which we mean that for a high enough security level, we have to increase the size of the finite field so much that the computations on the curve become too inefficient to be competitive with other options (such as genus 1 and 2 curves).

Under heuristic assumptions, in joint work in progress with Jetchev, Milio, Vuille, and Wesolawski, we give an algorithm that breaks the discrete logarithm for almost all genus 3 curves. That is, we give an algorithm that, on a sufficiently generic genus 3 curve C over $\mathbb{F}_q$, given P and nP in $\mathcal{J}(C)(\mathbb{F}_q)$, computes n in time $O(q)$. The strategy is as follows:

- If C is plane quartic, use the algorithm of Diem and Smith. Else, construct a plane quartic C' and an isogeny $\phi : \mathcal{J}(C) \to \mathcal{J}(C')$.
- Compute $\phi(nP) = n\phi(P)$.
- Compute n in time $O(q)$ using the algorithm of Diem and Smith.

Our contribution to this is the construction in (1), which we now address. We use our knowledge of isogeny graphs to use a simple path-walking algorithm to find such a curve and isogeny in polynomial time, heuristically almost all of the time.

Definition. A isogeny graph of principally polarised abelian varieties is an undirected graph for which each vertex represents a principally polarised abelian variety with maximal over a field $\mathbb{F}_q$ up to (polarisation preserving) isomorphism, and an edge between A and A$'$ represents a (polarisation preserving) isogeny A $\to$ A$'$ defined over $\mathbb{F}_q$ together with its dual isogeny $(A')^\vee \to A^\vee$ (again, up to isomorphism).

Note that the μ-isogeny graphs of the previous section will be subgraphs of the whole isogeny graph. Note also that we are interested in *curves* and the isogeny graph refers to *abelian varieties*. However, by Torelli's theorem, every principally polarised simple abelian variety of dimension 3 is the Jacobian of a genus 3 curve. Furthermore, we mentioned plane quartic genus 3 curves already, and in fact a genus 3 curve can always be written as a hyperelliptic curve or a plane quartic curve. So, it suffices to give an algorithm that, given the Jacobian of a hyperelliptic genus 3 curve, computes an isogeny to the Jacobian of a plane quartic curve in polynomial time with high probability.

Definition. We define an isogeny graph G of principally polarised abelian varieties of dimension 3 over $\mathbb{F}_q$ to be *good* if there exists a constant $0 < c < 1$ such that

$$\#\{\text{non-hyp vertices}\} \geq c\#\{\text{hyp vertices}\},$$

and the non-hyperelliptic vertices are 'sufficiently randomly distributed' in each of the connected components of G.

Then, we can use our knowledge of isogeny graphs to find a 'random-looking' point on the isogeny graph connected to the original curve. Under the following heuristic assumptions, a short random walk from this point should result in a plane quartic curve:

Heuristics.

- There exists a constant $c > 0$, independent of q, such that a randomly chosen ordinary isogeny class over $\mathbb{F}_q$ is good with probability 1.
- There exists a constant $c > 0$, independent of q, such that each ordinary isogeny class over $\mathbb{F}_q$ is good.

We have written code to verify these heuristics experimentally, and we will still compute more data before we are willing to make a conjecture to the above effect, but practically, based on our experiments, this attack has a high probability of being effective.

We give a brief outline of how to find a 'random-looking' point. For a generic principally polarised abelian 3-fold (A, ξ) defined over $\mathbb{F}_q$, the endomorphism algebra $\mathrm{End}(\mathrm{A}) \otimes \mathbb{Q}$ is isomorphic to a CM-field K of degree 6. Let K_0 be the maximal totally real subfield of K and let $\mathcal{O}_{K_0}$ be the ring of integers of K_0. Suppose that $\mathrm{End}(\mathrm{A})$ differs locally from $\mathcal{O}_K$ at rational primes $\ell_1, \ldots, \ell_s$. Let ℓ be a prime in this list, and let G_ℓ be the connected component of the (ℓ, ℓ, ℓ)-isogeny graph containing (A, ξ). We partition the G_ℓ into RM layers as follows: a principally polarised abelian 3-fold (A, ξ) is in the i^{th} RM layer if and only if, locally at ℓ, we have that

$$[\mathcal{O}_{K_0} : \mathrm{End}(\mathrm{A})|_{K_0}] = \ell^i. \tag{1}$$

In the upcoming paper with Jetchev, Milio, Vuille, and Wesolowski, we show that from every principally polarised abelian 3-fold in the $0 \neq i^{\text{th}}$ RM layer there is exactly one (ℓ, ℓ, ℓ)-isogeny to a principally polarised abelian 3-fold in a j^{th} RM layer with $j < i$, and we show to deterministically compute this isogeny. Via these isogenies, we can compute an isogeny from the starting 3-fold to a 3-fold with locally maximal real multiplication, or 'almost maximal' (meaning that the index (**??**) is ℓ)– but the 'almost maximal' case turns out to be non-generic. Doing this process for each ℓ in the list $\ell_1, \ldots, \ell_s$ we compute an isogeny to a 3-fold with maximal real multiplication. We are then in the subgraph of **??**, and for most (all but finitely many) totally positive prime elements $\mu \in \mathcal{O}_{K_0}$, the subgraph is a cycle. Thus, walking on the union of the cycle graphs we get to a distinguinshably random 3-fold with maximal real multiplication in very

few steps by rapid mixing. To walk on this layer, i.e., to compute μ-isogenies of 3-folds, we can use ideas of [**?**]. However, most of the vertices in the isogeny graph have *minimal* real multiplication. So, the final step is to deterministically walk down through the RM layers until we reach the bottom layer, for each ℓ (we also show how to do this in our upcoming paper). Note that the minimal real multiplication is $\mathbb{Z}[\pi + \overline{\pi}]$ where π is the Frobenius of A. Once we reach the bottom layer, we should be at a 'random-looking' point, thus under the heuristics above a short random walk should yield a plane quartic 3-fold.

References

[BJW] Brooks, Jetchev, and Wesolowski *Isogeny graphs of ordinary abelian varieties* `https://arxiv.org/abs/1609.09793` (2016)

[DJRV] Dudeanu, Jetchev, Robert, and Vuille *Cyclic Isogenies for Abelian Varieties with Real Multiplication* `https://arxiv.org/abs/1710.05147` (2017)

[Mar] Martindale, *Isogeny Graphs, Modular Polynomials, and Applications*, PhD thesis, available at `www.martindale.info` (2018)