Isogeny graphs of abelian varieties and applications to the discrete logarithm problem

Chloe Martindale

December 13, 2017

These notes are from a talk given in the Heilbronn seminar at the Heilbronn Institute, Bristol. This talk includes joint work 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

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

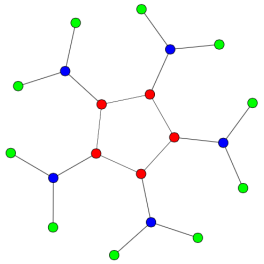
where $[\ell]$ denotes the multiplication-by-ℓ morphism.

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 $E/\mathbb{F}_q$ 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.

Remark. The depth is given by $\max\{r \in \mathbb{Z} : \ell^r | [\mathcal{O}_K : \mathbb{Z}[\pi]]\}$, where π is the q-power Frobenius endomorphism of E and $K = \mathbb{Q}(\pi)$. So the depth is as easy to compute as the Frobenius endomorphism. (We'll come back to this later). 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. Locally at ℓ, the vertices occurring in level V_i have endomorphism ring $\ell^i \mathcal{O}_K$, so 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 - which for all purposes of this talk means 'nice'. 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 $\mathrm{End}(\mathrm{A}) \otimes \mathbb{Q} = K$. 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 p.p.o.a.vs is an undirected graph for which each vertex represents a p.p.o.a.v. 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* $V_0 \in \{I, R_1, R_2, C_n\}$*.*

Remark. As before, the subgraph V_0 is easy to compute, as is the depth of the volcano:

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

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. As before, the levels of the volcano correspond to different endomorphism rings locally at μ. That is, locally at μ, the vertices A in V_i have endomorphism ring $\mu^i \mathcal{O}_K$.

Remark. A similar theorem (but not with μ-isogenies) was given for the genus 2 case by Ionica and Thomé in [IT]. Independently, Brooks, Jetchev, and Wesolowski proved a similar statement (in arbitrary dimension) in [BJW].

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 hyperelliptic, use the algorithm of Diem and Smith. Else, construct a plane quartic C' and an isogeny $\phi : \mathcal{J}(C) \to \mathcal{J}(C')$. (The existence of

such an isogeny for a generic curve is part of the heuristic assumptions, at least for now).

- 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.

4 Constructing an isogeny to the Jacobian of a plane quartic curve

Recall that we have been studying isogeny graphs of principally polarised ordinary abelian varieties. We will need a few facts about 3-dimensional principally polarised abelian varieties over finite fields.

1. By Torelli's theorem, every principally polarised abelian variety is the Jacobian of a genus 3 curve.
2. Every genus 3 curve can be written as either a hyperelliptic curve or a plane quartic curve.
3. Abelian varieties with $\mathrm{End(A)}\otimes\mathbb{Q} = K$, where K is a CM-field, are generic in the class of all principally polarised abelian 3-folds over $\mathbb{F}_q$.
4. Over $\mathbb{F}_q$, up to $\overline{\mathbb{F}_q}$-isomorphism there are $q^6 + 1$ plane quartics (this result is due to Bergstrom).
5. Over $\mathbb{F}_q$, up to $\overline{\mathbb{F}_q}$-isomorphism there are $2q^5 + O(q^4)$ hyperelliptic curves of genus 3.

In particular, in is not unreasonable to assume that a generic isogeny class of principally polarised abelian 3-folds contains a high proportion of Jacobians of plane quartic curves. We assume this, and additionally we assume that the plane quartics are randomly-distributed within the isogeny class. We hope to remove these assumptions, or at least verify them computationally, but this is work in progress.

The idea is to compute an isogeny from the starting curve to a sufficiently random point in the isogeny graph, so that under our heuristic assumptions, there will exist many low-degree isogenies to plane quartic curves.

Before getting into this, we need to study isogeny graphs a little further. Recall that the Volcano Theorem gave the structure of μ-isogeny graphs for principally polarised ordinary abelian varieties with $\mathcal{O}_{K_0} \subseteq \mathrm{End(A)}$. The composition of all the μ-isogeny graphs for all μ gives a subgraph of the whole graph, specifically the subgraph with vertices with maximal real multiplication. To reach all the elements of the isogeny class, we have to additionally use (ℓ, ℓ, ℓ)-*isogenies*.

Definition. An (ℓ, ℓ, ℓ)-isogeny $f : \mathrm{A} \to \mathrm{A}'$ is an isogeny of abelian 3-folds with maximal isotropic kernel of size ℓ^3.

Examples.

- If ℓ does not split in K_0, then an ℓ-isogeny is a (ℓ, ℓ, ℓ)-isogeny.
- If ℓ splits completely in K_0 as $I_1 I_2 I_3 = \ell \mathcal{O}_{K_0}$ and each I_i is principally generated by a totally positive element μ_i, then every (ℓ, ℓ, ℓ)-isogeny between abelian varities with maximal real multiplication is the composition of a μ_1-, a μ_2-, and a μ_3-isogeny.

Definition. An (ℓ, ℓ, ℓ)-isogeny graph of p.p.o.a.vs is an undirected graph for which each vertex represents a p.p.o.a.v over a field $\mathbb{F}_q$ up to (polarisation preserving) isormophism, and an edge between A and Ab' represents a (ℓ, ℓ, ℓ)-isogeny $\mathrm{A} \to \mathrm{A}'$ defined over $\mathbb{F}_q$ together with its dual isogeny $(\mathrm{A}')^\vee \to \mathrm{A}^\vee$ (again, up to isomorphism).

The connected components of an (ℓ, ℓ, ℓ)-isogeny graph are not as beautiful as those of μ-isogeny graphs, but we can still say something about the structure.

We partition the graph into RM layers. We define the i^{th} layer L_i of the (ℓ, ℓ, ℓ)-isogeny graph to be the subgraph containing the vertices A for which

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

There are $r + 1$ layers, where

$$r = \max\{i \in \mathbb{Z} : \ell^i | [\mathcal{O}_{K_0} : \mathbb{Z}[\pi + \overline{\pi}]]\},$$

and for all but finitely many primes ℓ, we have that $r = 0$.

Lemma. *Every principally polarised ordinary abelian variety* A *with* $\mathrm{End}(\mathrm{A}) \otimes \mathbb{Q} = K$ *(where* K *is a CM-field) is isogenous to a principally polarised ordinary abelian variety* A' *with* $\mathrm{End}(\mathrm{A}') = \mathcal{O}_K$ *via a composition of* (ℓ, ℓ, ℓ)*-isogenies and* μ*-isogenies.*

Lemma. *For* $i > 0$*, for each vertex in* L_i*, there exists an* (ℓ, ℓ, ℓ)*-isogeny landing in* L_{i-1}*. This isogeny is the 'RM-ascending' isogeny.*

These lemmas yield the following algorithm:

Algorithm 1.
INPUT: A hyperelliptic genus 3 curve $C/\mathbb{F}_q$ with Frobenius π and $\mathrm{End}(\mathcal{J}(C)) \otimes \mathbb{Q} = \mathbb{Q}(\pi)$ such that $\mathbb{Q}(\pi)$ is a CM-field K.
OUTPUT: A plane quartic curve curve $D/\mathbb{F}_q$, and an isogeny $\phi : \mathcal{J}(C) \to \mathcal{J}(D)$.

1. List $L = (\ell_1, \ldots, \ell_n)$ such that $h > 0$ in the ℓ_i-isogeny graph, and $M = (\mu_1, \ldots, \mu_m)$ such that $d > 0$ in the μ_i-isogeny graph.
2. For $\ell \in L$, walk to L_0 in the (ℓ, ℓ, ℓ)-isogeny graph by computing the unique RM-ascending (ℓ, ℓ, ℓ)-isogeny.
3. For $\mu \in M$, walk to the subgraph V_0 of the μ-isogeny graph.

4. For 'enough' $\mu \notin M$, do a random walk on the cycle for 'enough' steps.

5. Walk randomly in the (ℓ, ℓ, ℓ)-isogeny graph for different ℓ and check at each step if you land on the Jacobian of a plane quartic curve D. If true, output D and the path that was taken to D from C.

Remarks. 1. For Step 1, one only needs to be able to compute the endomorphism algebra and the Frobenius as an algebraic integer.

2. Vuille and Milio are currently working on an implementation of (ℓ, ℓ, ℓ)-isogenies and μ-isogenies, with which we can 'walk' in the (ℓ, ℓ, ℓ)- and μ-isogeny graphs.

3. The precise definitions of 'enough' in Step 4 is work in progress, and will come from a more precise formulation of the heuristic assumptions.

4. Termination relies on the heuristic assumptions.

5 Application to the Discrete Logarithm Problem for Elliptic Curves

Joux and Vitse [**?**] constructed explicit covering maps

$$\pi : H/\mathbb{F}_q \to E/\mathbb{F}_{q^3}$$

from hyperelliptic curves of genus 3 over $\mathbb{F}_q$ to elliptic curves over $\mathbb{F}_{q^3}$ for several families of elliptic curves.

Suppose that $E/\mathbb{F}_{q^3}$ has a hyperelliptic cover $\pi : H \to E$. Using Algorithm 1, we can efficiently construct a plane quartic curve C and an isogeny $\phi : \mathcal{J}(C) \to \mathcal{J}(H)$. Via π and ϕ we can translate the Discrete Logarithm problem on $E/\mathbb{F}_{q^3}$ to the Discrete Logarithm Problem on $\mathcal{J}(C)$, where it can be solved in time $O(q) < O((q^3)^{1/2})$ using the Diem-Smith attack, hence the Discrete Logarithm Problem would be broken for all the elliptic curves in the families detailed by Joux and Vitse.

In future work, we hope to construct more such families of elliptic curves.

References

[BGLMMST] Ballentine, Guillevic, Lorenzo-Garcia, Martindale, Massierer, Smith, and Top, *Isogenies for point counting on genus 2 hyperelliptic curves with maximal real multiplication* `https://arxiv.org/abs/1701.01927` (2017)

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

[DH] Dipippo, Howe, *Real polynomials with all roots on the unit circle and abelian varieties over finite fields*, J. Number Theory 73 (1998), 426450; Corrig., J. Number Theory 83 (2000), 182.

[IT] Ionica and Thomé, *Isogeny graphs with maximal real multiplication*, `https://eprint.iacr.org/2014/230` (2014)

[Mar] Martindale, *Isogeny Graphs, Modular Polynomials, and Applications*, PhD thesis (in preparation), available at `www.martindale.info` (2017)

[Mil] Milio, *A quasi-linear time algorithm for computing modular polynomials in dimension 2*, `https://arxiv.org/abs/1411.0409` (2014)

[Oor] Oort, *Abelian Varieties over Finite Fields*, `http://www.math.nyu.edu/~tschinke/books/finite-fields/final/05_oort.pdf` (2007).

[Sch] Schoof, *Counting points on elliptic curves over finite fields*, Journal de Théorie des Nombres de Bordeaux 7 (1995), 219-254.