Isogeny Graphs in Genus 2

Chloe Martindale (Universiteit Leiden and Université de Bordeaux)
Supervised by Marco Streng (Leiden) and Damien Robert (Bordeaux)

March 5, 2015

Abstract

Traditionally, an isogeny graph is a graph whose vertices are elliptic curves and whose edges are isogenies of a given degree between them. Arranging these graphs in a way that uses the complex multiplication structure of the elliptic curves (in the cases where this can be done) makes the connected components of the graph into what have been labelled isogeny volcanoes. These graphs have nice consequences in number theory and in cryptography, which has motivated us to analyse the graph structure for curves higher genus. I will talk about the structure of the graph for genus 2 curves, and about some of the mathematics that goes into understanding this structure, such as computing models for surfaces coming from Hilbert modular forms.

Contents

These notes are from a talk presented at the 2015 meeting for ALGANT-doc students, held at the University of Regensburg. The purpose of the talk was to present some of the ideas which will go into the PhD thesis of the author.

1 Motivation

The main motivation for looking at isogeny graphs (which will be defined later in this talk) comes from attempting to improve our understanding of ordinary abelian varieties over finite fields in terms of their endomorphism rings. One of the reasons this leads us to look at isogenies (i.e. surjective morphisms with finite kernel) is that the endomorphism algebra, $\mathrm{End}^0(A) := \mathrm{End}(A) \otimes \mathbb{Q}$, of such an abelian variety A is invariant under isogeny; this motivates us to try and classify abelian varieties lying in the same isogeny class by endomorphism ring. We first consider elliptic curves, in which case we can easily define which type of isogeny we want to look at.

Definition 1.1. an *ℓ-isogeny* of elliptic curves, for ℓ prime, is a surjective morphism with kernel of size ℓ.

In 1996, David Kohel introduced the notion of ℓ-isogeny graphs for elliptic curves over finite fields in his PhD thesis ([**?**]), which gives a very nice solution to the problem of classifying elliptic curves over finite fields which lie in the same ℓ-isogeny class by endomorphism ring. His thesis deals with both ordinary and supersingular elliptic curves, but here we only summarize his results for ordinary elliptic curves.

1.1 Isogeny graphs of elliptic curves

To motivate the generalization to abelian varieties, we give here a brief summary of Kohel results in the ordinary case. For the interested reader, there is a very nice book on this topic by Sutherland ([**?**]). Let E be an ordinary elliptic curve defined over a field k with q elements. Then by e.g. [**?**] there exists a CM-field K (i.e. a totally imaginary number field) of degree 2 such that the endomorphism algebra of E, $\mathrm{End}^0(E)$ is isomorphic to K (i.e. E has complex multiplication). Further, as mentioned in the previous paragraph, for any elliptic curve E' which is ℓ-isogeneous to E, we also have that $\mathrm{End}^0(E') \cong K$.

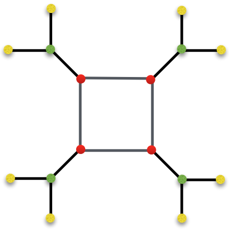
Definition 1.2. An *ℓ-isogeny graph of elliptic curves* is a graph whose vertices are given by ordinary elliptic curves defined over k (a finite field with q elements) and whose edges are given by ℓ-isogenies.

Kohel's results show that every connected component of such a graph has the following properties:

- There is exactly one cycle, where each vertex in the cycle corresponds to an elliptic curve with endomorphism ring isomorphic to $\mathcal{O}_K$, the maximal order of K.
- Each vertex of the graph has exactly ℓ+1 edges, except for the end points of

the graph, where each vertex has exactly 1 edge.
- The graph is completely symmetrical.
- The graph is finite. (The number of edges between the cycle and any given end point is given by n, where $[\mathcal{O}_K : \mathbb{Z}[\pi]] = \ell^n$, for π the Frobenius of k. This follows from the fact that $\mathbb{Z}[\pi] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_K$, and that passing to an ℓ-isogeneous elliptic curve either preserves the complex multiplication or changes it by index ℓ.)

So for example, if $\ell = 2$, our ℓ-isogeny graph could look like this:



Here the red vertices correspond to elliptic curves with endomorphism ring isomorphic to $\mathcal{O}_K$, the green vertices correspond to elliptic curves with endomorphism ring isomorphic to $\mathbb{Z} + \ell\mathcal{O}_K$ and the yellow vertices correspond to elliptic curves with endomorphism ring isomorphic to $\mathbb{Z} + \ell^2\mathcal{O}_K = \mathbb{Z}[\pi]$. One of the reasons why this picture is helpful, is that given an elliptic curve over some finite field, one can easily determin its endomorphism ring in the following way:
- Compute its ℓ-isogeny graph.
- Compute which curves, say $E_1, .., E_{\ell+1}$, are ℓ-isogeneous to it. (Using the modular polynomial of level ℓ, see below).
- For each of $E_1, ..., E_{\ell+1}$, choose 1 curve which is ℓ-isogeneous to it.
- Continue doing this until there are no curves which are ℓ-isogeneous to at least one of your $\ell + 1$ options; this means that you have reached the end ('the floor') of your isogeny graph.
- The number of steps taken corresponds exactly to which level of the graph you started at (which colour on the example), and hence tells us the endomorphism ring!

To find the ℓ-isogeneous elliptic curves we rely use the modular polynomial of level ℓ, which is something we have generalised to genus 2 (and g where possible) and so we state the definition here.

Definition 1.3. The *modular polynomial of level* ℓ, for ℓ prime, is a polynomial $\Phi_\ell \in \mathbb{Z}[X, Y]$ such that

$$\Phi_\ell(j(E_1, j(E_2)) = 0 \Leftrightarrow E_1 \text{ and } E_2 \text{ are } \ell\text{-isogeneous},$$

where $j(\bullet)$ denotes the j-invariant of $\bullet$.

These are easy compute!

2 Defining isogeny graphs in genus 2

The work of the author is to find the structure of isogeny graphs for ordinary abelian varieties over finite fields. The first obvious question is: what do we draw?

2.1 Vertices

To use all of the available techniques, it is useful to pass between abelian varities over finite fields and abelian varieties defined over $\mathbb{C}$ with complex multiplication. There are 'lifting theorems' which tell us how to do this, but we have not yet thought about how do formalize this in our situation, so for now we just say that for simplicity, take A to be an ordinary abelian variety of genus 2 defined over $\mathbb{C}$ with complex multiplication by an order $\mathcal{O}$ in a totally imaginary number field of degree 4 (=2 times the genus), K. If this is too technical, A being 'an ordinary abelian variety of genus 2 defined over $\mathbb{C}$' means that we can write $A \cong \mathbb{C}^2/\Lambda$, where Λ is a lattice of rank 2 in $\mathbb{C}^2$, and A having 'complex multiplication by $\mathcal{O}$' means that there exists an embedding $\iota : \mathcal{O} \hookrightarrow \mathrm{End}(A)$. We make one further restriction to the type of abelian variety, which is that they should be principally polarized, i.e. that A comes with a polarization map $A \to A^\vee$, where $A^\vee$ denotes the dual of A, which is an isomorphism. One of the reasons that we make this restriction is that then there exists a $\tau \in \mathrm{SL}_2(\mathcal{O}^+)\backslash\mathbb{H}^2$ such that

$$A_\tau \cong \mathbb{C}^2/(\mathcal{O}^+ + \tau\mathcal{O}^+).$$

Here, $\mathcal{O}^+$ denotes the totally positive subring of $\mathcal{O}$, $\mathbb{H}^2$ denotes 2 copies of the upper half plane and $\mathrm{SL}_2(\mathcal{O}^+)$ is the special linear group of dimension 2 with entries in $\mathcal{O}^+$. This acts on $\mathbb{H}^2$ in a canonincal way, see any book on Hilbert modular forms, e.g. [**?**].

Definition 2.1. Principally polarized abelian varieties with complex multiplication by $\mathcal{O}$ an order in K a quartic totally imaginary number field, $A_\tau \cong \mathbb{C}^2/(\mathcal{O}^+ + \tau\mathcal{O}^+$, are the vertices of the isogeny graph in genus 2.

2.2 Edges

We now generalise the notion of the ℓ-isogeny for elliptic curves. It is a little more complicated in this case because we also need to consider the polarisations (polarisation maps are just the identity for elliptic curves). So let

$$f : A_\tau \to A_{\tau'}$$

be an isogeny, and let

$$\xi_\tau : A_\tau \to \ A_\tau^\vee \quad \xi_{\tau'} : A_{\tau'} \to \ A_{\tau'}^\vee$$

be principal polarisation maps.

Definition 2.2. With $f, \xi_\tau, \xi_{\tau'}$ as above, if exists $\lambda \in \operatorname{End}(A_\tau)$ such that the diagram

$$\begin{tikzcd}
A_\tau \arrow[dr, "\xi_\tau"'] & A_\tau \arrow[l, "\lambda"] \arrow[r, "f"] & A_{\tau'} \arrow[d, "\xi_{\tau'}"] \\
 & A_\tau^\vee & A_{\tau'}^\vee \arrow[l, "f^\vee"]
\end{tikzcd}$$

commutes, then f is a λ-*isogeny.*

These λ-isogenies will be the edges of our isogeny graph of genus 2. In order for such a λ to exist, it can be shown that λ must in fact be totally positive. This definition may look a little strange: in practise we have 2 cases, either λ is a prime in $\mathbb{Z}$, so that f has degree ℓ^2, or λ is a totally positive element of prime norm in K_0, the maximal totally real subfield of K, so that f has degree $N_{K_0/\mathbb{Q}}(\lambda)$. The second case is the most natural extension of the case of elliptic curves, but is not always possible, which is why we also allow the first case.

3 Summary of results and ongoing research

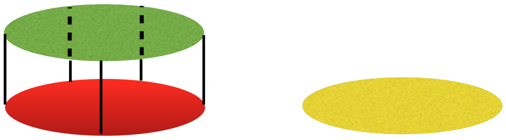
The author has two main projects, one which is completed but not yet available, and one which is very much still work in progress.

3.1 Generalising the modular polynomial

The completed project is an algorithm which gives a generalisation of the modular polynomial for genus 2 curves, in the sense of Hilbert modular forms, so a set of polynomials depending on K_0 and λ whose zeros correspond to invariants of λ-isogeneous abelian varieties of genus 2. One of the main parts of this project was writing down a nice generalisation of the j-invariant for elliptic curves. An example for which this was already in the literature is for $K_0 = \mathbb{Q}(\sqrt{5})$; these are called Gundlach invariants, see e.g. [**?**].

3.2 The structure of isogeny graphs in genus 2

The work in progress is joint work with Ionica, Robert and Streng. We are working on proving the structure of isogeny graphs in genus 2 in general; it turns out that this is more interesting in the case $\lambda = \ell$ for ℓ a prime in $\mathbb{Z}$. For abelian varieties whose endomorphism rings satisfy $K_0 \cap \operatorname{End}(A) = \mathcal{O}_{K_0}$, where K_0 has narrow class number 1, Ionica and Thomé showed in [**?**] that for λ totally positive in K_0 of prime norm, the connected components of the isogeny graphs look the same as in the elliptic curve case, with a cycle and branches coming from the cycle (this has come to be called 'volcano' structure). So if ℓ a prime in $\mathbb{Z}$ splits into totally positive elements in K_0 then the ℓ-isogeny graph structure can be deduced from this and is also volcano-like. In fact, the ℓ-isogeny graph has this structure also when ℓ is ramified or inert in K_0. But this does not give the full isogeny graph, since there are also abelian varieties with $K_0 \cap \mathrm{End}(A) \subset \mathcal{O}_{K_0}$. In this case, the endomorphism ring can be of 2 types. We believe that we can then show that vertices with endomorphism ring of type (1) are all ℓ-isogeneous to a vertex with $K_0 \cap \mathrm{End}(A) = \mathcal{O}_{K_0}$, and so form another layer of volcano in the graph, joined by cross-layer descending ℓ-isogenies (see picture below). We believe that the volcano structure should also be inherited from the top layer. Further, we believe that for vertices with endomorphism ring of type (2), there does not exist a rational ℓ-isogeny to a vertex A with $K_0 \cap \mathrm{End}(A) = \mathcal{O}_{K_0}$, and so these vertices form a separate connected component of our graph. It is not unreasonable to hope that this component will also have a volcano-like structure, although we are not yet sure if this will be true! So in conclusion, we believe that the picture should look like:



where the green layer is a volcano graph whose vertices have endomorphism ring containing $\mathcal{O}_{K_0}$, the red layer is a volcano graph whose vertices have endomorphism ring contained in $\mathcal{O}_{K_0}$ of type (1), and the yellow layer has vertices whose endomorphism rings are contained in $\mathcal{O}_{K_0}$ and are of type (2).