Isogeny Graphs and Endomorphism Rings of Ordinary Abelian Varieties

Gaetan Bisson

Moscow, February 2018

I started working in Tahiti in September 2013 and Alexey arrived in November. His research interests being much deeper and more theoretical than my own, I believed it would be quite challenging for us to work together. Then Dimitar visited us in January 2017.

This talk: background and prior work.
Next talk (Dimitar): our contribution.

1 Isogeny Graphs

Consider **principally polarized abelian varieties of dimension one and two** over a finite field. **Isogenies** are morphisms of such varieties with finite kernel and cokernel.

Definition. *Let k a finite group and $g \geq 1$; define $G_k^g(\mathbb{F}_q)$ as the graph with:*

- *nodes: isomorphism classes of abelian varieties of dimension g*
- *edges: isogenies with kernel isomorphic to k*

The first result towards understanding its structure is:

Theorem (Tate). *$\mathscr{A}$ and $\mathscr{B}$ are isogenous $\iff \zeta_{\mathscr{A}} = \zeta_{\mathscr{B}} \iff \chi_\pi(\mathscr{A}) = \chi_\pi(\mathscr{B})$.*

The existence of an isogeny $\mathscr{A} \to \mathscr{B}$ is thus easy to compute, but finding an explicit one remains a difficult problem for which it is critical to understand the graph structure.

Consider absolutely simple, ordinary varieties. Knowing χ_π is essentially equivalent to knowing $K = \mathbb{Q}(\pi)$, an imaginary quadratic extension of a totally real number field K_0. We use the endomorphism ring $\mathcal{O}_{\mathscr{A}}$ as a finer invariant: it is an order of K containing $\mathbb{Z}[\pi, \overline{\pi}]$; for a given Weil polynomial χ_π there are finitely many possibilities.

Lemma. *If $\mathscr{A}$ and $\mathscr{B}$ are adjacent nodes of $G^g_{(\mathbb{Z}/\ell)^g}$ then $[\mathcal{O}_{\mathscr{A}} + \mathcal{O}_{\mathscr{B}} : \mathcal{O}_{\mathscr{A}} \cap \mathcal{O}_{\mathscr{B}}]$ divides ℓ^{2g-1}.*

Theorem (Shimura). *The subgraph of varieties with endomorphism ring $\mathcal{O}$ is a Cayley graph for $\{\mathfrak{a} : \mathcal{O}/\mathfrak{a} \simeq k\} \subset \mathfrak{C}(\mathcal{O})$.*

For example, if $|k| = \ell$ is inert in K, this subgraph is trivial.

2 Elliptic Curves

Multiple simplifications: $K_0 = \mathbb{Q}$ (unique polarization, lattice of orders is locally linear), isogenies are products of prime-degree ones for which $\mathscr{A} \to \mathscr{B} \Leftrightarrow \mathscr{O}_A \subset \mathscr{O}_B$ or vice versa.

The structure of isogeny graphs of elliptic curves was made entirely explicit (Kohel, 1996) and became known as a volcano; see Figure 1. The computation of isogenies (Vélu, 1971) allows exploiting it for:

- computation of endomorphism rings
- computation of modular polynomials (point counting)
- computation of class polynomials (generating curves with prescribed orders)
- reducibility of discrete logarithms (analyzing the security of cryptosystems)

3 Abelian Surfaces

Isogenies of type $(\mathbb{Z}/\ell)^2$ preserving polarizations have been computable for nearly ten years (Lubicz–Robert, 2009). More recently, some of type $(\mathbb{Z}/\ell)$ too.

The graph structure is not nearly as explicit as for $g = 1$. *[Draw a non-linear lattice with orders jumping index ℓ and ℓ^2, then an isogeny graph with donught rim and non-balanced trees hanging with horizontal jumps across and within trees.]* See Figure 2.

Recent results exist for the case $\mathscr{O} \cap K_0 = \mathscr{O}_{K_0}$ where orders are easy to describe. Dimitar's talk will present a theoretical approach for understanding the graph structure in general; here as an appetizer we present an approach that rely solely on the structure of horizontal isogenies.

Theorem (B, 2015). *Endomorphism rings can be computed in heuristic average time $L(q)^{g^2\sqrt{3}/2+o(1)}$.*

Proof. The main idea is to exploit Shimura's complex multiplication: since the action is faithful, if $\mathfrak{a}$ is trivial in $\mathfrak{C}(\mathscr{O})$ and $\varphi_{\mathfrak{a}}(\mathscr{A}) \not\simeq \mathscr{A}$ then $\mathscr{O} \not\subseteq \mathscr{O}_{\mathscr{A}}$.

Algorithm (very high-level overview).

INPUT: *An absolutely simple, ordinary abelian surface $\mathscr{A}/\mathbb{F}_q$.*
OUTPUT: *Its endomorphism ring.*

1. *Compute the order $\mathscr{O}' = \mathbb{Z}[\pi, \overline{\pi}]$.*
2. *For each order $\mathscr{O}$ of which $\mathscr{O}'$ is a maximal suborder:*
3. *Find enough ideals $\mathfrak{a}$ trivial in $\mathfrak{C}(\mathscr{O})$.*
4. *If all $\varphi_{\mathfrak{a}}(\mathscr{A})$ are isomorphic to $\mathscr{A}$:*
5. *Set $\mathscr{O}' \leftarrow \mathscr{O}$ and go back to Step 2.*
6. *Return $\mathscr{O}'$.*

Uses point counting, factoring discriminant, enumerating orders, selecting ideals for which $\varphi_{\mathfrak{a}}$ is efficiently computable, identifying subgroup corresponding to $\mathfrak{a}$, pushing to theta coordinates, computing isogenies, Mestre's method to obtain a minimal variety, showing that knowing enough ideals trivial in $\mathfrak{C}(\mathscr{O})$ are trivial in $\mathfrak{C}(\mathscr{O}_{\mathscr{A}})$ actually implies $\mathscr{O} \subset \mathscr{O}_{\mathscr{A}}$. Assumes typical smoothness behavior for ideals, conductors, and discriminants.

(For elliptic curves, all can be proven very neatly under GRH.) □

This allows us to explore isogeny graphs without understanding their vertical structure. Dimitar will now present a better approach.

Спасибо за внимание!

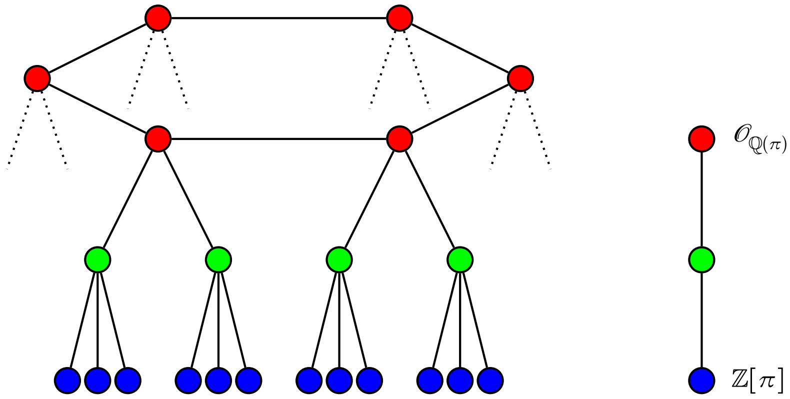

Figure 1: Typical connected component of $G^1_{\mathbb{Z}/3}$ and corresponding lattice of orders.

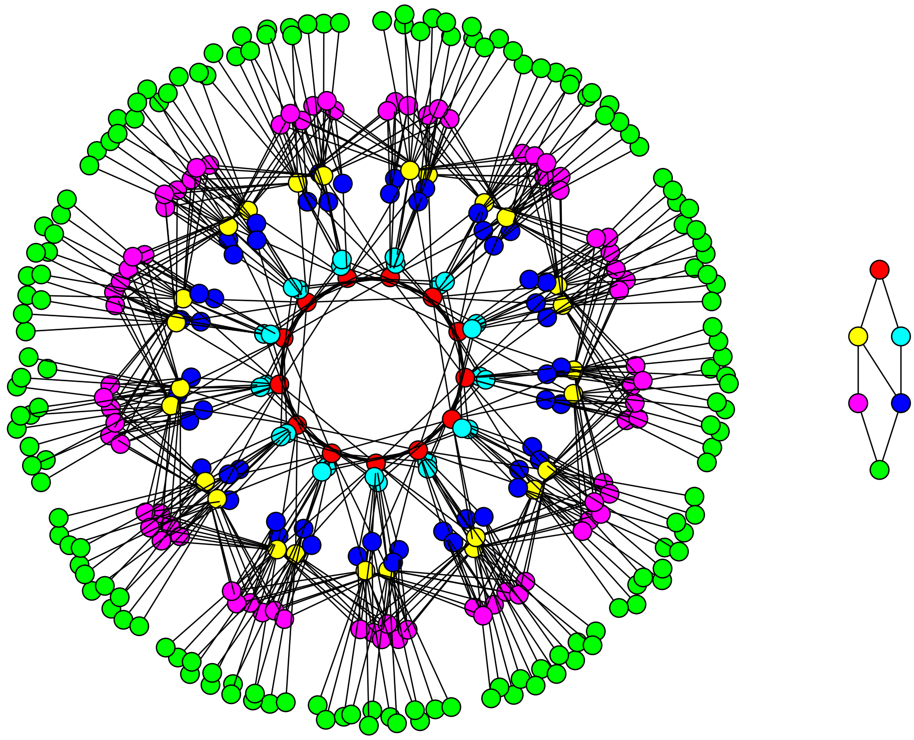

Figure 2: Typical connected component of $G^2_{(\mathbb{Z}/3)^2}$ and corresponding lattice of orders.