How to find a stationary distribution

Random walks in genus 2 isogeny graphs

Enric Florit Zacarías

2022 Departmental Workshop
"Computer Science Meets Mathematics"

September 7, 2022

What is this talk about?

I want to explain a theorem about *random walks* on *graphs* formed by *abelian varieties*.

- Joint work with Ben Smith (Inria & LIX).
- Done during my Erasmus internship, right after my Bachelor's thesis in Spring 2020.
- $\Longrightarrow$ I've got a full email record of the development of this project!

What is this talk about?

I want to explain a theorem about *random walks* on *graphs* formed by *abelian varieties*.

- Joint work with Ben Smith (Inria & LIX).
- Done during my Erasmus internship, right after my Bachelor's thesis in Spring 2020.
- $\implies$ I've got a full email record of the development of this project!

An atlas of the Richelot isogeny graph [arXiv:2101.00917]

Automorphisms and Isogeny Graphs of Abelian Varieties, with Applications to the Superspecial Richelot Isogeny Graph [arXiv:2101.00919]

Existing hard problems for cryptography

Public key cryptography is based on apparently hard problems:

- Factoring integers
- Discrete logarithms in finite groups

The usual problems for public key cryptography should be easily solved with a full-scale quantum computer.

Can we find other hard problems?

Hard problems from graphs

Problem

Given a graph G, can we find length-n paths between any two nodes $u, v \in E(G)$?

If this is an actual "hard" problem, then

- Nodes can be public information
- Paths between them can serve as private keys

A particular kind of graphs where path-finding is thought to be difficult are *isogeny graphs*.

Isogeny-based cryptography

Fix a prime $p > 3$.

An isogeny graph is a finite graph G consisting of

- Elliptic curves (up to isomorphism) as nodes,

$$E(\mathbb{Z}/p\mathbb{Z}) = \{(x, y) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \mid y^2 = x^3 + Ax + B\} \cup \{\infty\}.$$

Isogeny-based cryptography

Fix a prime $p > 3$.

An isogeny graph is a finite graph G consisting of

- Elliptic curves (up to isomorphism) as nodes,

  $$E(\mathbb{Z}/p\mathbb{Z}) = \{(x, y) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \mid y^2 = x^3 + Ax + B\} \cup \{\infty\}.$$

- Morphisms of elliptic curves as edges **[Isogenies]**.

  Usually of fixed degree n (i.e. $\phi : E_1 \to E_2$ is n-to-1).

  For each $E_1 \to E_2$, there is a dual $E_2 \to E_1$ of the same degree.

Isogeny-based cryptography

Fix a prime $p > 3$.

An isogeny graph is a finite graph G consisting of

- Elliptic curves (up to isomorphism) as nodes,

  $$E(\mathbb{Z}/p\mathbb{Z}) = \{(x, y) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \mid y^2 = x^3 + Ax + B\} \cup \{\infty\}.$$

- Morphisms of elliptic curves as edges **[Isogenies]**.

  Usually of fixed degree n (i.e. $\phi : E_1 \to E_2$ is n-to-1).

  For each $E_1 \to E_2$, there is a dual $E_2 \to E_1$ of the same degree.

Our graphs have $\sim \frac{p}{12}$ nodes.

Isogeny-based cryptography

Fix a prime $p > 3$.

An isogeny graph is a finite graph G consisting of

- Elliptic curves (up to isomorphism) as nodes,

  $E(\mathbb{Z}/p\mathbb{Z}) = \{(x, y) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \mid y^2 = x^3 + Ax + B\} \cup \{\infty\}.$

- Morphisms of elliptic curves as edges **[Isogenies]**.

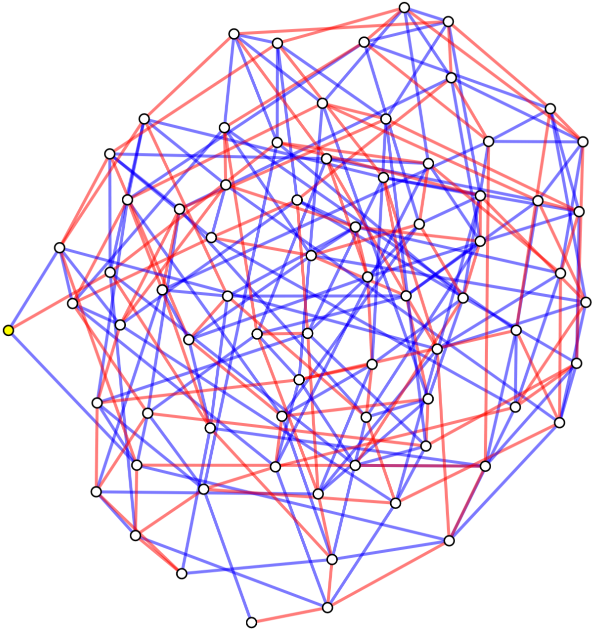
  Usually of fixed degree n (i.e. $\phi : E_1 \to E_2$ is n-to-1).

  For each $E_1 \to E_2$, there is a dual $E_2 \to E_1$ of the same degree.

Our graphs have $\sim \frac{p}{12}$ nodes.

Several proposed protocols: SIDH/SIKE, CGL, CSIDH, SQI-Sign...

The 2-3-isogeny graph for $p = 863$



Generalisation to abelian surfaces

We consider two kinds of abelian surfaces:

- Jacobians of hyperelliptic curves (g=2),

$$y^2 = x^5 + a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0,$$

Generalisation to abelian surfaces

We consider two kinds of abelian surfaces:

- Jacobians of hyperelliptic curves (g=2),

$$y^2 = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0,$$

- Products of elliptic curves $E_1 \times E_2$,

$$E_1 : y^2 = x^3 + A_1x + B_1,$$
$$E_1 : y^2 = x^3 + A_2x + B_2.$$

Generalisation to abelian surfaces

We consider two kinds of abelian surfaces:

- Jacobians of hyperelliptic curves (g=2),

$$y^2 = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0,$$

- Products of elliptic curves $E_1 \times E_2$,

$$E_1 : y^2 = x^3 + A_1x + B_1,$$
$$E_1 : y^2 = x^3 + A_2x + B_2.$$

With these we build finite graphs with surfaces as nodes and morphisms as edges. We can only compute isogenies of degree 4, which forms a 15-out-regular graph.

These have $\sim \frac{p^3}{2880} + O(p^2)$ nodes, of which $\sim \frac{p^2}{288}$ are products.

Generalisation to abelian surfaces

We consider two kinds of abelian surfaces:

- Jacobians of hyperelliptic curves (g=2),

$$y^2 = x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0,$$

- Products of elliptic curves $E_1 \times E_2$,

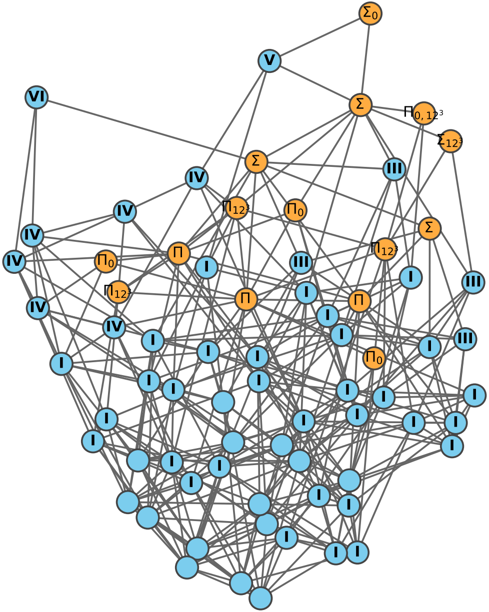
$$E_1 : y^2 = x^3 + A_1x + B_1,$$
$$E_1 : y^2 = x^3 + A_2x + B_2.$$

With these we build finite graphs with surfaces as nodes and morphisms as edges. We can only compute isogenies of degree 4, which forms a 15-out-regular graph.

These have $\sim \frac{p^3}{2880} + O(p^2)$ nodes, of which $\sim \frac{p^2}{288}$ are products.

This graph has now been used to break SIDH!

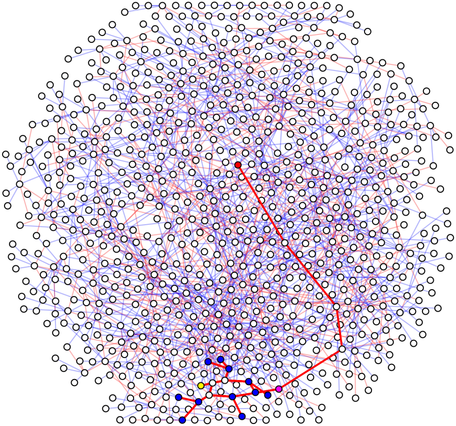
The 4-isogeny graph for $p = 47$



Finding paths

Now we have our graphs set up. How do we find length-d paths $u \to v$? A generic meet-in-the-middle strategy:

1. Explore & store neighborhood of u, of depth f
2. Randomly do DFS from v with length $d - f$.



Finding paths

Now we have our graphs set up. How do we find length-d paths $u \to v$? A generic meet-in-the-middle strategy:

1. Explore & store neighborhood of u, of depth f
2. Randomly do DFS from v with length $d - f$.

Complexity of doing this is $O(p^{1/2})$ in the elliptic curve graph, and $O(p^{3/2})$ in the abelian surface graph.

Finding paths with a distinguished subgraph

Suppose we want to find paths $u \to v$ in a graph G.

If G has a connected subgraph H where path-finding is easier, we can:

Finding paths with a distinguished subgraph

Suppose we want to find paths $u \to v$ in a graph G.

If G has a connected subgraph H where path-finding is easier, we can:

- Find a path $u \to u' \in H$,
- Find a path $v \to v' \in H$,
- Find a path $u' \to v'$ in H.

Finding paths with a distinguished subgraph

Suppose we want to find paths $u \to v$ in a graph G.

If G has a connected subgraph H where path-finding is easier, we can:

- Find a path $u \to u' \in H$,
- Find a path $v \to v' \in H$,
- Find a path $u' \to v'$ in H.

For the abelian surface graph (Costello – Smith, 2019):

- Use subgraph of products of elliptic curves.
- Speedup from $O(p^{3/2})$ to $O(p)$.

Random walks

For this strategy to work, we need to get *on average* short paths for u to H.

- If H is too small, it will be hard to reach;
- If H is too large, we will get little improvement.

Random walks

For this strategy to work, we need to get *on average* short paths for u to H.

- If H is too small, it will be hard to reach;
- If H is too large, we will get little improvement.

To study how good our subgraph is, we use the random walk model:

- Start with a node $u_0 \in G$
- For each $n \geq 0$, choose a neighbor u_{n+1} of u_n with probability $\frac{1}{\deg u_n}$.

Random walks

For this strategy to work, we need to get *on average* short paths for u to H.

- If H is too small, it will be hard to reach;
- If H is too large, we will get little improvement.

To study how good our subgraph is, we use the random walk model:

- Start with a node $u_0 \in G$
- For each $n \geq 0$, choose a neighbor u_{n+1} of u_n with probability $\frac{1}{\deg u_n}$.

If G is a regular graph, we should go into H with probability $\frac{\#H}{\#G}$ at each step $\rightsquigarrow$ geometric distribution.

Stationary distribution

The random walk forms a *Markov chain*. We can show:

Theorem

For our isogeny graph of abelian surfaces, the random walk converges to a distribution on the nodes π.

This distribution π is the eigenvector (of eigenvalue 1) corresponding to the stochastic adjacency matrix M.

$$\lim_{n\to\infty} M^n \varphi_0 = \pi$$

$$M\pi = M.$$

An experiment

While `lockdown`:

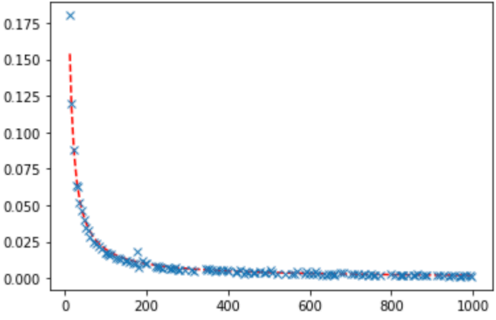
1. Start with a random abelian surface.
2. Do a random walk until we hit a product of elliptic curves.
3. Write down the number of steps.
4. Repeat.

We expected to hit $E \times E'$ with probability $\frac{10}{p}$.

Subject: puzzling numbers (March 26)

However, the actual distribution has parameter between 1.5/p and 2/p, which is about 5 to 6 times lower than predicted. This is consistent across primes up to 1000 (although I don't have much more than 20 or 30 walks recorded for primes > 200).

```
plt.plot(actual_primes, [2/p for p in actual_primes], 'r--')
plt.plot(actual_primes, geometric_parameters, 'x')
plt.show()
```



Adjacency matrices

- Computing these "times until elliptic curve products" is expensive and wasteful.
- Hence, we switched to computing adjacency matrices.
- We computed the 4-isogeny graph for each prime p up to ~ 600. This took three or four weeks.
- For comparison, we can compute elliptic product graphs up to $p \sim 30000$ in an afternoon.

Subject: Jacobians (April 1)

Soon we noticed something: the adjacency matrix of our graphs are not symmetric.

I've checked the proportion of "defective" edges in our graphs, and I've noticed two things:

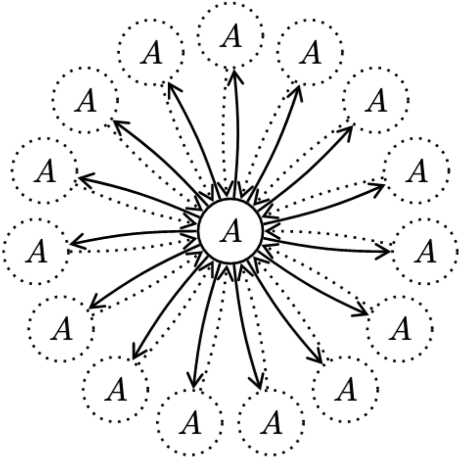
1) This proportion seems to go down with p (at p=607, only 5% of the edges have some disagreement on the number of isogenies going each way),
2) Most (almost all) defective edges are between jacobians.

So, we'll have to take a look at jacobians, automorphisms and numbers of isogenies. It looks like some work has been done very recently: https://arxiv.org/abs/2003.00633 ... On the other hand, knowing something about these (numbers of) defective edges could be extremely helpful in knowing the stationary distribution of random walks in J_p (I have some ideas on how to work this out) and the geometric parameter I've talking about.

The paper is "Counting Richelot isogenies between superspecial abelian surfaces" by Katsura and Takashima.

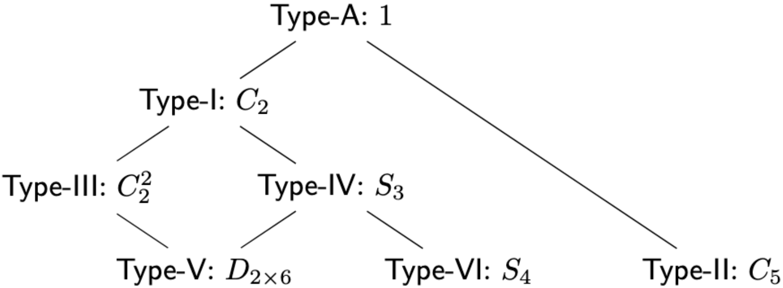
Neighborhoods of surfaces in the 4-isogeny graph

Generically, a surface has the following neighborhood:



Automorphism groups of surfaces

... however, surfaces can have automorphism groups. We can describe $\mathrm{Aut}(\mathcal{A})/\langle \pm 1 \rangle$:



These were computed in the 1880s.

Automorphism groups of products

We also had to compute automorphism groups of $E \times E'$, using GAP:

$$
\begin{tikzcd}
 & \text{Type-}\Pi\text{: } C_2 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\text{Type-}\Pi_0\text{: } C_6 \arrow[d, dash] \arrow[dr, dash] & \text{Type-}\Sigma\text{: } C_2^2 \arrow[dl, dash] \arrow[dr, dash] & \text{Type-}\Pi_{12^3}\text{: } C_4 \arrow[dl, dash] \arrow[d, dash] \\
\text{Type-}\Sigma_0\text{: } C_6 \times S_3 & \text{Type-}\Pi_{0,12^3}\text{: } C_{12} & \text{Type-}\Sigma_{12^3}\text{: } C_2^2 \rtimes C_4
\end{tikzcd}
$$

Automorphism groups of products

We also had to compute automorphism groups of $E \times E'$, using GAP:

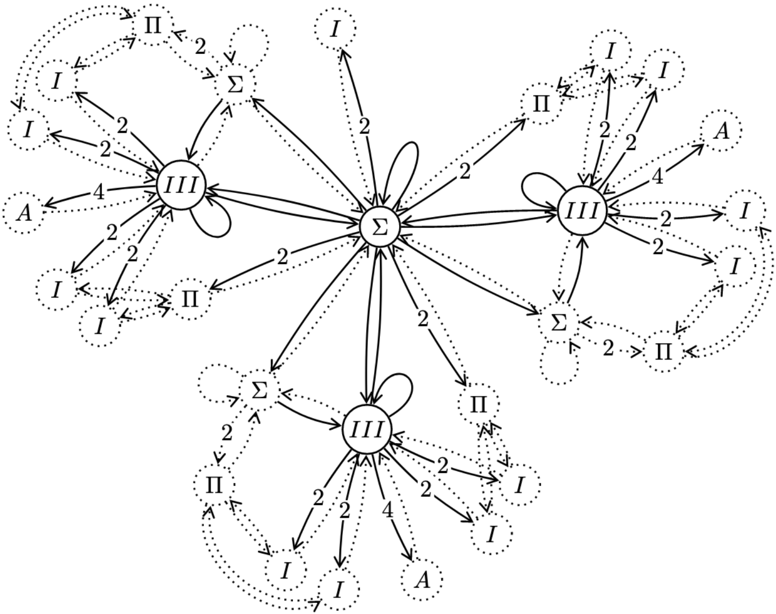
$$
\begin{tikzcd}[arrows=dash]
 & \text{Type-}\Pi\text{: } C_2 \arrow[dl] \arrow[d] \arrow[dr] & \\
\text{Type-}\Pi_0\text{: } C_6 \arrow[d] \arrow[dr] & \text{Type-}\Sigma\text{: } C_2^2 \arrow[dl] \arrow[dr] & \text{Type-}\Pi_{12^3}\text{: } C_4 \arrow[dl] \arrow[d] \\
\text{Type-}\Sigma_0\text{: } C_6 \times S_3 & \text{Type-}\Pi_{0,12^3}\text{: } C_{12} & \text{Type-}\Sigma_{12^3}\text{: } C_2^2 \rtimes C_4
\end{tikzcd}
$$

For example, if $\mathrm{Aut}(E) = \langle \alpha \rangle$ with $\alpha^d = 1$, then

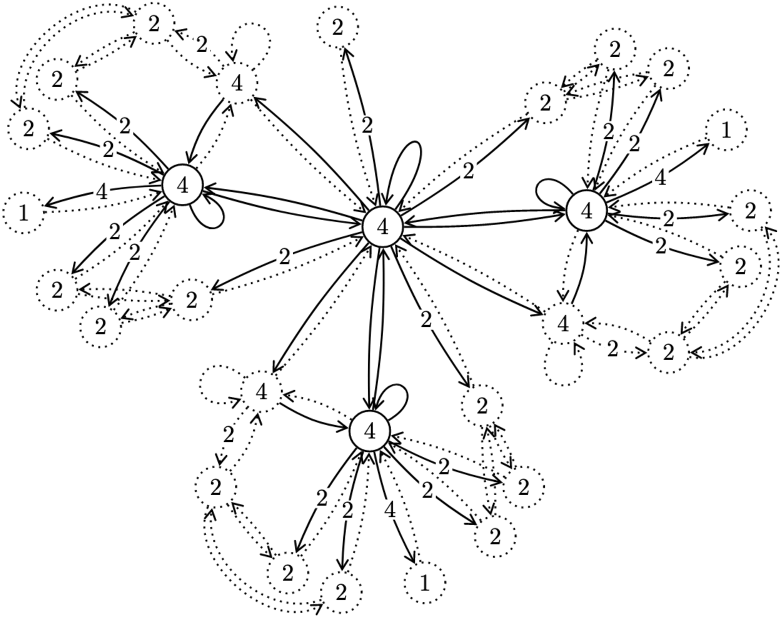
$$\mathrm{Aut}\,(E \times E) \cong \left\langle a, b, \tau \mid a^d = b^d = \tau^2 = 1, ab = ba, a\tau = \tau b \right\rangle$$

and GAP can identify $\mathrm{Aut}(E \times E)/\pm 1$.

Neighborhoods and automorphisms



Neighborhoods and automorphisms



Remarks on arrow multiplicities (May 9)

1) Every isogeny from a type-I curve to one with RA=0 must have maximal multiplicity,
2) An isogeny ZZ/2ZZ —> S3 has to be a double isogeny
3) If we have an n-fold (n=1 or 2) isogeny ZZ/2ZZ —> (ZZ/2ZZ)^2, then there have to be 2n isogenies coming back
4) An isogeny (ZZ/2ZZ)^2 —> S3 has to be a double isogeny.

We already know (1) is true. In the cases p != 1, 19 mod 24 (i.e., when the curves D12 and S4 appear) similar conditions on the number of edges could be imposed, but I suspect they are easy to check given the uniqueness of such curves.

A key lemma

We extract a result from observing neighborhoods:

Lemma

$$\#\,\mathsf{Aut}(\mathcal{A}) \cdot \#\{\mathcal{A}' \to \mathcal{A}\} = \#\,\mathsf{Aut}(\mathcal{A}') \cdot \#\{\mathcal{A} \to \mathcal{A}'\}.$$

Theorem (F.-Smith)

The stationary distribution of the random walk on $\Gamma_g(\ell; p)$ is given, after normalization, by

$$\pi_{\mathcal{A}} \sim \frac{1}{\#\,\mathrm{Aut}(\mathcal{A})}.$$

Moreover, convergence to this distribution is given by

$$\left|\mathrm{Prob}[\mathcal{A}_n = \mathcal{A}] - \frac{C}{\#\,\mathrm{Aut}(\mathcal{A})}\right| \leq \lambda_\star^n \cdot \sqrt{\frac{\#\mathrm{Aut}\,(\mathcal{A}_0)}{\#\mathrm{Aut}(\mathcal{A})}}$$

where $\lambda_\star$ is the **second largest eigenvalue** of the adjacency matrix of $\Gamma_g(\ell; p)$, and $\mathcal{A}_0$ is the starting node in the walk.

Future work

Two questions remain:

- What is the expected distance to a product of elliptic curves?
- We have to look at "the chain of random walks that survive forever", also known as a *Killed process*.

Future work

Two questions remain:

- What is the expected distance to a product of elliptic curves?
- We have to look at "the chain of random walks that survive forever", also known as a *Killed process*.
- What is the mixing rate of the random walk? I.e., can we compute a sharp bound on the eigenvalues of the adjacency matrices?
- We would need to propose and prove conjectures for Siegel modular forms with level "of middle parahoric type" (cf. work of Ibukiyama).

How to find a stationary distribution

Random walks in genus 2 isogeny graphs

Enric Florit Zacarías

2022 Departmental Workshop
"Computer Science Meets Mathematics"

September 7, 2022