Grafs d'isogènies superespecials en gènere 2

Enric Florit Zacarías

SIMBa

3 de juny de 2020

1. Random walks on graphs
2. Expander graphs
3. Isogenies
4. Genus 2 graphs

Random walks on graphs

- Let $G = (V, E)$ be a graph (undirected, simple edges).
- Start at a vertex $u \in V$.
- At each step, choose a new vertex v uniformly at random from $N(u)$. This gives a random sequence $X_0, X_1, X_2 \dots$ taking values in V.
- For all $u, v \in V$,

$$P(X_{i+1} = v \mid X_i = u) = \begin{cases} \frac{1}{\deg u}, \text{if } v \in N(u), \\ 0, \text{otherwise.} \end{cases}$$

Random walk matrix

The random sequence of vertices visited by the walk,

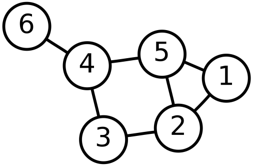
$$X_0, X_1, X_2, \ldots$$

is a **Markov chain** with state space V and transition matrix

$$M = \left(\frac{\epsilon_{uv}}{\deg u}\right)_{u,v \in V}$$

where $\epsilon_{uv} = 1$ if u, v are connected and 0 otherwise.

Random walk: an example



$$M^T = \begin{pmatrix} 0 & 1/3 & 0 & 0 & 1/3 & 0 \\ 1/2 & 0 & 1/2 & 0 & 1/3 & 0 \\ 0 & 1/3 & 0 & 1/3 & 0 & 0 \\ 0 & 0 & 1/2 & 0 & 1/3 & 1 \\ 1/2 & 1/3 & 0 & 1/3 & 0 & 0 \\ 0 & 0 & 0 & 1/3 & 0 & 0 \end{pmatrix}$$

Stationary distributions

By the Perron-Frobenius theorem, if G is a connected undirected acyclic graph there exists unique positive vector ν with $||\nu||_1 = 1$ such that

$$M^T \nu = \nu.$$

Moreover, for all $u \in V$,

$$\lim_{n \to \infty} (M^T)^n e_u = \nu,$$

where $e_u = (\delta_{uv})_{v \in V}$.

Stationary distributions

By the Perron-Frobenius theorem, if G is a connected undirected acyclic graph there exists unique positive vector ν with $||\nu||_1 = 1$ such that

$$M^T \nu = \nu.$$

Moreover, for all $u \in V$,

$$\lim_{n \to \infty} (M^T)^n e_u = \nu,$$

where $e_u = (\delta_{uv})_{v \in V}$.

The same is true if G is directed, as long as it is **strongly connected** and acyclic.

Undirected case

If $G = (V, E)$ is an undirected graph, then the random walk on G has a stationary distribution given by the vector ν, where for $u \in V$,

$$\nu_u = \frac{\deg u}{2|E|}.$$

It is trivial to check this is a stationary distribution, for we have the equality

$$\nu_u = \frac{\deg u}{2|E|} = \sum_{v \in N(u)} \frac{1}{\deg v} \frac{\deg v}{2|E|}.$$

Directed case (I)

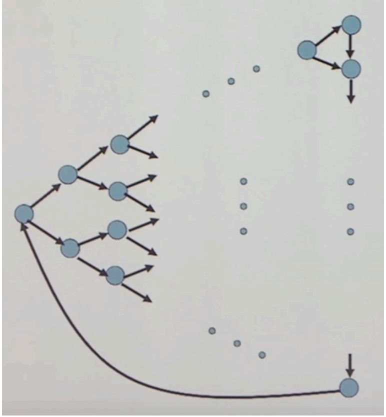
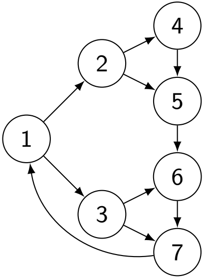


Figure: https://www.youtube.com/watch?v=w0HZX22i0mQ

Directed case (II)



$$M^T = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1/2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1/2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1/2 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1/2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1/2 & 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\nu = \left(\frac{2}{9}, \frac{1}{9}, \frac{1}{9}, \frac{1}{18}, \frac{1}{9}, \frac{1}{6}, \frac{2}{9} \right)^T$$

Expander graphs

Let G be a d-regular connected undirected graph. Then its adjacency matrix is symmetric, and its n (real) eigenvalues satisfy

$$d = \lambda_1 > \lambda_2 \geq \cdots \geq \lambda_n \geq -d.$$

G is non-bipartite $\iff \lambda_n > -d$.

Definition

We say G is an ϵ-expander if

$$\max(|\lambda_2|, |\lambda_n|) \leq (1-\epsilon)d.$$

$\implies$ every regular, undirected, connected, non-bipartite graph is an ϵ-expander for some $\epsilon > 0$.
(conversely, a regular undirected graph is an ϵ-expander for $\epsilon > 0 \iff$ it is connected and non-bipartite)

Mixing rate

The stationary distribution for a regular undirected graph is

$$\mathbf{u} = (1, \dots, 1)^T / n.$$

Let G be an ϵ-expander, set $\alpha = 1 - \epsilon$. Let A be the adjacency matrix of G, and let $\hat{A} := \frac{1}{d} A$ be the random walk matrix.

Theorem

For any distribution vector $\mathbf{p}$ and any positive integer k,

$$||\hat{A}^k \mathbf{p} - \mathbf{u}||_1 \leq \sqrt{n} \cdot \alpha^k.$$

So the **spectral gap** α tells us how fast the distribution converges to the stationary one.

Ramanujan property

Theorem

For every d-regular graph with n vertices, $\max(|\lambda_2|, |\lambda_n|) \geq 2\sqrt{d-1} - o_n(1)$, where $o_n(1) \to 0$ when d is fixed and $n \to \infty$.

Definition

We say a d-regular graph is **Ramanujan** if $\max(|\lambda_2|, |\lambda_n|) \leq 2\sqrt{d-1}$.

Elliptic curves and isogenies

We will consider elliptic curves E defined over finite fields $F = \mathbb{F}_q$, $q = p^r$, $p > 3$:

$$E\colon y^2 = x^3 + Ax + B.$$

Each elliptic curve E/F is both an abelian group and an algebraic curve.

Isogenies

An **isogeny** between E and E' is a nonconstant rational map $\phi\colon E \to E'$ that induces a group homomorphism $\phi\colon E(\bar{F}) \to E'(\bar{F})$.

- Isogenies have a **degree** $\deg \phi$, and if $p \nmid \deg \phi$ then $\# \ker \phi = \deg \phi$.
- Any isogeny $\phi\colon E \to E'$ has a **dual** $\hat{\phi}\colon E' \to E$ such that

$$\hat{\phi} \circ \phi = \phi \circ \hat{\phi} = [\deg \phi].$$

Quotient isogenies

Theorem

If $P \in E$ is a point of order n, there exists a curve E' and an isogeny $\phi \colon E \to E'$ such that $\ker \phi = \langle P \rangle$. We say $E' = E/\langle P \rangle$.

Number of torsion points

For a prime $\ell \neq p$, any curve $E/\bar{\mathbb{F}}_q$ has $\ell + 1$ points of order ℓ.
We say E is a **supersingular curve** if $E[p] = 0$, and an **ordinary curve** otherwise.

For $p \equiv 1 \mod 12$, the **supersingular ℓ-isogeny graph** is an $(\ell + 1)$-regular undirected graph with $\frac{p-1}{12}$ vertices, and it is **Ramanujan**.

Digression: automorphism groups

In general, any curve E: $y^2 = f(x)$ has an involution

$$(x, y) \overset{-1}{\mapsto} (x, -y).$$

$E_2 : y^2 = x^3 + x$

$\mathrm{Aut}(E_2) \cong \mathbb{Z}/4\mathbb{Z}$, generated by $(x, y) \mapsto (-x, iy)$.

$E_3 : y^2 = x^3 + 1$

$\mathrm{Aut}(E_3) \cong \mathbb{Z}/6\mathbb{Z}$, generated by $(x, y) \mapsto (\omega^2 x, -y)$, where ω is a primitive third root of unity.

Reduced automorphism group

$$RA(E) := \mathrm{Aut}(E)/\langle \pm 1 \rangle.$$

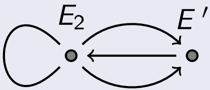
Automorphisms and isogenies

- If $\phi\colon E \to E'$ is an isogeny and $\alpha \in \mathrm{Aut}(E)$, then $\phi \circ \alpha$ is also an isogeny, and $\alpha(\ker(\phi \circ \alpha)) = \ker \phi$.
- If $P \in E$ has finite order, then $E/\langle P\rangle \cong E/\langle \alpha(P)\rangle$. This means that if $\alpha(P) \notin \langle P\rangle$, two different isogenies have the same codomain!
- But $[\pm 1](P) = \pm P \in \langle P\rangle$. So this phenomenon only happens when $RA(E)$ is not trivial.

The case $p \not\equiv 1 \mod 12$

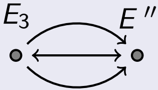
$p \equiv 3 \mod 4$ ($p \equiv 7, 11 \mod 12$)

In this case, $E_2 \colon y^2 = x^3 + x$ is supersingular.



$p \equiv 2 \mod 3$ ($p \equiv 5, 11 \mod 12$)

In this case, $E_3 \colon y^2 = x^3 + 1$ is supersingular.



Hence if $p \not\equiv 1 \mod 12$ the supersingular isogeny graph is **directed**!

The stationary distribution

The "non-undirectedness" is small enough that we can give a closed formula for the stationary distribution:

$$\tilde{\nu}_E = \begin{cases} 1, \text{ if } \operatorname{Aut}(E) = \{\pm 1\}, \\ \frac{1}{2}, \text{ if } \operatorname{Aut}(E) \cong \mathbb{Z}/4\mathbb{Z}, \\ \frac{1}{3}, \text{ if } \operatorname{Aut}(E) \cong \mathbb{Z}/6\mathbb{Z}, \end{cases}$$

and $\nu = \tilde{\nu}/||\tilde{\nu}||_1$. Notice that $\tilde{\nu}_E = \frac{1}{\#RA(E)}$.

When $p = 47$, the supersingular 2-isogeny graph has transition matrix

$$T_2 = \frac{1}{3}\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 3 & 0 & 2 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix} \text{ and } \tilde{\nu} = (1/3, 1, 1/2, 1, 1)^T.$$

Hyperelliptic curves

Let $f(x)$ be a polynomial of degree 5 or 6 with simple roots. We define a **hyperelliptic curve** of genus 2 as

$$\mathcal{C}\colon y^2 = f(x).$$

If f has degree 6, there are 15 possible factorizations of f as the product of three polynomials

$$f(x) = g_1(x)g_2(x)g_3(x)$$

each having degree 2. To each such factorization we associate a **Richelot isogeny**, which either gives us another hyperelliptic genus 2 curve $\mathcal{C}'\colon y^2 = g(x)$, or a product of elliptic curves $E \times E'$.

Richelot isogenies

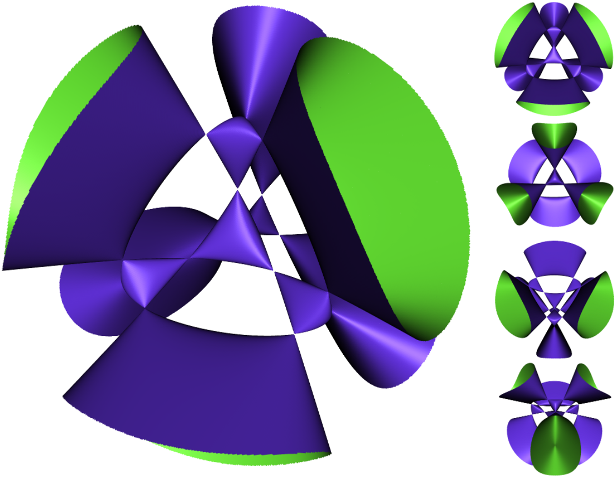
If $\det(g_1, g_2, g_3) \neq 0$, the Richelot isogeny actually gives us a rational map

$$\mathcal{C} \xrightarrow{\phi} \mathcal{C}'$$

which induces a map between the Picard groups (and thus between jacobians)

$$\mathrm{Pic}^0(\mathcal{C}) \xrightarrow{\phi_*} \mathrm{Pic}^0(\mathcal{C}')$$

with $\ker(\phi_*) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.
For each Richelot isogeny $\phi\colon \mathcal{C} \to \mathcal{C}'$, we have a dual $\psi\colon \mathcal{C}' \to \mathcal{C}$, and $(\psi_* \circ \phi_*) = [2]$.



The Picard group $\mathrm{Pic}^0(\mathcal{C})$ is isomorphic to the abelian surface $\mathrm{Jac}(\mathcal{C})$. The picture shows a Kummer surface, which represents the quotient $\mathrm{Jac}(\mathcal{C})/\langle \pm 1 \rangle$.

Genus 2 graphs

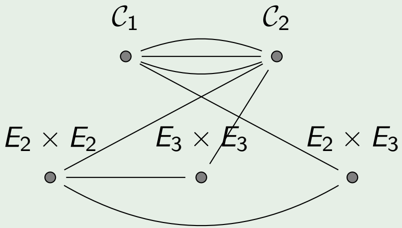
In practice, this gives us **genus 2 graphs**, where most vertices are (jacobians of isomorphism classes of) genus 2 hyperelliptic curves, and some vertices are products of elliptic curves.
We say a curve is **superspecial** if its connected component in the graph contains a product of supersingular elliptic curves.

Notation

- $\mathcal{G}_p$ is the superspecial genus two graph.
- $\mathcal{J}_p$ is the subgraph of the jacobians.
- $\mathcal{E}_p$ is the subgraph of the elliptic products.

An example

$p = 11$



$$\begin{cases} \mathcal{C}_1 \colon y^2 = (x^3-1)(x^3-3) \\ \mathcal{C}_2 \colon y^2 = x^6 - 1 \\ E_1 \colon y^2 = x^3 + x \\ E_2 \colon y^2 = x^3 + 1 \end{cases}$$

$$\begin{pmatrix} 3 & 4 & 0 & 1 & 0 \\ 9 & 3 & 3 & 3 & 0 \\ 0 & 4 & 6 & 0 & 3 \\ 3 & 4 & 0 & 3 & 4 \\ 0 & 0 & 6 & 8 & 8 \end{pmatrix}$$

We have $\max(|\lambda_2|, |\lambda_n|) = 7 + \sqrt{3} \approx 8.73$, but $2\sqrt{d-1} = 2\sqrt{14} =\approx 7.48$. Hence $\mathcal{G}_{11}$ is not Ramanujan. $\mathcal{G}_p$ is not Ramanujan *at least* until $p = 653$, and $\max(|\lambda_2|, |\lambda_n|) > 11$ for $p > 40$.

Reduced automorphism groups

$RA(C)$	Model	Number of curves over $\mathbb{F}_{p^2}$
0	$y^2 = f(x)$	$\sim p^3/2880$
$\mathbb{Z}/2\mathbb{Z}$	$y^2 = (x^2-1)(x^2-a^2)(x^2-b^2)$	$\sim p^2/48$
S_3	$y^2 = (x^3-1)(x^3-a^3)$	$\sim p/6$
V_4	$y^2 = (x^2-1)(x^2-u^2)(x^2-1/u^2)$	$\sim p/8$
D_{12}	$y^2 = x^6 - 1$	$\{1-(-3/p)\}/2$
S_4	$y^2 = x(x^4-1)$	$\{1-(-2/p)\}/2$
$\mathbb{Z}/5\mathbb{Z}$	$y^2 = x^5 - 1$	1 if $p \equiv 4 \mod 5$, 0 othw.

Automorphisms and Richelot isogenies

$RA(\mathcal{C})$	$\#(\mathcal{C} \to \mathcal{C}')$	$\#(\mathcal{C} \to E \times E')$
0	1,1,1,1,1,1,1,1,1,1,1,1,1,1,1	-
$\mathbb{Z}/2\mathbb{Z}$	1,1,1,1,1,1,2,2,2,2	1
S_3	1,1,1,3,3,3	3
V_4	1,2,2,2,2,4	1,1
D_{12}	2,3,6	1,3
S_4	1,4,4	6
$\mathbb{Z}/5\mathbb{Z}$	5,5,5	-

Stationary distributions (I)

Conjecture

The stationary distribution for the random walk restricted to jacobians is

$$\tilde{\nu}_{\mathcal{C}} = \begin{cases} 15, & \text{if } RA(\mathcal{C}) = 0, \\ 7, & \text{if } RA(\mathcal{C}) = \mathbb{Z}/2\mathbb{Z}, \\ 2, & \text{if } RA(\mathcal{C}) = S_3, \\ \frac{13}{4}, & \text{if } RA(\mathcal{C}) = (\mathbb{Z}/2\mathbb{Z})^2, \\ \frac{11}{12}, & \text{if } RA(\mathcal{C}) = D_{12}, \\ \frac{3}{8}, & \text{if } RA(\mathcal{C}) = S_4, \\ 3, & \text{if } RA(\mathcal{C}) = \mathbb{Z}/5\mathbb{Z}, \\ 0, & \text{otherwise.} \end{cases}$$

Questions

- For $G \in \{\mathcal{G}_p, \mathcal{J}_p, \mathcal{E}_p\}$, is the stationary ditribution for the random walk in G given by $\tilde{\nu}_i = \frac{\deg_G(v_i)}{\#RA(v_i)}$?
- Is $\mathcal{J}_p$ connected? What is its diameter?
- What is the mixing rate of these random walks?

Some references

- L. Lovász. *Random Walks on Graphs: A Survey*.
- T. Tao. *Basic theory of expander graphs*.
- S. Hoory, N. Linial, A. Wigderson. *Expander graphs and their applications*.
- D. Kohel. *Endomorphism rings of elliptic curves over finite fields*.
- C. Costello, B. Smith. *The supersingular isogeny problem in genus 2 and beyond*.
- T. Katsura, K. Takashima. *Counting superspecial Richelot isogenies and its cryptographic application*.
- B. Jordan, Y. Zaytman. *Isogeny graphs of superspecial abelian varieties and generalized Brandt matrices*.