Random walks in genus 2 isogeny graphs

Enric Florit [1] Ben Smith [2]

[1] Inria, Universitat de Barcelona

[2] Inria, École Polytechnique

ANTS XIV Rump Session – July 2020

Context

- Consider the graph $\mathcal{G}_p$ of **superspecial** PPAS in characteristic p, connected by $(2, 2)$-isogenies, a.k.a. Richelot isogenies (Castryck-Decru-Smith).

Context

- Consider the graph $\mathcal{G}_p$ of **superspecial** PPAS in characteristic p, connected by $(2,2)$-isogenies, a.k.a. Richelot isogenies (Castryck-Decru-Smith).
- $\mathcal{G}_p$ is a genus 2 analogue of the supersingular 2-isogeny graph.

Context

- Consider the graph $\mathcal{G}_p$ of **superspecial** PPAS in characteristic p, connected by $(2,2)$-isogenies, a.k.a. Richelot isogenies (Castryck-Decru-Smith).
- $\mathcal{G}_p$ is a genus 2 analogue of the supersingular 2-isogeny graph.
- Jordan-Zaytman: the graph is connected, and **not Ramanujan** (at least for $p = 11$).

Context

- Consider the graph $\mathcal{G}_p$ of **superspecial** PPAS in characteristic p, connected by $(2,2)$-isogenies, a.k.a. Richelot isogenies (Castryck-Decru-Smith).
- $\mathcal{G}_p$ is a genus 2 analogue of the supersingular 2-isogeny graph.
- Jordan-Zaytman: the graph is connected, and **not Ramanujan** (at least for $p = 11$).
- The Ramanujan property is related to the random walk on the graph: we want to study the **stationary distribution** and **mixing rate** of this walk. In expander (and Ramanujan) graphs, this distribution is uniform!

Reduced automorphism groups

Katsura-Takashima (monday) showed that we have to consider reduced automorphisms to see which and how many isogenies have the same domain and codomain.

Reduced automorphism groups

Katsura-Takashima (monday) showed that we have to consider reduced automorphisms to see which and how many isogenies have the same domain and codomain.
For a PPAV $\mathcal{A}$, we define the reduced automorphism group as

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

$\mathrm{RA}(\mathcal{J}(C))$	Number
0	$\sim p^3/2880$
C_2	$\sim p^2/48$
S_3	$\sim p/6$
V_4	$\sim p/8$
D_{12}	0 or 1
S_4	0 or 1
C_5	0 or 1

$\mathrm{RA}(\mathcal{E} \times \mathcal{E}')$	Number
C_2	$\sim p^2/144$
V_4	$\sim p/12$
C_4	$\sim p/12$
C_6	$\sim p/12$
$C_6 \times S_3$	0 or 1
$V_4 \rtimes C_4$	0 or 1
C_{12}	0 or 1

Isogeny multiplicities

Lemma

Let $K \subset \mathcal{A}[2]$ be a Lagrangian subgroup, and $\phi : \mathcal{A} \to \mathcal{A}' = \mathcal{A}/K$.
Let $K' \subset \mathcal{A}'[2]$ be the kernel of the dual isogeny $\phi^\dagger : \mathcal{A}' \to \mathcal{A}$.
Let S be the stabiliser of K in $\mathrm{RA}(\mathcal{A})$.

Isogeny multiplicities

Lemma

Let $K \subset \mathcal{A}[2]$ be a Lagrangian subgroup, and $\phi : \mathcal{A} \to \mathcal{A}' = \mathcal{A}/K$.
Let $K' \subset \mathcal{A}'[2]$ be the kernel of the dual isogeny $\phi^\dagger : \mathcal{A}' \to \mathcal{A}$.
Let S be the stabiliser of K in $\mathrm{RA}(\mathcal{A})$.

1. The isogeny ϕ induces a subgroup S' of $\mathrm{RA}(\mathcal{A}')$ isomorphic to S, and S' is the stabiliser of K' in $\mathrm{RA}(\mathcal{A}')$.

Isogeny multiplicities

Lemma

Let $K \subset \mathcal{A}[2]$ be a Lagrangian subgroup, and $\phi : \mathcal{A} \to \mathcal{A}' = \mathcal{A}/K$.
Let $K' \subset \mathcal{A}'[2]$ be the kernel of the dual isogeny $\phi^\dagger : \mathcal{A}' \to \mathcal{A}$.
Let S be the stabiliser of K in $\mathrm{RA}(\mathcal{A})$.

1. The isogeny ϕ induces a subgroup S' of $\mathrm{RA}(\mathcal{A}')$ isomorphic to S, and S' is the stabiliser of K' in $\mathrm{RA}(\mathcal{A}')$.
2. The $(2,2)$-isogeny graph has $\#\mathrm{RA}(\mathcal{A})/\#S$ edges from $[\mathcal{A}]$ to $[\mathcal{A}']$ and $\#\mathrm{RA}(\mathcal{A}')/\#S$ edges from $[\mathcal{A}']$ to $[\mathcal{A}]$.

Isogeny multiplicities

Lemma

Let $K \subset \mathcal{A}[2]$ be a Lagrangian subgroup, and $\phi : \mathcal{A} \to \mathcal{A}' = \mathcal{A}/K$.
Let $K' \subset \mathcal{A}'[2]$ be the kernel of the dual isogeny $\phi^\dagger : \mathcal{A}' \to \mathcal{A}$.
Let S be the stabiliser of K in $\mathrm{RA}(\mathcal{A})$.

1. The isogeny ϕ induces a subgroup S' of $\mathrm{RA}(\mathcal{A}')$ isomorphic to S, and S' is the stabiliser of K' in $\mathrm{RA}(\mathcal{A}')$.
2. The $(2,2)$-isogeny graph has $\#\mathrm{RA}(\mathcal{A})/\#S$ edges from $[\mathcal{A}]$ to $[\mathcal{A}']$ and $\#\mathrm{RA}(\mathcal{A}')/\#S$ edges from $[\mathcal{A}']$ to $[\mathcal{A}]$.

In particular we obtain the ratio

$$\frac{\#E([\mathcal{A}],[\mathcal{A}'])}{\#E([\mathcal{A}'],[\mathcal{A}])} = \frac{\#\mathrm{RA}(\mathcal{A})}{\#\mathrm{RA}(\mathcal{A}')}.$$

Stationary distribution

From the previous ratio principle we get stationary distributions for $\mathcal{G}_p$, and also the subgraphs $\mathcal{J}_p$ (Jacobians) and $\mathcal{E}_p$ (elliptic products).

Theorem

For $G \in \{\mathcal{G}_p, \mathcal{J}_p, \mathcal{E}_p\}$, the stationary ditribution for the random walk in G is $\phi = \tilde{\phi}/||\tilde{\phi}||_1$, where the vector $(\tilde{\phi}_{[\mathcal{A}]})_{[\mathcal{A}]\in V(G)}$ is given by

$$\tilde{\phi}_{[\mathcal{A}]} = \frac{\deg_G(\mathcal{A})}{\#RA(\mathcal{A})}.$$

Stationary distribution

From the previous ratio principle we get stationary distributions for $\mathcal{G}_p$, and also the subgraphs $\mathcal{J}_p$ (Jacobians) and $\mathcal{E}_p$ (elliptic products).

Theorem

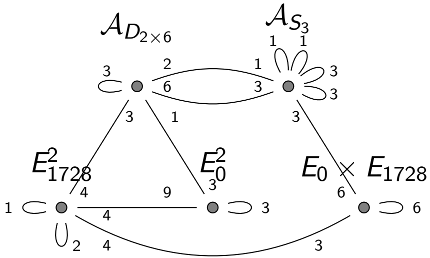
For $G \in \{\mathcal{G}_p, \mathcal{J}_p, \mathcal{E}_p\}$, the stationary ditribution for the random walk in G is $\phi = \tilde{\phi}/||\tilde{\phi}||_1$, where the vector $(\tilde{\phi}_{[\mathcal{A}]})_{[\mathcal{A}] \in V(G)}$ is given by

$$\tilde{\phi}_{[\mathcal{A}]} = \frac{\deg_G(\mathcal{A})}{\# RA(\mathcal{A})}.$$

Looks familiar? This is the same as in the supersingular elliptic curve case:

$$\tilde{\phi}_{[\mathcal{E}]} = \begin{cases} 1, & \text{if } \mathrm{RA}(\mathcal{E}) \cong 0, \\ \frac{1}{2}, & \text{if } \mathrm{RA}(\mathcal{E}) \cong C_2 \\ \frac{1}{3}, & \text{if } \mathrm{RA}(\mathcal{E}) \cong C_3. \end{cases}$$

An example: $p = 11$



$$\tilde{\phi}_{\mathcal{G}_p} = 15(\frac{1}{12}, \frac{1}{6}, \frac{1}{16}, \frac{1}{36}, \frac{1}{12}),$$

$$\tilde{\phi}_{\mathcal{J}_p} = (\frac{11}{12}, \frac{12}{6}),$$

$$\tilde{\phi}_{\mathcal{E}_p} = (\frac{12}{16}, \frac{12}{36}, \frac{9}{12}),$$

Second eigenvalues

- The second eigenvalue of the random walk matrix determines the mixing rate (this is why we care about Ramanujan-ness: $\max\{|\lambda_2|, |\lambda_n|\} \leq 2\sqrt{d-1}$).
- $\mathcal{G}_p$ is not Ramanujan *at least* until $p = 653$, and $\max(|\lambda_2|, |\lambda_n|) > 11$ for $p > 40$.
- $\mathcal{J}_p$: for $40 < p \leq 653$, $\max(|\lambda_2|, |\lambda_n|) > 11$.

Questions

- Can we give upper bounds on $|\lambda_2|, |\lambda_n|$?
- Can we prove "non-Ramanujan" in general?

Isogenies in dimension 1

Isogenies in dimension 1+ε

Thank you!

*Meme by Lorenz Panny