RIMS Kôkyûroku Bessatsu
B90 (2022), 145–151

Proving connectedness of isogeny graphs with strong approximation

By

Yevgeny Zaytman[*]

Abstract

We report on joint work with Bruce Jordan on isogeny graphs of principally polarized superspecial abelian varieties, especially the result that these graphs are connected, but not in general Ramanujan.

Acknowledgments

This work was supported by the Research Institute for Mathematical Sciences, an International Joint Usage/Research Center located in Kyoto University.

§ 1. Introduction

We will use the notation and results of Bruce Jordan's paper [2] in this volume.

Our main result is that all the isogeny graphs defined by Jordan are connected.

Theorem 1.1. *The big isogeny graph $Gr_g(\ell, p)$, the little isogeny graph $gr_g(\ell, p)$, and the enhanced isogeny graph $\widetilde{gr}_g(\ell, p)$ are connected.*

We've also computed some examples.

Theorem 1.2.

1. *The regular graphs $Gr_2(2, 5)$, $Gr_2(2, 7)$, $Gr_2(3, 7)$, and $Gr_3(2, 3)$ are Ramanujan.*
2. *The regular graphs*
   - $Gr_2(2, p)$ *for* $7 < p \leq 311$,

Received December 24, 2020. Revised May 8, 2021.

[*]Center for Communications Research, 805 Bunn Drive, Princeton, NJ 08540-1966, USA
e-mail: ykzaytm@idaccr.org

© 2022 Research Institute for Mathematical Sciences, Kyoto University. All rights reserved.

- $Gr_2(3,5)$ *and* $Gr_2(3,p)$ *for* $7 < p \leq 257$*,*
- $Gr_2(5,p)$ *for* $3 < p \leq 173$*,*
- $Gr_3(2,p)$ *for* $3 < p \leq 41$*, and*
- $Gr_3(3,p)$ *for* $2 < p \leq 23$*.*

are **not** *Ramanujan.*

§ 2. Preliminaries

§ 2.1. Adèles and Notation

Let $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$ be the profinite completion of $\mathbb{Z}$ and $\widehat{\mathbb{Q}} = \widehat{\mathbb{Z}} \otimes \mathbb{Q}$.

Definition 2.1. The *ring of adèles* is the restricted product $\mathbb{A} = \prod'_v \mathbb{Q}_v$, where the product is taken over all places v of $\mathbb{Q}$ with $\mathbb{Q}_\infty = \mathbf{R}$. By *restricted* we mean that the value must be in $\mathbb{Z}_v$ for all but finitely many v's. Notice that $\mathbb{A} \cong \mathbf{R} \times \widehat{\mathbb{Q}}$.

Suppose G is an algebraic group over $\mathbb{Q}$ and S is a finite set of places of $\mathbb{Q}$. We will set $G_{\mathbb{Q}_v} = G(\mathbb{Q}_v)$. Let the *adéle group* of G be $G_{\mathbb{A}} = \prod'_v G_{\mathbb{Q}_v}$.

Set $G_S \subset G_{\mathbb{A}}$ to be the S-component $\prod_{v \in S} G_{\mathbb{Q}_v} \subset G_{\mathbb{A}}$ and $G_{\mathbb{Q}} \subset G_{\mathbb{A}}$ to be the $\mathbb{Q}$-rational points of G.

§ 2.2. The strong approximation theorem

Let $S \ni \infty$ be a finite set of places of $\mathbb{Q}$. Let G be a linear algebraic group over $\mathbb{Q}$.

Definition 2.2. The pair (G,S) has strong approximation if $G_S G_{\mathbb{Q}}$ is dense in $G_{\mathbb{A}}$. A connected noncommutative algebraic group H is (*absolutely*) *simple* if it has no proper positive-dimensional normal subgroups.

We now give a statement of Strong Approximation sufficient for our purposes:

Theorem 2.3 (Kneser [3]). *Let G be a simply connected and absolutely simple linear algebraic group over $\mathbb{Q}$. Suppose G_S is not compact. Then (G,S) has strong approximation.*

§ 3. Application to the elliptic case $g = 1$

To illustrate the use of strong approximation in showing that isogeny graphs are connected, we will show that for supersingular elliptic curves $gr_1(\ell,p)$, $Gr_1(\ell,p)$, and $\widetilde{gr}_1(\ell,p)$ are connected (with $gr_1(\ell,p)$ and $Gr_1(\ell,p)$ not bipartite).

We need a lemma on quaternion algebras, with (reduced) norm Nm of elements and ideals in a quaternion algebra $\mathbb{H}$ as defined in [2, Sect. 2] and [2, Sect. 3], respectively.

Lemma 3.1. *Let $\mathbb{H}$ be an arbitrary definite rational quaternion algebra with maximal order $\mathcal{O}_{\mathbb{H}}$ over $\mathbb{Z}$, let I be a fractional right $\mathcal{O}_{\mathbb{H}}$-ideal of norm* 1, *and let ℓ be a prime unramified in $\mathbb{H}$. Then there exists an element in $I \otimes \mathbb{Z}[1/\ell]$ of norm* 1.

Proof. We will use the group $G = \{\beta \in \mathbb{H}^\times \,|\, \mathrm{Nm}(\beta) = 1\}$. Topologically G is the 3-sphere, which is simply connected. And G is the compact real form of SL_2, so it is simple.

Note that $\mathbb{H}^\times$ itself doesn't satisfy the hypotheses of Strong Approximation: it is not simple because $\mathbf{R}^\times \subset \mathbb{H}^\times$ is normal.

We will use $S = \{\ell, \infty\}$. Note that $G_{\mathbb{Q}_\ell} \cong \mathrm{SL}_2(\mathbb{Q}_\ell)$ is not compact. Hence, by Theorem 2.3 (G, S) has strong approximation.

Let $U = \{x \in G_{\mathbb{A}} \mid x_q \in (I \otimes \mathbb{Z}_q) \cap G_{\mathbb{Q}_q}$ for finite primes $q \neq \ell\}$.

Since every right ideal in a quaternion algebra is locally principal, there exist z_q such that $I \otimes \mathbb{Z}_q = z_q \mathbb{Z}_q$. Since $\mathrm{Nm}(I) = 1$, we have $z_q \in G_{\mathbb{Q}_q}$.

Notice that $U \subset G_{\mathbb{A}}$ is an open subset which is nonempty since $(z_q, x_p)_{q \notin S,\, p \in S} \in U$, x_p arbitrary.

Hence there exists an element of $G_S G_{\mathbb{Q}}$ in U; i.e., there exists some

$$\beta \in \bigcap_{q \neq \ell} (I \otimes \mathbb{Z}_q) \cap G = (I \otimes \mathbb{Z}[1/\ell]) \cap G.$$

□

Suppose $E/\overline{\mathbb{F}}_p$ and $E'/\overline{\mathbb{F}}_p$ are supersingular elliptic curves with $\mathcal{O} = \mathcal{O}_E = \mathrm{End}(E)$ and $\mathcal{O}' = \mathcal{O}_{E'} = \mathrm{End}(E')$ maximal orders in $\mathbb{H}_p$. Then $\mathrm{Hom}(E, E')$ is a module with left order $\mathcal{O}'$ and right order $\mathcal{O}$.

We will also use the following lemma:

Lemma 3.2. *If $\psi \in \mathrm{Hom}(E', E)$ with degree $N \neq 0$, then the right ideal $\mathcal{O}$-ideal $I = \{\psi \circ \phi | \phi \in \mathrm{Hom}(E, E')\}$ has reduced norm N.*

Proof. We will begin with the case when ϕ is separable. Then we have

$$I = \{\alpha \in \mathrm{End}(E) = \mathcal{O} \mid \widehat{\alpha}(\ker \phi) = 0\}.$$

Thus for each prime power $\ell^k \| N$, considering the condition locally at $\mathcal{O} \otimes \mathbb{Z}_\ell$ gives us a condition of index ℓ^{2k}. Combining these together we see that I has index N^2 in $\mathcal{O}$ and hence has reduced norm N.

Now suppose ϕ is inseparable. Let ϕ' be a separable map from E' to E of degree N'. Let $\beta = \phi \circ \widehat{\phi}'$. Let

$$I' = \{\phi' \circ \psi \mid \psi \in \mathrm{Hom}(E, E')\} \subseteq \mathcal{O}.$$

Then by the above case $\mathrm{Nm}(I') = N'$. Also $I = \frac{\beta}{N'} I'$ and taking norms of both sides we get that $\mathrm{Nm}(I) = N$. □

We are now ready to prove connectedness for supersingular elliptic curves.

Theorem 3.3. *Let $\ell \neq p$ be prime.*

(a) *The big isogeny graph $Gr_1(\ell, p)$ and the little isogeny graph $gr_1(\ell, p)$ for supersingular elliptic curves are connected.*

(b) *The graphs $Gr_1(\ell, p)$ and $gr_1(\ell, p)$ are not bipartite, i.e., given any two supersingular elliptic curves E and E' in characteristic p, there exists an isogeny $\phi : E \to E'$ such that the degree of ϕ is an even power of ℓ.*

(c) *The enhanced isogeny graph $\widetilde{gr}_1(\ell, p)$ is connected.*

Proof. It clearly suffices to show that given any two supersingular elliptic curves E and E' in characteristic p, there exists an isogeny $\phi : E \to E'$ such that the degree of ϕ is an even power of ℓ.

By Tate's theorem E and E' are isogenous. Hence there exists an isogeny $\psi \in \mathrm{Hom}(E', E)$ with some degree $N \neq 0$. Consider the right ideal $I \subset \mathcal{O}_E$ defined by $I = \{\psi \circ \phi | \phi \in \mathrm{Hom}(E, E')\}$. Note that by Lemma 3.2, I has reduced norm N. Let $\alpha \in \mathbb{H}_p$ be an element of norm N; such an α exists by the Hasse-Minkowski theorem. Then the fractional right ideal $I_1 = \alpha^{-1} I$ has $\mathrm{Nm}(I') = 1$.

Now by Lemma 3.1, there exists an element $\beta \in I_1 \otimes \mathbb{Z}[1/\ell]$ of norm 1. Let ℓ^n be a sufficiently high power of ℓ so that $\ell^n \beta \in I_1$. Then $\alpha \ell^n \beta \in I$ and thus is equal to $\psi \circ \phi$ for some $\phi \in \mathrm{Hom}(E, E')$. Computing norms we see that $\deg(\psi \circ \phi) = N \deg(\phi) = \mathrm{Nm}(\alpha \ell^n \beta) = N \ell^{2n} 1$. So the degree of ϕ is ℓ^{2n}.

Now by [2, Theorem 4.5] the enhanced isogeny graph $\widetilde{gr}_1(\ell, p)$ is the double cover of the little isogeny graph $gr_1(\ell, p)$ which is connected and not bipartite. Hence, $\widetilde{gr}_1(\ell, p)$ is connected. □

§ 4. The higher genus case $g > 1$

We will make use of the following lemma, proved in our paper [1].

Lemma 4.1. *All positive-definite g-dimensional unimodular quaternion Hermitian forms over $\mathcal{O}_{\mathbb{H}} \otimes \mathbb{Z}_{(q)}$ are isomorphic.*

Specifically, for any prime q and any Hermitian $H \in \mathrm{Mat}_{g\times g}(\mathcal{O}_{\mathbb{H}} \otimes \mathbb{Z}_{(q)})$ which is positive definite of determinant 1, there is a matrix $M \in \mathrm{Mat}_{g\times g}(\mathcal{O}_{\mathbb{H}} \otimes \mathbb{Z}_{(q)})$ such that $H = M^\dagger M$.

Recall that $\mathbb{Z}_{(q)} = \{\frac{a}{b} \mid (b,q) = 1\}$.

We are now ready to show the main result.

Theorem 4.2. *Let $\ell \neq p$ be a prime and $g > 1$, $Gr_g(\ell, p)$, the big $(\ell)^g$-isogeny graph for superspecial principally polarized g-dimensional abelian varieties in characteristic p is connected and not bipartite.*

This follows from the Lemma 4.5 as well as the following two results from our paper [1].

Proposition 4.3. ([1, Proposition 31]) *Let $A = E^g$ with principal polarizations $\lambda = \lambda_H$, $\lambda' = \lambda_{H'}$ for $H, H' \in \mathrm{SL}_g(\mathcal{O})$ positive-definite Hermitian matrices using the notation of* [2, §2]. *Let $\psi : A \to A$ be an isogeny given by $M \in \mathrm{Mat}_{g\times g}(\mathcal{O})$ of degree ℓ^{gm}. Then $\psi^*\lambda' = \ell^m\lambda$ if and only if $M^\dagger H' M = \ell^m H$.*

Theorem 4.4. ([1, Theorem 34]) *Let $\mathscr{A} = (A, \lambda)$ and $\mathscr{A}' = (A', \lambda')$ with $[\mathscr{A}], [\mathscr{A}'] \in \mathrm{SP}_g(p)_0$ for $g > 1$ and let $\ell \neq p$ be a prime. Suppose $\psi : A' \to A$ is an isogeny such that $\psi^*(\lambda) = \ell^m\lambda'$ for $m \geq 1$. Then there exist principally polarized superspecial abelian varieties*

$$(A_1, \lambda_1) = \mathscr{A}_1 = \mathscr{A}' = (A, \lambda'),\ \mathscr{A}_2 = (A_2, \lambda_2), \ldots, \mathscr{A}_m = (A_m, \lambda_m),$$
$$(A_{m+1}, \lambda_{m+1}) = \mathscr{A}_{m+1} = \mathscr{A} = (A', \lambda)$$

with $(\ell)^g$-isogenies $\psi_i : A_i \to A_{i+1}$ such that $\psi_i^*(\lambda_{i+1}) = \ell\lambda_i$ for $1 \leq i \leq m$ and $\psi = \psi_m \circ \psi_{m-1} \circ \cdots \circ \psi_1$:

$$\psi : A = A_1 \xrightarrow{\psi_1} A_2 \xrightarrow{\psi_2} \cdots \xrightarrow{\psi_{m-1}} A_m \xrightarrow{\psi_m} A_{m+1} = A'.$$

Lemma 4.5. (cf. [4, Lemma 7.9]) *Let ℓ be a prime unramified in $\mathbb{H}$. Then given any two Hermitian matrices $H, H' \in \mathrm{Mat}_{g\times g}(\mathcal{O}_E)$, there exists a matrix $M \in \mathrm{Mat}_{g\times g}(\mathcal{O}_E)$ such that $M^\dagger H M = \ell^{2n} H'$ for some positive integer n.*

Proof. It clearly suffices to show this for $H' = I$. Let $M_0 \in \mathrm{Mat}_{g\times g}(\mathcal{O}_{\mathbb{H}} \otimes \mathbb{Q})$ satisfy $M_0^\dagger M_0 = H$, by Lemma 4.1 M_0 exists.

We are now ready to apply the strong approximation theorem 2.3. Let $G = \mathrm{U}_g(\mathbb{H}) = \{M \in \mathrm{Mat}_{g\times g}(\mathbb{H}) \mid M^\dagger M = I\}$. G is the compact real form of Sp_{2g}, so is simple.

As before, let $S = \{\ell, \infty\}$.

Let $U = \{M \in G_{\mathbb{A}} \mid (M_0^{-1}M)_q \in \mathrm{Mat}_{g\times g}(\mathcal{O}_{\mathbb{H}} \otimes \mathbb{Z}_q) \text{ for } q \neq \ell\}$.

By Lemma 4.1 there exist $N_q \in \mathrm{Mat}_{g\times g}(\mathcal{O}_{\mathbb{H}} \otimes \mathbb{Z}_{(q)})$ such that $H = N_q^\dagger N_q$. Then $M_0 N_q^{-1} \in \mathrm{U}_g(\mathcal{O}_{\mathbb{H}} \otimes \mathbb{Q}_q) = G_{\mathbb{Q}_q}$.

Again U is an open subset and nonempty since $(M_0 N_q^{-1}, M_p)_{q\notin S, p\in S} \in U$, for M_p arbitrary.

Hence by strong approximation, Theorem 2.3, there exists $M' \in \mathrm{Mat}_{g\times g}(\mathbb{H})$ such that $M'^\dagger M' = I$ and $M_0^{-1}M' \in \mathrm{Mat}_{g\times g}(\mathcal{O}_{\mathbb{H}}[1/\ell])$.

Let ℓ^n be a sufficiently high power of ℓ such that $\ell^n M_0^{-1}M' \in \mathrm{Mat}_{g\times g}(\mathcal{O}_{\mathbb{H}})$. Let $M = \ell^n M_0^{-1}M'$. Then $M^\dagger H M = M^\dagger M_0^\dagger M_0 M = \ell^{2n} M'^\dagger M' = \ell^{2n} I$. □

We have shown that big isogeny graph $Gr_g(\ell, p)$ is connected and not bipartite. That the little graph $gr_g(\ell, p)$ is also connected and not bipartite and that the extended graph $\widetilde{gr}_g(\ell, p)$ is connected follows as in the $g = 1$ case from this. In particular this proves Theorem 1.1.

§ 5. Examples: The Ramanujan property

We computed $Gr_g(\ell, p)$ for all primes $p \leq p_{\max}$ and $(g, \ell, p_{\max})$ one of $(2, 2, 311)$, $(2, 3, 257)$, $(2, 5, 173)$, $(3, 2, 41)$, $(3, 3, 23)$ to see whether it's Ramanujan.

The graph is trivially Ramanujan, due to having only one vertex, when $(g, p) = (2, 2)$, $(2, 3)$, $(3, 2)$ and ℓ arbitrary – the number of vertices only depends on (g, p) and not on ℓ.

Otherwise, the only Ramanujan examples we found are when (g, ℓ, p) is one of $(2, 2, 5)$, $(2, 2, 7)$, $(2, 3, 7)$, $(3, 2, 3)$. (All these graphs have two vertices, but not every two-vertex graph is Ramanujan.)

References

[1] Jordan, B. and Zaytman, Y., Isogeny graphs of superspecial abelian varieties and Brandt matrices, `arXiv:2005.09031v4`.

[2] Jordan, B., Isogeny graphs of superspecial abelian varieties, this volume.

[3] Kneser, M., Strong approximation, *Algebraic Groups and Discontinuous Subgroups* (*Proc. Sympos. Pure Math., Boulder, Colo., 1965*), Amer. Math. Soc., Providence, R.I, (1966): 187–196.

[4] Oort, F., A stratification of a moduli space of abelian varieties, *Moduli of abelian varieties (Texel Island, 1999)*, *Progr. Math.*, Birkhäuser, Basel, **195** (2001), 345–416.