Canad. J. Math. 2023, pp. 1–26
http://dx.doi.org/10.4153/S0008414X23000676

Isogeny graphs on superspecial abelian varieties: eigenvalues and connection to Bruhat–Tits buildings

Yusuke Aikawa, Ryokichi Tanaka, and Takuya Yamauchi

Abstract. We study for each fixed integer $g \geq 2$, for all primes ℓ and p with $\ell \neq p$, finite regular directed graphs associated with the set of equivalence classes of ℓ-marked principally polarized superspecial abelian varieties of dimension g in characteristic p, and show that the adjacency matrices have real eigenvalues with spectral gaps independent of p. This implies a rapid mixing property of natural random walks on the family of isogeny graphs beyond the elliptic curve case and suggests a potential construction of the Charles–Goren–Lauter-type cryptographic hash functions for abelian varieties. We give explicit lower bounds for the gaps in terms of the Kazhdan constant for the symplectic group when $g \geq 2$. As a byproduct, we also show that the finite regular directed graphs constructed by Jordan and Zaytman also has the same property.

1 Introduction

Isogeny graphs are finite graphs associated with elliptic curves, more generally, abelian varieties over finite fields. They have attracted attention not only in arithmetic geometry but also in cryptography since the objects can be used as a building block in a prospective secure encryption scheme. It is believed that finding a path between an arbitrary pair of points is highly intractable in those graphs whereas a relatively short random walk path ends up with a fairly randomized vertex. In this paper, we study a random walk, thus mainly concerning the latter, on the isogeny graphs based on principally polarized superspecial abelian varieties over $\overline{\mathbb{F}}_p$ of dimension g at least 2 formed by $(\ell)^g$-isogenies with $p \neq \ell$ for primes p and ℓ. This is one of natural generalizations beyond the supersingular elliptic curves, the case corresponding to dimension 1.

1.1 Main theorems

To go into further explanation, we need to fix some notation and the details are left to the relevant sections. Let p be a prime, and let g be a positive integer. Fix an

Received by the editors April 6, 2022; revised September 24, 2023; accepted October 16, 2023.
Published online on Cambridge Core October 20, 2023.
Y.A. is supported by JST, ACT-X Grant Number JPMJAX2001, Japan. R.T. is partially supported by JSPS Grant-in-Aid for Scientific Research JP20K03602 and JST, ACT-X Grant Number JPMJAX190J, Japan. T.Y. is partially supported by JSPS KAKENHI Grant Number (B) 19H01778.
AMS subject classification: **11F55, 11G10, 14G50, 51E24.**
Keywords: Isogeny graphs, cryptographic hash functions, superspecial abelian varieties, isogeny graphs, Bruhat–Tits buildings.

algebraically closed field $\overline{\mathbb{F}}_p$ of the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. We say an abelian variety over $\overline{\mathbb{F}}_p$ is *superspecial* if it is isomorphic, as an abelian variety, to a product of a supersingular elliptic curve over $\overline{\mathbb{F}}_p$. Let $SS_g(p)$ be the set of isomorphism classes of all principally polarized superspecial abelian varieties over $\overline{\mathbb{F}}_p$ which are of dimension g. We write $[(A, \mathcal{L})]$ in $SS_g(p)$ for such a class, where A is a superspecial abelian variety and $\mathcal{L}$ an endowed principal polarization (an ample line bundle with trivial Euler–Poincaré characteristic).

Fix a representative $(A_0, \mathcal{L}_0)$ in a class of $SS_g(p)$ and a prime $\ell \neq p$. For each $(A, \mathcal{L})$ in a class of $SS_g(p)$, there exists an isogeny $\phi_A : A_0 \longrightarrow A$ of ℓ-power degree such that $\mathrm{Ker}(\phi_A)$ is a maximal totally isotropic subspace of $A[\ell^n]$ for some $n \geq 0$ (cf. Theorem 2.6 in Section 2.5 or [JZ21, Theorem 34]). We call ϕ_A *an* ℓ*-marking* of $(A, \mathcal{L})$ from $(A_0, \mathcal{L}_0)$. If ϕ_A and ψ_A are ℓ-markings of $(A, \mathcal{L})$, then $\psi_A = f \circ \phi_A$ for some element f in

$$\Gamma(A_0)^\dagger := \{f \in (\mathrm{End}(A_0) \otimes_{\mathbb{Z}} \mathbb{Z}[1/\ell])^\times \mid f \circ f^\dagger = f^\dagger \circ f \in \mathbb{Z}[1/\ell]^\times \mathrm{id}_{A_0}\},$$

where † stands for the Rosati involution associated with $\mathcal{L}_0$ (see Proposition 2.3).

Consider the set of triples $(A, \mathcal{L}, \phi_A)$ where $[(A, \mathcal{L})]$ in $SS_g(p)$ and ϕ_A is an ℓ-marking of $(A, \mathcal{L})$. On this set, we define an equivalence relation by saying $(A, \mathcal{L}, \phi_A) \sim (A', \mathcal{L}', \phi'_A)$ if there exists an isomorphism $f : (A, \mathcal{L}) \longrightarrow (A', \mathcal{L}')$ such that $f \circ \phi_A$ is an ℓ-marking on $(A', \mathcal{L}')$. Let $SS_g(p, \ell, A_0, \mathcal{L}_0)$ be the associated set of equivalence classes.

We are now ready to define the (ℓ-marked) $(\ell)^g$-isogeny graph $\mathcal{G}_g^{SS}(\ell, p)$ for $SS_g(p, \ell, A_0, \mathcal{L}_0)$. Let C be a maximal totally isotropic subgroup (or a Lagrangian subspace in other words) of $A[\ell]$. Then the quotient $A_C = A/C$ yields an object, say $(A_C, \mathcal{L}_C)$ in a class in $SS_g(p)$ and the natural surjection $f_C : A \longrightarrow A_C$ is called an $(\ell)^g$-isogeny (see Proposition 2.1 and Definition 2.1). Any $(\ell)^g$-isogeny between two objects in $SS_g(p)$ arises in this way. We remark that the number of maximal totally isotropic subgroups $A[\ell]$ is $N_g(\ell) := \prod_{k=1}^{g} (\ell^k + 1)$ for each A. The (ℓ-marked) $(\ell)^g$-*isogeny graph* $\mathcal{G}_g^{SS}(\ell, p)$ is defined as a directed graph such that:

- the set of vertices $V(\mathcal{G}_g^{SS}(\ell, p))$ is $SS_g(p, \ell, A_0, \mathcal{L}_0)$ and
- the set of directed edges between two vertices v_1 and v_2 is the set of equivalence classes of $(\ell)^g$-isogenies between corresponding principally polarized superspecial abelian varieties commuting with marking isogenies representing v_1 and v_2. In other words, if v_1 and v_2 correspond to $[(A_1, \mathcal{L}_1, \phi_{A_1})]$ and $[(A_2, \mathcal{L}_2, \phi_{A_2})]$ with ℓ-markings $\phi_{A_1} : (A_0, \mathcal{L}_0) \longrightarrow (A_1, \mathcal{L}_1)$ and $\phi_{A_2} : (A_0, \mathcal{L}_0) \longrightarrow (A_2, \mathcal{L}_2)$ respectively, then an edge from v_1 to v_2 is an $(\ell)^g$-isogeny $f : (A_1, \mathcal{L}_1) \longrightarrow (A_2, \mathcal{L}_2)$.

Our graph is regular since it has $N_g(\ell)$-outgoing edges from each vertex, possibly loops and multiple edges from one to another. The associated random walk operator for $\mathcal{G}_g^{SS}(\ell, p)$ is self-adjoint with respect to a weighted inner product by the inverse of the order of the reduced automorphism group (see Section 5.2). We define the normalized Laplacian Δ on a regular directed multigraph $\mathcal{G}$ of degree d by $\Delta = 1 - (1/d)M$ for the adjacency matrix M of $\mathcal{G}$. Note that Δ has the simple smallest

https://doi.org/10.4153/S0008414X23000676 Published online by Cambridge University Press

eigenvalue 0 provided that the graph is strongly connected, i.e., there exists a directed edge path from any vertex to any other vertex. Our first main result is the following.

Theorem 1.1 *Let $g \geq 2$, and let ℓ be a prime. Then there exists $c_{g,\ell} > 0$ such that for all primes $p \neq \ell$, we have $\lambda_2(\mathcal{G}_g^{SS}(\ell, p)) \geq c_{g,\ell}$, where λ_2 is the second smallest eigenvalue of the normalized Laplacian.*

As for the constant in the claim, we may take

$$c_{g,\ell} = \frac{1}{4(g+2)} \left(\frac{\ell - 1}{2(\ell - 1) + 3\sqrt{2\ell(\ell + 1)}} \right)^2,$$

(Corollary 5.5 in Section 5.4). In the course of the proof of Theorem 1.1, we relate $\mathcal{G}_g^{SS}(\ell, p)$ to a finite quotient $\Gamma \backslash \mathcal{S}_g$ (see Section 3.3) of the special 1-complex $\mathcal{S}_g$ defined in terms of the Bruhat–Tits building for $PGSp_g(\mathbb{Q}_\ell)$ (see Theorem 2.6 and Section 4.4). We then move on $\mathcal{S}_g$ to prove the desired property by using Kazhdan's Property (T) of $PGSp_g(\mathbb{Q}_\ell)$ for $g \geq 2$.

In [JZ21], Jordan and Zaytman introduced a *big isogeny graph* $Gr_g(\ell, p)$ based on $SS_g(p)$. We will show in Sections 2 and 3 that there exist natural identifications

$$SS_g(p) \overset{\sim}{\longleftarrow} SS_g(p, \ell, A_0, \mathcal{L}_0) \overset{\sim}{\longrightarrow} \Gamma \backslash \mathcal{S}_g$$

which induce natural isomorphisms as graphs between three objects:

(1) $Gr_g(\ell, p)$,
(2) $\mathcal{G}_g^{SS}(\ell, p)$, and
(3) the regular directed graph defined by $\Gamma \backslash \mathcal{S}_g$.

As a consequence, the adjacency matrices of the above three graphs agree with each other. Therefore, the structure of Jordan–Zaytman's graph $Gr_g(\ell, p)$ is revealed by our main theorem.

Theorem 1.2 *Let p be a prime. For each fixed integer $g \geq 2$ and for each fixed prime $\ell \neq p$, the finite $N_g(\ell)$-regular directed multigraph $Gr_g(\ell, p)$ has the same property as in Theorem 1.1.*

This result implies the rapid mixing property of a lazy version of the walk (see [FS22, Theorem 4.9]).

In the case when $g = 1$, it has been shown that if $p \equiv 1 \bmod 12$, then $Gr_1(\ell, p)$ can be defined as a regular undirected graph and it is Ramanujan by Eichler's theorem via Jacquet–Langlands theory (see [Piz98]). His graphs are regular "undirected" graphs, while in general $Gr_1(\ell, p)$ is not necessarily undirected.

Jordan–Zaytman's graphs $Gr_g(\ell, p)$ are useful and fit into the computational implementations (cf. [CDS20, FS21, FS22, KT20]) as explained in the next subsection. However, it may be hard to directly obtain the uniform estimation of the eigenvalues of the normalized Laplacian. Our graphs do not, unfortunately, well behave in the computational aspects. However, there is a natural correspondence between $SS_g(p, \ell, A_0, \mathcal{L}_0)$ and $\mathcal{S}_g$ as explained. A point here is that these two objects have markings from a fixed object, while $SS_g(p)$ does not have it. However, fortunately, there is a natural correspondence between $SS_g(p)$ and $SS_g(p, \ell, A_0, \mathcal{L}_0)$. Then eventually, we can relate $SS_g(p)$ with $\mathcal{S}_g$ via the intermediate object $SS_g(p, \ell, A_0, \mathcal{L}_0)$.

It seems interesting to consider the moduli space of principal polarized superspecial abelian varieties with a nontrivial-level structure so that the reduced automorphism group of any object is trivial. This will be discussed somewhere else.

1.2 Motivation from isogeny-based cryptography

This study is motivated by construction of cryptographic hash functions from isogeny graphs. Charles, Lauter, and Goren constructed hash functions from random walks on isogeny graphs $Gr_1(\ell, p)$ of supersingular elliptic curves [CGL09]. Due to Pizer's work [Piz90, Piz98], the Ramanujan property of $Gr_1(\ell, p)$ for $p \equiv 1 \bmod 12$ guarantees efficient mixing processing of these functions (for most precise results, see [LP16]).

Castryck, Decru, and Smith generalized this construction to design an analogue with genus 2 [CDS20]. To investigate the properties of this function, the study of the big isogeny graphs $Gr_g(\ell, p)$ has progressed. For $g = 2$, the classification of possible automorphism groups arising from Jacobians and elliptic product was done by Ibukiyama, Katsura, and Oort [IKO86]. Based on these results, the combinatorial structure of the local neighborhood of each vertex of $Gr_2(2, p)$ is computed in [FS21, KT20]. Moreover, in [FS22], they also investigated behavior of random walks on the big isogeny graphs and gave numerical experiments of the mixing rate of $Gr_2(2, p)$.

However, we know little about expansion properties of these graphs so far. In this paper, good mixing property of the big isogeny graphs $Gr_g(\ell, p)$ is shown as a result of proving that the isogeny graphs $\mathcal{G}_g^{SS}(\ell, p)$ defined in this paper have good expansion property and they are equivalent to the big isogeny graphs $Gr_g(\ell, p)$. Therefore, random walks on the graphs $\mathcal{G}_g^{SS}(\ell, p)$ (and $Gr_g(\ell, p)$) tend to the natural stationary distribution rapidly. This gives an evidence that the big isogeny graphs $Gr_g(\ell, p)$ may be suitable for construction of cryptographic hash functions from superspecial abelian varieties. See Figure 1, the one of examples for the graph $Gr_g(\ell, p)$ computed in [CDS20, KT20].

1.3 Organization of this paper

In Section 2, we give two interpretations of $SS_g(p)$ according to works of Ibukiyama–Katsura–Oort–Serre and Jordan–Zaytman. The former is helpful to compute the cardinality of $SS_g(p)$, while the latter is helpful to make the compatibility of Hecke operators at ℓ transparent. As mentioned before, this is a crucial step to apply Property (T) (hence, Theorem 5.4) with our family $\{\mathcal{G}_g^{SS}(\ell, p)\}_{p \neq \ell}$. In Section 3, we discuss a comparison between the graph $\mathcal{G}_g^{SS}(\ell, p)$ and that of Jordan–Zaytman $Gr_g(\ell, p)$. In Section 4, we study Bruhat–Tits buildings for symplectic groups. Then, in Section 5, the main result is proved in terms of the terminology in the precedent sections.

1.4 Notations

Let n be a positive integer, and let I_n be the identity matrix of size n. Let GSp_n be the generalized symplectic group associated with $J_n = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$ with the similitude $\nu : GSp_n \longrightarrow GL_1$. Put $Sp_n := \mathrm{Ker}(\nu)$, which is called the symplectic group of rank n.

https://doi.org/10.4153/S0008414X23000676 Published online by Cambridge University Press

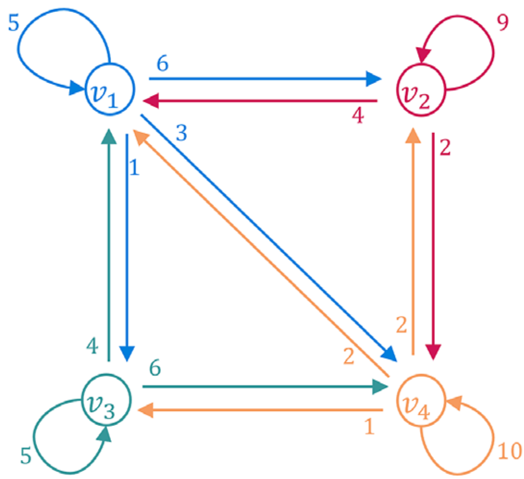

Figure 1: An illustration of $Gr_2(2, 13)$. The vertices v_1, v_2, and v_3 denote the Jacobians of some curves of genus 2. The vertex v_4 denotes the product of some supersingular elliptic curves. The number on the side of a directed edge denotes the multiplicity of each edge. For a more detailed illustration, see Section 7.1 of [KT20].

In the sections related to abelian varieties, we put $n = g$, while we keep n in Sections 4 and 5.

2 Superspecial abelian varieties

In this section, we refer [Mum70] for some general facts of abelian varieties. The purpose here is to understand Theorem 2.10 of [IKO86] in terms of the adelic language which is implicitly given there. Another formulation is also given in terms of ℓ-adic Tate modules (see also Theorem 46 of [JZ21] in more general setting). This explains the compatibility of Hecke operators on principally polarized superspecial abelian varieties and the special 1-complex of the Bruhat–Tits building in question. This result will be plugged into the main result in Section 5 to prove Theorem 1.1.

2.1 Superspecial abelian varieties

Let p be a prime number and $k = \overline{\mathbb{F}}_p$. Let A be an abelian variety over k of dimension $g > 0$, and we denote by $\widehat{A} = \mathrm{Pic}^0(A)$ the dual abelian variety (cf. Section 9 of [Mil86]).

The abelian variety A is said to be superspecial if A is isomorphic to $E^g = \overbrace{E \times \cdots \times E}^{g}$ for some supersingular elliptic curve E over k (see Sections 1.6 and 1.7 of [LO98] for another definition in terms of a-number). As explained in loc. cit., for any fixed supersingular elliptic curve E_0 over k, every superspecial abelian variety of dimension $g \geq 2$ is isomorphic to E_0^g. (Here, the assumption $g \geq 2$ is essential, and indeed, this

https://doi.org/10.4153/S0008414X23000676 Published online by Cambridge University Press

is not true for $g = 1$. See also Theorem 4.1 in Chapter V of [Sil09].) Throughout this section, we fix a supersingular elliptic curve E_0.

2.2 Principal polarizations

Let A be an abelian variety over $k = \overline{\mathbb{F}}_p$. A polarization is a class of the Néron–Severi group $\mathrm{NS}(A) := \mathrm{Pic}(A)/\mathrm{Pic}^0(A)$ which is represented by an ample line bundle on A. The definition of polarizations here is different from the usual one, but it is equivalent by Remark 13.2 of [Mil86] since $k = \overline{\mathbb{F}}_p$.

For each ample line bundle $\mathcal{L}$, we define an isogeny $\phi_{\mathcal{L}} : A \longrightarrow \widehat{A},\ x \mapsto t_x^*(\mathcal{L}) \otimes \mathcal{L}^{-1}$ where t_x stands for the translation by x and we denote by t_x^* its pullback.

Proposition 2.1 *Let $(A, \mathcal{L})$ be a principally polarized abelian variety over k. Let ℓ be a prime number different from p, and let C be a maximal totally isotropic subspace of $A[\ell^n]$ for $n \in \mathbb{Z}_{\geq 0}$ with respect to the Weil pairing associated with $\mathcal{L}$. Then, there exists an ample line bundle $\mathcal{L}_C$ on the quotient abelian variety $A_C := A/C$ which is unique up to isomorphism such that $(A_C, \mathcal{L}_{A_C})$ is a principally polarized abelian variety in characteristic p such that $f_C^*\mathcal{L}_{A_C} = \mathcal{L}^{\otimes \ell^n}$ where $f_C : A \longrightarrow A_C$ is the natural surjection.*

Proof Notice that $\mathcal{L}$ is symmetric. The claim follows from (11.25) Proposition of [EGM]. ∎

Definition 2.1 Let $(A_1, \mathcal{L}_1)$ and $(A_2, \mathcal{L}_2)$ be two principally polarized abelian varieties in characteristic p. Let ℓ be a prime different from p.

(1) An isogeny $f : A_1 \longrightarrow A_2$ is said to be an $(\ell)^g$-isogeny if $\mathrm{Ker}(f)$ is a maximal totally isotropic subspace of $A[\ell]$ with respect to the Weil pairing associated with $\mathcal{L}_1$, and $f^*\mathcal{L}_2 \simeq \mathcal{L}_1^{\otimes \ell}$.

(2) An isogeny $f : A_1 \longrightarrow A_2$ is said to be an ℓ-marking of $(A_2, \mathcal{L}_2)$ from $(A_1, \mathcal{L}_1)$ if $f^*\mathcal{L}_2 = \mathcal{L}_1^{\otimes \ell^m}$ for some integer $m \geq 0$.

Proposition 2.2 *Keep the notation in Definition 2.1. Let $f : A_1 \longrightarrow A_2$ be an ℓ-marking of $(A_2, \mathcal{L}_2)$ from $(A_1, \mathcal{L}_1)$, then there exists an ℓ-marking $\widetilde{f} : A_2 \longrightarrow A_1$ of $(A_1, \mathcal{L}_1)$ from $(A_2, \mathcal{L}_2)$ such that $f \circ \widetilde{f} = [\ell^m]_{A_2}$ and $\widetilde{f} \circ f = [\ell^m]_{A_1}$ for some integer $m \geq 0$.*

Proof By Theorem 34 of [JZ21], we may assume f is an $(\ell)^g$-isogeny. Put $C = \mathrm{Ker} f$. Then $(A_2, \mathcal{L}_2) = (A_{1,C}, \mathcal{L}_{A_{1,C}})$ where $A_{1,C} = A_1/C$. It is easy to see that $D := A_1[\ell]/C$ is a maximal totally isotropic subspace of $A_{1,C}[\ell]$ with respect to the Weil pairing associated with $\mathcal{L}_{A_{1,C}}$. Therefore, we have an $(\ell)^g$-isogeny $\widetilde{f} : A_2 \longrightarrow A_{1,C}/D$. However, $A_{1,C}/D = A/A[\ell] \simeq A$ and the later isomorphism induces the identification of $(A_{1,C}/D, \mathcal{L}_D)$ and $(A_1, \mathcal{L}_1)$ where $\mathcal{L}_D$ stands for a unique descend of $\mathcal{L}_{A_{1,C}}$ on $A_{1,C}/D$ (see Proposition 2.1). The proportion of f and $\widetilde{f}$ is symmetric, and hence we have the claim. ∎

We study the difference of two ℓ-markings. Let us keep the notation in Definition 2.1. By using the principal polarization $\mathcal{L}_1$, we define the Rosati-involution † on $\mathrm{End}(A_1)$ by

$$f^\dagger = \phi_{\mathcal{L}_1}^{-1} \circ \widehat{f} \circ \phi_{\mathcal{L}_1},\ f \in \mathrm{End}(A_1). \tag{2.2}$$

Notice that † is an anti-involution.

https://doi.org/10.4153/S0008414X23000676 Published online by Cambridge University Press

Proposition 2.3 *Let us still keep the notation in Definition 2.1. Let $f, h : A_1 \longrightarrow A_2$ be two ℓ-markings. Then there exists $\psi \in \mathrm{End}(A_1) \otimes \mathbb{Z}[1/\ell]$ such that $f \circ \psi = h$ and $\psi \circ \psi^\dagger = \psi^\dagger \circ \psi = [\ell^m]_{A_1}$ for some integer m.*

Proof For f, let $\widetilde{f} : A_2 \longrightarrow A_1$ be an $(\ell)^g$-isogeny in Proposition 2.2. Put $\psi_1 = \widetilde{f} \circ h \in \mathrm{End}(A_1)$. Then we have, by definition,

$$\psi_1 \circ \psi_1^\dagger = (\widetilde{f} \circ h) \circ (\phi_{\mathcal{L}_1}^{-1} \circ \widehat{h} \circ \widehat{\widetilde{f}} \circ \phi_{\mathcal{L}_1}).$$

By [JZ21, Theorem 34] and Definition 2.1 that $\widehat{\widetilde{f}} \circ \phi_{\mathcal{L}_1} \circ \widetilde{f} = \phi_{\mathcal{L}_2^{\otimes \ell^m}} = \ell^m \phi_{\mathcal{L}_2}$ and $\widehat{h} \circ \phi_{\mathcal{L}_2} \circ h = \phi_{\mathcal{L}_1^{\otimes \ell^{m'}}} = \ell^{m'} \phi_{\mathcal{L}_1}$ for some integers $m', m \geq 0$. This yields

$$\psi_1 \circ \psi_1^\dagger = \ell^m \widetilde{f} \circ \phi_{\mathcal{L}_2}^{-1} \circ \widehat{\widetilde{f}} \circ \phi_{\mathcal{L}_1} = \ell^{m+m'} \mathrm{id}_{A_1}.$$

Further, $f \circ \psi = (f \circ \widetilde{f}) \circ h = \ell^m h$. Therefore, we may put $\psi = \ell^{-m} \psi_1$ as desired. ∎

2.3 Class number of the principal genus for quaternion Hermitian lattices

In this subsection, we refer Section 3.2 of [Ibu20] for the facts and the notation. Let p be a prime number, and let n be a positive integer. Let B be the definite quaternion algebra ramified only at p and ∞. Let us fix a maximal order $\mathcal{O}$ of B.

For a commutative ring R, we extend the conjugation on $\mathcal{O} \subset B$ to $\mathcal{O} \otimes_{\mathbb{Z}} R$ by $\overline{x \otimes r} := \overline{x} \otimes r$ for each $x \in \mathcal{O}$ and $r \in R$. Further, for each $\gamma = (\gamma_{ij}) \in M_n(\mathcal{O} \otimes_{\mathbb{Z}} R)$ (the set of $n \times n$ matrices over $\mathcal{O} \otimes_{\mathbb{Z}} R$), we define $\overline{\gamma} := (\overline{\gamma}_{ij})$. We define the algebraic group G_n over $\mathbb{Z}$ which represents the following functor from the category of rings to the category of sets:

$$\underline{G}_n : (Rings) \longrightarrow (Sets),\ R \mapsto \underline{G}_n(R) := \{\gamma \in M_n(\mathcal{O} \otimes_{\mathbb{Z}} R) \mid \gamma \cdot {}^t\overline{\gamma} \\ = \nu(\gamma) I_n \text{ for some } \nu(\gamma) \in R^\times\},$$

where I_n stands for the identity matrix of size n. The similitude map $\nu : G_n \mapsto GL_1$ is defined by $\gamma \mapsto \nu(\gamma)$. Put $G_n^1 := \mathrm{Ker}(\nu)$ as an algebraic group. The group scheme G_n (resp. G_n^1) over $\mathbb{Z}$ is said to be the generalized unitary symplectic group (unitary symplectic group), and it is symbolically denoted by $G_n = GUSp_n$ (resp. $G_n^1 = USp_n$). It is easy to see that $G_n(\mathbb{R})$ is compact modulo center and $G_n^1(\mathbb{R})$ is, in fact, compact, since B is definite. By definition, G_n (resp. G_n^1) is an inner form of GSp_n (resp. Sp_n).

Let $\mathbb{A}_{\mathbb{Q}}$ be the ring of adeles of $\mathbb{Q}$, and let $\mathbb{A}_f$ be the finite part of $\mathbb{A}_{\mathbb{Q}}$. For an $\mathcal{O}$-lattice L of B^n and each rational prime p, put $K_p(L) := \{\gamma_p \in G_n(\mathbb{Q}_p) \mid (L \otimes_{\mathbb{Z}} \mathbb{Z}_p)\gamma_p = L \otimes_{\mathbb{Z}} \mathbb{Z}_p\}$ which is an open compact subgroup of $G_n(\mathbb{Q}_p)$. Then $K(L) := \prod_p K_p(L)$ makes up an open compact subgroup of $G_n(\mathbb{A}_f)$.

2.4 Ibukiyama–Katsura–Oort–Serre's result in terms of adelic language

Let us fix a prime p and put $k = \overline{\mathbb{F}}_p$. We denote by $SS_g(p)$ the set of all isomorphism classes of principally polarized abelian variety over k of dimension g. Henceforth, we assume $g \geq 2$. According to [IKO86], we describe $SS_g(p)$ in terms of adelic language. Let us first recall the main result in [IKO86].

https://doi.org/10.4153/S0008414X23000676 Published online by Cambridge University Press

Theorem 2.4 (Ibukiyama–Katsura–Oort–Serre's theorem) *There is a one-to-one correspondence between $SS_g(p)$ and $K(\mathcal{O}^g)\backslash G_g(\mathbb{A}_f)/G_g(\mathbb{Q})$.*

We denote by $Z_{G_g} \simeq GL_1$ the center of $G_g = GUSp_g$. Recall the open compact subgroup $K(\mathcal{O}^g) = \prod_p K_p(\mathcal{O}^g)$. For each prime $\ell \neq p$, put $K(\mathcal{O}^g)^{(\ell)} = \prod_{p \neq \ell} K_p(\mathcal{O}^g)$. Clearly, $K(\mathcal{O}^g) = K(\mathcal{O}^g)^{(\ell)} \times G_g(\mathbb{Z}_\ell)$. We identify $B_\ell = B \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ (resp. $\mathcal{O}_\ell = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$) with $M_2(\mathbb{Q}_\ell)$ (resp. $M_2(\mathbb{Z}_\ell)$). Under this identification, we have $G_g(R) = GSp_g(R)$ for $R = \mathbb{Z}_\ell$ or $\mathbb{Q}_\ell$ (cf. Lemma 4 of [Ghi04]). Therefore, for any subring M of $\mathbb{Q}_\ell$, $G_g(M)$ is naturally identified with a subgroup of $G_g(\mathbb{Q}_\ell) = GSp_g(\mathbb{Q}_\ell)$ under the inclusion $M \subset \mathbb{Q}_\ell$.

Proposition 2.5 *For each prime $\ell \neq p$, there is a one-to-one correspondence between $SS_g(p)$ and $G_g(\mathbb{Z}[1/\ell])\backslash GSp_g(\mathbb{Q}_\ell)/Z_{GSp_g}(\mathbb{Q}_\ell)GSp_g(\mathbb{Z}_\ell)$.*

Proof For any algebraic closed field F, $G_g^1(F) = USp_g(F) = Sp_g(F)$. Since Sp_g is simply connected as a group scheme over $\mathbb{Z}$, so is $G_g^1 = USp_g$. Let $\mathbb{A}_f^{(\ell)}$ be the finite adeles of $\mathbb{Q}$ outside ℓ. By the strong approximation theorem (cf. Theorem 7.12, p.427 in Section 7.4 of [PR94]) for G_g^1 with respect to $S = \{\infty, \ell\}$ and using the exact sequence $1 \longrightarrow G_g^1 \longrightarrow G_g \xrightarrow{\nu} GL_1 \longrightarrow 1$, we have a decomposition

$$G_g(\mathbb{A}_f) = G_g(\mathbb{A}_f^{(\ell)}) \times G_g(\mathbb{Q}_\ell) = G_g(\mathbb{Q})(K(\mathcal{O}^g)^{(\ell)} \times G_g(\mathbb{Q}_\ell)). \tag{2.3}$$

Combining Theorem 2.4 with (2.3), we have

$$\begin{aligned} SS_g(p) &\simeq K(\mathcal{O}^g)\backslash G_g(\mathbb{A}_f)/G_g(\mathbb{Q}) \\ &\simeq G_g(\mathbb{Q})\backslash G_g(\mathbb{A}_f)/K(\mathcal{O}^g) \\ &= G_g(\mathbb{Q})\backslash(G_g(\mathbb{Q})(K(\mathcal{O}^g)^{(\ell)} \times G_g(\mathbb{Q}_\ell)))/K(\mathcal{O}^g) \\ &= G_g(\mathbb{Z}[1/\ell])\backslash GSp_g(\mathbb{Q}_\ell)/GSp_g(\mathbb{Z}_\ell) \\ &= G_g(\mathbb{Z}[1/\ell])\backslash GSp_g(\mathbb{Q}_\ell)/Z_{GSp_g}(\mathbb{Q}_\ell)GSp_g(\mathbb{Z}_\ell). \end{aligned} \tag{2.4}$$

We complete the proof. ∎

2.5 Another formulation due to Jordan–Zaytman

Let $\ell \neq p$ be a prime. Both of $SS_g(p)$ and the Bruhat–Tits building $GSp_g(\mathbb{Q}_\ell)/Z_{GSp_g}(\mathbb{Q}_\ell)GSp_g(\mathbb{Z}_\ell)$ endowed with Hecke theory at ℓ. However, it is not transparent to see the compatibility of Hecke actions on both sides under the one-to-one correspondence (2.4). To overcome this, due to Jordan and Zaytman [JZ21], we use another formulation of $SS_g(p)$ and its connection to $SS_g(p, \ell, A_0, \mathcal{L}_0)$ by using ℓ-adic Tate modules.

Pick $(A, \mathcal{L})$ from a class in $SS_g(p)$. For a positive integer n, let $A[\ell^n] := \{P \in A(\overline{\mathbb{F}}_p) \mid \ell^n P = 0_A\} \simeq (\mathbb{Z}/\ell^n\mathbb{Z})^{\oplus 2g}$ and put $A[\ell^\infty] = \bigcup_{n \geq 1} A[\ell^n]$. We denote by $T_\ell(A)$ the ℓ-adic Tate module and by $V_\ell(A) := T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ the ℓ-adic rational Tate module (cf. Section 18 of Chapter IV of [Mum70]). Let us define the coefficient ring R_V to be $\mathbb{Z}/\ell^n\mathbb{Z}$ if $V = A[\ell^n]$, $\mathbb{Z}_\ell$ if $V = T_\ell(A)$, and $\mathbb{Q}_\ell$ if $V = V_\ell(A)$. The principal polarization $\phi_{\mathcal{L}} : A \xrightarrow{\sim} \widehat{A}$ yields $V \simeq V^* = \mathrm{Hom}_{R_V}(V, R_V)$, and it induces a non-degenerate alternating pairing $\langle *, * \rangle : V \times V \longrightarrow R_V$. Let C be a maximal isotropic subgroup of $A[\ell^n]$ for some $n \geq 1$. Consider the exact sequence

$$0 \longrightarrow T_\ell(A) \xrightarrow{\subset} V_\ell(A) \xrightarrow{\pi} V_\ell(A)/T_\ell(A) \simeq A[\ell^\infty] \longrightarrow 0.$$

Then, $T_C := \pi^{-1}(C)$ is a lattice of $V_\ell(A)$. The quotient $A_C := A/C$ is also a superspecial abelian variety and the line bundle $\mathcal{L}$ is uniquely descend to a principal polarization $\mathcal{L}_C$ on A_C by Corollary of Theorem 2 in Section 23 of Chapter IV of [Mum70] (see also Proposition 11.25 of [EGM] for the uniqueness). Therefore, $T_C \simeq T_\ell(A_C)$ has a symplectic $\mathbb{Z}_\ell$-basis $\{f_{C,i}\}_{i=1}^{2g} \subset \mathbb{Q}_\ell^{2g}$ which means the matrix $P_C := (f_{C,1}, \dots, f_{C,2g}) \in M_{2g}(\mathbb{Q}_\ell)$ belongs to $GSp_g(\mathbb{Q}_\ell)$. Another choice of a symplectic $\mathbb{Z}_\ell$-basis of T_C yields $P_C\gamma$ for some $\gamma \in GSp_g(\mathbb{Z}_\ell)$. For each $h \in \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}[1/\ell]$ which is invertible (hence h is an isogeny of degree a power of ℓ), we see easily that $P_{h(C)} = h^* P_C$ where h^* is the endomorphism of $V_\ell(A)$ induced from h. In fact, by the functorial property of the pairing (see page 228 of [Mum70]). We identify $G_g(\mathbb{Z}[1/\ell])$ with

$$\Gamma(A)^\dagger := \{f \in (\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}[1/\ell])^\times \mid f \circ f^\dagger = f^\dagger \circ f \in \mathbb{Z}[1/\ell]^\times \mathrm{id}_A\} \tag{2.5}$$

under the natural inclusion $(\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}[1/\ell])^\times \hookrightarrow \mathrm{Aut}((V_\ell(A), \langle *, * \rangle)) = GSp_g(\mathbb{Q}_\ell)$.

Fix $(A, \mathcal{L})$ in a class of $SS_g(p)$. We introduce the following sets which play an important role in the construction of the isogeny graphs:

$$\mathrm{Iso}_{\ell^\infty}(A, \mathcal{L}) := \{[(A_C, \mathcal{L}_C)] \in SS_g(p) \mid n \geq 1,\ C \subset A[\ell^n] : \text{a maximal isotropic subgroup}\} \tag{2.6}$$

and

$$SS_g(p, \ell, A, \mathcal{L}) := \{[(B, \mathcal{M}, \phi_B)] \mid [(B, \mathcal{M})] \in SS_g(p)\}, \tag{2.7}$$

where $\phi_B : A \longrightarrow B$ is an ℓ-marking and $[(B, \mathcal{M}, \phi_B)]$ stands for the equivalent class of $(B, \mathcal{M}, \phi_B)$. Here, such two objects $(A_1, \mathcal{L}_1, \phi_{A_1})$ and $(A_2, \mathcal{L}_2, \phi_{A_2})$ are said to be equivalent if there exists an isomorphism $f : (A_1, \mathcal{L}_1) \longrightarrow (A_2, \mathcal{L}_2)$ such that $f \circ \phi_{A_1}$ and ϕ_{A_2} differ by only an element in $\Gamma(A_1)^\dagger$. By definition, the natural map from $SS_g(p, \ell, A, \mathcal{L})$ to $\mathrm{Iso}_{\ell^\infty}(A, \mathcal{L})$ is surjective, while $\mathrm{Iso}_{\ell^\infty}(A)$ is included in $SS_g(p)$. With the above observation, we have obtained a map

$$\mathrm{Iso}_{\ell^\infty}(A, \mathcal{L}) \longrightarrow G_g(\mathbb{Z}[1/\ell]) \backslash GSp_g(\mathbb{Q}_\ell)/GSp_g(\mathbb{Z}_\ell),\ [(A_C, \mathcal{L}_C)] \mapsto G_g(\mathbb{Z}[1/\ell]) P_C GSp_g(\mathbb{Z}_\ell). \tag{2.8}$$

We then show a slightly modified version of Jordan–Zaytman's theorem, Theorem 46 of [JZ21] in conjunction with $SS_g(p, \ell, A, \mathcal{L})$.

Theorem 2.6 *Fix $(A, \mathcal{L})$ in a class of $SS_g(p)$. Keep the notation being as above. It holds that $\mathrm{Iso}_{\ell^\infty}(A, \mathcal{L}) = SS_g(p)$ and the map (2.8) induces a bijection*

$$\mathrm{Iso}_{\ell^\infty}(A, \mathcal{L}) \xrightarrow{\sim} G_g(\mathbb{Z}[1/\ell]) \backslash GSp_g(\mathbb{Q}_\ell)/GSp_g(\mathbb{Z}_\ell) = G_g(\mathbb{Z}[1/\ell]) \backslash GSp_g(\mathbb{Q}_\ell)/Z_{GSp_g}(\mathbb{Q}_\ell) GSp_g(\mathbb{Z}_\ell).$$

Further, the natural map $SS_g(p, \ell, A, \mathcal{L}) \longrightarrow \mathrm{Iso}_{\ell^\infty}(A, \mathcal{L})$ is also bijective.

Proof Surjectivity of (2.8) follows in reverse from the construction by using Corollary of Theorem 2 in Section 23 of Chapter IV of [Mum70] to guarantee the existence

https://doi.org/10.4153/S0008414X23000676 Published online by Cambridge University Press

of a principal polarization. By Proposition 2.5 and $\mathrm{Iso}_{\ell^\infty}(A,\mathcal{L}) \subset SS_g(p)$, we have

$$|SS_g(p)| = |G_g(\mathbb{Z}[1/\ell])\backslash GSp_g(\mathbb{Q}_\ell)/Z_{GSp_g}(\mathbb{Q}_\ell)GSp_g(\mathbb{Z}_\ell)| \le |\mathrm{Iso}_{\ell^\infty}(A,\mathcal{L})| \le |SS_g(p)|,$$

and it yields first two claims. With a natural surjection $SS_g(p,\ell,A,\mathcal{L}) \longrightarrow \mathrm{Iso}_{\ell^\infty}(A,\mathcal{L})$ and (2.8), we have a surjective map

$$SS_g(p,\ell,A,\mathcal{L}) \longrightarrow G_g(\mathbb{Z}[1/\ell])\backslash GSp_g(\mathbb{Q}_\ell)/Z_{GSp_g}(\mathbb{Q}_\ell)GSp_g(\mathbb{Z}_\ell).$$

However, by construction and the identification $(\mathrm{End}(A)\otimes_{\mathbb{Z}}\mathbb{Z}[1/\ell])^\times = G_g(\mathbb{Z}[1/\ell])$, two objects of $SS_g(p,\ell,A,\mathcal{L})$ which go to one element in the target differ by only ℓ-markings. Therefore, the above map is bijective. Hence, $SS_g(p,\ell,A,\mathcal{L}) \xrightarrow{\sim} \mathrm{Iso}_{\ell^\infty}(A,\mathcal{L}) = SS_g(p)$.

Note that the factor $Z_{GSp_g}(\mathbb{Q}_\ell) \simeq \mathbb{Q}_\ell^\times$ is intentionally inserted in front of $GSp_g(\mathbb{Z}_\ell)$ as explained in the proof of Proposition 2.5. ■

As a byproduct, we have the following.

Corollary 2.7 *Let ℓ be a prime different from p. Let $\mathcal{G}_g^{SS}(\ell,p)$ is the isogeny graph defined in Section 1. Then, $\mathcal{G}_g^{SS}(\ell,p)$ is a connected graph.*

Proof By the proof of Theorem 2.6, we have $SS_g(p,\ell,A,\mathcal{L}) \xrightarrow{\sim} \mathrm{Iso}_{\ell^\infty}(A,\mathcal{L}) = SS_g(p)$ for any fixed $(A,\mathcal{L})$ in a class of $SS_g(p)$. This means that any two classes are connected by isogenies of degree a power of ℓ and such an isogeny can be written as a composition of some $(\ell)^g$-isogenies by Theorem 34 of [JZ21]. This shows the claim. ■

2.6 The Hecke operator at ℓ

Finally, we discuss a relation of the map (2.8) with the Hecke operator at ℓ. We refer Section 3 in Chapter VII of [CF90] for general facts and Sections 16–19 of [Gee08] as a reader's friendly reference. For each prime ℓ different from p and a class $[(A,\mathcal{L},\phi_A)] \in SS_g(p,\ell,A_0,\mathcal{L}_0)$, we define the (geometric) Hecke correspondences $T(\ell)^{\mathrm{geo}}_{(A_0,\mathcal{L}_0)}$ at ℓ:

$$T(\ell)^{\mathrm{geo}}_{(A_0,\mathcal{L}_0)}([(A,\mathcal{L},\phi_A)]) := \sum_{\substack{C\subset A[\ell] \\ \text{maximal isotropic}}} [(A_C,\mathcal{L}_C,f_C\circ\phi_A)], \tag{2.9}$$

where $f_C : A \longrightarrow A_C$ is the natural projection. Similarly, we also define the (geometric) Hecke correspondences $T(\ell)^{\mathrm{geo}}$ at ℓ on $SS_g(p)$:

$$T(\ell)^{\mathrm{geo}}([(A,\mathcal{L})]) := \sum_{\substack{C\subset A[\ell] \\ \text{maximal isotropic}}} [(A_C,\mathcal{L}_C)]. \tag{2.10}$$

Recall $GSp_g(\mathbb{Q}_\ell) = GSp(\mathbb{Q}_\ell^{2g}, \langle *,*\rangle)$ where $\langle *,*\rangle$ is the standard symplectic pairing on $\mathbb{Q}_\ell^{2g}\times\mathbb{Q}_\ell^{2g}$. Put $V=\mathbb{Q}_\ell^{2g}$. As seen before, each element of $GSp_g(\mathbb{Q}_\ell)/GSp_g(\mathbb{Z}_\ell)$ can be regarded as a lattice L of V such that $\langle *,*\rangle_{L\times L}$ gives a $\mathbb{Z}_\ell$-integral symplectic structure on L. Using this interpretation, each element of $GSp_g(\mathbb{Q}_\ell)/Z_{GSp_g}(\mathbb{Q}_\ell)GSp_g(\mathbb{Z}_\ell)$ can be regard as a homothety class $[L]$ for such an L. For each L being as above, we define the Hecke correspondence on

https://doi.org/10.4153/S0008414X23000676 Published online by Cambridge University Press

$GSp_g(\mathbb{Q}_\ell)/GSp_g(\mathbb{Z}_\ell)$ at ℓ

$$T(\ell)([L]) := \sum_{\substack{L\subset L_1\subset \ell^{-1}L\\ L_1/L:\text{maximal isotropic}}} [L_1], \tag{2.11}$$

where L_1 runs over all lattice enjoying $L \subset L_1 \subset \ell^{-1}L$ as denoted and that L_1/L is a maximal isotropic subgroup of $\ell^{-1}L/L$ with respect to the symplectic pairing $\langle *, *\rangle_{\ell^{-1}L/L\times\ell^{-1}L/L}$. Clearly, the action of $G_g(\mathbb{Z}[1/\ell])$ (given by multiplication from the left) on lattices are equivariant under $T(\ell)$. Therefore, it also induces a correspondence on $G_g(\mathbb{Z}[1/\ell])\backslash GSp_g(\mathbb{Q}_\ell)/Z_{GSp_g}(\mathbb{Q}_\ell)GSp_g(\mathbb{Z}_\ell)$ and by abusing notation, we denote it by $T(\ell)$. For a set X, we write $\mathrm{Div}(X)_{\mathbb{Z}} := \bigoplus_{P\in X}\mathbb{Z}P$. The identification (2.8) with the bijection

$$SS_g(p,\ell,A_0,\mathcal{L}_0) \xrightarrow{\sim} SS_g(p),\ [(A,\mathcal{L},\phi_A)] \mapsto [(A,\mathcal{L})] \tag{2.12}$$

yields a bijection

$$SS_g(p,\ell,A_0,\mathcal{L}_0) \longrightarrow G_g(\mathbb{Z}[1/\ell])\backslash GSp_g(\mathbb{Q}_\ell)/GSp_g(\mathbb{Z}_\ell). \tag{2.13}$$

Then we have obtained the following.

Theorem 2.8 *The following diagram is commutative:*

$$\begin{tikzcd}
\mathrm{Div}(SS_g(p))_{\mathbb{Z}} \arrow[d, "T(\ell)^{\mathrm{geo}}"'] & \mathrm{Div}(SS_g(p,\ell,A_0,\mathcal{L}_0))_{\mathbb{Z}} \arrow[l, "(2.12)", "\sim"'] \arrow[d, "T(\ell)^{\mathrm{geo}}_{(A_0,\mathcal{L}_0)}"'] \\
\mathrm{Div}(SS_g(p))_{\mathbb{Z}} & \mathrm{Div}(SS_g(p,\ell,A_0,\mathcal{L}_0))_{\mathbb{Z}} \arrow[l, "(2.12)", "\sim"']
\end{tikzcd}$$

$$\begin{tikzcd}
{} \arrow[r, "(2.13)", "\sim"'] & \mathrm{Div}(G_g(\mathbb{Z}[1/\ell])\backslash GSp_g(\mathbb{Q}_\ell)/Z_{GSp_g}(\mathbb{Q}_\ell)GSp_g(\mathbb{Z}_\ell))_{\mathbb{Z}} \arrow[d, "T(\ell)"'] \\
{} \arrow[r, "(2.13)", "\sim"'] & \mathrm{Div}(G_g(\mathbb{Z}[1/\ell])\backslash GSp_g(\mathbb{Q}_\ell)/Z_{GSp_g}(\mathbb{Q}_\ell)GSp_g(\mathbb{Z}_\ell))_{\mathbb{Z}}.
\end{tikzcd}$$

2.7 The Hecke action and automorphisms

In this subsection we describe the behavior of the Hecke action of $T(\ell)$ on the finite set

$$G_g(\mathbb{Z}[1/\ell])\backslash GSp_g(\mathbb{Q}_\ell)/GSp_g(\mathbb{Z}_\ell) = G_g(\mathbb{Z}[1/\ell])\backslash GSp_g(\mathbb{Q}_\ell)/Z_{GSp_g}(\mathbb{Q}_\ell)GSp_g(\mathbb{Z}_\ell)$$

in terms of automorphism groups of objects in $SS_g(p,\ell,A_0,\mathcal{L}_0)$.

Put $\Gamma = G_g(\mathbb{Z}[1/\ell])$, $G = GSp_g(\mathbb{Q}_\ell)$, $Z = Z_{GSp_g}(\mathbb{Q}_\ell)$, and $K = GSp_g(\mathbb{Z}_\ell)$ for simplicity. We write

$$\Gamma\backslash G/K = \{\Gamma x_1 ZK, \ldots, \Gamma x_h ZK\},\ x_1,\ldots x_h \in G,$$

https://doi.org/10.4153/S0008414X23000676 Published online by Cambridge University Press

where $h = h_g(p,1) = |\Gamma\backslash G/ZK|$. For each $i \in \{1,\dots,h\}$, the coset $\Gamma x_i ZK$ is naturally identified with

$$\Gamma/\Gamma \cap x_i ZK x_i^{-1} = (\Gamma Z/Z)/((\Gamma \cap x_i ZK x_i^{-1})Z/Z).$$

Lemma 2.9 *Keep the notation being as above. Let $(A_i, \mathcal{L}_i, \phi_{A_i})$ be an element in the class corresponding to $\Gamma x_i K$. There is a natural group isomorphism between $\widetilde{\Gamma}_i := (\Gamma \cap x_i ZK x_i^{-1})Z/Z$ and $\mathrm{Aut}((A_i, \mathcal{L}_i))/\{\pm 1\}$ where $\mathrm{Aut}((A_i, \mathcal{L}_i))$ is the group of automorphisms of $(A_i, \mathcal{L}_i)$.*

Proof By construction, we have $T_\ell(A_i) = x_i \mathbb{Z}_\ell^{2g}$ under the inclusion $T_\ell(A_i) \hookrightarrow V_\ell(A_0) = \mathbb{Q}_\ell^{2g}$ induced by the ell -marking of $(A_i, \mathcal{L}_i)$. Then the group $(\Gamma \cap x_i ZK x_i^{-1})$ obviously acts on $T_\ell(A_i)$. Thus, we have an injection $(\Gamma \cap x_i ZK x_i^{-1}) \subset \mathrm{End}(T_\ell(A_i))$. On the other hand, by Tate' theorem (cf. Theorem 1 of [Tate66]), $\mathrm{End}(T_\ell(A_i)) \simeq \mathrm{End}(A_i) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. Hence, we may have $(\Gamma \cap x_i ZK x_i^{-1}) \subset \mathrm{End}(A_i) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ which is compatible with the identification $\Gamma \subset \Gamma^\dagger(A_i)$. Since each element of $\Gamma^\dagger(A_i)$ is an ℓ-isogeny, it preserves the polarization of A_i up to the multiplication by Z. Therefore, $\widetilde{\Gamma}_i \subset \mathrm{Aut}((A_i, \mathcal{L}_i))/\{\pm 1\}$. The opposite inclusion follows by Tate' theorem again. ∎

Next, we study the image of each element of $\Gamma\backslash G/K = \Gamma\backslash G/ZK$ under the Hecke action of $T(\ell)$. Since $T(\ell)$ is defined in terms of lattices (see (2.11)), we define another formulation in terms of elements in G. Let $t_\ell := \mathrm{diag}(\overbrace{1,\dots,1}^{g}, \overbrace{\ell,\dots,\ell}^{g}) \in G$. We decompose

$$K t_\ell K = \coprod_{t \in T} g_t K, \tag{2.14}$$

where T is the index set so that $|T| = N_g(\ell)$. For each $i, j \in \{1,\dots,h\}$, we define

$$m_{ij} := \{t \in T \mid \Gamma x_i g_t ZK = \Gamma x_j ZK\}, \tag{2.15}$$

which is independent of the choice of the representatives $\{g_t\}_{t\in T}$. Let $W(\ell) := \{g_t ZK \mid t \in T\}$. Then, for each $i \in \{1,\dots,h\}$, recall $\widetilde{\Gamma}_i = (\Gamma \cap x_i ZK x_i^{-1})Z/Z$, and the finite group $x_i^{-1}\widetilde{\Gamma}_i x_i \subset KZ/Z$ acts on $W(\ell)$ from the left by multiplication. The action induces the orbit decomposition

$$W(\ell) = \coprod_{t \in T'} O_{x_i^{-1}\widetilde{\Gamma}_i x_i}(g_t KZ) \tag{2.16}$$

for some subset $T' \subset T$.

Lemma 2.10 *Keep the notation being as above. For each $i \in \{1,\dots,h\}$ and $t \in T'$, if $\Gamma x_i g_t ZK = \Gamma x_j ZK$ for some $j \in \{1,\dots,h\}$, the stabilizer $\mathrm{Stab}_{x_i^{-1}\widetilde{\Gamma}_i x_i}(g_t KZ)$ is isomorphic to a subgroup S_i of $\widetilde{\Gamma}_j$.*

Proof By assumption, $x_j = \gamma x_i g_t z k$ for some $\gamma \in \Gamma$, $z \in Z$, and $k \in K$. For each $\alpha Z \in x_i^{-1}\widetilde{\Gamma}_i x_i = (x_i^{-1}\Gamma x_i \cap K)Z/Z$, let us consider the element $k g_t^{-1} \alpha g_t k^{-1} Z$ in G/Z. By using $x_j = \gamma x_i g_t z k$, we see that the element belongs to $x_j^{-1}\Gamma x_j Z/Z$. Further, if αZ is an element of $\mathrm{Stab}_{x_i^{-1}\widetilde{\Gamma}_i x_i}(g_t KZ)$, $k g_t^{-1} \alpha g_t k^{-1} Z$ also belongs to K. Therefore, we have

https://doi.org/10.4153/S0008414X23000676 Published online by Cambridge University Press

a group homomorphism

$$\mathrm{Stab}_{x_i^{-1}\widetilde{\Gamma}_i x_i}(g_t KZ) \overset{\text{the conjugation by } kg_t^{-1}}{\longrightarrow} (x_j^{-1}\Gamma x_j \cap K)Z/Z \simeq \widetilde{\Gamma}_j.$$

Clearly, this map is injective and we have the claim. ∎

We also study the converse of the correspondence from $\Gamma x_i g_t ZK$ to $\Gamma x_i ZK$ for each $i \in \{1, \dots, h\}$. Clearly, $g_t^{-1}ZK \in W(\ell)$.

Lemma 2.11 *For each $i \in \{1, \dots, h\}$ and $t \in T'$, if $\Gamma x_i g_t ZK = \Gamma x_j ZK$ for some $j \in \{1, \dots, h\}$, then $|\mathrm{Stab}_{x_i^{-1}\widetilde{\Gamma}_i x_i}(g_t KZ)| = |\mathrm{Stab}_{x_j^{-1}\widetilde{\Gamma}_j x_j}(g_t^{-1}KZ)|$. In particular, it holds*

$$|\widetilde{\Gamma}_j| \cdot |O_{x_i^{-1}\widetilde{\Gamma}_i x_i}(g_t KZ)| = |\widetilde{\Gamma}_i| \cdot |O_{x_j^{-1}\widetilde{\Gamma}_j x_j}(g_t^{-1}KZ)|.$$

Proof As in the proof of the previous lemma, if we write $x_j = \gamma x_i g_t z k$, then the conjugation by $g_t k^{-1}$ yields the isomorphism from $\mathrm{Stab}_{x_j^{-1}\widetilde{\Gamma}_j x_j}(g_t^{-1}KZ)$ to $\mathrm{Stab}_{x_i^{-1}\widetilde{\Gamma}_i x_i}(g_t KZ)$. The claim follows from this. ∎

Finally, we study the corresponding results in $SS_g(p, \ell, A_0, \mathcal{L}_0)$ under the identification

$$SS_g(p, \ell, A_0, \mathcal{L}_0) \longrightarrow G_g(\mathbb{Z}[1/\ell])\backslash GSp_g(\mathbb{Q}_\ell)/GSp_g(\mathbb{Z}_\ell) \tag{2.17}$$

given by Theorem 2.6. We write

$$SS_g(p, \ell, A_0, \mathcal{L}_0) = \{w_i = [(A_i, \mathcal{L}_i, \phi_{A_i})] \mid i = 1, \dots, h\}.$$

Let us fix $i \in \{1, \dots, h\}$, and we denote by $\mathrm{LG}_i(\ell) = \{C_t\}_{t \in T}$ the set of all totally maximal isotropic subspace of $A_i[\ell]$ with respect to the Weil pairing associated with $\mathcal{L}_i$. Here, we use the same index T as $W(\ell)$ defined before. Then the group $\mathrm{RA}_i := \mathrm{Aut}((A_i, \mathcal{L}_i))/\{\pm 1\}$ acts on $\mathrm{LG}(\ell)$ since each element there preserves the polarization. As in (2.16), we also have the decomposition

$$\mathrm{LG}(\ell) = \coprod_{t \in T'} O_{\mathrm{RA}_i}(C_t).$$

Suppose $\Gamma x_i ZK$ corresponds to $w_i = [(A_i, \mathcal{L}_i, \phi_{A_i})]$ under (2.17).

Proposition 2.12 *Keep the notation being as above. The followings holds.*

(1) *The pullback of ϕ_{A_i} induces an identification between $\mathrm{LG}_i(\ell)$ and $W(\ell)$.*
(2) *Suppose $C_t \in \mathrm{LG}_i(\ell)$ corresponds to $g_t ZK \in W(\ell)$ for $t \in T$ under the above identification. Let $f_{C_t} : (A_i, \mathcal{L}_{A_i}) \longrightarrow (A_{i,C_t}, \mathcal{L}_{A_{i,C_t}})$ be the $(\ell)^g$-isogeny defined by C_t and suppose $[(A_{i,C_t}, \mathcal{L}_{(A_{i,C_t}}, f_{C_t} \circ \phi_{A_i})] = w_j$ for some $j \in \{1, \dots, h\}$ and thus f_{C_t} is regarded as an $(\ell)^g$-isogeny from $(A_i, \mathcal{L}_{A_i})$ to $(A_i, \mathcal{L}_{A_j})$. Let $\widetilde{f}_{C_t} : (A_i, \mathcal{L}_{A_j}) \longrightarrow (A_i, \mathcal{L}_{A_i})$ the $(\ell)^g$-isogeny obtained in Proposition 2.2 for f_{C_t}. Then it holds:*
   - *the kernel of $\widetilde{f}$ corresponds to $g_t^{-1}ZK$ under the above identification,*
   - $|\mathrm{RA}_i| = |\widetilde{\Gamma}_i|$,
   - $|O_{\mathrm{RA}_i}(C_t)| = |O_{x_i^{-1}\widetilde{\Gamma}_i x_i}(g_t KZ)|$, $|O_{\mathrm{RA}_j}(\mathrm{Ker}\widetilde{f}_{C_t})| = |O_{x_j^{-1}\widetilde{\Gamma}_j x_j}(g_t^{-1}KZ)|$, *and*
   - $|\mathrm{RA}_j| \cdot |O_{\mathrm{RA}_i}(C_t)| = |\mathrm{RA}_i| \cdot |O_{\mathrm{RA}_j}(\mathrm{Ker}\widetilde{f}_{C_t})|$.

https://doi.org/10.4153/S0008414X23000676 Published online by Cambridge University Press

Proof The claim follows from the construction of (2.17) with Lemma 2.9 through Lemma 2.11. ∎

We remark that the fourth claim of (2) in the above proposition was proved in Lemma 3.2 of [FS22].

3 A comparison between two graphs

In this section we check, by passing to $SS_g(p, \ell, A_0, \mathcal{L}_0)$, that the graph defined by the special 1-complex $G_g(\mathbb{Z}[1/\ell])\backslash GSp_g(\mathbb{Q}_\ell)/Z_{GSp_g}(\mathbb{Q}_\ell)GSp_g(\mathbb{Z}_\ell)$ is naturally identified with Jordan–Zaytman's big isogeny graph in [JZ21].

3.1 Jordan–Zaytman's big isogeny graph

We basically follow the notation in Sections 7.1 and 5.3 of [JZ21]. The $(\ell)^g$-isogeny (big) graph $Gr_g(\ell, p)$ due to Jordan–Zaytman for $SS_g(p)$ is defined as a directed (regular) graph where:

- the set of vertices $V(Gr_g(\ell, p))$ is $SS_g(p)$ and
- the set of directed edges between two vertices $v_1 = [(A_1, \mathcal{L}_1)]$ and $v_2 = [(A_2, \mathcal{L}_2)]$ is the set of equivalence classes of $(\ell)^g$-isogenies between $(A_1, \mathcal{L}_1)$ and $(A_2, \mathcal{L}_2)$. Here, two isogenies $f, h : (A_1, \mathcal{L}_1) \longrightarrow (A_2, \mathcal{L}_2)$ are said to be equivalent if there exist automorphisms $\phi \in \mathrm{Aut}(A_1, \mathcal{L}_1)$ and $\psi \in \mathrm{Aut}(A_2, \mathcal{L}_2)$ such that $\psi \circ h = f \circ \phi$.

The case when $g = 1$ is nothing but Pizer's graph $G(1, p; \ell)$ handled in [Piz90].

3.2 The (ℓ-marked) $(\ell)^g$-isogeny graph

Similarly, the (ℓ-marked) $(\ell)^g$-isogeny graph $\mathcal{G}_g^{SS}(\ell, p)$ for $SS_g(p, \ell, A_0, \mathcal{L}_0)$ is defined as a directed (regular) graph where:

- the set of vertices $V(\mathcal{G}_g^{SS}(\ell, p))$ is $SS_g(p, \ell, A_0, \mathcal{L}_0)$ and
- the set of edges between two vertices v_1 and v_2 is the set of equivalence classes of $(\ell)^g$-isogenies between corresponding principally polarized superspecial abelian varieties commuting with marking isogenies representing v_1 and v_2 under the identification. In other words, if v_1 and v_2 correspond to $[(A_1, \mathcal{L}_1, \phi_{A_1})]$ and $[(A_2, \mathcal{L}_2, \phi_{A_2})]$ with ℓ-markings $\phi_{A_1} : (A_0, \mathcal{L}_0) \longrightarrow (A_1, \mathcal{L}_1)$ and $\phi_{A_2} : (A_0, \mathcal{L}_0) \longrightarrow (A_2, \mathcal{L}_2)$ respectively, then an edge from v_1 to v_2 is an $(\ell)^g$-isogeny $f : (A_1, \mathcal{L}_1) \longrightarrow (A_2, \mathcal{L}_2)$.

3.3 The graph defined by the special 1-complex

Put $\Gamma = G_g(\mathbb{Z}[1/\ell])$, $G = GSp_g(\mathbb{Q}_\ell)$, $Z = Z_{GSp_g}(\mathbb{Q}_\ell)$, and $K = GSp_g(\mathbb{Z}_\ell)$ for simplicity. We consider the graph associated with the quotient $\Gamma\backslash\mathcal{S}_g$ where $\Gamma = G_g(\mathbb{Z}[1/\ell])$ and $\mathcal{S}_g = GSp_g(\mathbb{Q}_\ell)/Z_{GSp_g}(\mathbb{Q}_\ell)GSp_g(\mathbb{Z}_\ell)$.

Two elements $v_1 = \Gamma g_1 ZK$ and $v_2 = \Gamma g_2 ZK$ in $\Gamma\backslash G/ZK$ said to be adjacent if $v_2 = \Gamma g_1 g_t ZK$ for some $t \in T$ where $\{g_t\}_{t \in T}$ is defined in (2.14).

The graph in question, say $\mathrm{BTQ}_g^1(\ell, p)$, is a directed (regular) graph where:

- the set of vertices $V(\mathrm{BTQ}_g^1(\ell, p))$ is $\Gamma\backslash G/ZK$ and
- the set of directed edges between two vertices $v_1 = \Gamma g_1 ZK$ and $v_2 = \Gamma g_2 ZK$ is defined by the adjacency condition in the above sense. Namely, an edge from v_1 from v_2 is g_t with $t \in T$ such that $v_2 = \Gamma g_1 g_t ZK$.

3.4 Comparison theorem

Let us keep the notation in this section. We define

$$\mathrm{RA}(v) := \begin{cases} \mathrm{RA}(A, \mathcal{L}), & \text{if } v = [(A, \mathcal{L})] \in SS_g(p) \text{ or } v = [(A, \mathcal{L}, \phi_A)] \in SS_g(p, \ell, A_0, \mathcal{L}_0), \\ (\Gamma \cap xZKx^{-1})Z/Z, & \text{if } v = \Gamma xZK \text{ in the case of } \mathrm{BTQ}_g^1(\ell, p). \end{cases}$$

Further, we also define

$$\mathrm{Ker}(e) := \begin{cases} \mathrm{Ker}(f), & \text{if } e \text{ is a class of } (\ell)^g\text{-isogeny } f \text{ in the case of } SS_g(p) \text{ or } SS_g(p, \ell, A_0, \mathcal{L}_0), \\ g_t, & \text{if } e \text{ is an edge defined by } g_t,\ t \in T \text{ in the case of } \mathrm{BTQ}_g^1(\ell, p). \end{cases}$$

We will prove the following comparison theorem which plays an important role in our study.

Theorem 3.1 *The identifications (2.12) and (2.13) induce the following graph isomorphisms:*

$$Gr_g(\ell, p) \overset{(2.12)}{\underset{\sim}{\longleftarrow}} \mathcal{G}_g^{SS}(\ell, p) \overset{(2.13)}{\underset{\sim}{\longrightarrow}} \mathrm{BTQ}_g^1(\ell, p).$$

Further, the following properties are preserved under the isomorphisms:

- *The Hecke action of $T(\ell)^{\mathrm{geo}}$, $T(\ell)^{\mathrm{geo}}_{(A_0, \mathcal{L}_0)}$, or $T(\ell)$ on each set of the vertices defines $N_g(\ell)$-neighbors of a given vertex.*
- *Each edge e from v_1 to v_2 has an opposite $\widehat{e}$ such that*

$$|\mathrm{RA}(v_2)| \cdot |O_{\mathrm{RA}(v_1)}(\mathrm{Ker}(e))| = |\mathrm{RA}(v_1)| \cdot |O_{\mathrm{RA}(v_2)}(\mathrm{Ker}(\widehat{e}))|.$$

Proof As in the claim already, the identifications between the sets of vertices are given by (2.12) and (2.13). The compatibility of the Hecke operators follows from Theorem 2.8, and this yields the first property in the latter claim. The remaining formula follows from Proposition 2.12. ∎

Corollary 3.2 *Keep the notation being as above. The random walk matrices for $Gr_g(\ell, p)$, $\mathcal{G}_g^{SS}(\ell, p)$, and $\mathrm{BTQ}_g^1(\ell, p)$ coincide each other.*

We remark that Theorem 2.8 is insufficient to prove the above corollary, while Theorem 3.1 tells us more finer information for the relation of the reduced automorphisms and the multiplicity of each edge.

Remark 3.3 As shown in Theorem 3.1 or Section 3 of [FS22], the group of reduced automorphisms gives a finer structure of its orbit of a given Lagrangian subspace defining an $(\ell)^g$-isogeny. The edges in Figure 1 can be more precise as in the figure in 7A, page 297 of [KT20].

4 Bruhat–Tits buildings for symplectic groups

In this and the following chapter, we introduce a more general framework than the case to which we apply. The purpose is to simplify the notations and to indicate that the methods we use are applicable in a wider context. The reader may assume that $F = \mathbb{Q}_\ell$ and $\varpi = \ell$ in the following discussion.

4.1 Symplectic groups revisited for the buildings

Let F be a non-archimedean local field of characteristic different from 2, and let O be the ring of integers. We fix a uniformizer ϖ and identify the residue field $O/\varpi O$ with a finite field $\mathbb{F}_q$ of order q. Further, we denote by $F^\times$ and $O^\times$ the multiplicative groups in F and O, respectively. Let ord_ϖ be a discrete valuation in F, normalized so that $\mathrm{ord}_\varpi(F^\times) = \mathbb{Z}$. For example, we consider the ℓ-adic field $\mathbb{Q}_\ell$ for a prime ℓ with the ring of integers $\mathbb{Z}_\ell$, where ℓ is a uniformizer and the residue field is $\mathbb{F}_\ell = \mathbb{Z}/\ell\mathbb{Z}$.

For a positive integer n, let $V := F^{2n}$ be the symplectic space over F equipped with the standard symplectic pairing $\langle *, * \rangle$ defined by $\langle v, w \rangle = {}^t v J_n w$ for $v, w \in F^{2n}$. For V, there exists a basis $\{v_1, \dots, v_n, w_1, \dots, w_n\}$ such that $\langle v_i, w_j \rangle = \delta_{ij}$ and $\langle v_i, v_j \rangle = \langle w_i, w_j \rangle = 0$ for all $i, j = 1, \dots, n$, where δ_{ij} equals 1 if $i = j$ and 0 if $i \neq j$, and we call it a symplectic basis of $(V, \langle *, * \rangle)$. Each choice of a symplectic basis yields an isomorphism between the isometry group and $Sp_n(F)$.

Note that the following elements are in $GSp_n(F)$:

$$t_\lambda := \mathrm{diag}(1, \dots, 1, \lambda, \dots, \lambda) = \begin{pmatrix} I_n & 0 \\ 0 & \lambda I_n \end{pmatrix} \quad \text{for } \lambda \in F^\times.$$

In the subsequent sections, we consider the projectivized groups: let $PSp_n(F)$ and $PGSp_n(F)$ be the groups $Sp_n(F)$ and $GSp_n(F)$ modulo the centers, respectively. If we naturally identify $PSp_n(F)$ with a normal subgroup of $PGSp_n(F)$, then the quotient group $PGSp_n(F)/PSp_n(F)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times O^\times$, which is generated by the images of $t_\lambda = \mathrm{diag}(1, \dots, 1, \lambda, \dots, \lambda)$ for $\lambda \in \varpi O^\times$. Similarly, letting $PSp_n(O)$ and $PGSp_n(O)$ be the groups $Sp_n(O)$ and $GSp_n(O)$ modulo the centers, respectively, we consider $PSp_n(O)$ as a subgroup in $PGSp_n(O)$.

4.2 Bruhat–Tits building: the construction

Let $(V, \langle *, * \rangle)$ be a symplectic space over F of dimension $2n$. We define a lattice Λ in V as a free O-module of rank $2n$. Note that if Λ is a lattice, then $\Lambda/\varpi\Lambda$ is a vector space over $\mathbb{F}_q$ of dimension $2n$. We say that a lattice Λ is *primitive* if $\langle \Lambda, \Lambda \rangle \subseteq O$ where $\langle \Lambda, \Lambda \rangle := \{\langle v, w \rangle \mid v, w \in \Lambda\}$, and $\langle *, * \rangle$ induces a non-degenerate alternating form on $\Lambda/\varpi\Lambda$ over $\mathbb{F}_q$.

Let Λ_i for $i = 1, 2$ be lattices in V, and we say that they are homothetic if $\Lambda_1 = \alpha\Lambda_2$ for some $\alpha \in F^\times$. This defines an equivalence relation in the set of lattices in V. We denote the homothety class of a lattice Λ by $[\Lambda]$. Let us define the set $\mathbb{L}_n$ of homothety classes $[\Lambda]$ of lattices such that there exist a representative Λ of $[\Lambda]$ and a primitive lattice Λ_0 satisfying that $\varpi\Lambda_0 \subseteq \Lambda \subseteq \Lambda_0$ and $\langle \Lambda, \Lambda \rangle \subseteq \varpi O$. By the definition, if $[\Lambda] \in \mathbb{L}_n$, then a representative Λ yields a subspace $\Lambda/\varpi\Lambda_0$ of $\Lambda_0/\varpi\Lambda_0$

with some primitive lattice Λ_0 such that it is *totally isotropic*, i.e., the induced non-degenerate alternating form $\langle *, * \rangle$ vanishes on $\Lambda/\varpi\Lambda_0$ in $\Lambda_0/\varpi\Lambda_0$. Further, we define the incidence relation in $\mathbb{L}_n$ and denote by $[\Lambda_1] \sim [\Lambda_2]$ for two distinct homothety classes if there exist representatives Λ_i of $[\Lambda_i]$ for $i = 1, 2$ and a primitive lattice Λ_0 such that $\varpi\Lambda_0 \subseteq \Lambda_i \subseteq \Lambda_0$ for $i = 1, 2$, and either $\Lambda_1 \subseteq \Lambda_2$ or $\Lambda_2 \subseteq \Lambda_1$ holds.

The *Bruhat–Tits building* $\mathcal{B}_n$ (in short, *building*) for the group $PGSp_n(F)$ (or $Sp_n(F)$) is the clique complex whose set of vertices $\mathrm{Ver}(\mathcal{B}_n)$ is $\mathbb{L}_n$, i.e., $\sigma \subset \mathrm{Ver}(\mathcal{B}_n)$ defines a simplex if any distinct vertices in σ are incident. The building $\mathcal{B}_n$ is a simplicial complex of dimension n; note that each chamber (i.e., a simplex of maximal dimension) $[\Lambda_0], [\Lambda_1], \ldots, [\Lambda_n]$ corresponds to a sequence of lattices $\Lambda_0 \subseteq \Lambda_1 \subseteq \cdots \subseteq \Lambda_n \subseteq \varpi^{-1}\Lambda_0$, where $\varpi^{-1}\Lambda_0$ is primitive, such that

$$\{0\} \subseteq \Lambda_1/\Lambda_0 \subseteq \Lambda_2/\Lambda_0 \subseteq \cdots \subseteq \Lambda_n/\Lambda_0 \subseteq \varpi^{-1}\Lambda_0/\Lambda_0$$

forms a complete flag of a maximal totally isotropic subspace Λ_n/Λ_0 in $\varpi^{-1}\Lambda_0/\Lambda_0$ over $\mathbb{F}_q$.

The group $Sp_n(F)$ acts on $\mathcal{B}_n$ as simplicial automorphisms: let us fix a symplectic basis $\{v_1, \ldots, v_n, w_1, \ldots, w_n\}$ of $(V, \langle *, * \rangle)$, which we identify with the standard symplectic space over F. Then the action is defined by $[\Lambda] \mapsto [M\Lambda]$ for $[\Lambda] \in \mathrm{Ver}(\mathcal{B}_n)$ and $M \in Sp_n(F)$, and this action is simplicial since it preserves the incidence relation. Moreover, this yields the action of the projectivized group $PSp_n(F)$ on $\mathcal{B}_n$.

We define the label (or, color) on the set of vertices $\mathrm{Ver}(\mathcal{B}_n)$. For any lattice Λ, there exists some $\gamma \in GL_{2n}(F)$ such that $\gamma u_1, \ldots, \gamma w_n$ form an O-basis of Λ. Let

$$\mathbf{lab}_n[\Lambda] := \mathrm{ord}_{\varpi}(\det \gamma) \mod 2n.$$

Note that this depends only on the homothety class of Λ since $\det(\alpha\gamma) = \alpha^{2n}\det(\gamma)$ for $\alpha \in F^\times$ and for $\gamma \in GL_{2n}(F)$, and $\det \gamma \in O^\times$ for $\gamma \in GL_{2n}(O)$. Hence, the function $\mathbf{lab}_n : \mathrm{Ver}(\mathcal{B}_n) \to \mathbb{Z}/2n\mathbb{Z}$ is well defined and we call $\mathbf{lab}_n[\Lambda]$ the *label* of a vertex $[\Lambda] \in \mathrm{Ver}(\mathcal{B}_n)$. For example, let us consider a sequence of lattices $\Lambda_0, \ldots, \Lambda_n$, where

(4.1)

$$\Lambda_k := Ou_1 \oplus \cdots \oplus Ou_k \oplus O\varpi u_{k+1} \oplus \cdots \oplus O\varpi w_1 \oplus \cdots \oplus O\varpi w_n \quad \text{for } 0 \leq k < n,$$

and $\Lambda_n := Ou_1 \oplus \cdots \oplus Ou_n \oplus O\varpi w_1 \oplus \cdots \oplus O\varpi w_n$. Then $\Lambda_0 \subseteq \cdots \subseteq \Lambda_n \subseteq \varpi^{-1}\Lambda_0$ and $\varpi^{-1}\Lambda_0$ is primitive, and since the chain $\Lambda_1/\Lambda_0 \subseteq \cdots \subseteq \Lambda_n/\Lambda_0$ forms a maximal totally isotropic flag in $\varpi^{-1}\Lambda_0/\Lambda_0$ over $\mathbb{F}_q$, the corresponding homothety classes $[\Lambda_0], \ldots, [\Lambda_n]$ define a chamber in $\mathcal{B}_n$. In this case, we have that $\mathbf{lab}_n[\Lambda_k] = 2n - k \mod 2n$ for $0 \leq k \leq n$. We call the chamber determined by $[\Lambda_0], \ldots, [\Lambda_n]$ the *fundamental chamber* $\mathcal{C}_0$. Here, we note that $\mathbf{lab}_n$ misses the values $1, \ldots, n-1$ in $\mathbb{Z}/2n\mathbb{Z}$. It is known that $Sp_n(F)$ acts transitively on the set of *chambers* [Gar97, Section 20.5], i.e., every chamber is of the form $\gamma\mathcal{C}_0$ for $\gamma \in Sp_n(F)$. By definition, the action of $Sp_n(F)$ preserves the labels on $\mathrm{Ver}(\mathcal{B}_n)$. It thus implies that the action is not vertex-transitive for any $n \geq 1$.

4.3 Apartments

Let us introduce a system of apartments in the building $\mathcal{B}_n$. See [Gar97, Chapter 20] and [She07] for basics and more details. A *frame* is an unordered n-tuple: $\{\lambda_1^1, \lambda_1^2\}$,

$\ldots, \{\lambda_n^1, \lambda_n^2\}$, such that each $\{\lambda_i^1, \lambda_i^2\}$ is an unordered pair of lines which span a two-dimensional symplectic subspace with the induced alternating form for $i = 1, \ldots, n$, and

$$V = V_1 \oplus \cdots \oplus V_n \quad \text{where } V_i := \lambda_i^1 \oplus \lambda_i^2 \text{ and } V_i \perp V_j \text{ if } i \neq j,$$

i.e., $\langle v, v' \rangle = 0$ for all $v \in V_i$ and all $v' \in V_j$ if $i \neq j$. An *apartment* defined by a frame $\{\lambda_i^1, \lambda_i^2\}$ for $i = 1, \ldots, n$ is a maximal subcomplex of $\mathcal{B}_n$ on the set of vertices $[\Lambda]$ such that

$$\Lambda = \bigoplus_{i=1}^{n} \left(M_i^1 \oplus M_i^2\right) \quad \text{where } M_i^j \text{ is a rank one free } O\text{-module in } \lambda_i^j \text{ for } j = 1, 2,$$

for some (equivalently, every) representative Λ in the homothety class. We define a system of apartments as a maximal set of apartments.

Following [She07], we fix a symplectic basis $\{u_1, \ldots, u_n, w_1, \ldots, w_n\}$ of V and a uniformizer ϖ in F and lighten the notation: we denote a lattice

$$\Lambda = O\varpi^{a_1}u_1 \oplus \cdots \oplus O\varpi^{a_n}u_n \oplus O\varpi^{b_1}w_1 \oplus \cdots \oplus O\varpi^{b_n}w_n \quad \text{for } a_i, b_i \in \mathbb{Z}, i = 1, \ldots, n,$$

by $\Lambda = (a_1, \ldots, a_n; b_1, \ldots, b_n)$, and the homothety class by $[\Lambda] = [a_1, \ldots, a_n; b_1, \ldots, b_n]$. For Λ, we have $\langle \Lambda, \Lambda \rangle \subset O$ if and only if $\langle \varpi^{a_i}u_i, \varpi^{b_i}w_i \rangle = \varpi^{a_i+b_i} \in O$ for all $i = 1, \ldots, n$. This is equivalent to that $a_i + b_i \geq 0$ for all $i = 1, \ldots, n$, in which case, $\Lambda/\varpi\Lambda$ is a non-degenerate alternating space with the induced form over the residue field $O/\varpi O$ if and only if $a_i + b_i = 0$ for all $i = 1, \ldots, n$.

For the fixed basis, let $\lambda_i^1 := Fu_i$ and $\lambda_i^2 := Fw_i$ for $i = 1, \ldots, n$. The frame $\{\lambda_i^1, \lambda_i^2\}_{i=1,\ldots,n}$ determines an apartment Σ_0 in the building $\mathcal{B}_n$ for $Sp_n(F)$. We call Σ_0 the *fundamental apartment*. The chain of lattice $\Lambda_0 \subsetneq \cdots \subsetneq \Lambda_n$ in (4.1) defines a chamber $\mathcal{C}_0$ in Σ_0 containing $[\Lambda_0]$. The rest of chambers in the apartment Σ_0 are obtained by the action of the affine Weyl group (of type $\widetilde{C}_n$) attached to the building.

Example 4.1 If $n = 2$, then we have eight chambers containing vertex $[\Lambda_0] = [1,1;1,1]$ in a fixed apartment, where the fundamental chamber $\mathcal{C}_0$ is defined by the chain

$$\Lambda_0 = (1,1;1,1) \subset (0,1;1,1) \subset (0,0;1,1) \subset (0,0;0,0) = \varpi^{-1}\Lambda_0.$$

4.4 Special vertices and the special 1-complex

For any lattice Λ in a symplectic space $(V, \langle *, * \rangle)$, let us define the dual by $\Lambda^* := \{v \in V \mid \langle v, w \rangle \in O \text{ for all } w \in \Lambda\}$. Note that Λ^* is also a lattice in V. For every $\alpha \in F^\times$, we have that $(\alpha\Lambda)^* = \alpha^{-1}\Lambda^*$, whence the homothety class $[\Lambda^*]$ depends only on $[\Lambda]$. Let us call a vertex $[\Lambda]$ in the building $\mathcal{B}_n$ *self-dual* if $[\Lambda^*] = [\Lambda]$. Below we characterize self-dual vertices in terms of labels – it is essentially proved in [She07, Proposition 3.1]; so we omit the proof.

Lemma 4.2 *Fix an integer $n \geq 1$. For $[\Lambda] \in \mathrm{Ver}(\mathcal{B}_n)$, we have that $[\Lambda^*] = [\Lambda]$ if and only if* $\mathbf{lab}_n[\Lambda] = 0$ *or* $n \mod 2n$.

For $[\Lambda] \in \mathrm{Ver}(\mathcal{B}_n)$, let us call $[\Lambda]$ a *special vertex* if $[\Lambda^*] = [\Lambda]$. We define the *special* 1*-complex* $\mathcal{S}_n$ as a one-dimensional subcomplex of $\mathcal{B}_n$ based on the set of special vertices

$$\mathrm{Ver}(\mathcal{S}_n) := \{[\Lambda] \in \mathrm{Ver}(\mathcal{B}_n) \mid [\Lambda^*] = [\Lambda]\},$$

and 1-simplices (edges) are defined between two incident vertices in $\mathcal{B}_n$ (cf. Section 4.1): for $[\Lambda_1]$, $[\Lambda_2]$ in $\mathrm{Ver}(\mathcal{S}_n)$, we have $[\Lambda_1] \sim [\Lambda_2]$ if and only if there exist representatives Λ_1 and Λ_2 from $[\Lambda_1]$ and $[\Lambda_2]$, respectively, such that either $\varpi^{-1}\Lambda_1$ is primitive and $\Lambda_1 \subseteq \Lambda_2 \subseteq \varpi^{-1}\Lambda_1$, or the analogous relation where the roles of Λ_1 and Λ_2 are interchanged holds. Note that since special vertices are those that are self-dual, if $\varpi^{-1}\Lambda_1$ is primitive, then Λ_2/Λ_1 is a maximal totally isotropic subspace of $\varpi^{-1}\Lambda_1/\Lambda_1$ over $\mathbb{F}_q$. Lemma 4.2 shows that $[\Lambda] \in \mathrm{Ver}(\mathcal{S}_n)$ if and only if $\mathbf{lab}_n[\Lambda] = 0$ or $n \mod 2n$. The following proposition has been shown in [She07, Proposition 3.6].

Proposition 4.3 *For every integer $n \geq 1$, the special 1-complex $\mathcal{S}_n$ is connected.*

We note that $GSp_n(F)$ does not act on $\mathcal{B}_n$ through the linear transformation of lattices. Indeed, a vertex of label $2n-1 \mod 2n$ in the fundamental chamber $\mathcal{C}_0$ is sent by $t_\varpi \in GSp_n(F)$ to a vertex of label $n-1 \mod 2n$, which does not belong to $\mathrm{Ver}(\mathcal{B}_n)$. However, restricted on $\mathcal{S}_n$, the group $GSp_n(F)$ acts on $\mathcal{S}_n$. Moreover, the action of $GSp_n(F)$ on $\mathcal{S}_n$ is vertex-transitive since for $t_\varpi = \mathrm{diag}(1, \dots, 1, \varpi, \dots, \varpi)$ in $GSp_n(F)$, we have that

$$t_\varpi[\Lambda_0] = [\Lambda_n] \quad \text{where } t_\varpi = \begin{pmatrix} I_n & 0 \\ 0 & \varpi I_n \end{pmatrix} \text{ and } [\Lambda_0], [\Lambda_n] \in \mathcal{C}_0.$$

Note that t_ϖ permutes the labels on $\mathrm{Ver}(\mathcal{S}_n)$. This defines the action of $PGSp_n(F)$ on $\mathcal{S}_n$.

5 Property (T) and spectral gaps

5.1 Property (T)

Let G be a topological group, and let $(\pi, \mathcal{H})$ be a unitary representation of G, where we assume that any Hilbert space $\mathcal{H}$ is complex. For any compact subset Q in G, let

$$\kappa(G, Q, \pi) := \inf\left\{\max_{s \in Q} \|\pi(s)\varphi - \varphi\| \mid \varphi \in \mathcal{H},\ \|\varphi\| = 1\right\},$$

and further let $\kappa(G, Q) := \inf \kappa(G, Q, \pi)$, where the above infimum is taken over all equivalence classes of unitary representations $(\pi, \mathcal{H})$ without nonzero invariant vectors. We call $\kappa(G, Q)$ the *optimal Kazhdan constant* for the pair (G, Q). We say that G has *Property* (T) if there exists a compact set Q in G such that $\kappa(G, Q) > 0$. It is known that for a local field F, if $n \geq 2$, then $Sp_n(F)$ has Property (T), while if $n = 1$, then $Sp_1(F) = SL_2(F)$ and it fails to have Property (T) [BHV08, Theorem 1.5.3 and Example 1.7.4].

For any $n \geq 2$, $PSp_n(F)$ has Property (T) since $Sp_n(F)$ does [BHV08, Theorem 1.3.4]. Similarly, for any $n \geq 2$, the group $PGSp_n(F)$ has Property (T) since $PGSp_n(F)/PSp_n(F)$ admits a finite invariant Borel regular measure (see Section 4.1 and [BHV08, Theorem 1.7.1]). (We note that for any $n \geq 1$, the group $GSp_n(F)$ does

https://doi.org/10.4153/S0008414X23000676 Published online by Cambridge University Press

not have Property (T) because it admits a surjective homomorphism onto $\mathbb{Z}$ [BHV08, Corollary 1.3.5].)

We say that a subset Q of G is *generating* if the sub-semigroup generated by Q coincides with G. If G has Property (T) and Q is an arbitrary compact generating set of G (provided that it exists), then $\kappa(G, Q) > 0$ [BHV08, Proposition 1.3.2]. We will construct an appropriate compact generating set in the following.

5.2 A random walk operator

In this section, fix an integer $n \geq 1$. Recall that $K = PGSp_n(O)$, and letting $o := [\Lambda_0]$, we identify K with the stabilizer of o in $PGSp_n(F)$. Let $a := [t_\varpi] \in PGSp_n(F)$, and let us choose $\xi_i \in PSp_n(F)(\subset PGSp_n(F))$ for $i = 0, 1, \ldots, n+1$ such that $\xi_0 := \mathrm{id}$ and for $i = 1. \ldots, n+1$ each ξ_i projects onto the reflection s_i in the affine Weyl group acting on the fundamental apartment Σ_0.

Let us define a subset $\Omega := \{k\xi_i a k', k(\xi_i a)^{-1}k' \mid k, k' \in K, i = 0, \ldots, n+1\}$ in $PGSp_n(F)$, where we simply write

$$\Omega = K\Omega_0 K, \quad \text{where } \Omega_0 := \{\xi_0 a, \ldots, \xi_{n+1} a, (\xi_0 a)^{-1}, \ldots, (\xi_{n+1} a)^{-1}\}.$$

Note that Ω is compact and symmetric, i.e., $x \in \Omega$ if and only if $x^{-1} \in \Omega$. Let ν be a Haar measure on K normalized so that $\nu(K) = 1$. Let us define the probability measure μ on $PGSp_n(F)$ as the distribution of $k\zeta k'$ where k, k', and ζ are independent and k, k' are distributed according to ν and ζ is uniformly distributed on $\{\xi_i a, (\xi_i a)^{-1} \mid i = 0, \ldots, n+1\}$. In other words,

$$\mu = \nu * \mathrm{Unif}_{\Omega_0} * \nu, \quad \text{where } \mathrm{Unif}_{\Omega_0} := \frac{1}{2(n+2)} \sum_{i=0}^{n+1} \left(\delta_{\xi_i a} + \delta_{(\xi_i a)^{-1}}\right),$$

and δ_x denotes the Dirac distribution at x. We write the convolution $\mu_1 * \mu_2$ for two probability measures μ_1, μ_2 on a group G. Note that the support of μ is Ω. If we define the probability measure $\check{\mu}$ on $PGSp_n(F)$ as the distribution of x^{-1} where x has the law μ, then the definition of μ implies that $\check{\mu} = \mu$.

Lemma 5.1 *We have the following:*

(1) *The set Ω generates $PGSp_n(F)$ as a semigroup.*
(2) *Fix an integer $n \geq 1$. The double coset $K\backslash\Omega/K$ is represented by a finite set $\Omega_0 = \{\xi_i a, (\xi_i a)^{-1}, i = 0, \ldots, n+1\}$ and*

$$\min_{K\gamma K \in K\backslash\Omega/K} \mu(K\gamma K) = \frac{1}{2(n+2)}.$$

Moreover, if γ is distributed according to μ on $PGSp_n(F)$, then γo is uniformly distributed on the set of incident vertices to $o = [\Lambda_0]$ in $\mathcal{S}_n$.

Proof Let us show (1). If we let $K_0 := PSp_n(O)$ and define Δ in $K(= PGSp_n(O))$ as the image of $\{t_\lambda \mid \lambda \in O^\times\}$, then since K contains K_0 and Δ, and Ω contains $K\{a, a^{-1}\}K$, the set $\Omega \cdot \Omega$ contains $\bigcup_{i=1}^{n+1} K_0\xi_i K_0$ as well as K (and thus K_0 and Δ). The group K_0 acts on the set of apartments containing $o = [\Lambda_0]$ transitively, and this implies that $\bigcup_{i=1}^{n+1} K_0\xi_i K_0$ generates $PSp_n(F)$ as a semigroup, which follows by looking at the induced action of reflections on apartments (cf. Section 4.3). Since the quotient $PGSp_n(F)$ modulo $PSp_n(F)$ is generated by the images of $\{a, a^{-1}\}$ and Δ (cf. Section 4.1), we conclude that Ω generates $PGSp_n(F)$ as a semigroup.

Let us show (2). The first claim follows since $\Omega = K\Omega_0 K$ and the definition of μ shows that μ yields the uniform distribution on $K\backslash\Omega/K$. Concerning the second claim, in the fundamental apartment Σ_0, we note that $\xi_i ao = t_\varpi o$ if $i \neq 1$ and $\xi_1 ao = s_1 t_\varpi o$, and $(\xi_i a)^{-1} o = t_\varpi^{-1} o$ if $i \neq n+1$ and $(\xi_{n+1} a)^{-1} o = s_* t_\varpi o$ where s_* is a product of $s_1, s_2, \dots, s_n$ with some repetitions; we note that such an element s_* fixes o since it belongs to the spherical Weyl group. Furthermore, $K_0 (= PSp_n(O))$ acts on the set of apartments containing o and if we apply k whose distribution is the normalized Haar measure on $K(= PGSp_n(O))$ to an incidence vertex v of o, then kv is uniformly distributed on the incident vertices of o. This implies the claim. ■

For simplicity of notation, let $G := PGSp_n(F)$ in the following discussion. Recall that $\mathrm{Ver}(\mathcal{S}_n) = Go$ (cf. Section 4.3). Let us denote by $\ell^2(\mathcal{S}_n)$ the Hilbert space of square-summable complex-valued functions on $\mathrm{Ver}(\mathcal{S}_n)$ equipped with the inner product $\langle \varphi, \psi \rangle := \sum_{v \in \mathrm{Ver}(\mathcal{S}_n)} \varphi(v)\overline{\psi(v)}$ for $\varphi, \psi \in \ell^2(\mathcal{S}_n)$. Let us define an operator $\mathcal{A}_\mu : \ell^2(\mathcal{S}_n) \to \ell^2(\mathcal{S}_n)$ by

$$\mathcal{A}_\mu \varphi(\xi o) = \int_G \varphi(\xi \gamma o) d\mu(\gamma) \qquad \text{for } \xi \in G.$$

Note that $\mathcal{A}_\mu$ is well defined by the definition of μ since $\mathrm{Ver}(\mathcal{S}_n) = Go$ and K is the stabilizer of o. Lemma 5.1(2) shows that $\mathcal{A}_\mu$ is the normalized adjacency operator on $\mathcal{S}_n$. Since $\check{\mu} = \mu$, the operator $\mathcal{A}_\mu$ is self-adjoint on $\ell^2(\mathcal{S}_n)$. Similarly, if we define $\mathcal{A}_{\mu^{*t}} : \ell^2(\mathcal{S}_n) \to \ell^2(\mathcal{S}_n)$ in the same way with respect to the tth convolution power μ^{*t} of μ, then we have that by induction $\mathcal{A}_\mu^t = \mathcal{A}_{\mu^{*t}}$ for all positive integer $t \geq 1$.

Let us consider any closed subgroup Γ of G such that Γ acts on $\mathcal{S}_n$ from left with a compact quotient space $\Gamma\backslash\mathcal{S}_n$, where the action is given by $(\gamma, v) \mapsto \gamma v$ for $\gamma \in \Gamma$ and $v \in \mathcal{S}_n$. Since Γ acts on $\mathcal{S}_n$ by simplicial automorphisms (as $PGSp_n(F)$ does), the quotient $\Gamma\backslash\mathcal{S}_n$ naturally admits a finite (unoriented) graph structure induced from $\mathcal{S}_n$. Let us denote the finite graph by the same symbol $\Gamma\backslash\mathcal{S}_n$. Note that since $\mathcal{S}_n$ is connected by Proposition 4.3, the graph $\Gamma\backslash\mathcal{S}_n$ is connected for any such Γ. Here, however, we do not assume that Γ is torsion-free; thus, the graph $\Gamma\backslash\mathcal{S}_n$ may have loops and not regular. Although $\mathcal{S}_n$ admits a bipartite graph structure, $\Gamma\backslash\mathcal{S}_n$ is not necessarily bipartite unless Γ factors through $PSp_n(F)$.

For each $v \in \mathcal{S}_n$, let $\Gamma_v := \{\gamma \in \Gamma \mid \gamma v = v\}$. Note that Γ_v is finite and $|\Gamma_v|$ is independent of the choice of representatives for $v \in \Gamma\backslash\mathcal{S}_n$. Let us define $\ell^2(\Gamma\backslash\mathcal{S}_n)$ the space of complex-valued functions on $\Gamma\backslash\mathcal{S}_n$ equipped with the inner product defined by

$$\langle \varphi, \psi \rangle := \sum_{v \in \Gamma\backslash\mathcal{S}_n} \varphi(v)\overline{\psi(v)} \frac{1}{|\Gamma_v|} \quad \text{for } \varphi, \psi \in \ell^2(\Gamma\backslash\mathcal{S}_n).$$

The group Γ acts on $\ell^2(\mathcal{S}_n)$ by $\varphi \mapsto \varphi \circ \gamma^{-1}$ for $\gamma \in \Gamma$ and $\varphi \in \ell^2(\mathcal{S}_n)$, and since this Γ-action and $\mathcal{A}_\mu$ on $\ell^2(\mathcal{S}_n)$ commute, the following operator $\mathcal{A}_{\Gamma,\mu^{*t}}$ on $\ell^2(\Gamma\backslash\mathcal{S}_n)$ is well defined for all positive integer t:

$$\mathcal{A}_{\Gamma,\mu^{*t}} \varphi(\Gamma \xi o) = \int_G \varphi(\Gamma \xi \gamma o) d\mu^{*t}(\gamma) \qquad \text{for } \Gamma\xi o \in \Gamma\backslash\mathcal{S}_n \text{ and } \varphi \in \ell^2(\Gamma\backslash\mathcal{S}_n).$$

https://doi.org/10.4153/S0008414X23000676 Published online by Cambridge University Press

We have that $\mathcal{A}_{\Gamma,\mu}^t = \mathcal{A}_{\Gamma,\mu^{*t}}$ for all integer $t \geq 1$, and $\mathcal{A}_{\Gamma,\mu}$ is self-adjoint, i.e., $\langle \mathcal{A}_{\Gamma,\mu}\varphi, \psi\rangle = \langle \varphi, \mathcal{A}_{\Gamma,\mu}\psi\rangle$ for $\varphi, \psi \in \ell^2(\Gamma\backslash\mathcal{S}_n)$. In other words, the operator $\mathcal{A}_{\Gamma,\mu}$ defines a Markov chain on $\Gamma\backslash\mathcal{S}_n$ reversible with respect to the measure $1/|\Gamma_v|$ for each vertex v.

5.3 Spectral gap

We normalize the Haar measure on G in such a way that K has the unit mass. Let $L^2(\Gamma\backslash G)$ denote the complex L^2-space with respect to the (right) Haar measure for which each double coset $\Gamma\xi K$ has the mass $1/|\xi^{-1}\Gamma\xi \cap K|$. Note that the mass coincides with $1/|\Gamma_{\xi o}|$ since $\Gamma_{\xi o} = \Gamma \cap \xi K \xi^{-1}$. We consider $L^2(\Gamma\backslash G)^K$ the subspace of K-fixed vectors in $L^2(\Gamma\backslash G)$ and naturally identify it with $\ell^2(\Gamma\backslash\mathcal{S}_n)$ (including the inner product). Let us define the unitary representation π of G on $L^2(\Gamma\backslash G)$ by

$$\pi(\gamma)\varphi(\Gamma\xi) = \varphi(\Gamma\xi\gamma) \quad \text{for } \varphi \in L^2(\Gamma\backslash G) \text{ and } \xi, \gamma \in G.$$

Note that $\varphi \in L^2(\Gamma\backslash G)^K$ if and only if $\pi(k)\varphi = \varphi$ for all $k \in K$.

Let

$$T_\Gamma(\gamma)\varphi(\Gamma\xi) := \int_K \varphi(\Gamma\xi k\gamma)\, d\nu(k) \quad \text{for } \varphi \in L^2(\Gamma\backslash G) \text{ and } \gamma \in G,$$

where we recall that ν is the normalized Haar measure on K.

Lemma 5.2 *For every $n \geq 1$, and for all $\varphi \in L^2(\Gamma\backslash G)^K$, we have that*

$$\mathcal{A}_{\Gamma,\mu}\varphi = \frac{1}{2(n+2)} \sum_{\gamma\in\Omega_0} T_\Gamma(\gamma)\varphi.$$

Moreover, for all $\gamma \in \Gamma$ and for all $\varphi_1, \varphi_2 \in L^2(\Gamma\backslash G)^K$, we have that $\langle T_\Gamma(\gamma)\varphi_1, \varphi_2\rangle = \langle \pi(\gamma)\varphi_1, \varphi_2\rangle$.

Proof Let us show the first claim. Recalling that $\mu = \nu * \mathrm{Unif}_{\Omega_0} * \nu$, for $\varphi \in L^2(\Gamma\backslash G)^K$ and $\xi, \gamma \in G$, we have that

$$\begin{aligned}\mathcal{A}_{\Gamma,\mu}\varphi(\Gamma\xi) &= \int_G \varphi(\Gamma\xi\gamma)\, d\mu(\gamma) = \int_{K\times\Omega_0\times K} \varphi(\Gamma\xi k_1\gamma k_2)\, d\nu(k_1) d\mathrm{Unif}_{\Omega_0}(\gamma) d\nu(k_2)\\ &= \frac{1}{2(n+2)} \sum_{\gamma\in\Omega_0} \int_K \varphi(\Gamma\xi k\gamma)\, d\nu(k) = \frac{1}{2(n+2)} \sum_{\gamma\in\Omega_0} T_\Gamma(\gamma)\varphi(\Gamma\xi),\end{aligned}$$

where the third equality follows since φ is a K-fixed vector and the last identity follows from the definition of $T_\Gamma(\gamma)$. Hence, the first claim holds. The second claim follows from a formal computation based on the right-invariance of the Haar measure on $\Gamma\backslash G$, so we omit the details. ■

Let us denote by $\ell_0^2(\Gamma\backslash\mathcal{S}_n)$ the orthogonal complement to the space of constant functions in $\ell^2(\Gamma\backslash\mathcal{S}_n)$. Note that $\mathcal{A}_{\Gamma,\mu}$ acts on $\ell_0^2(\Gamma\backslash\mathcal{S}_n)$ since the operator is self-adjoint. Given the right representation $(\pi, L^2(\Gamma\backslash G))$, letting $L_0^2(\Gamma\backslash G)$ be the orthogonal complement to constant functions in $L^2(\Gamma\backslash G)$, we define $(\pi_0, L_0^2(\Gamma\backslash G))$ by restricting π to $L_0^2(\Gamma\backslash G)$. The space $\ell_0^2(\Gamma\backslash\mathcal{S}_n)$ is identified with the space of K-fixed vectors in $L_0^2(\Gamma\backslash G)$ under the identification between $\ell^2(\Gamma\backslash\mathcal{S}_n)$ and $L^2(\Gamma\backslash G)^K$. It is crucial that π_0 has no nonzero invariant vector.

https://doi.org/10.4153/S0008414X23000676 Published online by Cambridge University Press

Proposition 5.3 *For every $n \geq 1$, let Γ be a closed subgroup of $G = PGSp_n(F)$ such that $\Gamma\backslash\mathcal{S}_n$ is finite. For all $\varphi \in \ell_0^2(\Gamma\backslash\mathcal{S}_n)$ with $\|\varphi\| = 1$, we have that*

$$\langle (I - \mathcal{A}_{\Gamma,\mu})\varphi, \varphi\rangle \geq \frac{1}{4(n+2)}\kappa(G,\Omega)^2,$$

where $\kappa(G,\Omega)$ is the optimal Kazhdan constant for the pair (G,Ω).

Proof For $\varphi \in \ell_0^2(\Gamma\backslash\mathcal{S}_n)$, it follows that $\langle (I - \mathcal{A}_{\Gamma,\mu})\varphi, \varphi\rangle$ equals

$$\langle \varphi, \varphi\rangle - \frac{1}{2(n+2)}\sum_{\gamma\in\Omega_0}\langle \pi(\gamma)\varphi, \varphi\rangle = \frac{1}{4(n+2)}\sum_{\gamma\in\Omega_0}\|\varphi - \pi_0(\gamma)\varphi\|^2,$$

where identifying φ with a K-fixed vector, we have used Lemma 5.2, and the equality follows since π_0 is the restriction of π and

$$\|\varphi - \pi_0(\gamma)\varphi\|^2 = \langle \varphi, \varphi\rangle - \langle \pi_0(\gamma)\varphi, \varphi\rangle - \langle \pi_0(\gamma^{-1})\varphi, \varphi\rangle + \langle \pi_0(\gamma)\varphi, \pi_0(\gamma)\varphi\rangle,$$

and $\pi_0(\gamma)$ is unitary, and furthermore $\gamma \in \Omega_0$ if and only if $\gamma^{-1} \in \Omega_0$. Moreover, we have that

$$\sum_{\gamma\in\Omega_0}\|\varphi - \pi_0(\gamma)\varphi\|^2 \geq \max_{\gamma\in\Omega_0}\|\varphi - \pi_0(\gamma)\varphi\|^2 = \max_{\gamma\in\Omega}\|\varphi - \pi_0(\gamma)\varphi\|^2,$$

which follows from the first claim of Lemma 5.1(2) and since φ is a K-fixed vector and π_0 is a unitary representation. Therefore, we obtain

$$\langle (I - \mathcal{A}_{\Gamma,\mu})\varphi, \varphi\rangle \geq \frac{1}{4(n+2)}\max_{\gamma\in\Omega}\|\varphi - \pi_0(\gamma)\varphi\|^2.$$

Since π_0 has no nonzero invariant vector, we conclude the claim. ∎

Theorem 5.4 *If we fix an integer $n \geq 2$, then there exists a positive constant $c_n > 0$ such that for any closed subgroup Γ in $PGSp_n(F)$ with finite quotient $\Gamma\backslash\mathcal{S}_n$, we have $\lambda_2(\Delta_{\Gamma,\mu}) \geq c_n$, where $\Delta_{\Gamma,\mu} = I - \mathcal{A}_{\Gamma,\mu}$.*

Proof Since we have that $\lambda_2(\Delta_{\Gamma,\mu}) = \inf_{\varphi\in\ell_0^2(\Gamma\backslash\mathcal{S}_n),\ \|\varphi\|=1}\langle (I - \mathcal{A}_{\Gamma,\mu})\varphi, \varphi\rangle$, Proposition 5.3 implies that $\lambda_2(\Delta_{\Gamma,\mu}) \geq (4(n+2))^{-1}\kappa(G,\Omega)^2$. Furthermore, $\kappa(G,\Omega) > 0$ since $G = PGSp_n(F)$ has Property (T) if $n \geq 2$ and Ω is a compact generating set of G by Lemma 5.1(1) (cf. Section 5.1). Letting $c_n := (4(n+2))^{-1}\kappa(G,\Omega)^2$, we obtain the claim. ∎

The proof of Theorem 1.1 now follows from Theorem 5.4 with Γ applied to $G_g(\mathbb{Z}[1/\ell])$ modulo the center and Corollary 3.2.

5.4 An explicit lower bound for the spectral gap

Appealing to the results by Oh [Oh02], we obtain explicit lower bounds for the second smallest eigenvalues of Laplacians on the graphs $\mathcal{G}_g^{SS}(\ell, p)$ for $g \geq 2$.

Corollary 5.5 *For every integer $g \geq 2$, for all primes ℓ and p with $p \neq \ell$,*

$$\lambda_2\left(\mathcal{G}_g^{SS}(\ell,p)\right) \geq \frac{1}{4(g+2)}\left(\frac{\ell-1}{2(\ell-1)+3\sqrt{2\ell(\ell+1)}}\right)^2.$$

Proof We keep the notations in the preceding subsections and put $n = g$. Let $F := \mathbb{Q}_\ell$. Note that Ω^2 contains K and a^2. The definition of the optimal Kazhdan constant shows that

$$\kappa\left(G, \Omega^2\right) \geq \kappa\left(PSp_n(\mathbb{Q}_\ell), \Omega^2 \cap PSp_n(\mathbb{Q}_\ell)\right).$$

Furthermore, the right-hand side is at least $\kappa\left(Sp_n(\mathbb{Q}_\ell), \Omega_*\right)$, where

$$\Omega_* := \{Sp_n(\mathbb{Z}_\ell), s\} \quad \text{and} \quad s := \mathrm{diag}(\ell^{-1}, \dots, \ell^{-1}; \ell, \dots, \ell).$$

Applying [Oh02, Theorem 8.4] to $Sp_n(\mathbb{Q}_\ell)$ for $n \geq 2$ with a maximal strongly orthogonal system L in the case of $C_n(n \geq 2)$ [Oh02, Appendix], we have that

$$\kappa\left(Sp_n(\mathbb{Q}_\ell), \Omega_*\right) \geq \chi_{\mathrm{L}}(s) = \frac{\sqrt{2(1-\xi_{\mathrm{L}}(s))}}{\sqrt{2(1-\xi_{\mathrm{L}}(s))}+3},$$

where

$$\xi_{\mathrm{L}}(s) \leq \frac{2(\ell-1)+(\ell+1)}{\ell(\ell+1)} = \frac{3\ell-1}{\ell(\ell+1)}.$$

Hence, we have for all $n \geq 2$ and all prime ℓ,

$$\kappa\left(Sp_n(\mathbb{Q}_\ell), \Omega_*\right) \geq \frac{\sqrt{2}(\ell-1)}{\sqrt{2}(\ell-1)+3\sqrt{\ell(\ell+1)}},$$

and since $\kappa(G, \Omega) \geq (1/2)\kappa(G, \Omega^2)$, we obtain

$$\kappa(G, \Omega) \geq \frac{\ell-1}{2(\ell-1)+3\sqrt{2\ell(\ell+1)}}.$$

Combining the above inequality with $c_n = (4(n+2))^{-1}\kappa(G, \Omega)^2$ in the proof of Theorem 5.4, we conclude that for all $n \geq 2$ and all prime ℓ,

$$\lambda_2(\Delta_{\Gamma,\mu}) \geq \frac{1}{4(n+2)}\left(\frac{\ell-1}{2(\ell-1)+3\sqrt{2\ell(\ell+1)}}\right)^2.$$

Applying to the case when Γ is $G_g(\mathbb{Z}[1/\ell])$ modulo the center together with Corollary 3.2 yields the claim. ∎

Acknowledgment We would like to thank Professors Yevgeny Zaytman and Bruce Jordan for informing us of issues in the first version of this paper and correcting references; the current version has been revised substantially since then – we greatly acknowledge them for their comments. We would also like to thank Professor Tsuyoshi Takagi for many helpful discussions and encouragement, and Professor Ken-ichi Kawarabayashi for fostering an ideal environment which made this collaboration possible.

References

[BHV08] B. Bekka, P. de la Harpe, and A. Valette, *Kazhdan's property (T)*, New Mathematical Monographs, 11, Cambridge University Press, Cambridge, 2008.

[CDS20] W. Castryck, T. Decru, and B. Smith, *Hash functions from superspecial genus-2 curves using Richelot isogenies*. J. Math. Cryptol. **14**(2020), no. 1, 268–292.

[CF90] C-L. Chai and G. Faltings, *Degeneration of abelian varieties*, with an appendix by David Mumford, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], 22, Springer, Berlin, 1990, xii + 316 pp.

[CGL09] D.-X. Charles, K. Lauter, and E.-Z. Goren, *Cryptographic hash functions from expander graphs*. J. Cryptol. **22**(2009), no. 1, 93–113.

[EGM] B. Edixhoven, G. van der Geer, and B. Moonen, *Abelian varieties*. Draft for a book on abelian varieties. Available at http://page.mi.fu-berlin.de/elenalavanda/BMoonen.pdf.

[Fal84] G. Faltings, *Finiteness theorems for abelian varieties over number fields*. In: E. Shipz (ed.), Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 9–27.

[FS21] E. Florit and B. Smith, *An atlas of the Richelot isogeny graph*. RIMS Kôkyûroku Bessatsu. **B90**(2022), 195–219.

[FS22] E. Florit and B. Smith, *Automorphisms and isogeny graphs of abelian varieties, with applications to the Superspecial Richelot isogeny graph*. In: Arithmetic, geometry, cryptography, and coding theory 2021, Contemporary Mathematics, 779, American Mathematical Society, Providence, RI, 2022, pp. 103–132.

[Gar97] P. Garrett, *Buildings and classical groups*, Chapman & Hall, London, 1997, xii + 373 pp.

[Ghi04] A. Ghitza, *Hecke eigenvalues of Siegel modular forms (mod p) and of algebraic modular forms*. J. Number Theory **106**(2004), no. 2, 345–384.

[Ibu20] T. Ibukiyama, *Principal polarizations of supersingular abelian surfaces*. J. Math. Soc. Japan. **72**(2020), no. 4, 1161–1180.

[IKO86] T. Ibukiyama, T. Katsura, and F. Oort, *Supersingular curves of genus two and class numbers*. Compos. Math. **57**(1986), no. 2, 127–152.

[JZ21] B.-W. Jordan and Y. Zaytman, *Isogeny graphs of superspecial abelian varieties and Brandt matrices*. Preprint, 2023. arXiv:2005.09031

[KT20] T. Katsura and K. Takashima, *Counting Richelot isogenies between superspecial abelian surfaces*. In: S. D. Galbraith (ed.), Proceedings of the fourteenth algorithmic number theory symposium. Vol. 4, The Open Book Series, 1, Mathematical Sciences Publishers, Berkeley, CA, 2020, pp. 283–300.

[LO98] K.-Z. Li and F. Oort, *Moduli of supersingular abelian varieties*, Lecture Notes in Mathematics, 1680, Springer, Berlin, 1998, iv + 116 pp.

[LP16] E. Lubetzky and Y. Peres, *Cutoff on all Ramanujan graphs*. Geom. Funct. Anal. **26**(2016), no. 4, 1190–1216.

[Mil86] J.-S. Milne, *Abelian varieties*. In: Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150.

[Mum70] D. Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, 5, Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London, 1970, viii + 242 pp.

[Oh02] H. Oh, *Uniform pointwise bounds for matrix coefficients of unitary representations and applications to Kazhdan constants*. Duke Math. J. **113**(2002), no. 1, 133–192.

[Piz90] A.-K. Pizer, *Ramanujan graphs and Hecke operators*. Bull. Amer. Math. Soc. (N.S.) **23**(1990), no. 1, 127–137.

[Piz98] A.-K. Pizer, *Ramanujan graphs*. In: Computational perspectives on number theory (Chicago, IL, 1995), AMS/IP Studies in Advanced Mathematics, 7, American Mathematical Society, Providence, RI, 1998, pp. 159–178.

[PR94] V. Platonov and A. Rapinchuk, *Algebraic groups and number theory*, Translated from the 1991 Russian original by Rachel Rowen, Pure and Applied Mathematics, 139, Academic Press, Boston, MA, 1994, xii + 614 pp.

[She07] T. R. Shemanske, *The arithmetic and combinatorics of buildings for* Sp_n. Trans. Amer. Math. Soc. **359**(2007), no. 7, 3409–3423.

[Sil09] J.-H. Silverman, *The arithmetic of elliptic curves*. 2nd ed., Graduate Texts in Mathematics, 106, Springer, Dordrecht, 2009, xx + 513 pp.

[Tate66] J. Tate, *Endomorphisms of abelian varieties over finite fields*. Invent. Math. **2**(1966), 134–144.

[Gee08] G. van der Geer, *Siegel modular forms and their applications*. In: The 1–2–3 of modular forms, Universitext, Springer, Berlin, 2008, pp. 181–245.

Graduate School of Information Science and Technology, The University of Tokyo, Tokyo 113-8656, Japan
e-mail: aikawa@mist.i.u-tokyo.ac.jp

Department of Mathematics, Kyoto University, Kyoto 606-8502, Japan
e-mail: rtanaka@math.kyoto-u.ac.jp

Mathematical Institute, Tohoku University, Sendai 980-8578, Japan
e-mail: takuya.yamauchi.c3@tohoku.ac.jp