

# 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  $\ell$  and  $p$  with  $\ell \neq p$ , finite regular directed graphs associated with the set of equivalence classes of  $\ell$ -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  $g \geq 2$ , and discuss optimal values in view of the theory of automorphic representations when  $g = 2$ . As a by-product, we also show that the finite regular directed graphs constructed by Jordan-Zaytman also has the same property.

## CONTENTS

1. Introduction	2
1.1. Main Theorems	3
1.2. Motivation from isogeny-based cryptography	6
1.3. Organization of this paper	10
1.4. Notations	10
Acknowledgements	10
2. Superspecial abelian varieties	11
2.1. Superspecial abelian varieties	11
2.2. Principal polarizations	11
2.3. Class number of the principal genus for quaternion Hermitian lattices	14
2.4. Ibukiyama-Katsura-Oort-Serre's result in terms of adelic language	15
2.5. Another formulation due to Jordan-Zaytman	17

---

*Date:* March 21, 2022.

*Key words and phrases.* Isogeny graphs, cryptographic hash functions, automorphic forms.

2.6.	The Hecke operator at $\ell$	20
2.7.	The Hecke action and automorphisms	21
3.	A comparison between two graphs	24
3.1.	Jordan-Zaytman's big isogeny graph	24
3.2.	The ( $\ell$ -marked) ( $\ell$ ) <sup>g</sup> -isogeny graph	24
3.3.	The graph defined by the special 1-complex	25
3.4.	Comparison theorem	25
4.	Bruhat-Tits buildings for symplectic groups	26
4.1.	Symplectic groups revisited for the buildings	26
4.2.	Bruhat-Tits building: the construction	27
4.3.	Apartments	29
4.4.	Self-dual vertices	31
4.5.	Special vertices and the special 1-complex	32
5.	Property (T) and spectral gaps	34
5.1.	Property (T)	34
5.2.	A random walk operator	34
5.3.	Spectral gap	38
5.4.	An explicit lower bound for the spectral gap	41
6.	Some remarks on Algebraic modular forms for $GUSp_g$	42
6.1.	Gross's definition	43
6.2.	A speculation for bounds of eigenvalues of $T(\ell)$	44
6.3.	Not being Ramanujan is not necessary fared	45
	References	46

## 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 consist 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  $\ell$ . 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  $g$  be a positive integer. Fix an algebraically closed field  $\overline{\mathbb{F}}_p$  of the finite field  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ . 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 denote such an abelian variety  $A$  endowed with the principal polarization  $\mathcal{L}$  which is an ample line bundle  $\mathcal{L}$  on  $A$  with the trivial Euler-Poincaré characteristic. For a principally polarized superspecial abelian variety  $(A, \mathcal{L})$  we write  $[(A, \mathcal{L})]$  for the class of  $(A, \mathcal{L})$  in  $SS_g(p)$ . It is known that  $SS_g(p)$  is a finite set and more precisely that

$$C_1(g)p^{g(g+1)/2} \leq |SS_g(p)| \leq C_2(g)p^{g(g+1)/2}$$

for all large enough  $p$  and for some positive constants  $C_1(g)$  and  $C_2(g)$  depending only on  $g$  (it follows from the mass formula (1.2) in p.1419 of [Yu12]).

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  $\phi_A : A_0 \rightarrow A$  of  $\ell$ -power degree such that  $\text{Ker}(\phi_A)$  is a maximal totally isotropic subspace of  $A[\ell^n]$  for some  $n \geq 0$  (it follows from Theorem 2.7 in Section 2.5 in this paper and Theorem 34 of [JZ21]). We call  $\phi_A$  an  $\ell$ -marking of  $(A, \mathcal{L})$  from  $(A_0, \mathcal{L}_0)$ . Two  $\ell$ -markings of  $(A, \mathcal{L})$  from  $(A_0, \mathcal{L}_0)$  differ by only an element in

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

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

We define

$$(1.1) \quad SS_g(p, \ell, A_0, \mathcal{L}_0) := \{(A, \mathcal{L}, \phi_A)\} / \sim$$

where  $[(A, \mathcal{L})] \in SS_g(p)$  and  $\phi_A$  is an  $\ell$ -marking from  $(A_0, \mathcal{L}_0)$ . Here 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  $f : (A_1, \mathcal{L}_1) \rightarrow (A_2, \mathcal{L}_2)$  such that  $f \circ \phi_{A_1}$  and  $\phi_{A_2}$  differ by only an element of  $\Gamma(A_0)^\dagger$  in which case we write  $(A_1, \mathcal{L}_1, \phi_{A_1}) \sim (A_2, \mathcal{L}_2, \phi_{A_2})$ . We write  $[(A, \mathcal{L}, \phi_A)] \in SS_g(p, \ell, A_0, \mathcal{L}_0)$  for the class of  $(A, \mathcal{L}, \phi_A)$  where  $(A, \mathcal{L})$  is a principally polarized superspecial abelian variety with an  $\ell$ -marking  $\phi_A$  from  $(A_0, \mathcal{L}_0)$ . 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  $f_C : A \rightarrow A_C$  is called an  $(\ell)^g$ -isogeny (see Proposition 2.1 and Definition 2.3). 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  $A$ .

We are now ready to define the  $(\ell)$ -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 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 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  $\ell$ -markings  $\phi_{A_1} : (A_0, \mathcal{L}_0) \rightarrow (A_1, \mathcal{L}_1)$  and  $\phi_{A_2} : (A_0, \mathcal{L}_0) \rightarrow (A_2, \mathcal{L}_2)$  respectively, then an edge from  $v_1$  to  $v_2$  is an  $(\ell)^g$ -isogeny  $f : (A_1, \mathcal{L}_1) \rightarrow (A_2, \mathcal{L}_2)$  such that two markings  $f \circ \phi_{A_1}$  and  $\phi_{A_2}$  of  $(A_2, \mathcal{L}_2)$  from  $(A_0, \mathcal{L}_0)$  differ by an element of  $\Gamma(A_0)^\dagger$ .

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). Our first main result is the following:

**Theorem 1.1.** *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  $\mathcal{G}_g^{SS}(\ell, p)$  has the second largest eigenvalue of the normalized Laplacian satisfying that*

$$\lambda_2(\mathcal{G}_g^{SS}(\ell, p)) \geq c_{g,\ell} > 0,$$

where  $c_{g,\ell}$  is a positive constant depending only on  $g$  and  $\ell$ .

We defined the normalized Laplacian  $\Delta$  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  $\Delta$  has the simple smallest eigenvalue 0 provided that the graph is strongly connected, i.e., there exists a directed edge path from any vertex to any other vertex. In Theorem 1.1, we actually have an explicit lower bound for  $\lambda_2$ : For

every integer  $g \geq 2$ , for all primes  $\ell$  and  $p$  with  $p \neq \ell$ ,

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

(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 Subsection 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 2.7 and Section 4.5). 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 Section 2 and Section 3 that there exist natural identifications

$$SS_g(p) \xleftarrow{1:1} SS_g(p, \ell, A_0, \mathcal{L}_0) \xrightarrow{1:1} \Gamma \backslash \mathcal{S}_g$$

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  $\Gamma \backslash \mathcal{S}_g$ .

It follows from this that 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  $\ell \neq p$ , a 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 [FS21b, Theorem 4.9].

We discuss some theoretical features for each of our work and previous works due to Pizer and Jordan-Zaytman. Instead of using  $Gr_1(\ell, p)$ , Pizer handled the moduli space of supersingular elliptic curves with non-trivial levels to avoid that non-trivial automorphisms happen (see [Piz98], [Piz90]). Therefore, his graphs are regular undirected graphs so that they are Ramanujan by Eichler's theorem via Jacquet-Langlands theory. However, if  $p \equiv 1 \pmod{12}$ , then each vertex of  $Gr_1(\ell, p)$  does not have non-trivial automorphisms other than  $-1$ .

Jordan-Zaytman's graphs  $Gr_g(\ell, p)$  are useful and fit into the computational implementations (cf. [CDS20], [KT20], [FS21a], [FS21b]) 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 non-trivial level 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 largely motivated by a possible approach to cryptographic hash functions from isogeny graphs. Let us begin with a brief review of the notation of hash functions, which are widely used in computer science. For a general reference on hash functions in cryptographic context, see Chapter 5 of [KL14] for example.

A hash function  $H$  is an efficiently computable function taking as input a message of any length and outputting a value of fixed length  $s$ , i.e.  $H : \{0, 1\}^* \rightarrow \{0, 1\}^s$ , where  $\{0, 1\}^* = \cup_{n=1}^{\infty} \{0, 1\}^n$ . A standard condition required for hash functions in cryptography is collision resistance; it is computationally hard for any probabilistic polynomial-time algorithm to find a pair of distinct messages  $(m_1, m_2)$  such that  $H(m_1) = H(m_2)$ . Collision resistant hash functions have numerous applications in cryptography. For example, such functions are used as components of pseudo-random generators, Hash-based Message Authentication Code, digital signatures and so on.

However, despite its importance, it is hard to construct such a function because to design a collision resistant hash function requires suitable mixing and compressing bit strings of any length. As one can see in [Gol11], [CGL09], there is an approach to design hash functions by employing expander graphs on which random walks mix rapidly. Due to Pizer's work [Piz90], [Piz98], isogeny graphs of supersingular elliptic curves have attracted attention as a tool for realizing a good expansion property. In this subsection, we explain this research direction and state our research question.

*CGL hash functions.* Let  $p$  and  $\ell$  be distinct prime numbers. Moreover, we impose  $p \equiv 1 \pmod{12}$ . In this case, the vertices on  $Gr_1(\ell, p)$  have no automorphism other than  $\pm 1$ . Charles, Goren and Lauter [CGL09] proposed construction of hash functions based on  $Gr_1(\ell, p)$ .

We explain the recipe of their construction of a hash function from the graph  $Gr_1(2, p)$  as follows. Let  $E_0 : y^2 = f(x)$  be a fixed curve in  $SS_1(p)$  where  $f(x)$  is a monic cubic, and  $(E_0, E_{-1})$  be a fixed edge. We remark that the edges are undirected due to the existence of the dual isogeny.

The non-trivial 2-torsion points are points  $P_i^0 = (x_i, 0)$  where  $x_i$  are roots of the cubic  $f(x)$  for  $i = 0, 1, 2$ . Subgroups generated by each  $P_i$  lead 2-isogenies outgoing from  $E_0$ . Here, the points are numbered by some order of  $\mathbb{F}_{p^2}$  and we suppose that the edge  $(E_{-1}, E_0)$  corresponds to the subgroup  $\langle P_2 \rangle$ . Let  $m = (m_{n-1}, \dots, m_0) \in \{0, 1\}^n$  be a random  $n$ -bit message. The message  $m$  determines a non-backtracking walk <sup>1</sup> on  $Gr_1(2, p)$  in the following way.

First, we compute an isogeny  $\phi_0 : E_0 \rightarrow E_1$  with kernel  $\langle P_{m_0}^0 \rangle$  by using Vélu's formula [Vél71]. Second, we have non-trivial three 2-torsion points on  $E_1$  and we number one of them corresponding the dual of  $\phi_0$  with  $P_2^1$ . The remaining two 2-torsion points are numbered by the order in  $\mathbb{F}_{p^2}$ ;  $P_0^1$  and  $P_1^1$ . Then, we do a similar procedure for  $E_1$  and obtain  $E_2$  by computing the isogeny with kernel generated by  $P_{m_1}^0$ . Finally, by repeating this computation, the end-point  $E_n \in SS_1(p)$  is obtained as the terminal of the sequence of supersingular elliptic curves  $(E_0, E_1, \dots, E_{n-1})$  such that  $j_{E_{i-1}} \neq j_{E_i}$  for  $i = 1, \dots, n-1$ . To get a compressed value of  $m$  from  $E_n$ , in [CGL09], the authors propose using some linear function  $f : \mathbb{F}_{p^2} \rightarrow \mathbb{F}_p$ ; that is,  $H(m) := f(j_{E_n})$ . In this way, we construct the function  $H : \{0, 1\}^* \rightarrow \{0, 1\}^{\lfloor \log_2(p) \rfloor + 1}$  from non-backtracking random walks on  $\mathcal{G}_1^{SS}(2, p)$ , which is called CGL hash function now. In a similar fashion, the hash function using 3-isogeny is also investigated in [TTT17].

The Ramanujan property of  $Gr_1(2, p)$  for  $p \equiv 1 \pmod{12}$  guarantees efficient mixing processing of these functions (for most precise results, see [LP16, Theorems 1 and 3.5]). In view of security of these functions, the collision resistant property is supported by assumptions on hardness of computing a chain of isogenies between given isogenous supersingular elliptic curves. Indeed, finding collisions yield to pairs of supersingular elliptic curves  $(E, E')$  and two chains of  $\ell$ -isogenies between them whose kernels are distinct each other.

*Isogeny-based Cryptography.* We provide a little bit about the recent progress in public-key cryptography using supersingular isogenies. The above construction of the cryptographic hash function from supersingular isogenies opens the door to a new research area of practical public key cryptography whose security relies on computational hardness of computing isogenies between given two supersingular elliptic curves. Public key cryptography in such style is called isogeny-based cryptography now.

---

<sup>1</sup>To avoid trivial collision, we impose the condition of non-backtrack on walks in this construction.

Here, what is important is that there is currently no known polynomial-time (even quantum) algorithm to compute an isogeny between given two supersingular elliptic curves unlike the integer factorization problem or the discrete logarithm problem. Indeed, an isogeny-based cryptography is regarded as an important object in the context of post-quantum cryptography: it has been proposed as cryptographic primitives, for example, SIDH (Supersingular Isogeny Diffie-Hellman)[DJP14, JD11] and CSIDH (Commutative Supersingular Isogeny Diffie-Hellman)[CLM+18]. Therefore, isogeny-based cryptography is one of the promising candidates of post-quantum cryptography among lattice-based cryptography, code-based cryptography and multivariate cryptography.

*Toward higher dimensional analogue of CGL hash functions.* There have been several studies on the big isogeny graph  $Gr_g(\ell, p)$  defined in [JZ21] from both number theoretic and cryptographic viewpoints. In the rest of this section, we describe recent progress in studies on the graphs  $Gr_g(\ell, p)$  and a contribution of our work in this context.

Concerning the two dimensional case, the CGL-like construction of hash functions was first attempted by Takashima [Tak18], which used the supersingular  $(2)^2$ -isogeny graph (*i.e.*, the case when  $g = 2$  and  $\ell = 2$ ). However, Flynn and Ti [FT19] showed that this graph has many short cycles from which trivial collisions of random walks may be derived. After these works, Castryck, Decru and Smith [CDS20] modified Takashima's construction and suggested to use a subgraph of isogeny graphs  $Gr_2(2, p)$  of superspecial abelian varieties consisting of Jacobians of curves of genus 2. The idea here is to keep choosing paths to become good extension, which allow us to avoid trivial collisions. Moreover, they counted the number of good extensions of a  $(2)^2$ -isogeny (see Proposition 3 in [CDS20]). There are eight good extensions for an isogeny between Jacobians, which are suitable for associating 3-bit information to one step of a random walk.

In the case of abelian varieties of dimension  $\geq 2$ , the existence of nontrivial automorphisms complicates the structure of graphs. 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, in the case when  $g = 2$  and  $\ell = 2$ , Katsura and Takashima [KT20] counted the number of Richelot isogenies and decomposed Richelot isogenies up to isomorphism outgoing from Jacobians and those outgoing from elliptic products and computed the multiplicity of each edge. Moreover, advancing this work further, Florit and Smith [FS21a] studied the local neighborhoods of vertices and edges in  $Gr_2(2, p)$  and gave many illustrations. In [FS21b], 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. Our contribution is to give an affirmative answer to this question in Theorem 1.1 and Theorem 1.2. In this paper, good mixing property of the big isogeny  $Gr_g(\ell, p)$  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  $Gr_g(\ell, p)$ . So, 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  $Gr_g(\ell, p)$ , which have been investigated, may be suitable for construction of cryptographic hash functions from superspecial abelian varieties.

Finally, we give an example of an illustration of a graph considered in this paper, i.e.  $\mathcal{G}_g^{SS}(\ell, p)$ , which is equivalent to the big isogeny graph  $Gr_g(\ell, p)$ . For  $\ell = 2$  and  $p = 13$ , the graph  $Gr_g(\ell, p)$  is computed in [CDS20] and [KT20] as illustrated below.

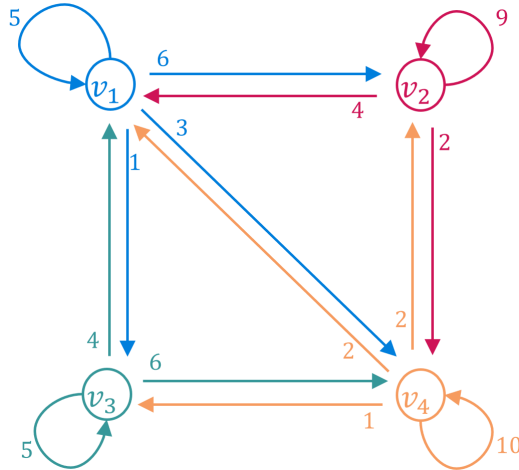


FIGURE 1.1. An illustration of  $Gr_2(2, 13)$ . The vertices  $v_1$ ,  $v_2$  and  $v_3$  denote the Jacobians of curves defined by  $C_1 : y^2 = (x^3 - 1)(x^3 + 4 - \sqrt{2})$ ,  $C_2 : y^2 = x(x^2 - 1)(x^2 + 5 + 2\sqrt{6})$  and  $C_3 : y^2 = x^5 - x$ , respectively. The vertex  $v_4$  denotes the product of supersingular elliptic curves  $y^2 = (x - 1)(x - 3 + 2\sqrt{2})$ . The number on the side of a directed edge denotes the multiplicity of each edge. For a more detailed illustration, see §7.1 of [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  $\ell$  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. Finally, in Section 6.1 we give a speculation in view of the theory of automorphic forms.

**1.4. Notations.** For a set  $X$ , the cardinality is denoted by  $|X|$ . Throughout the paper, we use the Landau asymptotic notations: for positive real-valued functions  $f(n)$  and  $g(n)$  for integers  $n$ , we denote by  $f(n) = o(g(n))$  if  $f(n)/g(n) \rightarrow 0$  as  $n \rightarrow \infty$ , by  $f(n) = O(g(n))$  if there exists a positive constant  $C > 0$  such that  $f(n) \leq Cg(n)$  for all large enough  $n$ , and  $f(n) = \Theta(g(n))$  if we have both  $f(n) = O(g(n))$  and  $g(n) = O(f(n))$ .

Let  $n$  be a positive integer and  $I_n$  the identity matrix of size  $n$ . Put

$$J_n = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}.$$

We define a functor  $G : (\text{Rings}) \rightarrow (\text{Sets})$  from the category of rings to the category of sets by

$$G(R) := \{M \in M_{2n}(R) \mid {}^t M J_n M = \nu(M) M, \text{ for some } \nu(M) \in R^\times\}$$

for each commutative ring  $R$  and we call  $\nu(M)$  the similitude of  $M$ . It is well-known that the functor  $G$  is represented by a smooth group scheme  $GS p_n$  over  $\mathbb{Z}$ . The similitude defines a homomorphism  $\nu : GS p_n \rightarrow GL_1$  as group schemes over  $\mathbb{Z}$ . We define  $Sp_n := \text{Ker}(\nu)$  which is called the symplectic group of rank  $n$ . The similitude splits and in fact it is given by  $a \mapsto \text{diag}(I_n, aI_n)$ . It follows from this that  $G \simeq Sp_n \times GL_1$ . In the sections related to abelian varieties, we put  $n = g$  while we keep  $n$  in Section 4 through 5.

For any algebraic group  $H$  over a field, we denote by  $Z_H$  the center of  $H$ .

**Acknowledgements.** 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. 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) No.19H01778.

## 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  $\ell$ -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  $k$  be an algebraically closed field of a finite field of characteristic  $p$ . In our purpose, we may put  $k = \overline{\mathbb{F}}_p$ . Let  $A$  be an abelian variety over  $k$  of dimension  $g > 0$  and we denote by  $\widehat{A} = \text{Pic}^0(A)$  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 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  $\text{NS}(A) := \text{Pic}(A)/\text{Pic}^0(A)$  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 a homomorphism

$$\phi_{\mathcal{L}} : A \longrightarrow \widehat{A}, \quad x \mapsto t_x^*(\mathcal{L}) \otimes \mathcal{L}^{-1}$$

where  $t_x$  stands for the translation by  $x$  and we denote by  $t_x^*$  its pullback. By APPLICATION 1, p.60 in Section 6 of Chapter II in [Mum70],  $\phi_{\mathcal{L}}$  is an isogeny, hence it has a finite kernel since  $\mathcal{L}$  is ample. If we write  $D$  for an ample divisor on  $A$  corresponding to  $\mathcal{L}$ , namely,  $\mathcal{L} \simeq \mathcal{O}(D)$ , then by Riemann-Roch theorem in p.150 of loc.cit., we have

$$(2.1) \quad \chi(\mathcal{L}) = \frac{(D^g)}{g!}, \quad \chi(\mathcal{L})^2 = \deg \phi_{\mathcal{L}}$$

where  $\chi(\mathcal{L})$  stands for the Euler-Poincare characteristic of  $\mathcal{L}$  and  $(D^g)$  is the  $g$ -fold self-intersection number of  $D$ . Since  $\mathcal{L}$  is ample,  $\chi(\mathcal{L}) > 0$ .

**Definition 2.2.** *Keep the notation being as above.*

- (1) *An ample line bundle  $\mathcal{L} \simeq \mathcal{O}(D)$  on  $A$  is said to be a principal polarization if  $\deg \phi_{\mathcal{L}} = 1$ , equivalently,  $(D^g) = g!$ .*
- (2) *For a principal polarization  $\mathcal{L}$  on  $A$ , we call a couple  $(A, \mathcal{L})$  a principally polarized abelian variety. For two polarized abelian varieties  $(A_1, \mathcal{L}_1)$ ,  $(A_2, \mathcal{L}_2)$ , a morphism between them is a homomorphism  $f : A_1 \rightarrow A_2$  such that  $\phi_{\mathcal{L}_1} = \widehat{f} \circ \phi_{\mathcal{L}_2} \circ f$  where  $\widehat{f}$  is the dual of  $f$  defined by the pullback of  $f$  on line bundles. Since  $\widehat{f} \circ \phi_{\mathcal{L}_2} \circ f = \phi_{f^*\mathcal{L}_2}$ , the above condition is equivalent to  $\phi_{f^*\mathcal{L}_2} = \phi_{\mathcal{L}_1}$ .*

**Proposition 2.1.** *Let  $(A, \mathcal{L})$  be a principally polarized abelian variety in characteristic  $p$ . Let  $\ell$  be a prime number different from  $p$  and  $C$  be a maximal totally isotropic subspace of  $A[\ell^n]$  for  $n \in \mathbb{Z}_{\geq 0}$  with respect to the Weil pairing associated to  $\mathcal{L}$ . 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  $f_C : A \rightarrow A_C$  is the natural surjection.*

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

**Definition 2.3.** *Let  $(A_1, \mathcal{L}_1)$  and  $(A_2, \mathcal{L}_2)$  be two principally polarized abelian varieties in characteristic  $p$ . Let  $\ell$  be a prime different from  $p$ .*

- (1) *An isogeny  $f : A_1 \rightarrow A_2$  is said to be an  $(\ell)^g$ -isogeny if*
  - *$\text{Ker}(f)$  is a maximal totally isotropic subspace of  $A[\ell]$  with respect to the Weil pairing associated to  $\mathcal{L}_1$ , and*
  - *$f^*\mathcal{L}_2 \simeq \mathcal{L}_1^{\otimes \ell}$ .*
- (2) *An isogeny  $f : A_1 \rightarrow A_2$  is said to be an  $\ell$ -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 2.3. Let  $f : A_1 \rightarrow A_2$  be an  $\ell$ -marking of  $(A_2, \mathcal{L}_2)$  from  $(A_1, \mathcal{L}_1)$ , then there exists an  $\ell$ -marking  $\tilde{f} : A_2 \rightarrow A_1$  of  $(A_1, \mathcal{L}_1)$  from  $(A_2, \mathcal{L}_2)$  such that  $f \circ \tilde{f} = [\ell^m]_{A_2}$  and  $\tilde{f} \circ f = [\ell^m]_{A_1}$  for some integer  $m \geq 0$ .*

*Proof.* By Theorem 34 of [JZ21], we may assume  $f$  is an  $(\ell)^g$ -isogeny. Put  $C = \text{Ker } f$ . 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 to  $\mathcal{L}_{A_{1,C}}$ . Therefore, we have an  $(\ell)^g$ -isogeny  $\tilde{f} : A_2 \rightarrow A_{1,C}/D$ . 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  $\tilde{f}$  is symmetric and hence we have the claim.  $\square$

We study the difference of two  $\ell$ -markings. Let us keep the notation in Definition 2.3. By using the principal polarization  $\mathcal{L}_1$  we define the Rosati-involution  $\dagger$  on  $\text{End}(A_1)$  by

$$(2.4) \quad f^\dagger = \phi_{\mathcal{L}_1}^{-1} \circ \widehat{f} \circ \phi_{\mathcal{L}_1}, \quad f \in \text{End}(A_1).$$

Notice that  $\dagger$  is an anti-involution.

**Proposition 2.3.** *Let us still keep the notation in Definition 2.3. Let  $f, h : A_1 \rightarrow A_2$  be two  $\ell$ -markings. Then there exists  $\psi \in \text{End}(A_1) \otimes \mathbb{Z}[1/\ell]$  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  $\tilde{f} : A_2 \rightarrow A_1$  be an  $(\ell)^g$ -isogeny in Proposition 2.2. Put  $\psi_1 = \tilde{f} \circ h \in \text{End}(A_1)$ . Then we have, by definition,

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

It follows from Theorem 34 of [JZ21] and Definition 2.3 that  $\widehat{\tilde{f}} \circ \phi_{\mathcal{L}_1} \circ \tilde{f} = \phi_{\mathcal{L}_2^{\otimes \ell^m}} = \ell^m \phi_{\mathcal{L}_2}$  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

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

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

**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  $n$  be a positive integer. Let  $B$  be the definite quaternion algebra ramified only at  $p$  and  $\infty$  (see Proposition 5.1, p.368 of [Piz80] for an explicit realization). We write  $B = \left(\frac{a, b}{\mathbb{Q}}\right) = \mathbb{Q} \cdot 1 \oplus \mathbb{Q} \cdot i \oplus \mathbb{Q} \cdot j \oplus \mathbb{Q} \cdot ij$  with  $i^2 = a$ ,  $j^2 = b$ , and  $ij = -ji$ . For each  $x = x_0 + x_1i + x_2j + x_3ij$ , the conjugation of  $x$  is defined by  $\bar{x} = x_0 - x_1i - x_2j - x_3ij$ . Then  $N(x) = x\bar{x}$ ,  $\text{Tr}(x) = x + \bar{x}$  are called the norm and the trace of  $x$  respectively. Let us fix a maximal order  $\mathcal{O}$  of  $B$  which is also explicitly given in Proposition 5.2 of [Piz80]. The pairing  $(*, *)$  on  $B^n$  is defined by the following manner:

$$(x, y) = \sum_{i=1}^n x_i \bar{y}_i \text{ for } x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in B^n.$$

A submodule  $L \subset B^n$  is said to be  $\mathcal{O}$ -lattice if

- $L$  is a  $\mathbb{Z}$ -lattice in  $B^n$ , hence  $L \otimes_{\mathbb{Z}} \mathbb{Q} = B^n$ ;
- $L$  is a left  $\mathcal{O}$ -module.

For an  $\mathcal{O}$ -lattice  $L$ , we define by  $N(L)$  the two sided (fractional) ideal of  $B$  generated by  $(x, y)$ ,  $x, y \in L$ . The ideal  $N(L)$  is called the norm of  $L$ .

For a commutative ring  $R$ , we extend the conjugation on  $\mathcal{O} \subset B$  to  $\mathcal{O} \otimes_{\mathbb{Z}} R$  by  $\overline{x \otimes r} := \bar{x} \otimes r$  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  $\bar{\gamma} := (\bar{\gamma}_{ij})$ . 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:

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

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  $G_n^1 := \text{Ker}(\nu)$  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.  $Sp_n$ ).

**Remark 2.4.** *Historically, automorphic forms on  $G_n^1 = USp_n$  for  $n \geq 2$  were studied by Ihara-Ibukiyama (see [Ibu18] and suitable references there). After Ibukiyama's joint works with Ihara, he and his collaborators have pursued an analogue of Jacquet-Langlands correspondence for  $GL_2$ .*

Let us keep introducing some notation. For two  $\mathcal{O}$ -lattices  $L_1, L_2$  of  $B^n$ , they are said to be globally equivalent (locally equivalent at a rational prime  $p$ ) if  $L_1 = L_2\gamma$  for some  $\gamma \in G_n(\mathbb{Q})$  ( $L_1 \otimes_{\mathbb{Z}} \mathbb{Z}_p = (L_2 \otimes_{\mathbb{Z}} \mathbb{Z}_p)\gamma$  for some  $\gamma \in G_n(\mathbb{Q}_p)$ ). We also say  $L_1$  and  $L_2$  belong to the same genus if  $L_1$  is locally equivalent to  $L_2$  for each rational prime  $p$ . For each  $\mathcal{O}$ -lattice  $L$ , we denote by  $\mathcal{L}(L)$  the set of all  $\mathcal{O}$ -lattices  $L_1$  such that  $L_1$  and  $L$  belong to the same genus. The set  $\mathcal{L}(L)$  is called a genus and we denote by  $\mathcal{L}(L)/\sim$  the set of globally equivalent classes of  $\mathcal{L}(L)$ .

**Definition 2.5.** For each  $\mathcal{O}$ -lattice  $L$ , the cardinality  $H(L)$  of  $\mathcal{L}(L)/\sim$  is called the class number of  $L$ . In particular,  $\mathcal{L}(\mathcal{O}^n)/\sim$  is said to be the principal genus class and put

$$H_n(p, 1) := H(\mathcal{O}^n) = |\mathcal{L}(\mathcal{O}^n)/\sim|.$$

Let  $\mathbb{A}_{\mathbb{Q}}$  be the ring of adèles of  $\mathbb{Q}$  and  $\mathbb{A}_f$  be the finite part of  $\mathbb{A}_{\mathbb{Q}}$ . For an  $\mathcal{O}$ -lattice  $L$  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  $G_n(\mathbb{A}_f)$ . For each element  $\gamma = (\gamma_p)_p$  of  $G_n(\mathbb{A}_{\mathbb{Q}})$  and an  $\mathcal{O}$ -lattice  $L$ , put

$$L\gamma := \bigcap_{p < \infty} L\gamma_p \cap B^n$$

and it is easy to see that  $L\gamma$  is also an  $\mathcal{O}$ -lattice which is locally equivalent to  $L$  at each prime  $p$ . Hence we have

$$(2.6) \quad K(L) \backslash G_n(\mathbb{A}_f) / G_n(\mathbb{Q}) \xrightarrow{\sim} \mathcal{L}(L) / \sim, \quad K(L)\gamma G_n(\mathbb{Q}) \mapsto [L\gamma]$$

where  $G(\mathbb{Q})$  is diagonally embedded in  $G_n(\mathbb{A}_f)$  as  $h \mapsto (h)_p$ . As for the computation of the class number of the principal genus, the case of  $n = 1$  is due to Eichler [Eic38] (see also Theorem 1.12, p.346 of [Piz80]) and the case of  $n = 2$  is handled by Hashimoto-Ibukiyama [HI80].

**2.4. Ibukiyama-Katsura-Oort-Serre's result in terms of adelic language.** Let us fix a prime  $p$  and put  $k = \overline{\mathbb{F}}_p$ . For each positive integer, 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  $E_0$  be a supersingular elliptic curve over  $k$ . It is well-known that  $B := \text{End}(E_0) \otimes_{\mathbb{Z}} \mathbb{Q}$  is the definite quaternion algebra ramified only at  $p$  and  $\infty$  with a maximal order  $\mathcal{O} = \text{End}(E_0)$ .

For each prime  $q$ , put  $\mathcal{O}_q := \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_q$ . Put  $A_0 = E_0^g$  and define a divisor on  $A_0$  by

$$D := \sum_{i=0}^{g-1} E_0^i \times \{0_{E_0}\} \times E_0^{g-i-1}$$

where  $0_{E_0}$  stands for the origin of  $E_0$ . By using suitable parallel transformations, it is easy to see that  $(D^g) = g!$ . It follows from (2.1) that  $\mathcal{L}_0 := \mathcal{O}(D)$  is a principal polarization. Let us fix the principally polarized abelian variety  $(A_0, \mathcal{L}_0)$ . Pick another principally polarized abelian variety  $(A, \mathcal{L})$ . As explained before,  $A$  is isomorphic to  $A_0$  and by pulling back  $\mathcal{L}$  to  $A_0$ , there is one to one correspondence between  $SS_g(p)$  and the set  $PP_g(A_0)$  of isomorphism classes of principal polarizations on  $A_0$ . Therefore, we have

$$(2.7) \quad SS_g(p) \simeq PP_g(A_0) \xrightarrow{\subset} \text{NS}(A_0) \xrightarrow{j} \text{End}(A_0) = M_g(\mathcal{O}),$$

where  $j$  is defined by  $j(\mathcal{L}) = \phi_{\mathcal{L}_0}^{-1} \circ \phi_{\mathcal{L}}$  for each class  $[\mathcal{L}] \in PP_g(A_0)$ . By Proposition 2.8 of [IKO86], the image of  $SS_g(p)$  under the map (2.7) is given by

$$(2.8) \quad \{X \in GL_g(\mathcal{O}) \mid X = {}^t\bar{X} > 0\}.$$

We remark that the Hauptnorm  $\text{HNm}$  in p.144 of [IKO86] is nothing but the reduced norm of  $M_g(\mathcal{O})$  and for  $X \in M_g(\mathcal{O})$ ,  $\text{HNm}(X) = 1$  if and only if  $X \in GL_g(\mathcal{O})$ . Pick  $X$  from the set (2.8). By Lemma 2.4 of [IKO86], for each prime  $q$ , there exists  $\delta_q \in GL_g(\mathcal{O}_q)$  such that  $X = \delta_q {}^t\bar{\delta}_q$ . Consider an  $\mathcal{O}$ -lattice  $L := \bigcap_q \mathcal{O}^g \delta_q \cap B^n$ . By Corollary 2.2 of [IKO86], there exists  $\gamma \in GL_g(B)$  such that  $L = \mathcal{O}^g \gamma$ . Since  $\mathcal{O}_q^g \gamma = L_q = \mathcal{O}_q^g \delta_q = \mathcal{O}_q^g$ ,  $h := \gamma {}^t\bar{\gamma} \in GL_g(\mathcal{O})$  and clearly  $h = {}^t\bar{h} > 0$ . Therefore, by Lemma 2.3 of [IKO86], we conclude that  $[L] \in \mathcal{L}(\mathcal{O}^g)/\sim$ . It follows from Lemma 2.3 of [IKO86] again that the association from  $X$  to  $[L]$  is bijection. Summing up, we have the following:

**Proposition 2.5.** (*Ibukiyama-Katsura-Oort-Serre's theorem*) *There is a one-to-one correspondence between  $SS_g(p)$  and  $\mathcal{L}(\mathcal{O}^g)/\sim$ .*

We denote by  $Z_{G_g} \simeq GL_1$  the center of  $G_g = GUSp_g$ . Recall the open compact subgroup  $K(\mathcal{O}^g) = \prod_p K_p(\mathcal{O}^g)$  from (2.6) for  $L = \mathcal{O}^g$ . 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 2.6.** *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 adèles of  $\mathbb{Q}$  outside  $\ell$ . 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

$$(2.9) \quad G_g(\mathbb{A}_f) = G_g(\mathbb{A}_f^{(\ell)}) \times G_g(\mathbb{Q}_\ell) = G_g(\mathbb{Q})(K(\mathcal{O}^g)^{(\ell)} \times G_g(\mathbb{Q}_\ell)).$$

Combining (2.6) with (2.9), we have

$$(2.10) \quad \begin{aligned} \mathcal{L}(\mathcal{O}^g) / \sim &\xleftarrow{\sim} K(\mathcal{O}^g) \backslash G_g(\mathbb{A}_f) / G_g(\mathbb{Q}) \\ &\simeq G_g(\mathbb{Q}) \backslash G_g(\mathbb{A}_f) / K(\mathcal{O}^g) \\ &= G_g(\mathbb{Q}) \backslash (G_g(\mathbb{Q})(K(\mathcal{O}^g)^{(\ell)} \times G_g(\mathbb{Q}_\ell))) / K(\mathcal{O}^g) \\ &= G_g(\mathbb{Z}[1/\ell]) \backslash GSp_g(\mathbb{Q}_\ell) / GSp_g(\mathbb{Z}_\ell) \\ &= G_g(\mathbb{Z}[1/\ell]) \backslash GSp_g(\mathbb{Q}_\ell) / Z_{GSp_g}(\mathbb{Q}_\ell) GSp_g(\mathbb{Z}_\ell). \end{aligned}$$

We remark that at the last line  $Z_{GSp_g}(\mathbb{Q}_\ell)$  is intentionally inserted due to the formulation in terms of Bruhat-Tits building handled later on. Further, the centers of  $G_g(\mathbb{Z}[1/\ell])$  and  $GSp_g(\mathbb{Z}_\ell)$  are  $\mathbb{Z}[1/\ell]^\times$  and  $\mathbb{Z}_\ell^\times$  respectively. The equality  $\mathbb{Z}[1/\ell]^\times \mathbb{Z}_\ell^\times = \mathbb{Q}_\ell^\times$  explains how  $Z_{GSp_g}(\mathbb{Q}_\ell)$  shows up there. We have also used  $K(\mathcal{O}^g)^{(\ell)} \cap G_g(\mathbb{Q}) = G_g(\mathbb{Z}[1/\ell])$  to obtain the fourth line.  $\square$

**2.5. Another formulation due to Jordan-Zyrtman.** 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  $\ell$ . However, it is not transparent to see the compatibility of Hecke actions on both sides under the one-to-one correspondence (2.10). To overcome this, due to Jordan-Zyrtman [JZ21], we use another formulation of  $SS_g(p)$  and its connection to  $SS_g(p, \ell, A_0, \mathcal{L}_0)$  by using  $\ell$ -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  $\ell$ -adic Tate module and by  $V_\ell(A) := T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$  the  $\ell$ -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  $V \simeq V^* = \text{Hom}_{R_V}(V, R_V)$  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). It follows from this that  $T_C \simeq T_\ell(A_C)$  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  $GSpg(\mathbb{Q}_\ell)$ . Another choice of a symplectic  $\mathbb{Z}_\ell$ -basis of  $T_C$  yields  $P_C\gamma$  for some  $\gamma \in GSpg(\mathbb{Z}_\ell)$ . For each  $h \in \text{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}[1/\ell]$  which is invertible (hence  $h$  is an isogeny of degree a power of  $\ell$ ), we see easily that  $P_{h(C)} = h^*P_C$  where  $h^*$  is the endomorphism of  $V_\ell(A)$  induced from  $h$ . In fact, it follows from the functorial property of the pairing (see p.228 of [Mum70]). We identify  $G_g(\mathbb{Z}[1/\ell])$  with

$$(2.11) \quad \Gamma(A)^\dagger := \{f \in (\text{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}[1/\ell])^\times \mid f \circ f^\dagger = f^\dagger \circ f \in \mathbb{Z}[1/\ell]^\times \text{id}_A\}$$

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

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:

$$(2.12) \quad \text{Iso}_{\ell^\infty}(A, \mathcal{L}) := \{[(A_C, \mathcal{L}_C)] \in SS_g(p) \mid n \geq 1, C \subset A[\ell^n] : \text{a maximal isotropic subgroup}\}.$$

and

$$(2.13) \quad SS_g(p, \ell, A, \mathcal{L}) := \{[(B, \mathcal{M}, \phi_B)] \mid [(B, \mathcal{M})] \in SS_g(p)\}$$

where  $\phi_B : A \longrightarrow B$  is an  $\ell$ -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  $\phi_{A_2}$  differ by only an element in  $\Gamma(A_1)^\dagger$ . By definition, the natural map from  $SS_g(p, \ell, A, \mathcal{L})$  to  $\text{Iso}_{\ell^\infty}(A, \mathcal{L})$  is surjective while  $\text{Iso}_{\ell^\infty}(A)$  is included in  $SS_g(p)$ . With the above observation, we have obtained a map

$$(2.14) \quad \text{Iso}_{\ell^\infty}(A, \mathcal{L}) \longrightarrow G_g(\mathbb{Z}[1/\ell]) \backslash GSp_g(\mathbb{Q}_\ell) / GSp_g(\mathbb{Z}_\ell), [(A_C, \mathcal{L}_C)] \mapsto G_g(\mathbb{Z}[1/\ell]) P_C GSp_g(\mathbb{Z}_\ell)$$

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

**Theorem 2.7.** *Fix  $(A, \mathcal{L})$  in a class of  $SS_g(p)$ . Keep the notation being as above. It holds that  $\text{Iso}_{\ell^\infty}(A, \mathcal{L}) = SS_g(p)$  and the map (2.14) induces a bijection*

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

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

*Proof.* Surjectivity of (2.14) follows in reverse from the construction by using Corollary of Theorem 2 in Section 23 of Chapter IV of [Mum70] to guarantee the existence of a principal polarization. By Proposition 2.6 and  $\text{Iso}_{\ell^\infty}(A, \mathcal{L}) \subset SS_g(p)$ , we have

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

and it yields first two claims. With a natural surjection  $SS_g(p, \ell, A, \mathcal{L}) \longrightarrow \text{Iso}_{\ell^\infty}(A, \mathcal{L})$  and (2.14), 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  $(\text{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}[1/\ell])^\times = G_g(\mathbb{Z}[1/\ell])$ , two objects of  $SS_g(p, \ell, A, \mathcal{L})$  which go to one element in the target differ by only  $\ell$ -markings. Therefore, the above map is bijective. Hence,  $SS_g(p, \ell, A, \mathcal{L}) \xrightarrow{\sim} \text{Iso}_{\ell^\infty}(A, \mathcal{L}) = SS_g(p)$ .

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 2.6.  $\square$

As a byproduct we have

**Corollary 2.8.** *Let  $\ell$  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 2.7, we have  $SS_g(p, \ell, A, \mathcal{L}) \xrightarrow{\sim} \text{Iso}_{\ell^\infty}(A, \mathcal{L}) = SS_g(p)$  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  $\ell$  and such an isogeny can be written as a composition of some  $(\ell)^g$ -isogenies by Theorem 34 of [JZ21]. This shows the claim.  $\square$

**2.6. The Hecke operator at  $\ell$ .** Finally we discuss a relation of the map (2.14) with the Hecke operator at  $\ell$ . We refer Section 3 in Chapter VII of [CF90] for general facts and Section 16 through 19 of [Gee08] as a reader's friendly reference. For each prime  $\ell$  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  $T(\ell)_{(A_0, \mathcal{L}_0)}^{\text{geo}}$  at  $\ell$ :

$$(2.15) \quad T(\ell)_{(A_0, \mathcal{L}_0)}^{\text{geo}}([(A, \mathcal{L}, \phi_A)]) := \sum_{\substack{C \subset A[\ell] \\ \text{maximal isotropic}}} [(A_C, \mathcal{L}_C, f_C \circ \phi_A)].$$

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

$$(2.16) \quad T(\ell)^{\text{geo}}([(A, \mathcal{L})]) := \sum_{\substack{C \subset A[\ell] \\ \text{maximal isotropic}}} [(A_C, \mathcal{L}_C)].$$

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 regarded as a homothety class  $[L]$  for such an  $L$ . For each  $L$  being as above, we define the Hecke correspondence on  $GSp_g(\mathbb{Q}_\ell)/GSp_g(\mathbb{Z}_\ell)$  at  $\ell$

$$(2.17) \quad T(\ell)([L]) := \sum_{\substack{L \subset L_1 \subset \ell^{-1}L \\ L_1/L: \text{maximal isotropic}}} [L_1]$$

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  $\text{Div}(X)_{\mathbb{Z}} := \bigoplus_{P \in X} \mathbb{Z}P$ . The identification (2.14) with the bijection

$$(2.18) \quad SS_g(p, \ell, A_0, \mathcal{L}_0) \xrightarrow{\sim} SS_g(p), \quad [(A, \mathcal{L}, \phi_A)] \mapsto [(A, \mathcal{L})]$$

yields a bijection

$$(2.19) \quad SS_g(p, \ell, A_0, \mathcal{L}_0) \longrightarrow G_g(\mathbb{Z}[1/\ell]) \backslash GSp_g(\mathbb{Q}_\ell) / GSp_g(\mathbb{Z}_\ell).$$

Then we have obtained the following:

**Theorem 2.9.** *The following diagram is commutative:*

$$\begin{array}{ccccc} \mathrm{Div}(SS_g(p))_{\mathbb{Z}} & \xleftarrow{\sim (2.18)} & \mathrm{Div}(SS_g(p, \ell, A_0, \mathcal{L}_0))_{\mathbb{Z}} & \xrightarrow{\sim (2.19)} & \mathrm{Div}(G_g(\mathbb{Z}[1/\ell]) \backslash GSp_g(\mathbb{Q}_\ell) / Z_{GSp_g}(\mathbb{Q}_\ell) GSp_g(\mathbb{Z}_\ell))_{\mathbb{Z}} \\ T(\ell)^{\mathrm{geo}} \downarrow & & T(\ell)_{(A_0, \mathcal{L}_0)}^{\mathrm{geo}} \downarrow & & T(\ell) \downarrow \\ \mathrm{Div}(SS_g(p))_{\mathbb{Z}} & \xleftarrow{\sim (2.18)} & \mathrm{Div}(SS_g(p, \ell, A_0, \mathcal{L}_0))_{\mathbb{Z}} & \xrightarrow{\sim (2.19)} & \mathrm{Div}(G_g(\mathbb{Z}[1/\ell]) \backslash GSp_g(\mathbb{Q}_\ell) / Z_{GSp_g}(\mathbb{Q}_\ell) GSp_g(\mathbb{Z}_\ell))_{\mathbb{Z}}. \end{array}$$

**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

$$\Gamma \backslash G / K = \{\Gamma x_1 Z K, \dots, \Gamma x_h Z K\}, \quad x_1, \dots, x_h \in G$$

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

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

**Lemma 2.10.** *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  $\tilde{\Gamma}_i := (\Gamma \cap x_i Z K x_i^{-1}) Z / Z$  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  $(\Gamma \cap x_i Z K x_i^{-1})$  obviously acts on  $T_\ell(A_i)$ . Thus, we have an injection  $(\Gamma \cap x_i Z K x_i^{-1}) \subset \mathrm{End}(T_\ell(A_i))$ . On the other hand, by Faltings' theorem (cf. Theorem 4 of [Fal84]),  $\mathrm{End}(T_\ell(A_i)) \simeq \mathrm{End}(A_i) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ . Hence we may have  $(\Gamma \cap x_i Z K x_i^{-1}) \subset \mathrm{End}(A_i) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$  which is compatible with the identification  $\Gamma \subset \Gamma^\dagger(A_i)$ . Since each element of  $\Gamma^\dagger(A_i)$  is an  $\ell$ -isogeny, it preserves the polarization of  $A_i$  up to the multiplication by

$Z$ . It follows from this that  $\tilde{\Gamma}_i \subset \text{Aut}((A_i, \mathcal{L}_i))/\{\pm 1\}$ . The opposite inclusion follows by Faltings' theorem again.  $\square$

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 (2.17)), we define another formulation in terms of elements in  $G$ . Let  $t_\ell := \text{diag}(\overbrace{1, \dots, 1}^g, \overbrace{\ell, \dots, \ell}^g) \in G$ . We decompose

$$(2.20) \quad Kt_\ell K = \coprod_{t \in T} g_t K$$

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

$$(2.21) \quad m_{ij} := \{t \in T \mid \Gamma x_i g_t ZK = \Gamma x_j ZK\}$$

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  $\tilde{\Gamma}_i = (\Gamma \cap x_i ZK x_i^{-1})Z/Z$ . and the finite group  $x_i^{-1} \tilde{\Gamma}_i x_i \subset KZ/Z$  acts on  $W(\ell)$  from the left by multiplication. The action induces the orbit decomposition

$$(2.22) \quad W(\ell) = \coprod_{t \in T'} O_{x_i^{-1} \tilde{\Gamma}_i x_i}(g_t KZ)$$

for some subset  $T' \subset T$ .

**Lemma 2.11.** *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  $\text{Stab}_{x_i^{-1} \tilde{\Gamma}_i x_i}(g_t KZ)$  is isomorphic to a subgroup  $S_i$  of  $\tilde{\Gamma}_j$ .*

*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  $\alpha Z \in x_i^{-1} \tilde{\Gamma}_i x_i = (x_i^{-1} \Gamma x_i \cap K)Z/Z$ , 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  $\alpha Z$  is an element of  $\text{Stab}_{x_i^{-1} \tilde{\Gamma}_i x_i}(g_t KZ)$ ,  $k g_t^{-1} \alpha g_t k^{-1} Z$  also belongs to  $K$ . Therefore, we have a group homomorphism

$$\text{Stab}_{x_i^{-1} \tilde{\Gamma}_i x_i}(g_t KZ) \xrightarrow{\text{the conjugation by } k g_t^{-1}} (x_j^{-1} \Gamma x_j \cap K)Z/Z \simeq \tilde{\Gamma}_j.$$

Clearly, this map is injective and we have the claim.  $\square$

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 2.12.** *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  $|\text{Stab}_{x_i^{-1}\tilde{\Gamma}_i x_i}(g_t KZ)| = |\text{Stab}_{x_j^{-1}\tilde{\Gamma}_j x_j}(g_t^{-1} KZ)|$ . In particular, it holds*

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

*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  $\text{Stab}_{x_j^{-1}\tilde{\Gamma}_j x_j}(g_t^{-1} KZ)$  to  $\text{Stab}_{x_i^{-1}\tilde{\Gamma}_i x_i}(g_t KZ)$ . The claim follows from this.  $\square$

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

$$(2.23) \quad SS_g(p, \ell, A_0, \mathcal{L}_0) \longrightarrow G_g(\mathbb{Z}[1/\ell]) \backslash GSp_g(\mathbb{Q}_\ell) / GSp_g(\mathbb{Z}_\ell)$$

given by Theorem 2.7. 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  $\text{LG}_i(\ell) = \{C_t\}_{t \in T}$  the set of all totally maximal isotropic subspace of  $A_i[\ell]$  with respect to the Weil pairing associated to  $\mathcal{L}_i$ . Here we use the same index  $T$  as  $W(\ell)$  defined before. Then the group  $\text{RA}_i := \text{Aut}((A_i, \mathcal{L}_i)) / \{\pm 1\}$  acts on  $\text{LG}(\ell)$  since each element there preserves the polarization. As in (2.22) we also have the decomposition

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

Suppose  $\Gamma x_i ZK$  corresponds to  $w_i = [(A_i, \mathcal{L}_i, \phi_{A_i})]$  under (2.23).

**Proposition 2.13.** *Keep the notation being as above. The followings holds.*

- (1) *The pullback of  $\phi_{A_i}$  induces an identification between  $\text{LG}_i(\ell)$  and  $W(\ell)$ .*
- (2) *Suppose  $C_t \in \text{LG}_i(\ell)$  corresponds to  $g_t ZK \in W(\ell)$  for  $t \in T$  under the above identification. Let  $f_{C_t} : (A_i, \mathcal{L}_{A_i}) \longrightarrow (A_i, \mathcal{L}_{A_i, C_t})$  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  $\tilde{f}_{C_t} : (A_i, \mathcal{L}_{A_j}) \longrightarrow (A_i, \mathcal{L}_{A_i})$  the  $(\ell)^g$ -isogeny obtained in Proposition 2.2 for  $f_{C_t}$ . Then it holds*

- *the kernel of  $\tilde{f}$  corresponds to  $g_t^{-1} ZK$  under the above identification,*
- $|\text{RA}_i| = |\tilde{\Gamma}_i|,$
- $|O_{\text{RA}_i}(C_t)| = |O_{x_i^{-1}\tilde{\Gamma}_i x_i}(g_t KZ)|, |O_{\text{RA}_j}(\text{Ker} \tilde{f}_{C_t})| = |O_{x_j^{-1}\tilde{\Gamma}_j x_j}(g_t^{-1} KZ)|,$  and
- $|\text{RA}_j| \cdot |O_{\text{RA}_i}(C_t)| = |\text{RA}_i| \cdot |O_{\text{RA}_j}(\text{Ker} \tilde{f}_{C_t})|.$

*Proof.* The claim follows from the construction of (2.23) with Lemma 2.10 through Lemma 2.12.  $\square$

We remark that the fourth claim of (2) in the above proposition was proved in Lemma 3.2 of [FS21b].

### 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-Zyrtman's big isogeny graph in [JZ21].

**3.1. Jordan-Zyrtman's big isogeny graph.** We basically follow the notation in §7.1 and §5.3 of [JZ21]. The  $(\ell)^g$ -isogeny (big) graph  $Gr_g(\ell, p)$  due to Jordan-Zyrtman 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  $f, h : (A_1, \mathcal{L}_1) \rightarrow (A_2, \mathcal{L}_2)$  are said to be equivalent if there exist automorphisms  $\phi \in \text{Aut}(A_1, \mathcal{L}_1)$  and  $\psi \in \text{Aut}(A_2, \mathcal{L}_2)$  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  $(\ell)$ -marked  $(\ell)^g$ -isogeny graph.** Similarly, the  $(\ell)$ -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  $\ell$ -markings  $\phi_{A_1} : (A_0, \mathcal{L}_0) \rightarrow (A_1, \mathcal{L}_1)$  and  $\phi_{A_2} : (A_0, \mathcal{L}_0) \rightarrow (A_2, \mathcal{L}_2)$  respectively, then an edge from  $v_1$  to  $v_2$  is an  $(\ell)^g$ -isogeny  $f : (A_1, \mathcal{L}_1) \rightarrow (A_2, \mathcal{L}_2)$  such that two markings  $f \circ \phi_{A_1}$  and  $\phi_{A_2}$  of  $(A_2, \mathcal{L}_2)$  from  $(A_0, \mathcal{L}_0)$  differ by only an element in  $\Gamma(A_0)^\dagger$ .



**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 to 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 (2.20).

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

- the set of vertices  $V(\text{BTQ}_g^1(\ell, p))$  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  $v_1$  to  $v_2$  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

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

Further we also define

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

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

**Theorem 3.1.** *The identifications (2.18) and (2.19) induce the following graph isomorphisms*

$$\text{Gr}_g(\ell, p) \xleftarrow{(2.18)} \mathcal{G}_g^{SS}(\ell, p) \xrightarrow{(2.19)} \text{BTQ}_g^1(\ell, p).$$

*Further, the following properties are preserved under the isomorphisms:*

- the Hecke action of  $T(\ell)^{\text{geo}}$ ,  $T(\ell)_{(A_0, \mathcal{L}_0)}^{\text{geo}}$ , 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  $\hat{e}$  such that

$$|\text{RA}(v_2)| \cdot |O_{\text{RA}(v_1)}(\text{Ker}(e))| = |\text{RA}(v_1)| \cdot |O_{\text{RA}(v_2)}(\text{Ker}(\hat{e}))|$$

*Proof.* As in the claim already, the identifications between the sets of vertices are given by (2.18) and (2.19). The compatibility of the Hecke operators follows from Theorem 2.9 and this yields the first property in the latter claim. The remaining formula follows from Proposition 2.13.  $\square$

**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  $BTQ_g^1(\ell, p)$  coincide each other.*

We remark that Theorem 2.9 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 [FS21b], 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 1.1 can be more precise as in the figure in 7A, p.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  $O$  be the ring of integers. We fix a uniformizer  $\varpi$  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  $\text{ord}_\varpi$  be a discrete valuation in  $F$ , normalized so that  $\text{ord}_\varpi(F^\times) = \mathbb{Z}$ . For example, we consider the  $\ell$ -adic field  $\mathbb{Q}_\ell$  for a prime  $\ell$  with the ring of integers  $\mathbb{Z}_\ell$ , where  $\ell$  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

$$\langle v_i, w_j \rangle = \delta_{ij} \quad \text{and} \quad \langle v_i, v_j \rangle = \langle w_i, w_j \rangle = 0 \quad \text{for any } i, j = 1, \dots, n,$$

where  $\delta_{ij}$  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  $GSp_n(F)$ ,

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

(See also Section 1.4). In the subsequent sections, we consider the projectivised 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  $t_\lambda = \text{diag}(1, \dots, 1, \lambda, \dots, \lambda)$  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 identify  $PSp_n(O)$  with 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  $\Lambda$  in  $V$  as a free  $O$ -module of rank  $2n$ . Note that if  $\Lambda$  is a lattice, then  $\Lambda/\varpi\Lambda$  is a vector space over  $\mathbb{F}_q$  of dimension  $2n$ . We say that a lattice  $\Lambda$  is primitive if

$$\langle \Lambda, \Lambda \rangle \subseteq O \quad \text{where } \langle \Lambda, \Lambda \rangle := \{\langle v, w \rangle \mid v, w \in \Lambda\},$$

and  $\langle *, * \rangle$  induces a non-degenerate alternating form on  $\Lambda/\varpi\Lambda$  over  $\mathbb{F}_q$ .

Let  $\Lambda_i$  for  $i = 1, 2$  be lattices in  $V$ , and we say that they are homothetic if

$$\Lambda_1 = \alpha\Lambda_2 \quad \text{for some } \alpha \in F^\times.$$

This defines an equivalence relation in the set of lattices in  $V$ . We denote the homothety class of a lattice  $\Lambda$  by  $[\Lambda]$ . Let us define the set  $\mathbb{L}_n$  of homothety classes  $[\Lambda]$  of lattices such that there exist a representative  $\Lambda$  of  $[\Lambda]$  and a primitive lattice  $\Lambda_0$  satisfying that

$$\varpi\Lambda_0 \subseteq \Lambda \subseteq \Lambda_0 \quad \text{and} \quad \langle \Lambda, \Lambda \rangle \subseteq \varpi O.$$

By the definition, if  $[\Lambda] \in \mathbb{L}_n$ , then a representative  $\Lambda$  yields a subspace  $\Lambda/\varpi\Lambda_0$  of  $\Lambda_0/\varpi\Lambda_0$  with some primitive lattice  $\Lambda_0$  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  $\Lambda_i$  of  $[\Lambda_i]$  for  $i = 1, 2$  and a primitive lattice  $\Lambda_0$  such that

$$\varpi\Lambda_0 \subseteq \Lambda_i \subseteq \Lambda_0 \quad \text{for } i = 1, 2,$$

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  $\text{Ver}(\mathcal{B}_n)$  is  $\mathbb{L}_n$ , i.e.,  $\sigma \subset \text{Ver}(\mathcal{B}_n)$  defines a simplex if any distinct vertices in  $\sigma$  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)  $[\Lambda_0], [\Lambda_1], \dots, [\Lambda_n]$  corresponds to a sequence of lattices

$$\Lambda_0 \subseteq \Lambda_1 \subseteq \dots \subseteq \Lambda_n \subseteq \varpi^{-1}\Lambda_0,$$

where  $\varpi^{-1}\Lambda_0$  is primitive, such that

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

forms a complete flag of a maximal totally isotropic subspace  $\Lambda_n/\Lambda_0$  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  $\{v_1, \dots, v_n, w_1, \dots, w_n\}$  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  $[\Lambda] \in \text{Ver}(\mathcal{B}_n)$  and  $M \in Sp_n(F)$ , and this action is simplicial since it preserves the incidence relation. Moreover, this yields the action of the projectivised group  $PSp_n(F)$  on  $\mathcal{B}_n$ .

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

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

Note that this depends only on the homothety class of  $\Lambda$  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  $\mathbf{lab}_n : \text{Ver}(\mathcal{B}_n) \rightarrow \mathbb{Z}/2n\mathbb{Z}$  is well-defined and we call  $\mathbf{lab}_n[\Lambda]$  the *label* of a vertex  $[\Lambda] \in \text{Ver}(\mathcal{B}_n)$ . For example, let us consider a sequence of lattices  $\Lambda_0, \dots, \Lambda_n$ , where

$$(4.1) \quad \Lambda_k := Ou_1 \oplus \dots \oplus Ou_k \oplus O\varpi u_{k+1} \oplus \dots \oplus O\varpi w_1 \oplus \dots \oplus O\varpi w_n \quad \text{for } 0 \leq k < n,$$

and  $\Lambda_n := Ou_1 \oplus \dots \oplus Ou_n \oplus O\varpi w_1 \oplus \dots \oplus O\varpi w_n$ . Then  $\Lambda_0 \subseteq \dots \subseteq \Lambda_n \subseteq \varpi^{-1}\Lambda_0$  and  $\varpi^{-1}\Lambda_0$  is primitive, and since the chain  $\Lambda_1/\Lambda_0 \subseteq \dots \subseteq \Lambda_n/\Lambda_0$  forms a maximal totally isotropic flag in  $\varpi^{-1}\Lambda_0/\Lambda_0$  over  $\mathbb{F}_q$ , the corresponding homothety classes  $[\Lambda_0], \dots, [\Lambda_n]$  define a chamber in  $\mathcal{B}_n$ . In this case, we have that  $\mathbf{lab}_n[\Lambda_k] = 2n - k \pmod{2n}$  for  $0 \leq k \leq n$ . We call the chamber determined by  $[\Lambda_0], \dots, [\Lambda_n]$  the *fundamental chamber*  $\mathcal{C}_0$ . Here we note that  $\mathbf{lab}_n$  misses the values  $1, \dots, n-1$  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  $\text{Ver}(\mathcal{B}_n)$ . 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  $\mathcal{B}_n$ , following [Gar97, Chapter 20] and [She07]. A *frame* is an unordered  $n$ -tuple,

$$\{\lambda_1^1, \lambda_1^2\}, \dots, \{\lambda_n^1, \lambda_n^2\},$$

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

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

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  $i = 1, \dots, n$  is a maximal subcomplex of  $\mathcal{B}_n$  on the set of vertices  $[\Lambda]$  such that

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

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

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

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

by  $\Lambda = (a_1, \dots, a_n; b_1, \dots, b_n)$ , and the homothety class by  $[\Lambda] = [a_1, \dots, a_n; b_1, \dots, b_n]$ . For  $\Lambda$ , 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  $i = 1, \dots, n$ . This is equivalent to that  $a_i + b_i \geq 0$  for all  $i = 1, \dots, n$ , 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  $i = 1, \dots, n$ .

For the fixed basis, let  $\lambda_i^1 := Fu_i$  and  $\lambda_i^2 := Fw_i$  for  $i = 1, \dots, n$ . The frame  $\{\lambda_i^1, \lambda_i^2\}_{i=1, \dots, n}$  determines an apartment  $\Sigma_0$  in the building  $\mathcal{B}_n$  for  $Sp_n(F)$ . We call  $\Sigma_0$  the *fundamental apartment*. The chain of lattice  $\Lambda_0 \subseteq \dots \subseteq \Lambda_n$  in (4.1) defines a chamber  $\mathcal{C}_0$  in  $\Sigma_0$  containing  $[\Lambda_0]$ :

$$\begin{aligned} \Lambda_0 &= (1, \dots, 1; 1, \dots, 1) \subset (0, 1, 1, \dots, 1; 1, \dots, 1) \\ &\subset (0, 0, 1, \dots, 1; 1, \dots, 1) \subset \dots \subset (0, 0, \dots, 0; 1, \dots, 1) \subset \varpi^{-1}\Lambda_0. \end{aligned}$$

Moreover, the following chain

$$\begin{aligned} \Lambda_0 &= (1, \dots, 1; 1, \dots, 1) \subset (1, 0, 1, \dots, 1; 1, \dots, 1) \\ &\subset (0, 0, 1, \dots, 1; 1, \dots, 1) \subset \dots \subset (0, 0, \dots, 0; 1, \dots, 1) \subset \varpi^{-1}\Lambda_0, \end{aligned}$$

where the lattices are the same as above except for the second one, defines a chamber which shares a codimension one face with  $\mathcal{C}_0$ .

We shall see the rest of chambers in the apartment  $\Sigma_0$  by an action of the affine Weyl group attached to the building. Denoting by  $\mathcal{N}_0$  and by  $\mathcal{I}_0$  the subgroups preserving  $\Sigma_0$  (as a set) and  $\mathcal{C}_0$  (pointwise) in  $Sp_n(F)$  respectively, the affine Weyl group is isomorphic to  $\mathcal{N}_0/(\mathcal{N}_0 \cap \mathcal{I}_0)$ , which naturally acts on the chambers in  $\Sigma_0$  transitively. For  $Sp_n(F)$ , the affine Weyl group is of type  $\tilde{C}_n$  with the Coxeter diagram



on  $(n+1)$  vertices. Each vertex  $i$  in the Coxeter diagram corresponds to a reflection  $s_i$  satisfying that  $s_i^2 = 1$  and  $s_i s_j$  has order  $m_{ij}$ , where

$$m_{12} = m_{n(n+1)} = 4, \quad m_{i(i+1)} = 3 \quad \text{for } i \neq 1, n, \text{ and } m_{ij} = 2 \quad \text{otherwise.}$$

The affine Weyl group of type  $\tilde{C}_n$  is generated by  $s_1, \dots, s_{n+1}$ . Given the symplectic basis  $\{u_1, \dots, u_n, w_1, \dots, w_n\}$ , the action on it is realized as in the following:

$s_1$  exchanges  $u_n$  and  $w_n$ , and fixes the others,

$s_j$  ( $2 \leq j \leq n$ ) exchanges  $u_{n-j+1}$  and  $u_{n-j+2}$ , and  $w_{n-j+1}$  and  $w_{n-j+2}$  simultaneously and fixes the others, and

$s_{n+1}$  maps  $u_1$  to  $\varpi w_1$  and  $w_1$  to  $\varpi^{-1} u_1$  and fixes the others.

In the fundamental apartment  $\Sigma_0$ , denoting a vertex by  $[a_1, \dots, a_n; b_1, \dots, b_n]$ , we have that

$$s_1[a_1, \dots, a_n; b_1, \dots, b_n] = [a_1, \dots, a_{n-1}, b_n; b_1, \dots, b_{n-1}, a_n],$$

$$s_j[a_1, \dots, a_n; b_1, \dots, b_n]$$

$$= [a_1, \dots, a_{n-j+2}, a_{n-j+1}, \dots, a_n; b_1, \dots, b_{n-j+2}, b_{n-j+1}, \dots, b_n] \quad \text{for } 2 \leq j \leq n,$$

and

$$s_{n+1}[a_1, \dots, a_n; b_1, \dots, b_n] = [b_1 - 1, a_2, \dots, a_n; a_1 + 1, b_2, \dots, b_n].$$

A direct computation shows that  $s_1, \dots, s_{n+1}$  satisfy the indicated Coxeter data. Deleting either  $s_1$  or  $s_{n+1}$  yields a group isomorphic to the spherical Weyl group of type  $C_n$ . Note that the vertex  $v = [a_1, \dots, a_n; b_1, \dots, b_n]$  is fixed by  $s_i$  for  $1 \leq i \leq n$  if and only if  $a_i = b_j$  for all  $1 \leq i, j \leq n$ , and  $v$  is fixed by  $s_i$  for  $2 \leq i \leq n+1$  if and only if  $a_i = b_i - 1$  for all  $1 \leq i \leq n$ . In the fundamental chamber  $\mathcal{C}_0$ , such vertices are  $[\Lambda_0] = [1, \dots, 1; 1, \dots, 1]$  and  $[\Lambda_n] = [0, \dots, 0; 1, \dots, 1]$

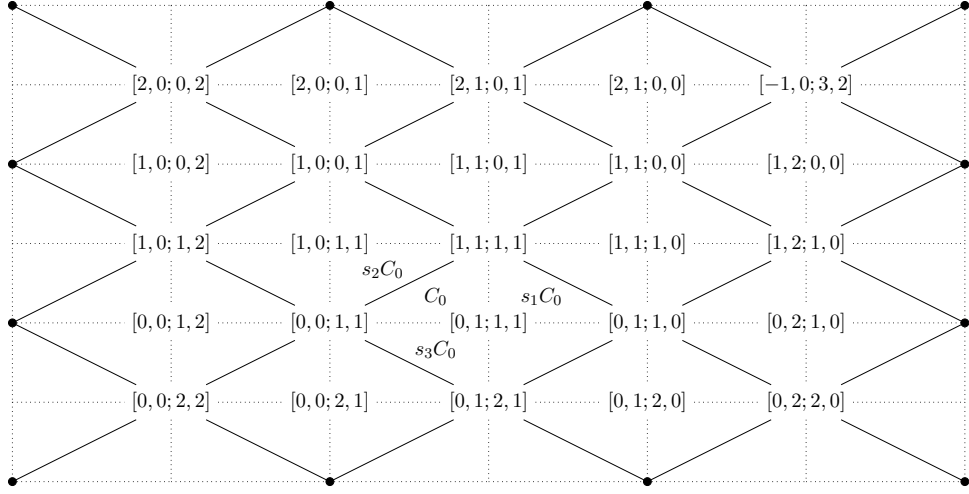


FIGURE 4.1. A part of the fundamental apartment  $\Sigma_0$  with the chambers  $C_0, s_1C_0, s_2C_0$  and  $s_3C_0$  for  $n = 2$ .

respectively. Although we do not use the fact, it is useful to note that the spherical Weyl group  $C_n$  is isomorphic to the signed permutation group  $(\mathbb{Z}/2\mathbb{Z})^n \rtimes \mathfrak{S}_n$  whose order is  $2^n n!$ .

**Example 4.1.** *If  $n = 2$ , then we have 8 chambers containing vertex  $[\Lambda_0] = [1, 1; 1, 1]$  in a fixed apartment, where the fundamental chamber  $C_0$  is defined by the chain*

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

*The locations of chambers  $C_0, s_1C_0, s_2C_0$  and  $s_3C_0$  are indicated for generators  $s_1, s_2, s_3$  of  $\tilde{C}_2$  in Figure 4.1.*

**4.4. Self-dual vertices.** For any lattice  $\Lambda$  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  $\Lambda^*$  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]; we give a proof for the sake of completeness.

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

*Proof.* Fix a symplectic basis of the space over  $F$  and identify the space with the standard symplectic space over  $F$ . Let  $\Lambda_0, \dots, \Lambda_n$  be the sequence of lattices (4.1) whose homothety classes form the fundamental chamber  $\mathcal{C}_0$  in the building  $\mathcal{B}_n$ . Note that  $\Lambda_0$  is primitive and  $\Lambda_0^* = \Lambda_0$ . For any lattice  $\Lambda$ , there exist  $\gamma_1, \gamma_2 \in GL_{2n}(F)$  such that  $\Lambda = \gamma_1 \Lambda_0$  and  $\Lambda^* = \gamma_2 \Lambda_0$ . Since  $\langle \Lambda^*, \Lambda \rangle \subset O$ , we have that  ${}^t \gamma_1 \gamma_2 \in GL_{2n}(O)$ , and thus  $\det {}^t \gamma_1 \gamma_2 \in O^\times$ . This implies that

$$\mathbf{lab}_n[\Lambda^*] = \text{ord}_\varpi(\det \gamma_2) = -\text{ord}_\varpi(\det \gamma_1) = -\mathbf{lab}_n[\Lambda] \pmod{2n}.$$

Therefore if  $[\Lambda^*] = [\Lambda]$ , then  $2\mathbf{lab}_n[\Lambda] = 0 \pmod{2n}$ , i.e.,  $\mathbf{lab}_n[\Lambda] = 0$  or  $n \pmod{2n}$ . Conversely if  $\mathbf{lab}_n[\Lambda] = 0$  or  $n \pmod{2n}$ , then  $\Lambda = \gamma \Lambda_0$  or  $\gamma \Lambda_n$  for some  $\gamma \in Sp_n(F)$  since  $Sp_n(F)$  acts on  $\mathcal{B}_n$  transitively on chambers and preserves the labels of vertices. Noting that  $[\Lambda_0^*] = [\Lambda_0]$  and  $[\Lambda_n^*] = [\Lambda_n]$ , as well as  $\Lambda^* = \gamma \Lambda_0^*$  if  $\Lambda = \gamma \Lambda_0$ , and  $\Lambda^* = \gamma \Lambda_n^*$  if  $\Lambda = \gamma \Lambda_n$  for  $\gamma \in Sp_n(F)$ , we conclude that  $[\Lambda^*] = [\Lambda]$ , as required.  $\square$

**Remark 4.3.** *If  $n \geq 2$ , then for the vertices  $[\Lambda] \in \text{Ver}(\mathcal{B}_n)$  with  $\mathbf{lab}_n[\Lambda] \neq 0, n \pmod{2n}$ , the homothety class  $[\Lambda^*]$  does not define a vertex, i.e.,  $[\Lambda^*] \notin \text{Ver}(\mathcal{B}_n)$ . Indeed, for the vertex  $[\Lambda]$  of label  $k \pmod{2n}$ , the homothety class of the dual  $[\Lambda^*]$  has the label  $2n - k \pmod{2n}$ . For example, if  $n = 2$ , then for the lattice  $\Lambda_1$  in (4.1), we have*

$$\Lambda_1^* = O\varpi^{-1}u_1 \oplus O\varpi^{-1}u_2 \oplus Ow_1 \oplus O\varpi^{-1}w_2,$$

and  $[\Lambda_1^*]$  has the label  $1 \pmod{2n}$ , and thus it does not belong to  $\text{Ver}(\mathcal{B}_2)$ .

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

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

and 1-simplices (edges) are defined between two incident vertices in  $\mathcal{B}_n$  (cf. Section 4.1): for  $[\Lambda_1], [\Lambda_2] \in \text{Ver}(\mathcal{S}_n)$ , we have  $[\Lambda_1] \sim [\Lambda_2]$  if and only if there exist representatives  $\Lambda_1$  and  $\Lambda_2$  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  $\Lambda_1$  and  $\Lambda_2$  are interchanged holds. Note that since special vertices are those that are self-dual, if  $\varpi^{-1}\Lambda_1$  is primitive, then  $\Lambda_2/\Lambda_1$  is a maximal totally isotropic subspace of  $\varpi^{-1}\Lambda_1/\Lambda_1$  over  $\mathbb{F}_q$ .

Lemma 4.2 shows that  $[\Lambda] \in \text{Ver}(\mathcal{S}_n)$  if and only if  $\mathbf{lab}_n[\Lambda] = 0$  or  $n \pmod{2n}$ , and we will see that  $\mathcal{S}_n$  is connected (Proposition 4.4 below). Although we do not use it in our main discussion, it



is useful to point out here that  $\mathcal{S}_n$  admits a structure of bipartite graph. Namely, if we decompose the set of vertices into two sets: the one of those with label  $0 \pmod{2n}$  and the other of those with label  $n \pmod{2n}$ , then the two extreme vertices of each edge have distinct labels.

We note that  $GS_{p_n}(F)$  does not act on  $\mathcal{B}_n$  through the linear transformation of lattices. Indeed, a vertex of label  $2n - 1 \pmod{2n}$  in the fundamental chamber  $\mathcal{C}_0$  is sent by  $t_\varpi \in GS_{p_n}(F)$  to a vertex of label  $n - 1 \pmod{2n}$ , which does not belong to  $\text{Ver}(\mathcal{B}_n)$ . However, restricted on  $\mathcal{S}_n$ , the group  $GS_{p_n}(F)$  acts on  $\mathcal{S}_n$ . Moreover, the action of  $GS_{p_n}(F)$  on  $\mathcal{S}_n$  is vertex-transitive since for  $t_\varpi = \text{diag}(1, \dots, 1, \varpi, \dots, \varpi)$  in  $GS_{p_n}(F)$ , 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  $t_\varpi$  permutes the labels on  $\text{Ver}(\mathcal{S}_n)$ . This defines the action of  $PGS_{p_n}(F)$  on  $\mathcal{S}_n$ . Letting  $o := [\Lambda_0]$ , we identify the stabilizer of  $o$  in  $PGS_{p_n}(F)$  with  $K := PGS_{p_n}(O)$ . If we define

$$\mathcal{S}_n^o := Sp_n(F)o \quad \text{and} \quad \mathcal{S}_n^{o^-} := t_\varpi \mathcal{S}_n^o,$$

then

$$\text{Ver}(\mathcal{S}_n) = \mathcal{S}_n^o \bigsqcup \mathcal{S}_n^{o^-},$$

and every edge in  $\mathcal{S}_n$  has one vertex in  $\mathcal{S}_n^o$  and the other vertex in  $\mathcal{S}_n^{o^-}$ . The following proposition has been shown by Shemanske; we give a proof for the sake of convenience.

**Proposition 4.4** (Proposition 3.6 in [She07]). *For every integer  $n \geq 1$ , the special 1-complex  $\mathcal{S}_n$  is connected.*

*Proof.* Given two special vertices (which are not incident each other), let us take two chambers in such a way that each chamber contains either one or the other vertex. Since for any two chambers there exists an apartment which contains both of them, applying an isometry of the building if necessary, we may assume that they are within the fundamental apartment  $\Sigma_0$ , and further one of them is the fundamental chamber  $\mathcal{C}_0$ . Noting that each reflection in the affine Weyl group maps  $\mathcal{C}_0$  to an adjacent chamber which shares at least one special vertex with  $\mathcal{C}_0$ . The other chamber is obtained by a successive application of reflections to  $\mathcal{C}_0$  and in the resulting sequence of chambers (called a gallery) we find an edge path (consisting of special vertices) connecting the given two special vertices. This shows that any two special vertices are connected by an edge path in the subcomplex based on the special vertices, i.e.,  $\mathcal{S}_n$  is connected.  $\square$

## 5. PROPERTY (T) AND SPECTRAL GAPS

**5.1. Property (T).** Let  $G$  be a topological group and  $(\pi, \mathcal{H})$  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 non-zero 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 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  $i = 0, 1, \dots, n+1$  such that  $\xi_0 := \text{id}$  and for  $i = 1, \dots, n+1$  each  $\xi_i$  projects onto the reflection  $s_i$  in the affine Weyl group acting on the fundamental apartment  $\Sigma_0$ .

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

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

Note that  $\Omega$  is compact and symmetric, i.e.,  $x \in \Omega$  if and only if  $x^{-1} \in \Omega$ . Let  $\nu$  be a Haar measure on  $K$  normalized so that  $\nu(K) = 1$ . Let us define the probability measure  $\mu$  on  $PGSp_n(F)$  as

the distribution of  $k\zeta k'$  where  $k, k'$  and  $\zeta$  are independent and  $k, k'$  are distributed according to  $\nu$  and  $\zeta$  is uniformly distributed on  $\{\xi_i a, (\xi_i a)^{-1} \mid i = 0, \dots, n+1\}$ . In other words,

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

and  $\delta_x$  denotes the Dirac distribution at  $x$ ; furthermore the convolution  $\mu_1 * \mu_2$  of two probability measures  $\mu_1, \mu_2$  on a group  $G$  is defined by

$$\mu_1 * \mu_2(A) = \mu_1 \times \mu_2(\{(\gamma_1, \gamma_2) \in G \times G \mid \gamma_1 \gamma_2 \in A\}),$$

for any measurable set  $A$  in  $G$ . Note that the support of  $\mu$  is  $\Omega$ . For any positive integers  $t \geq 1$ , we denote by  $\mu^{*t}$  the  $t$ -th convolution power of  $\mu$ , i.e.,  $\mu^{*1} := \mu$  and  $\mu^{*(t+1)} = \mu^{*t} * \mu$  for  $t \geq 1$ . If we define the probability measure  $\check{\mu}$  on  $PGSp_n(F)$  as the distribution of  $x^{-1}$  where  $x$  has the law  $\mu$ , then the definition of  $\mu$  implies that

$$(5.1) \quad \check{\mu} = \mu.$$

**Lemma 5.1.** *We have the following:*

- (1) *The set  $\Omega$  is generating in  $PGSp_n(F)$ , i.e.,  $\Omega$  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  $\Omega_0 = \{\xi_i a, (\xi_i a)^{-1}, i = 0, \dots, n+1\}$  and*

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

*Moreover, if  $\gamma$  is distributed according to  $\mu$  on  $PGSp_n(F)$ , then  $\gamma o$  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  $\Delta$  in  $K (= PSp_n(O))$  as the image of  $\{t_\lambda \mid \lambda \in O^\times\}$ , then since  $K$  contains  $K_0$  and  $\Delta$ , and  $\Omega$  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  $\Delta$ ). 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 as in Proposition 4.4. Since the quotient  $PGSp_n(F)$  modulo  $PSp_n(F)$  is generated by the images of  $\{a, a^{-1}\}$  and  $\Delta$  (cf. Section 4.1), we conclude that  $\Omega$  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  $\mu$  shows that  $\mu$  yields the uniform distribution on  $K \backslash \Omega / K$ . Concerning the second claim, in the fundamental apartment  $\Sigma_0$  we note that  $\xi_i a o = t_\varpi o$  if  $i \neq 1$  and  $\xi_1 a o = s_1 t_\varpi o$ , 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.  $\square$

For simplicity of notation, let  $G := PGSp_n(F)$  in the following discussion. Recall that  $\text{Ver}(\mathcal{S}_n) = Go$ . We define the Hilbert space

$$\ell^2(\mathcal{S}_n) := \left\{ \varphi : \text{Ver}(\mathcal{S}_n) \rightarrow \mathbb{C} \mid \sum_{v \in \text{Ver}(\mathcal{S}_n)} |\varphi(v)|^2 < \infty \right\},$$

equipped with the inner product

$$\langle \varphi, \psi \rangle := \sum_{v \in \text{Ver}(\mathcal{S}_n)} \varphi(v) \overline{\psi(v)}, \quad \text{for } \varphi, \psi \in \ell^2(\mathcal{S}_n).$$

Let us define an operator  $\mathcal{A}_\mu : \ell^2(\mathcal{S}_n) \rightarrow \ell^2(\mathcal{S}_n)$  by

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

Note that  $\mathcal{A}_\mu$  is well-defined by the definition of  $\mu$  since  $\text{Ver}(\mathcal{S}_n) = Go$  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  $\check{\mu} = \mu$  by (5.1), the operator  $\mathcal{A}_\mu$  is self-adjoint on  $\ell^2(\mathcal{S}_n)$ . Similarly if we define  $\mathcal{A}_{\mu^{*t}} : \ell^2(\mathcal{S}_n) \rightarrow \ell^2(\mathcal{S}_n)$  for any positive integer  $t \geq 1$ ,

$$\mathcal{A}_{\mu^{*t}} \varphi(\xi o) = \int_G \varphi(\xi \gamma o) d\mu^{*t}(\gamma) \quad \text{for } \xi \in G,$$

then we have that by induction

$$\mathcal{A}_\mu^t = \mathcal{A}_{\mu^{*t}} \quad \text{for all positive integer } t \geq 1.$$

Let us consider any closed subgroup  $\Gamma$  of  $G$  such that  $\Gamma$  acts on  $\mathcal{S}_n$  from left with a compact quotient space  $\Gamma \backslash \mathcal{S}_n$ , where the action is given by

$$(\gamma, v) \mapsto \gamma v \quad \text{for } \gamma \in \Gamma \text{ and } v \in \mathcal{S}_n.$$

Since  $\Gamma$  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 4.4, the graph  $\Gamma \backslash \mathcal{S}_n$  is connected for any such  $\Gamma$ . Here, however we do not assume that  $\Gamma$  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  $\Gamma$  factors through  $PSp_n(F)$ .

For each  $v \in \mathcal{S}_n$ , let

$$\Gamma_v := \{\gamma \in \Gamma \mid \gamma v = v\}.$$

Note that  $\Gamma_v$  is finite; indeed, if  $v = \xi o$  for  $\xi \in G$ , then  $\xi^{-1} \Gamma_v \xi$  is in  $K$ . Since  $\Gamma$  is a discrete subgroup of  $G$  and  $K$  is compact,  $\Gamma_v$  is a finite group. Since  $\Gamma_{\gamma v} = \gamma \Gamma_v \gamma^{-1}$  for  $\gamma \in \Gamma$  and  $v \in \mathcal{S}_n$ , whence  $|\Gamma_v|$  is independent of the choice of representatives for  $v \in \Gamma \backslash \mathcal{S}_n$ . Similarly, for  $v, w \in \mathcal{S}_n$  such that  $v$  and  $w$  are adjacent in  $\mathcal{S}_n$ , we define

$$\Gamma_{v,w} := \Gamma_v \cap \Gamma_w.$$

Considering the diagonal action of  $\Gamma$  on  $\mathcal{S}_n \times \mathcal{S}_n$ , we note that  $|\Gamma_{v,w}|$  is independent of the choice of representatives for  $[v, w]$  in  $\Gamma \backslash (\mathcal{S}_n \times \mathcal{S}_n)$ . 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  $\Gamma$  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  $\Gamma$ -action and  $\mathcal{A}_\mu$  on  $\ell^2(\mathcal{S}_n)$  commute, the following operator  $\mathcal{A}_{\Gamma, \mu}$  on  $\ell^2(\Gamma \backslash \mathcal{S}_n)$  is well-defined:

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

Note that since  $\mathcal{A}_\mu$  defines the simple random walk on  $\mathcal{S}_n$ , i.e., at each step the random walk jumps to a nearest neighbor vertex with equal probability  $1/D$  (where  $D$  is the degree of  $\mathcal{S}_n$ ), the operator  $\mathcal{A}_{\Gamma, \mu}$  defines a random walk (a Markov chain) on  $\Gamma \backslash \mathcal{S}_n$  with the transition probability

$$p(\Gamma \xi o, \Gamma \xi \gamma o) = \sum_{[v,w]} \frac{|\Gamma_v|}{D |\Gamma_{v,w}|},$$

where the summation runs over all those  $[v, w] \in \Gamma \backslash (\mathcal{S}_n \times \mathcal{S}_n)$  such that  $v$  and  $w$  are adjacent,  $\Gamma v = \Gamma \xi o$  and  $\Gamma w = \Gamma \xi \gamma o$ , and we set the probability 0 if there is no such pair  $[v, w]$ . (We recall that  $D = N_g(\ell)$  if  $F = \mathbb{Q}_\ell$  and  $n = g$ .) Since  $|\Gamma_{v,w}| = |\Gamma_{w,v}|$  for all  $[v, w]$  in  $\Gamma \backslash (\mathcal{S}_n \times \mathcal{S}_n)$ , we have that

$$\frac{1}{|\Gamma_v|} p(v, w) = \frac{1}{|\Gamma_w|} p(w, v) \quad \text{for } v, w \in \Gamma \backslash \mathcal{S}_n,$$

the associated random walk on  $\Gamma \backslash \mathcal{S}_n$  is reversible with respect to the measure  $1/|\Gamma_v|$  for each vertex  $v$ . This implies that  $\mathcal{A}_{\Gamma, \mu}$  is self-adjoint, i.e.,

$$\langle \mathcal{A}_{\Gamma, \mu} \varphi, \psi \rangle = \langle \varphi, \mathcal{A}_{\Gamma, \mu} \psi \rangle \quad \text{for } \varphi, \psi \in \ell^2(\Gamma \backslash \mathcal{S}_n).$$

Moreover,  $\mathcal{A}_{\Gamma, \mu^{*t}}$  is defined by

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

and  $\mathcal{A}_{\Gamma, \mu}^t = \mathcal{A}_{\Gamma, \mu^{*t}}$  holds for any positive integer  $t \geq 1$ .

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

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

where the third equality follows since  $\varphi$  is a  $K$ -fixed vector and the last identity follows from the definition of  $T_{\Gamma}(\gamma)$ . Hence the first claim holds.

Next let us show the second claim. If we denote the right-invariant Haar measure on  $\Gamma \backslash G$  by  $m_{\Gamma \backslash G}$ , then

$$\begin{aligned} \langle T_{\Gamma}(\gamma) \varphi_1, \varphi_2 \rangle &= \int_{\Gamma \backslash G} \left( \int_K \varphi_1(\Gamma \xi k \gamma) d\nu(k) \right) \overline{\varphi_2(\Gamma \xi)} dm_{\Gamma \backslash G}(\xi) \\ &= \int_K \int_{\Gamma \backslash G} \varphi_1(\Gamma \xi k \gamma) \overline{\varphi_2(\Gamma \xi)} dm_{\Gamma \backslash G}(\xi) d\nu(k) \\ &= \int_K \int_{\Gamma \backslash G} \varphi_1(\Gamma \xi \gamma) \overline{\varphi_2(\Gamma \xi)} dm_{\Gamma \backslash G}(\xi) d\nu(k) \\ &= \int_{\Gamma \backslash G} \varphi_1(\Gamma \xi \gamma) \overline{\varphi_2(\Gamma \xi)} dm_{\Gamma \backslash G}(\xi) = \langle \pi(\gamma) \varphi_1, \varphi_2 \rangle, \end{aligned}$$

where the second equality follows by the Fubini theorem and the third equality holds under the change of variables  $\Gamma \xi \mapsto \Gamma \xi k$  since  $m_{\Gamma \backslash G}$  is right-invariant,  $\varphi_2$  is a  $K$ -fixed vector, and  $\nu$  is normalized so that  $\nu(K) = 1$ . We conclude the second claim.  $\square$

Let us define

$$\ell_0^2(\Gamma \backslash \mathcal{S}_n) := \left\{ \varphi \in \ell^2(\Gamma \backslash \mathcal{S}_n) \mid \sum_{\Gamma v \in \Gamma \backslash \mathcal{S}_n} \varphi(\Gamma v) \frac{1}{|\Gamma v|} = 0 \right\},$$

i.e.,  $\ell_0^2(\Gamma \backslash \mathcal{S}_n)$  is 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  $\pi$  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  $\pi_0$  has no non-zero invariant vector.

**Proposition 5.3.** *For every  $n \geq 1$ , let  $\Gamma$  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  $(G, \Omega)$ .

*Proof.* For  $\varphi \in \ell_0^2(\Gamma \backslash \mathcal{S}_n)$ , it follows that

$$\begin{aligned} \langle (I - \mathcal{A}_{\Gamma, \mu})\varphi, \varphi \rangle &= \langle \varphi, \varphi \rangle - \frac{1}{2(n+2)} \sum_{\gamma \in \Omega_0} \langle T_\Gamma(\gamma)\varphi, \varphi \rangle \\ &= \langle \varphi, \varphi \rangle - \frac{1}{2(n+2)} \sum_{\gamma \in \Omega_0} \langle \pi(\gamma)\varphi, \varphi \rangle = \frac{1}{4(n+2)} \sum_{\gamma \in \Omega_0} \|\varphi - \pi_0(\gamma)\varphi\|^2, \end{aligned}$$

where identifying  $\varphi$  with a  $K$ -fixed vector, we have used Lemma 5.2 in the first and second lines, and the last equality follows since  $\pi_0$  is the restriction of  $\pi$  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  $\varphi$  is a  $K$ -fixed vector and  $\pi_0$  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  $\pi_0$  has no non-zero invariant vector, we conclude the claim.  $\square$

**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  $\Gamma$  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

$$\lambda_2(\Delta_{\Gamma, \mu}) \geq \frac{1}{4(n+2)} \kappa(G, \Omega)^2.$$



Furthermore,  $\kappa(G, \Omega) > 0$  since  $G = PGS p_n(F)$  has Property (T) if  $n \geq 2$  and  $\Omega$  is a compact generating set of  $G$  by Lemma 5.1 (1) (cf. Section 5.1). Letting

$$(5.2) \quad c_n := \frac{1}{4(n+2)} \kappa(G, \Omega)^2,$$

we obtain the claim.  $\square$

The proof of Theorem 1.1 now follows from Theorem 5.4 with  $\Gamma$  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  $\ell$  and  $p$  with  $p \neq \ell$ ,*

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

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

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

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

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

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

$$\kappa(Sp_n(\mathbb{Q}_\ell), \Omega_*) \geq \chi_L(s) = \frac{\sqrt{2(1 - \xi_L(s))}}{\sqrt{2(1 - \xi_L(s)) + 3}},$$

where

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

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

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

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 (5.2) in the proof of Theorem 5.4, we conclude that for all  $n \geq 2$  and all prime  $\ell$ ,

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

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

## 6. SOME REMARKS ON ALGEBRAIC MODULAR FORMS FOR $GUSp_g$

In this section, we study algebraic modular forms on  $G_g(\mathbb{A}_{\mathbb{Q}}) = GUSp_g(\mathbb{A}_{\mathbb{Q}})$  which can be also regarded as functions on  $SS_g(p)$ . When  $g = 1$ , Pizer applied the Jacquet-Langlands correspondence to study  $\text{Gr}_1(\ell, p)$  [Piz90] and he showed such graphs are Ramanujan.

However, for  $g \geq 2$ , the Jacquet-Langlands correspondence between  $G_g$  and  $GSp_g$  is not still fully understood well though in the case when  $g = 2$ , there are several important works which have recently come out (see [Hof21],[RW21]).

It seems morally possible to classify algebraic modular forms on  $G_g$  by using the trace formula approach as in [RW21] and relate them to Siegel modular forms on  $GSp_g$  though we need to prove the transfer theorem for Hecke operators with respect to the principal genus. Then Arthur's endoscopic classification (cf. [Art04],[Art13]) for  $GSp_g$  which is not still established except for  $g \leq 2$  would be used to obtain desired results for  $\mathcal{G}_2^{SS}(\ell, p)$ . From this picture, it would be easy for experts in the theory of automorphic representations to guess the upper bounds of Satake-parameters at  $\ell$  for Hecke eigen algebraic modular forms and Hecke eigen Siegel modular forms as well. It should be remarked that there are some classes of Hecke eigen Siegel modular forms which does not satisfy Ramanujan conjecture. They are so called CAP forms (cf. Section 3.9 of [Gan08]). However, such forms are expected to be negligible among all forms when  $p$  goes to infinity and this is in fact true for Siegel modular forms on  $GSp_g$  (see [KWY20],[KWY21]).

In fact, the third author showed that in fact, it is also true for  $M(K)$  when  $g = 2$  [Yam]. With this background from the theory of automorphic representations, in this section, we propose a conjecture that  $\mathcal{G}_g^{SS}(\ell, p)$  is asymptotically relatively Ramanujan when  $p$  goes to infinity (see Definition 6.7). We also give a conjecture related to Conjecture 1 of [FS21b] in our setting.

Henceforth, we use the index  $n$  to stand for  $G_n$  instead of the index  $g$  of  $G_g$  to avoid the confusion in which we use  $g$  as an element of the groups.

**6.1. Gross's definition.** We refer Chapter II of [Gro99] for the notation and basic facts. Recall the notation in Subsection 2.3. Put  $K = K(\mathcal{O}^n)$ . Since  $B$  is definite,  $G_n(\mathbb{R}) = GUSp_n(\mathbb{R})$  is compact modulo its center. It follows from (2.6) that

$$(6.1) \quad G_n(\mathbb{Q}) \backslash G_n(\mathbb{A}_{\mathbb{Q}}) / (K \times G_n(\mathbb{R})^+) = G_n(\mathbb{Q}) \backslash G_n(\mathbb{A}_f) / K$$

where  $G_n(\mathbb{R})^+$  stands for the connected component of the identity element and the cardinality of (6.1) is nothing but the class number  $H_n(p, 1)$  of the principal genus. According to Chapter II-4 of [Gro99], we define the  $\mathbb{C}$ -vector space  $M(K)$  consisting of all locally constant functions  $f : G_n(\mathbb{A}_{\mathbb{Q}}) \rightarrow \mathbb{C}$  such that

$$f(\gamma g k g_{\infty}) = f(g), \quad g \in G_n(\mathbb{A}_{\mathbb{Q}})$$

for all  $\gamma \in G_n(\mathbb{Q})$ ,  $k \in K$ , and  $g_{\infty} \in G_n(\mathbb{R})^+$ . Put  $h := H_n(p, 1)$  and pick  $\{\gamma_i\}_{i=1}^h$  with  $\gamma_i \in G_n(\mathbb{A}_f)$  a complete system of the representatives of (6.1). By definition, the space  $M(K)$  is generated by the characteristic functions  $\varphi_i$ ,  $1 \leq i \leq h$  of  $G_n(\mathbb{Q})\gamma_i K$ . Hence we have  $M(K) \simeq \mathbb{C}^{\oplus h}$ . We define a hermitian inner product  $(*, *)_K$  on  $M(K)$  by

$$(6.2) \quad (f_1, f_2)_K := \sum_{\gamma \in G_n(\mathbb{Q}) \backslash G_n(\mathbb{A}_f) / K} f_1(\gamma) \overline{f_2(\gamma)} \frac{1}{|\text{Aut}(\gamma)|}$$

for  $f_1, f_2 \in M(K)$  where  $\text{Aut}(\gamma) := (G_n(\mathbb{Q}) \cap \gamma K \gamma^{-1}) Z(\mathbb{A}_f) / Z(\mathbb{A}_f)$ . Let  $\varphi$  be a non-zero constant function on  $G_n(\mathbb{A}_{\mathbb{Q}})$ . We denote by  $M_0(K)$  the orthogonal complement of  $\mathbb{C}\varphi$  in  $M(K)$ . Clearly,  $\dim(M_0(K)) = h - 1 = H_n(p, 1) - 1$ .

**Definition 6.3.** Each element of  $M(K)$  is said to be an algebraic modular form on  $G_n(\mathbb{A}_{\mathbb{Q}}) = GUSp_n(\mathbb{A}_{\mathbb{Q}})$  of weight zero with level  $K$ .

For each prime  $\ell \neq p$  we define the (unramified) Hecke algebra

$$\mathcal{H}_{\ell} = \mathbb{C}[G_n(\mathbb{Z}_{\ell}) \backslash G_n(\mathbb{Q}_{\ell}) / G_n(\mathbb{Z}_{\ell})] \simeq \mathbb{C}[GSp_n(\mathbb{Z}_{\ell}) \backslash GSp_n(\mathbb{Q}_{\ell}) / GSp_n(\mathbb{Z}_{\ell})]$$

at  $\ell$  which is generated by the characteristic functions of form  $G_n(\mathbb{Z}_{\ell})gG_n(\mathbb{Z}_{\ell})$  for  $g \in G_n(\mathbb{Q}_{\ell})$ . Let  $e_{\ell}$  be the characteristic function of  $G_n(\mathbb{Z}_{\ell})$  which is the identity element of  $\mathcal{H}_{\ell}$ . Let  $\mathbb{T}^{(p)} = \otimes'_{\ell \neq p} \mathcal{H}_{\ell}$  be the restricted tensor product of  $\{\mathcal{H}_{\ell}\}_{\ell \neq p}$  with respect to the identity elements  $\{e_{\ell}\}_{\ell \neq p}$ . We call  $\mathbb{T}^{(p)}$  the Hecke ring outside  $p$  and it is well-known that  $\mathbb{T}^{(p)}$  acts on  $M(K)$  and also on  $M_0(K)$  (cf. Section 6 of [Gro99]).

**Definition 6.4.** Each element of  $M(K)$  is said to be a Hecke eigenform outside  $p$  if it is a simultaneous eigenform for all elements in  $\mathbb{T}^{(p)}$ .

By using the Hermitian paring (6.2), we can check that there exists an orthonormal basis  $HE(K)$  of  $M_0(K)$  which consists of Hecke eigenforms outside  $p$ . For each non-zero  $F$  in  $HE(K)$  and an element  $T \in \mathbb{T}^{(p)}$ , we denote by  $\lambda_F(T)$  the eigenvalue of  $F$  for  $T$ . Since  $F$  has the trivial central character,  $\lambda_T(F)$  is a real number. Recall the Hecke operator  $T(\ell)$  in Section 2.6. By definition  $T(\ell)$  is the characteristic function of  $G_n(\mathbb{Z}_\ell)t_\ell G_n(\mathbb{Z}_\ell)$  where  $t_\ell = \text{diag}(\overbrace{1, \dots, 1}^n, \overbrace{\ell, \dots, \ell}^n)$ .

As explained at the beginning of this section, under the background of the theory of automorphic representations, there are CAP forms in  $HE(K)$  which do not satisfy Ramanujan conjecture but they are expected to be negligible among all forms when  $p$  goes to infinity. In this vein, we propose the following:

**Conjecture 6.1.** *Put  $d_{n,p} := \dim M_0(K) = |HE(K)| = H_n(p, 1) - 1$ . For each  $\ell \neq p$ , it holds that*

$$\limsup_{p \rightarrow \infty} \frac{1}{d_{n,p}} \sum_{F \in HE(K)} |\lambda_F(T(\ell))| \leq 2^n \ell^{\frac{n(n+1)}{4}}.$$

The bound is nothing but the Ramanujan bound for  $T(\ell)$  for Siegel cusp forms on  $GS p_n$  whose automorphic representations are tempered at  $\ell$  (see Section 19 of [Gee08]). It also coincides with the spectral radius of the special 1-complex  $\mathcal{S}_n$  (see Proposition 2.6 of [Set13]).

**6.2. A speculation for bounds of eigenvalues of  $T(\ell)$ .** Let us consider the case when  $n = 2$ . Then we have three types of CAP forms in  $M(K)$  which are given by

- (1) cuspidal forms associated to Borel subgroup;
- (2) cuspidal forms associated to Klingen parabolic subgroup;
- (3) cuspidal forms associated to Siegel parabolic subgroup.

For the third case, historically, they are also called Saito-Kurokawa lifts [Gan08]. Any form in  $M(K)$  has the trivial central character and this shows the first case occurs only for the constant function. The second case also can not occur since such a form has a non-trivial central character. We remark that the eigenvalue of the constant function for  $T(\ell)$  is  $\ell^3 + \ell^2 + \ell + 1 = N_2(\ell)$ .

For the third case, the eigenvalue  $\lambda_{F_{\text{Siegel}}}(T(\ell))$  for each cuspidal form  $F_{\text{Siegel}}$  associated to Siegel parabolic subgroup satisfies

$$(6.5) \quad \ell^2 + 1 - 2\ell\sqrt{\ell} \leq \lambda_{F_{\text{Siegel}}}(T(\ell)) \leq \ell^2 + 1 + 2\ell\sqrt{\ell}.$$

As noticed before,  $\lambda_F(T(\ell))$  is always a real number for each  $F \in M(K)$  since  $F$  has a trivial central character.

For each non-CAP form  $F$  in  $M_0(K)$  we would expect that

$$(6.6) \quad |\lambda_F(T(\ell))| \leq 4\ell\sqrt{\ell}$$

and non-CAP forms are majority of  $M_0(K)$ .

It is easy to see that  $\ell^2 + 1 + 2\ell\sqrt{\ell}$  is the maximum among the upper bounds of (6.5) and (6.6) when  $\ell \geq 5$ . Let  $1 = \mu_1 > \mu_2 \geq \dots \geq \mu_m > -1$  be the eigenvalues of the random walk matrix (the normalized adjacency matrix) for  $\mathcal{G}_2^{SS}(\ell, p)$  with  $m = |SS_2(p)|$  and put  $\lambda_i = 1 - \mu_i$ .

**Conjecture 6.2.** *Assume  $p \geq 5$ . For each prime  $\ell \neq p$ , it holds that*

$$1 - \frac{\max\{4\ell\sqrt{\ell}, \ell^2 + 1 + 2\ell\sqrt{\ell}\}}{N_2(\ell)} \leq \lambda_i \leq 1 + \frac{4\ell\sqrt{\ell}}{N_2(\ell)}$$

*In particular, when  $\ell = 2$ ,*

$$1 - \frac{8\sqrt{2}}{15} = 0.24575\dots \leq \lambda_2, \quad 2 - \lambda_m \leq 1 + \frac{8\sqrt{2}}{15} = 1.75425\dots$$

**Remark 6.3.** *Comparing with Conjecture 1 of [FS21b], let*

$$\lambda_*(\mathcal{G}_2^{SS}(\ell, p)) = \min\{\lambda_2, 2 - \lambda_m\}.$$

*In particular, when  $\ell = 2$ , it yields*

$$1 - \frac{8\sqrt{2}}{15} = 0.24575\dots \leq \lambda_*(\mathcal{G}_2^{SS}(2, p)) \leq 1 + \frac{8\sqrt{2}}{15} = 1.75425\dots$$

*Further, we would be able to check the lower and upper bounds would be sharp by using the classification of Saito-Kurokawa forms due to Gan [Gan08] and equidistribution for Satake parameters of newforms in  $S_4(\Gamma_0(p))$  when  $p$  goes to infinity. Here  $S_4(\Gamma_0(p))$  stands for the space of elliptic cusp forms of weight 4 with respect to  $\Gamma_0(p) \subset SL_2(\mathbb{Z})$ . The assumption  $p \geq 5$  in Conjecture 6.2 is used to guarantee  $S_4(\Gamma_0(p)) \neq \{0\}$ .*

**6.3. Not being Ramanujan is not necessary fared.** As is expected naturally for experts in the theory of automorphic representations, the eigenvalues of the adjacency matrix for  $\mathcal{G}_g^{SS}(\ell, p)$  do not satisfy the Ramanujan bound when  $g \geq 2$ . However, in view of the theory of automorphic forms, it is plausible because of the existence of CAP forms violating Ramanujan property. Even one can prove, in fact, that it happens for  $\mathcal{G}_2^{SS}(\ell, p)$  for each  $\ell \geq 17$  and  $p \geq 5$  by using the results in [Gan08]. In Section 10.1 of [JZ21], they gave an example satisfying the Ramanujan bound but this is just possible only for small  $\ell$  (less than 13 to be precise). These things would happen similarly for general  $g$ . Nonetheless,  $\mathcal{G}_g^{SS}(\ell, p)$  has a nice property as Theorem 1.1 speaks out.

Therefore, a more conceptual, finer notation should be introduced to measure how good a family of regular graphs is. We here propose the following. Let  $\{X_i\}_{i \in I}$  be a family of  $d$ -regular graphs indexed by an ordered set  $I$  such that  $\lim_{i \rightarrow \infty} |X_i| = \infty$ . Let  $\lambda_{\text{mean}}(X_i)$  be the average of the absolute values of all eigenvalues of the normalized adjacency matrix for  $X_i$ . Suppose there exist a prime  $\ell$  and a reductive algebraic group  $G$  over  $\mathbb{Z}$  such that for each  $i \in I$ ,  $X_i = \Gamma_i \backslash G(\mathbb{Q}_\ell) / Z_G(\mathbb{Q}_\ell) G(\mathbb{Z}_\ell)$  for some lattice  $\Gamma_i$  in  $G(\mathbb{Q}_\ell)$  for each  $i \in I$ . Here  $Z_G$  is the center of  $G$ .

**Definition 6.7.** *We say  $\{X_i\}_{i \in I}$  is asymptotically relatively Ramanujan if*

$$\limsup_{i \rightarrow \infty} \lambda_{\text{mean}}(X_i) \leq \rho(\mathcal{B}^1(G^{\text{der}}))$$

where  $\mathcal{B}^1(G^{\text{der}})$  is a subgraph of the 1-skelton of the building  $\mathcal{B}(G)$  for  $G(\mathbb{Q}_\ell) / Z_G(\mathbb{Q}_\ell) G(\mathbb{Z}_\ell)$  such that  $G(\mathbb{Q}_\ell)$  acts transitively on  $\mathcal{B}^1(G^{\text{der}})$  and  $\rho(\mathcal{B}^1(G^{\text{der}}))$  stands for the spectral radius of the graph.

Our graph  $\mathcal{G}_g^{SS}(\ell, p)$  is related to  $G = GSp_g$  with  $G^{\text{der}} = Sp_g$  and its spectral radius is computed in Proposition 2.6 of [Set13] as already mentioned.

## REFERENCES

- [Art04] J. Arthur, Automorphic representations of  $GSp(4)$ . Contributions to automorphic forms, geometry, and number theory, 65 (2013) 81, Johns Hopkins Univ. Press, Baltimore, MD, 2004.
- [Art13] J. Arthur, The endoscopic classification of representations. Orthogonal and symplectic groups. American Mathematical Society Colloquium Publications, 61. American Mathematical Society, Providence, RI, 2013. xviii+590 pp.
- [BHV08] B. Bekka, P. de la Harpe, and A. Valette. *Kazhdan's Property (T)*, volume 11 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2008.
- [CLM+18] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes, CSIDH: An Efficient Post-Quantum Commutative Group Action. In: Peyrin T., Galbraith S. (eds) *Advances in Cryptology ASIACRYPT 2018*. Lecture Notes in Computer Science, vol 11274. Springer, Cham.
- [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-Verlag, Berlin, 1990. xii+316 pp.
- [CGL09] D-X. Charles, K. Lauter, and E-Z. Goren, Cryptographic hash functions from expander graphs. *J. Cryptology* 22 (2009), no. 1, 93-113.

- [Cou06] J-M. Couveignes, Hard Homogeneous Spaces, 2006. IACR Cryptography ePrint Archive 2006/291.
- [DJP14] L. De Feo, D. Jao, and J. Plût, “Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies” *J. Math. Cryptol.*, vol. 8, no. 3, 2014, pp. 209-247.
- [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>.
- [Eic38] M. Eichler, Über die Idealklassenzahl total definiter Quaternionenalgebren. *Math. Z.* 43 (1938), no. 1, 102-109.
- [Fal84] G. Faltings, Finiteness theorems for abelian varieties over number fields. by Edward Shipz. *Arithmetic geometry* (Storrs, Conn., 1984), 9–27, Springer, New York, 1986.
- [FS21a] E. Florit and B. Smith, An atlas of the superspecial Richelot isogeny graph, arXiv:2101.00917 (2021).
- [FS21b] E. Florit and B. Smith, Automorphisms and isogeny graphs of abelian varieties, with applications to the superspecial Richelot isogeny graph, arXiv:2101.00919 (2021).
- [FT19] E-V. Flynn, Y-B. Ti, Genus two isogeny cryptography. *Post-quantum cryptography*, 286306, Lecture Notes in Comput. Sci., 11505, Springer, Cham, 2019.
- [Gan08] W.T. Gan, *The Saito-Kurokawa space of  $PGSp_4$  and its transfer to inner forms*, Eisenstein series and applications, 87–123, *Progress in Math.* **258**, Birkhäuser Boston, 2008.
- [Gar97] P. Garrett, *Buildings and classical groups*. Chapman & Hall, London, 1997. xii+373 pp.
- [Gol11] O. Goldreich, Candidate one-way functions based on expander graphs. *Studies in complexity and cryptography*, Lecture Notes in Comput. Sci. 6650, 76–87, Springer, Heidelberg, 2011.
- [Gee08] G. van der Geer, Siegel modular forms and their applications. *The 1-2-3 of modular forms*, 181-245, Universitext, Springer, Berlin, 2008.
- [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.
- [Gro99] B-H. Gross, Algebraic modular forms. *Israel J. Math.* 113 (1999), 61-93.
- [HI80] K. Hashimoto and T. Ibukiyama, On class numbers of positive definite binary quaternion Hermitian forms. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* 27 (1980), no. 3, 549-601.
- [Hof21] P. van Hoften, A geometric Jacquet-Langlands correspondence for paramodular Siegel threefolds, *Math. Z.* 299 (2021), no. 3-4, 2029–2061.
- [Ibu18] T. Ibukiyama, Conjectures on correspondence of symplectic modular forms of middle parahoric type and Ihara lifts. *Res. Math. Sci.* 5 (2018), no. 2, Paper No. 18, 36 pp.
- [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. *Compositio Math.* 57 (1986), no. 2, 127-152.
- [JD11] D. Jao, L. De Feo, Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies. In: Yang BY. (eds) *Post-Quantum Cryptography. PQCrypto 2011*. Lecture Notes in Computer Science, vol 7071. Springer, Berlin, Heidelberg, 2011.

- [JZ21] B-W. Jordan and Y. Zaytman, Isogeny graphs of superspecial abelian varieties and Brandt matrices, arXiv:2005.09031, (2021).
- [KT20] T. Katsura and K. Takashima, Counting Richelot isogenies between superspecial abelian surfaces, Proceedings of the Fourteenth Algorithmic Number Theory Symposium (Steven D. Galbraith, ed.), vol. 4, The Open Book Series, no. 1, Mathematical Sciences Publishers, 2020, pp. 283–300.
- [KL14] J. Katz and Y. Lindell, Introduction to Modern Cryptography. 2nd ed., CRC Press, 2014.
- [KWY20] H-H. Kim, S. Wakatsuki, and T. Yamauchi, An equidistribution theorem for holomorphic Siegel modular forms for  $GSp_4$  and its applications. J. Inst. Math. Jussieu 19 (2020), no. 2, 351-419.
- [KWY21] H-H. Kim, S. Wakatsuki, and T. Yamauchi, Equidistribution theorems for holomorphic Siegel cusp forms of general degree: the level aspect, arXiv:2106.07811, (2021).
- [LO98] K-Z. Li, and F. Oort, Moduli of supersingular abelian varieties. Lecture Notes in Mathematics, 1680. Springer-Verlag, 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. Arithmetic geometry (Storrs, Conn., 1984), 103-150, Springer, New York, 1986.
- [Mum70] D. Mumford, Mumford, David 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.
- [Piz80] A-K. Pizer, An algorithm for computing modular forms on  $\Gamma_0(N)$ . J. Algebra 64 (1980), no. 2, 340-390.
- [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. Computational perspectives on number theory (Chicago, IL, 1995), 159–178, AMS/IP Stud. Adv. Math., 7, Amer. Math. Soc., Providence, RI, 1998.
- [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, Inc., Boston, MA, 1994. xii+614 pp.
- [RW21] M. Rösner and R. Weissauer, Global liftings between inner forms of  $GSp(4)$ , arXiv:2103.14715, (2021).
- [RS06] A. Rostovtsev and A. Stolbunov, Public-key cryptosystem based on isogenies, 2006. IACR Cryptology ePrint Archive 2006/145.
- [Set13] A. Setyadi, Expanders and the affine building of  $Sp_n$ . Ars Combin. 109 (2013), 497-510.
- [She07] Thomas R. Shemanske. The arithmetic and combinatorics of buildings for  $Sp_n$ . Trans. Amer. Math. Soc., 359(7):3409–3423, 2007.
- [Shim71a] G. Shimura, On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields. Nagoya Math. J. 43 (1971), 199-208.



- [Shim71b] G. Shimura, Introduction to the arithmetic theory of automorphic functions. Reprint of the 1971 original. Publications of the Mathematical Society of Japan, 11. Kan Memorial Lectures, 1. Princeton University Press, Princeton, NJ, 1994. xiv+271 pp.
- [Shin12] S-W. Shin, Automorphic Plancherel density theorem. Israel J. Math. 192 (2012), no. 1, 83-120.
- [Sil09] J-H. Silverman, The arithmetic of elliptic curves. Second edition. Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009. xx+513 pp.
- [Sor09] C-M. Sorensen, Level-raising for Saito-Kurokawa forms. Compos. Math. 145 (2009), no. 4, 915-953.
- [TTT17] H. Tachibana, K. Takashima, T. Takagi, Constructing an efficient hash function from 3-isogenies, JSIAM Letters, 2017, Volume 9, Pages 29-32, Released April 12, 2017.
- [Tak18] K. Takashima, Efficient algorithms for isogeny sequences and their cryptographic applications. Mathematical modelling for next-generation cryptography, 97-114, Math. Ind. (Tokyo), 29, Springer, Singapore, 2018.
- [Tate66] J. Tate, Endomorphisms of abelian varieties over finite fields. Invent. Math. 2 (1966), 134-144.
- [Wei09] R. Weissauer, Endoscopy for  $GSp(4)$  and the cohomology of Siegel modular threefolds. Lecture Notes in Mathematics 1968. Springer-Verlag, Berlin, 2009.
- [Vél71] J. Vélú, Isogénies entre courbes elliptiques, C.R. Acad. Sc. Paris, Série A., 273, pp. 238-241 (1971).
- [Yam] T. Yamauchi, On Ibukiyama conjecture for inner forms of  $GSp_4$ , in preparation.
- [Yu12] C-F. Yu, Superspecial abelian varieties over finite prime fields. J. Pure Appl. Algebra 216 (2012), no. 6, 1418-1427.

YUSUKE AIKAWA, INFORMATION TECHNOLOGY R&D CENTER, MITSUBISHI ELECTRIC CORPORATION JAPAN  
*Email address:* `Aikawa.Yusuke@bc.MitsubishiElectric.co.jp`

RYOKICHI TANAKA, DEPARTMENT OF MATHEMATICS, KYOTO UNIVERSITY, KYOTO 606-8502 JAPAN  
*Email address:* `rtanaka@math.kyoto-u.ac.jp`

TAKUYA YAMAUCHI, MATHEMATICAL INSTITUTE TOHOKU UNIVERSITY, SENDAI 980-8578 JAPAN  
*Email address:* `takuya.yamauchi.c3@tohoku.ac.jp`