

ISOGENY GRAPHS OF SUPERSPECIAL ABELIAN VARIETIES AND BRANDT MATRICES

BRUCE W. JORDAN AND YEVGENY ZAYTMAN

ABSTRACT. Fix primes p and ℓ with $\ell \neq p$. If (A, λ) is a g -dimensional principally polarized abelian variety, an $(\ell)^g$ -isogeny of (A, λ) has kernel a maximal isotropic subgroup of the ℓ -torsion of A ; the image has a natural principal polarization. In this paper we study the isogeny graphs of $(\ell)^g$ -isogenies of principally polarized superspecial abelian varieties in characteristic p . We define three isogeny graphs associated to such $(\ell)^g$ -isogenies – the big isogeny graph $Gr_g(\ell, p)$, the little isogeny graph $gr_g(\ell, p)$, and the enhanced isogeny graph $\tilde{gr}_g(\ell, p)$. We apply strong approximation for the quaternionic unitary group to prove both that $gr_g(\ell, p)$ and $Gr_g(\ell, p)$ are connected and that they are not bipartite. The connectedness of the enhanced isogeny graph $\tilde{gr}_g(\ell, p)$ then follows. The quaternionic unitary group has previously been applied to moduli of abelian varieties in characteristic p (sometimes invoking strong approximation) by Chai, Ekedahl/Oort, and Chai/Oort. The adjacency matrices of the three isogeny graphs are given in terms of the Brandt matrices defined by Hashimoto, Ibukiyama, Ihara, and Shimizu. We study some basic properties of these Brandt matrices and recast the theory using the notion of Brandt graphs. We show that the isogeny graphs $Gr_g(\ell, p)$ and $gr_g(\ell, p)$ are in fact our Brandt graphs. We give the ℓ -adic uniformization of $gr_g(\ell, p)$ and $\tilde{gr}_g(\ell, p)$. The $(\ell + 1)$ -regular isogeny graph $Gr_1(\ell, p)$ for supersingular elliptic curves is well known to be Ramanujan. We calculate the Brandt matrices for a range of $g > 1$, ℓ , and p . These calculations give four examples with $g > 1$ where the regular graph $Gr_g(\ell, p)$ has two vertices and is Ramanujan, and all other examples we computed with $g > 1$ and two or more vertices were not Ramanujan. In particular, the $(\ell)^g$ -isogeny graph is not in general Ramanujan for $g > 1$.

2010 *Mathematics Subject Classification*. Primary 14K02; Secondary 11G10, 14G15.

Key words and phrases. superspecial, abelian varieties, isogeny graphs, Brandt matrices, quaternionic unitary group.

CONTENTS

1. Introduction	3
Part 1. The quaternion infrastructure	6
2. Definite rational quaternion algebras	6
2.1. Hermitian matrices	6
2.2. Strong Approximation for $\mathbb{H}_1^\times$	7
2.2.1. Strong approximation	7
2.2.2. A key lemma	7
2.2.3. Consequences for $\text{Mat}_{g \times g}(\mathcal{O}_{\mathbb{H}})$	8
2.3. The quaternionic unitary group	8
3. Brandt matrices	10
3.1. Definition of Brandt matrices	10
3.2. Brandt matrices: Examples	13
3.2.1. $\mathbb{H} = \mathbb{H}_7$	13
3.2.2. $\mathbb{H} = \mathbb{H}_{11}$	14
3.3. First properties of Brandt matrices	14
3.3.1. The classical case: $g = 1$	14
3.3.2. The general case $g \geq 1$	15
4. The big and little Brandt graphs	18
4.1. Graphs	18
4.2. The big Brandt graph $Br_g(n, \mathcal{O}_{\mathbb{H}})$	19
4.3. The little Brandt graph $br_g(n, \mathcal{O}_{\mathbb{H}})$	19
Part 2. Applying the quaternion infrastructure to isogeny graphs	20
5. Superspecial abelian varieties, their principal and $[\ell]$ -polarizations, and their isogenies	20
6. The big, little, and enhanced isogeny graphs	25
6.1. The big isogeny graph $Gr_g(\ell, p)$	25
6.2. The little isogeny graph $gr_g(\ell, p)$	26
6.3. The enhanced isogeny graph $\tilde{gr}_g(\ell, p)$	27
7. Connectedness results for isogeny graphs	28
7.1. Connectedness for $g = 1$: supersingular elliptic curves	28
7.2. Connectedness for $g > 1$	29
8. The ℓ -adic uniformization of $gr_g(\ell, p)$ and $\tilde{gr}_g(\ell, p)$	30
8.1. The case $g = 1$: ℓ -adically uniformizing $gr_1(\ell, p)$ and $\tilde{gr}_1(\ell, p)$	32
8.2. The isogeny graphs $gr_1(\ell, p)$, $\tilde{gr}_1(\ell, p)$ and Shimura curves	32
8.3. The general case $g \geq 1$: ℓ -adically uniformizing $gr_g(\ell, p)$ and $\tilde{gr}_g(\ell, p)$	33
9. Computations: The Ramanujan property for $Gr_g(\ell, p)$ with $g > 1$	34
9.1. A non-Ramanujan example	34
9.2. A Ramanujan example	34
9.3. A range of computations	34
Acknowledgments	35
References	35

1. INTRODUCTION

A superspecial abelian variety $A/\overline{\mathbb{F}}_p$ of dimension g is isomorphic to a product of g supersingular elliptic curves. If $g > 1$, surprisingly all such products are isomorphic to each other by Theorem 1 below. Fix a supersingular elliptic curve $E/\overline{\mathbb{F}}_p$ with $\mathcal{O} = \mathcal{O}_E = \text{End}(E)$ a maximal order in the rational definite quaternion algebra $\mathbb{H}_p$ ramified at p .

Theorem 1. (Deligne, Ogus [Ogu79], Shioda [Shi79]) *Suppose $A/\overline{\mathbb{F}}_p$ is a superspecial abelian variety with $\dim A = g > 1$. Then $A \cong E^g$.*

So for dimension $g = 1$ there are *many* superspecial abelian varieties (= supersingular elliptic curves) each with *one* principal polarization, but for $g > 1$ there is *one* superspecial abelian variety with *many* principal polarizations.

Let $\mathcal{A} = (A = E^g, \lambda)$ be a principally polarized superspecial abelian variety of dimension g over $\overline{\mathbb{F}}_p$ with $\overline{\mathbb{F}}_p$ -isomorphism class $[\mathcal{A}]$. The principal polarization λ is an isomorphism from A to $\hat{A} = \text{Pic}^0(A)$ satisfying the conditions of Definition 23. The number $h = h_g(p)$ of such isomorphism classes $[\mathcal{A}]$ is finite and is a type of class number. For $g \geq 1$ set

$$\begin{aligned} \text{SP}_g(p)_0 &= \{\overline{\mathbb{F}}_p\text{-isomorphism classes } [\mathcal{A}]\} \\ &= \{[\mathcal{A}_1], \dots, [\mathcal{A}_h]\} \text{ with } \mathcal{A}_j = (A_j = E^g, \lambda_j) \text{ if } g > 1. \end{aligned} \tag{1}$$

So, for example,

$$\begin{aligned} \text{SP}_1(p)_0 &= \{\text{supersingular } j\text{-invariants in characteristic } p\} \text{ and} \\ \#\text{SP}_1(p)_0 &= h_1(p) = h(\mathbb{H}_p), \text{ the class number of the quaternion algebra } \mathbb{H}_p. \end{aligned}$$

A principal polarization λ on the abelian variety $A/\overline{\mathbb{F}}_p$ defines a Weil pairing on $A[n]$ with $(n, p) = 1$: $\langle \ , \ \rangle_{\lambda, n} : A[n] \times A[n] \rightarrow \mu_n$. For $(n, p) = 1$, put

$$\text{Iso}_n(\mathcal{A}) = \{\text{maximal isotropic subgroups } C \subseteq A[n]\} \text{ with } N_g(n) := \#\text{Iso}_n(\mathcal{A}). \tag{2}$$

Note that $N_g(n)$ is the number of maximal isotropic subgroups of the standard nondegenerate symplectic $\mathbb{Z}/n\mathbb{Z}$ -module of rank $2g$. In case $n = \ell \neq p$ is prime we have

$$\#\text{Iso}_\ell(\mathcal{A}) =: N_g(\ell) = \prod_{k=1}^g (\ell^k + 1); \tag{3}$$

see, for example, [Ple65, p. 419]. Suppose $C \subseteq A[\ell]$ is a subgroup with corresponding isogeny $\psi_C : A \rightarrow A/C =: A'$. Then there is a principal polarization λ' on A' so that $\psi_C^*(\lambda') = \ell\lambda$ if and only if $C \in \text{Iso}_\ell(\mathcal{A})$. In this case write $\mathcal{A}' = (A', \lambda') = \mathcal{A}/C$ and say that ψ_C is an $(\ell)^g$ -isogeny. If $[\mathcal{A}] \in \text{SP}_g(p)_0$, then $[\mathcal{A}'] \in \text{SP}_g(p)_0$. Such $(\ell)^g$ -isogenies induce correspondences from the finite set $\text{SP}_g(p)_0$ to itself. These correspondences can be used to define various graphs—in this paper we define *three* $(\ell)^g$ -isogeny graphs: the *big* isogeny graph $Gr_g(\ell, p)$, the *little* isogeny graph $gr_g(\ell, p)$, and the *enhanced* isogeny graph $\tilde{gr}_g(\ell, p)$. The literature seems to have only one isogeny graph; this ubiquitous graph is the big isogeny graph $Gr_g(\ell, p)$ for us.

Distinguishing between these three makes many results clearer and more precise. Take the case $g = 1$ for example: the little and enhanced isogeny graphs are uniformized by the Bruhat-Tits tree $\Delta = \Delta_\ell$ of $\text{SL}_2(\mathbb{Q}_\ell)$; the big isogeny graph $Gr_1(\ell, p)$ is not, cf. Section 8.1. And it is $gr_1(\ell, p)$ and $\tilde{gr}_1(\ell, p)$ which arise from the bad reduction of Shimura curves and not the familiar big isogeny graph $Gr_1(\ell, p)$ as we show in Section 8.2. For general $g \geq 1$,

the big isogeny graph $Gr_g(\ell, p)$ is a regular graph by Theorem 37(c), so it is natural to ask if it is Ramanujan, whereas the little isogeny graph $gr_g(\ell, p)$ and the enhanced isogeny graph $\tilde{gr}_g(\ell, p)$ are not regular.

In this introduction we content ourselves with defining the simplest of the three, the big isogeny graph $Gr = Gr_g(\ell, p)$:

Definition 2. The vertices of the graph $Gr = Gr_g(\ell, p)$ are $\text{Ver}(Gr) = \text{SP}_g(p)_0$, so $h = h_g(p) = \# \text{Ver}(Gr)$. The (directed) edges of Gr connecting the vertex $[\mathcal{A}_i] \in \text{SP}_g(p)_0$ to the vertex $[\mathcal{A}_j] \in \text{SP}_g(p)_0$ are

$$\text{Ed}(Gr)_{ij} = \{C \in \text{Iso}_\ell(\mathcal{A}_i) \mid [\mathcal{A}_i/C] = [\mathcal{A}_j]\}.$$

The adjacency matrix $\text{Ad}(Gr)_{ij} = \# \text{Ed}(Gr)_{ij}$ is a constant row-sum matrix by (2):

$$\sum_{j=1}^h \# \text{Ed}(Gr)_{ij} = \prod_{k=1}^g (\ell^k + 1). \quad (4)$$

This paper studies these three $(\ell)^g$ -isogeny graphs via definite quaternion algebras. It naturally divides into two parts – Part 1 (Sections 2 – 4) develops this infrastructure on definite quaternion algebras; Part 2 (Sections 5 – 9) connects the quaternion infrastructure to superspecial abelian varieties together with their polarizations and isogenies, and then applies it to our three isogeny graphs. In Section 2 we prove the foundational material required on the arithmetic of definite quaternion algebras together with the Hermitian forms and unitary groups defined from them. Section 3 introduces the Brandt matrices $B_g(\ell)$ for the maximal order $\mathcal{O}$ of $\mathbb{H}_p$, first defined for $g > 1$ in the 1980's by Hashimoto, Ibukiyama, Ihara, and Shimizu – see [Has80]. Gross's algebraic modular forms [Gro99] for the quaternionic unitary group subsequently provided a more general context for these matrices. In Section 4 we extend Brandt matrices to Brandt graphs $Br_g(\ell, p)$ and $br_g(\ell, p)$; we further extend Brandt graphs to Brandt simplicial complexes in [JZ]. Brandt graphs, like Brandt matrices, are defined entirely in terms of definite quaternion algebras and as such are amenable to machine computation. Brandt graphs contain slightly more information than Brandt matrices – the Brandt matrix $B_g(\ell)$ is the adjacency matrix of the big Brandt graph $Br_g(\ell, p)$ and the weighted adjacency matrix of the little Brandt graph with weights $br_g(\ell, p)$ (Proposition 22).

In Part 2 we turn to algebraic geometry. We consider superspecial abelian varieties, their polarizations, and their isogenies in Section 5. We introduce the key notion of an $[\ell]$ -polarized abelian variety and its $[\ell]$ -dual. Section 6 then defines the three $(\ell)^g$ -isogeny graphs $Gr_g(\ell, p)$, $gr_g(\ell, p)$, and $\tilde{gr}_g(\ell, p)$. Sections 7 – 9 contain our main results on isogeny graphs, which we now summarize.

A. Relationship between the quaternion infrastructure and our isogeny graphs.

We prove in Theorem 37 the fundamental result that big isogeny graph is the big Brandt graph: $Gr_g(\ell, p) = Br_g(\ell, p)$. Likewise the little isogeny graph with weights is the little Brandt graph with weights: $gr_g(\ell, p) = br_g(\ell, p)$ (Theorem 39). We further explain how to get the enhanced isogeny graph $\tilde{gr}_g(\ell, p)$ from the little isogeny graph $gr_g(\ell, p)$ in Theorem 40. Because of these theorems our three isogeny graphs can all be defined and computed entirely in terms of definite quaternion algebras – it is never necessary to write down superspecial abelian varieties or isogenies. In Section 9, we compute our isogeny graphs for a range of 174 triples (g, ℓ, p) with $g = 2, 3$ including 13 examples with $g = 3$ – an impossible feat working with explicit superspecial abelian varieties and $(\ell)^g$ -isogenies.

B. Connectedness theorems. It is well known that the ℓ -isogeny graph $\text{Gr}_1(\ell, p)$ for supersingular elliptic curves in characteristic p is connected. A main theorem of this paper is that the isogeny graphs $Gr_g(\ell, p)$, $gr_g(\ell, p)$, and $\tilde{gr}_g(\ell, p)$ are connected for $g \geq 1$; cf. Section 7. This had been conjectured for $g = \ell = 2$ in [CDS20, Conjecture 1], for example; we establish the result here for all ℓ and $g \geq 1$. Additionally we prove that $Gr_g(\ell, p)$ and $gr_g(\ell, p)$ are not bipartite. Besides results on polarizations, the main ingredients of the proof for $g > 1$ are strong approximation for the quaternionic unitary group (Theorem 43) and Theorem 35 on factoring isogenies which in turn follows from Theorem 36 on the symplectic group Sp_{2g} over $\mathbb{Z}/\ell^n\mathbb{Z}$. Note that knowing strong approximation still requires the results on factoring isogenies to deduce connectedness. The quaternionic unitary group has previously been applied to moduli of abelian varieties in characteristic p by Chai [Cha95, Prop. 1], Ekedahl/Oort [Oor01, §7], and Chai/Oort [CO11, Prop. 4.3]; a version of strong approximation for the quaternionic unitary group is given in [Oor01, Lemma 7.9].

C. ℓ -adic uniformization; Shimura curves when $g = 1$. Let $\Gamma_0 = \mathcal{O}[1/\ell]^\times$ viewed as a subgroup of $\text{GL}_2(\mathbb{Q}_\ell)$ with $\bar{\Gamma}_0$ its image in $\text{PGL}_2(\mathbb{Q}_\ell)$. Similarly let $\Gamma_1 = \{\gamma \in \Gamma_0 \mid \text{Nm}_{\mathbb{H}_p/\mathbb{Q}}(\gamma) = 1\}$ with $\bar{\Gamma}_1$ its image in $\text{PGL}_2(\mathbb{Q}_\ell)$. Let $\Delta = \Delta_\ell$ be the Bruhat-Tits tree for $\text{SL}_2(\mathbb{Q}_\ell) = \text{Sp}_2(\mathbb{Q}_\ell)$. We prove that $gr_1(\ell, p) = \Gamma_0 \backslash \Delta_\ell$ and $\tilde{gr}_1(\ell, p) = \Gamma_1 \backslash \Delta_\ell$ as graphs with weights in Theorem 49. We then generalize this to $g > 1$ in Theorem 54: Let $\mathcal{S}_{2g}$ be the special 1-skeleton of the Bruhat-Tits building $\mathcal{B}_{2g}$ for the symplectic group $\text{Sp}_{2g}(\mathbb{Q}_\ell)$ as in Remark 46. Let $U_g(\mathcal{O}[1/\ell])$ be the quaternionic unitary group with $\text{GU}_g(\mathcal{O}[1/\ell])$ the general quaternionic unitary group as in (9). Then we prove $gr_g(\ell, p) = \text{GU}_g(\mathcal{O}[1/\ell]) \backslash \mathcal{S}_{2g}$ and $\tilde{gr}_g(\ell, p) = U_g(\mathcal{O}[1/\ell]) \backslash \mathcal{S}_{2g}$ as graphs with weights—see Theorem 54.

When $g = 1$ we can use this result to connect the ℓ -isogeny graph $\tilde{gr}_1(\ell, p)$ for supersingular elliptic curves in characteristic p to the bad reduction of Shimura curves. Let B be the rational quaternion algebra of discriminant ℓp with $\mathcal{M} \subset B$ a maximal order. Let $V_B/\mathbb{Q}$ be the Shimura curve parametrizing abelian surfaces with quaternionic multiplication (QM) by $\mathcal{M}$ with $M_B/\mathbb{Z}$ the coarse moduli scheme model for $V_B/\mathbb{Q}$ constructed by Drinfeld [Dri76]. Then $M_B \times \mathbb{Z}_\ell$ is an *admissible curve* in the sense of [JL85, Defn. 3.1], and so has a dual graph [JL85, Defn. 3.2] $G(M_B \times \mathbb{Z}_\ell/\mathbb{Z}_\ell)$ which is a graph with lengths as in Definition 21(b). We show in Corollary 52(a) that $G(M_B \times \mathbb{Z}_\ell/\mathbb{Z}_\ell) = \tilde{gr}_1(\ell, p)$. But the dual graph $G(M_B \times \mathbb{Z}_\ell/\mathbb{Z}_\ell)$ governs vanishing cycles on the curve $M_B \times \mathbb{Z}_\ell/\mathbb{Z}_\ell$: the character group of the Néron model of the jacobian $\text{Jac}(V_B)/\mathbb{Q}_\ell$ is $H_1(G(M_B \times \mathbb{Z}_\ell/\mathbb{Z}_\ell), \mathbb{Z})$. The fact that the dual graph of the Shimura curve V_B in characteristic ℓ is an isogeny graph for supersingular elliptic curves in the different characteristic p is the key to Ribet’s proof [Rib90] of Serre’s Conjecture “Epsilon”, and so ultimately to Fermat’s Last Theorem.

Generalizing this picture to $g > 1$ is compelling: Relate $gr_g(\ell, p)$, $\tilde{gr}_g(\ell, p)$ to vanishing cycles for higher-dimensional Shimura varieties over $\mathbb{Q}_\ell$.

D. The Ramanujan property for $Gr_g(\ell, p)$. The big isogeny graph $Gr_g(\ell, p)$ is a regular graph, and one can ask whether it is Ramanujan. If $g = 1$ it is always Ramanujan, as follows from the Riemann hypothesis for curves over finite fields. Hence naively one might expect the Ramanujan property to continue to hold for $g \geq 2$ – see, for example, [CS20, Hypothesis 1]. The adjacency matrix $\text{Ad}(Gr_g(\ell, p))$ is the Brandt matrix $B_g(\ell)$, and so amenable to machine computation as discussed in **A** above. In Section 9 we give the results of checking the Ramanujan property over a range of ℓ and p with $g = 2, 3$. The memory requirements grow rapidly with ℓ and especially g ; we had no computations finish

with $g > 3$. We computed 174 examples with $g > 1$ and 2 or more vertices and found only 4 Ramanujan: $(g, \ell, p) = (2, 2, 5), (2, 2, 7), (2, 3, 7), (3, 2, 3)$ are Ramanujan. They all have two vertices, although not every 2-vertex $Gr_g(\ell, p)$ is Ramanujan. So seemingly for $g \geq 2$ the isogeny graph $Gr_g(\ell, p)$ is generically *not* Ramanujan. In Section 9.1 we compute $Gr_2(2, 11)$ in terms of superspecial abelian surfaces and Richelot isogenies, thereby giving a non-Ramanujan example computed entirely by algebraic geometry. In Section 9.2 we likewise compute $Gr_2(2, 7)$ in terms of abelian surfaces and Richelot isogenies to give a Ramanujan example computed entirely via algebraic geometry.

We conclude the introduction with brief comments on prior results. The case $g = 1$ was the setting for multiple proposals in post-quantum cryptography, and naturally the question of generalizing to $g > 1$ arose. Castryck, Decru, and Smith [CDS20] proposed the superspecial isogeny graph $Gr_2(2, p)$ as a good generalization to abelian surfaces. Previous work often concentrates on $Gr_2(2, p)$ where computations are feasible using classical Richelot isogenies – see, for example, Katsura and Takashima [KT20] and the references therein. (In contrast, we compute $Gr_g(\ell, p)$ by computing Brandt matrices for quaternion algebras.) The paper [ATY24] gives an alternate definition of $Gr_g(\ell, p)$ and develops this.

Part 1. The quaternion infrastructure

2. DEFINITE RATIONAL QUATERNION ALGEBRAS

Let $\mathbb{H}$ be a definite quaternion algebra over $\mathbb{Q}$ with a maximal order $\mathcal{O}_{\mathbb{H}}$, main involution $x \mapsto \bar{x}$, and reduced norm $\text{Nm}_{\mathbb{H}/\mathbb{Q}}(x) = \text{Nm}(x) = x\bar{x}$. Set $\mathbb{H}_1^\times = \{h \in \mathbb{H}^\times \mid \text{Nm}_{\mathbb{H}/\mathbb{Q}}(h) = 1\}$. The reduced norm $\text{Nm} : \mathbb{H} \rightarrow \mathbb{Q}$ generalizes to the reduced norm $\text{Nm} : \text{Mat}_{g \times g}(\mathbb{H}) \rightarrow \mathbb{Q}$ (given by a multiplicative polynomial of degree $2g$ in the entries of the matrix). Put

$$\text{SL}_g(\mathcal{O}_{\mathbb{H}}) = \{M \in \text{Mat}_{g \times g}(\mathcal{O}_{\mathbb{H}}) \mid \text{Nm}(M) = 1\} \quad (5)$$

with $\text{SL}_g(\mathbb{H})$ defined analogously. Note that

$$\text{SL}_g(\mathcal{O}_{\mathbb{H}}) = \text{GL}_g(\mathcal{O}_{\mathbb{H}}) = \{M \in \text{Mat}_{g \times g}(\mathcal{O}_{\mathbb{H}}) \mid M \text{ is invertible}\}.$$

Let $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$ be the profinite completion of $\mathbb{Z}$ and $\widehat{\mathbb{Q}} = \widehat{\mathbb{Z}} \otimes \mathbb{Q}$ the finite adèles of $\mathbb{Q}$. Then $\mathcal{O}_{\widehat{\mathbb{H}}} = \mathcal{O}_{\mathbb{H}} \otimes \widehat{\mathbb{Z}}$ is the profinite completion of $\mathcal{O}_{\mathbb{H}}$ and $\widehat{\mathbb{H}} = \mathcal{O}_{\widehat{\mathbb{H}}} \otimes \mathbb{Q}$ is the finite adèles of $\mathbb{H}$.

2.1. Hermitian matrices. Let $g \geq 1$ be an integer. A matrix $H \in \text{Mat}_{g \times g}(\mathcal{O}_{\mathbb{H}})$ is Hermitian if $H^\dagger := \overline{H}^t = H$. Set

$$\mathcal{H}_g(\mathcal{O}_{\mathbb{H}}) = \{H \in \text{Mat}_{g \times g}(\mathcal{O}_{\mathbb{H}}) \mid H \text{ is positive-definite Hermitian}\}. \quad (6)$$

The “Haupt norm” HNm of Braun-Koecher [BK66, Chap. 2, §4] (see also [Mum08, Thm. 6 and proof, §21]) is defined on Hermitian matrices in $\text{Mat}_{g \times g}(\mathbb{H})$ and gives a map $\text{HNm} : \mathcal{H}_g(\mathcal{O}_{\mathbb{H}}) \rightarrow \mathbb{N}$. It is characterized by $\text{HNm}(\text{Id}_{g \times g}) = 1$ and $\text{Nm}(H) = \text{HNm}(H)^2$ for a Hermitian matrix $H \in \text{Mat}_{g \times g}(\mathbb{H})$; see [Eke87, p. 152, 153], where HNm is denoted Pf and is defined via the usual Pfaffian on skew-symmetric matrices. For an integer $d \geq 1$ put

$$\mathcal{H}_{g,d}(\mathcal{O}_{\mathbb{H}}) = \{H \in \mathcal{H}_g(\mathcal{O}_{\mathbb{H}}) \mid \text{HNm}(H) = d\}. \quad (7)$$

The group $\text{SL}_g(\mathcal{O}_{\mathbb{H}}) = \text{GL}_g(\mathcal{O}_{\mathbb{H}})$ acts on $\mathcal{H}_{g,d}(\mathcal{O}_{\mathbb{H}})$ by $H \cdot M = M^\dagger H M$. Set

$$\overline{\mathcal{H}}_{g,d}(\mathcal{O}_{\mathbb{H}}) := \mathcal{H}_{g,d}(\mathcal{O}_{\mathbb{H}}) / \text{SL}_g(\mathcal{O}_{\mathbb{H}}) \quad (8)$$

with $[H] \in \overline{\mathcal{H}}_{g,d}(\mathcal{O}_{\mathbb{H}})$ the class defined by $H \in \mathcal{H}_{g,d}(\mathcal{O}_{\mathbb{H}})$. The sets $\overline{\mathcal{H}}_{g,d}(\mathcal{O}_{\mathbb{H}})$ for $d \geq 1$ are finite.

2.2. Strong Approximation for $\mathbb{H}_1^\times$. We now give the statement of strong approximation followed by several consequences for the multiplicative group of norm-1 quaternions. In Section 7 we will use strong approximation for the quaternionic unitary group.

2.2.1. Strong approximation. Let k be an algebraic number field with ∞ the set of all archimedean places of k . Let $S \supseteq \infty$ be a finite set of places of k . Let G be a linear algebraic group over k . Let $G_{\mathbb{A}}$ be the adèle group of G , $G_S \subset G_{\mathbb{A}}$ be the S -component $\prod_{v \in S} G_{k_v}$ of $G_{\mathbb{A}}$, and $G_k \subset G_{\mathbb{A}}$ be the k -rational points of G embedded diagonally.

Definition 3. The pair (G, S) has **strong approximation** if $G_S G_k$ is dense in $G_{\mathbb{A}}$.

Say that a connected noncommutative linear algebraic group G over a field k is **k -simple** if it has no positive-dimensional proper normal subgroups. We now give a statement of Strong Approximation sufficient for our purposes, quoting Platonov and Rapinchuk [PR94, Thm. 7.12]. The general result is due to Kneser [Kne66].

Theorem 4. *Let G be a simply connected and k -simple linear algebraic group over a number field k . Suppose G_S is not compact. Then (G, S) has strong approximation.*

2.2.2. A key lemma.

Lemma 5. *Let $\mathbb{H}/\mathbb{Q}$ be an arbitrary definite quaternion algebra with maximal order $\mathcal{O}_{\mathbb{H}}$, let I be a fractional right $\mathcal{O}_{\mathbb{H}}$ -ideal of norm 1, and let ℓ be a prime unramified in $\mathbb{H}$. Then there exists an element in $I \otimes \mathbb{Z}[1/\ell]$ of norm 1.*

Proof. Let G be the algebraic group over $\mathbb{Q}$ associated to $\mathbb{H}_1^\times = \{\beta \in \mathbb{H}^\times \mid \text{Nm}(\beta) = 1\}$; then $G(\mathbb{Q}) = \mathbb{H}_1^\times$. The algebraic group G is simply connected with a simple Lie algebra since $G(\mathbb{R}) \cong \text{SU}(2)$ is. (Let G' be the algebraic group over $\mathbb{Q}$ associated to $\mathbb{H}^\times$, so that $G'(\mathbb{Q}) = \mathbb{H}^\times$ and $G'(\mathbb{R}) = (\mathbb{H} \otimes_{\mathbb{Q}} \mathbb{R})^\times$ is the multiplicative group of Hamilton real quaternions. Note that G' doesn't satisfy the hypotheses of Theorem 4 (Strong Approximation): $G'(\mathbb{R}) = (\mathbb{H} \otimes_{\mathbb{Q}} \mathbb{R})^\times$ is topologically $\mathbb{R}^4$ minus the origin, which is simply connected, but as a Lie group, $G'(\mathbb{R})$ is $\mathbb{R}_{>0}^\times \times \text{SU}(2)$, which is not simple.) Let $S = \{\ell, \infty\}$. By Theorem 4, (G, S) has strong approximation.

Now consider the subset $U \subset G_{\mathbb{A}}$ given by the local conditions that at each prime $q \neq \ell$ we have $\beta \in (I \otimes \mathbb{Z}_q) \cap G(\mathbb{Q}_q)$. Notice that this local condition is the standard one that $\beta \in (\mathcal{O}_{\mathbb{H}} \otimes \mathbb{Z}_q)^\times$ at all finite primes away from the numerator and denominator of the fractional ideal I , hence U is open. That U is nonempty follows from the fact that every right ideal in a quaternion algebra is locally principal. Hence we see that $U \cap G_S G_{\mathbb{Q}}$ is nonempty and there exists some $\beta \in (I \otimes \mathbb{Z}[1/\ell]) \cap \mathbb{H}_1^\times$. $\square$

Lemma 6. *For each positive integer x and any prime ℓ not ramified in $\mathbb{H}$ there exists an element in $\mathcal{O}_{\mathbb{H}}[1/\ell]$ of norm x .*

Proof. Let I be an (integral) right ideal of $\mathcal{O}_{\mathbb{H}}$ of norm x and α an element of $\mathbb{H}$ also of norm x . Then $\alpha^{-1}I$ has norm 1 and we may apply Lemma 5 to obtain a $\beta \in \alpha^{-1}(I \otimes \mathbb{Z}[1/\ell])$ of norm 1. Then $\alpha\beta$ has norm x and $\alpha\beta \in I \otimes \mathbb{Z}[1/\ell] \subset \mathcal{O}_{\mathbb{H}}[1/\ell]$. $\square$

2.2.3. Consequences for $\text{Mat}_{g \times g}(\mathcal{O}_{\mathbb{H}})$.

Lemma 7. *For any prime q and any Hermitian $H \in \text{Mat}_{g \times g}(\mathcal{O}_{\mathbb{H}} \otimes \mathbb{Z}_{(q)})$ which is positive definite of reduced norm 1, there is a matrix $M \in \text{Mat}_{g \times g}(\mathcal{O}_{\mathbb{H}} \otimes \mathbb{Z}_{(q)})$ such that $H = M^\dagger M$. The matrix M satisfies $\text{Nm } M = 1$.*

Proof. Since H has reduced norm 1, there exists some $v \in (\mathcal{O}_{\mathbb{H}} \otimes \mathbb{Z}_{(q)})^g$ such that $x = v^\dagger H v \in \mathbb{Z}_{(q)}$ satisfies $x \notin q\mathbb{Z}_{(q)} \subset \mathbb{Z}_{(q)}$. By positive-definiteness $x > 0$ and after scaling v we may assume x^{-1} is an integer. Then by applying Lemma 6 for ℓ away from q and the ramified primes of $\mathbb{H}$ there exists an $\alpha \in \mathcal{O}_{\mathbb{H}} \otimes \mathbb{Z}_{(q)}$ of norm x^{-1} .

The proof is by induction on g . The assertion is trivial for $g = 1$: here $H = M = 1 \in \mathcal{O}_{\mathbb{H}} \otimes \mathbb{Z}_{(q)}$. For a general g , let $v_1 = v\alpha$ as above. Note that $v_1^\dagger H v_1 = 1$ and consider $\langle v_1 \rangle^\perp = \{w \in (\mathcal{O}_{\mathbb{H}} \otimes \mathbb{Z}_{(q)})^g \mid v_1^\dagger H w = 0\}$. The Hermitian form defined by H restricts to a positive definite Hermitian form of reduced norm 1 on $\langle v_1 \rangle^\perp$, so we're reduced to showing the theorem on $\langle v_1 \rangle^\perp \cong (\mathcal{O}_{\mathbb{H}} \otimes \mathbb{Z}_{(q)})^{g-1}$.

Finally we have

$$1 = \text{Nm}(H) = \text{Nm}(M^\dagger) \text{Nm}(M) = \text{Nm}(M)^2,$$

so $\text{Nm}(M) = 1$ since $\text{Nm}(M)$ is positive. $\square$

2.3. The quaternionic unitary group. If B is an algebra with anti-involution having fixed ring R and $M^\dagger$ is the conjugate-transpose defined using the anti-involution for $M \in \text{Mat}_{g \times g}(B)$, set

$$\begin{aligned} \text{U}_g(B) &= \{M \in \text{Mat}_{g \times g}(B) \mid M^\dagger M = \text{Id}_{g \times g}\} \\ \text{GU}_g(B) &= \{M \in \text{Mat}_{g \times g}(B) \mid M^\dagger M = \lambda \text{Id}_{g \times g} \text{ with } \lambda \in R^\times\}. \end{aligned} \tag{9}$$

For a Hermitian matrix $H \in \text{Mat}_{g \times g}(\mathcal{O}_{\mathbb{H}})$ set

$$\text{U}_H(\mathcal{O}_{\mathbb{H}}) = \{M \in \text{Mat}_{g \times g}(\mathcal{O}_{\mathbb{H}}) \mid M^\dagger H M = H\}.$$

Let $H_0 \in \mathcal{H}_{g,1}(\mathcal{O}_{\mathbb{H}})$ be the Hermitian matrix $\text{Id}_{g \times g}$. Then $\text{U}_{H_0}(\mathcal{O}_{\mathbb{H}}) = \text{U}_g(\mathcal{O}_{\mathbb{H}})$ as in (9).

Let $L \subset \mathbb{H}^g$ be a finitely generated right $\mathcal{O}_{\mathbb{H}}$ -submodule such that $L \otimes \mathbb{Q} \cong \mathbb{H}^g$. Such an L is **principally polarized** if there exists a $c \in \mathbb{Q}^\times$ such that cH_0 restricted to L is $\mathcal{O}_{\mathbb{H}}$ -valued and unimodular. We define the **dual** of L to be

$$\widehat{L} = c^{-1}L. \tag{10}$$

Remark 8. Notice that this agrees with the standard definition of dual with respect to a pairing; thus, if $L \subset L'$ then $\widehat{L}' \subset \widehat{L}$ and $[L' : L] = [\widehat{L} : \widehat{L}']$.

Theorem 9. *For $M \in \text{GU}_g(\widehat{\mathbb{H}})$, set $\gamma(M)$ equal to the principally polarized right $\mathcal{O}_{\mathbb{H}}$ -submodule of $\mathbb{H}^g$ given by $\gamma(M) = M\mathcal{O}_{\widehat{\mathbb{H}}}^g \cap \mathbb{H}^g$. The association $M \mapsto \gamma(M)$ induces a one-to-one correspondence between $\text{GU}_g(\widehat{\mathbb{H}})/\text{GU}_g(\mathcal{O}_{\widehat{\mathbb{H}}})$ and the set of principally polarized right $\mathcal{O}_{\mathbb{H}}$ -submodules of $\mathbb{H}^g$.*

Proof. The module $\gamma(M)$ is principally polarized since after tensoring with $\widehat{\mathbb{Z}}$, the Hermitian form is given by $M^\dagger M$ which is the identity times a scalar in $\widehat{\mathbb{Q}}^\times$, which can be approximated by an element of $\mathbb{Q}^\times$.

This map is well defined since if MU with $U \in \text{GU}_g(\mathcal{O}_{\widehat{\mathbb{H}}})$ is another representative of the same class in $\text{GU}_g(\widehat{\mathbb{H}})/\text{GU}_g(\mathcal{O}_{\widehat{\mathbb{H}}})$, then $U\mathcal{O}_{\widehat{\mathbb{H}}}^g = \mathcal{O}_{\widehat{\mathbb{H}}}^g$. Hence $MU\mathcal{O}_{\widehat{\mathbb{H}}}^g \cap \mathbb{H}^g = M\mathcal{O}_{\widehat{\mathbb{H}}}^g \cap \mathbb{H}^g$. It is

injective since if $M\mathcal{O}_{\widehat{\mathbb{H}}}^g \cap \mathbb{H}^g = M'\mathcal{O}_{\widehat{\mathbb{H}}}^g \cap \mathbb{H}^g$, we must have $MN = M'$ for some $N \in \mathrm{GL}_g(\mathcal{O}_{\widehat{\mathbb{H}}})$. But we also have $N = M'M^{-1} \in \mathrm{GU}_g(\widehat{\mathbb{H}})$. Therefore,

$$N \in \mathrm{GL}_g(\mathcal{O}_{\widehat{\mathbb{H}}}) \cap \mathrm{GU}_g(\widehat{\mathbb{H}}) = \mathrm{GU}_g(\mathcal{O}_{\widehat{\mathbb{H}}}),$$

and $[M] = [M']$.

Finally, to see that this map is surjective, let L be a principally polarized right $\mathcal{O}_{\mathbb{H}}$ -submodule. Since all finitely generated modules over $\mathcal{O}_{\mathbb{H}}$ are locally free, L is given by $N\mathcal{O}_{\widehat{\mathbb{H}}}^g \cap \mathbb{H}^g$ for some $N \in \mathrm{GL}_g(\widehat{\mathbb{H}})$. The Hermitian form on $L \otimes \widehat{\mathbb{Z}}$ is given by $N^\dagger N$, and since L is principally polarized, $cN^\dagger N$ is $\mathcal{O}_{\widehat{\mathbb{H}}}$ -valued and unimodular for some $c \in \mathbb{Q}^\times$. However, since all integral unimodular Hermitian forms are locally trivial (as follows, for example, from Lemma 7), there exists a $V \in \mathrm{GL}_g(\mathcal{O}_{\widehat{\mathbb{H}}})$ such that $V^\dagger cN^\dagger NV$ is the identity. So we can set $M = NV$ and have $M \in \mathrm{GU}_g(\widehat{\mathbb{H}})$ with $M\mathcal{O}_{\widehat{\mathbb{H}}}^g \cap \mathbb{H}^g = N\mathcal{O}_{\widehat{\mathbb{H}}}^g \cap \mathbb{H}^g = L$. $\square$

Definition 10. We define the classes of $\mathrm{GU}_g(\mathcal{O}_{\mathbb{H}})$, denoted $\mathcal{P}_g(\mathcal{O}_{\mathbb{H}})$, to be the equivalence classes of principally polarized right $\mathcal{O}_{\mathbb{H}}$ -submodules of $\mathbb{H}^g$ up to left multiplication by $\mathrm{GU}_g(\mathbb{H})$. Hence there is a one-to-one correspondence between $\mathrm{GU}_g(\mathbb{H}) \backslash \mathrm{GU}_g(\widehat{\mathbb{H}}) / \mathrm{GU}_g(\mathcal{O}_{\widehat{\mathbb{H}}})$ and $\mathcal{P}_g(\mathcal{O}_{\mathbb{H}})$ induced by the map γ of Theorem 9:

$$\mathcal{P}_g(\mathcal{O}_{\mathbb{H}}) \cong \mathrm{GU}_g(\mathbb{H}) \backslash \mathrm{GU}_g(\widehat{\mathbb{H}}) / \mathrm{GU}_g(\mathcal{O}_{\widehat{\mathbb{H}}}). \quad (11)$$

There are a finite number of classes of $\mathrm{GU}_g(\mathcal{O}_{\mathbb{H}})$. We will call $\#\mathcal{P}_g(\mathcal{O}_{\mathbb{H}})$ the **class number**. It is independent of the choice of maximal order $\mathcal{O}_{\mathbb{H}}$ since the isomorphism class of $\mathcal{O}_{\widehat{\mathbb{H}}}$ is independent of $\mathcal{O}_{\mathbb{H}}$ and consequently we denote it by $h_g(\mathbb{H})$. Let the principally polarized right $\mathcal{O}_{\mathbb{H}}$ -module L_i be a representative of the class $[L_i] \in \mathcal{P}_g(\mathcal{O}_{\mathbb{H}})$ for $1 \leq i \leq h = h_g(\mathbb{H})$.

Remark 11. Notice that L and $\widehat{L}$ belong to the same class. Also note that for $U \in \mathrm{GU}_g(\mathbb{H})$ we have $\widehat{U}\widehat{L} = (U^{-1})^\dagger \widehat{L}$.

When $g = 1$ we recover the standard description of the ideal classes $\mathcal{P}_1(\mathcal{O}_{\mathbb{H}})$ and the class number $h(\mathbb{H})$:

$$\mathcal{P}_1(\mathcal{O}_{\mathbb{H}}) \cong \mathbb{H}^\times \backslash \widehat{\mathbb{H}}^\times / \mathcal{O}_{\widehat{\mathbb{H}}}^\times \quad \text{and} \quad h_1(\mathbb{H}) = h(\mathbb{H}) = \# \mathbb{H}^\times \backslash \widehat{\mathbb{H}}^\times / \mathcal{O}_{\widehat{\mathbb{H}}}^\times, \quad (12)$$

cf. [Vig80, §3.5.B].

Theorem 12. If $g > 1$, then $\overline{\mathcal{H}}_{g,1}(\mathcal{O}_{\mathbb{H}})$ is in one-to-one correspondence with the classes of $\mathrm{GU}_g(\mathcal{O}_{\mathbb{H}})$, or equivalently with the double cosets

$$\mathrm{GU}_g(\mathbb{H}) \backslash \mathrm{GU}_g(\widehat{\mathbb{H}}) / \mathrm{GU}_g(\mathcal{O}_{\widehat{\mathbb{H}}}).$$

Proof. We first define the map

$$\iota : \overline{\mathcal{H}}_{g,1}(\mathcal{O}_{\mathbb{H}}) \rightarrow \mathrm{GU}_g(\mathbb{H}) \backslash \mathrm{GU}_g(\widehat{\mathbb{H}}) / \mathrm{GU}_g(\mathcal{O}_{\widehat{\mathbb{H}}}) \quad (13)$$

by the following procedure: for $[H] \in \overline{\mathcal{H}}_{g,1}(\mathcal{O}_{\mathbb{H}})$ write $H = M^\dagger M$ for $M \in \mathrm{SL}_g(\mathbb{H})$, such an M exists by Lemma 7. For each prime q write $H = N_q^\dagger N_q$ with $N_q \in \mathrm{SL}_g(\mathcal{O}_{\mathbb{H}} \otimes \mathbb{Z}_q)$ (again these exist by Lemma 7). Let $N = (N_q) \in \mathrm{SL}_g(\mathcal{O}_{\widehat{\mathbb{H}}})$, and notice that $(MN^{-1})^\dagger MN^{-1} = I$, so $MN^{-1} \in \mathrm{U}_g(\widehat{\mathbb{H}})$. Set $\iota(H) = MN^{-1}$ and define the map ι in (13) by

$$\iota([H]) = [\iota(H)] = [MN^{-1}]. \quad (14)$$

We must now prove that the map ι in (14) is well defined, injective, and surjective.

Well-definedness: Suppose $M' \in \mathrm{SL}_g(\mathbb{H})$ is another choice of M and $N' \in \mathrm{SL}_g(\mathcal{O}_{\widehat{\mathbb{H}}})$ another

choice of N satisfying $H = M'^\dagger M' = N'^\dagger N'$. Then $M'M^{-1} \in \mathrm{U}_g(\mathbb{H})$ and $NN'^{-1} \in \mathrm{U}_g(\mathcal{O}_{\widehat{\mathbb{H}}})$. Hence

$$[M'N'^{-1}] = [(M'M^{-1})(MN^{-1})(NN'^{-1})]$$

corresponds to the same class as $[MN^{-1}]$ in $\mathrm{GU}_g(\mathbb{H}) \backslash \mathrm{GU}_g(\widehat{\mathbb{H}}) / \mathrm{GU}_g(\mathcal{O}_{\widehat{\mathbb{H}}})$.

Now suppose $H' \in \mathcal{H}_{g,1}(\mathcal{O}_{\mathbb{H}})$ is another representative of the same class as H in $\overline{\mathcal{H}}_{g,1}(\mathcal{O}_{\mathbb{H}})$, i.e., $H' = U^\dagger H U$ for some $U \in \mathrm{SL}_g(\mathcal{O}_{\mathbb{H}})$. Thus if $H = M^\dagger M = N^\dagger N$ with $M \in \mathrm{SL}_g(\mathbb{H})$ and $N \in \mathrm{SL}_g(\mathcal{O}_{\widehat{\mathbb{H}}})$, then

$$H' = (MU)^\dagger M U = (NU)^\dagger N U$$

with $MU \in \mathrm{SL}_g(\mathbb{H})$, $NU \in \mathrm{SL}_g(\mathcal{O}_{\widehat{\mathbb{H}}})$, and $MU(NU)^{-1} = MN^{-1}$.

Injectivity: Suppose $\iota([H]) = \iota([H'])$. Let $H = M^\dagger M = N^\dagger N$ and $H' = M'^\dagger M' = N'^\dagger N'$ with $M, M' \in \mathrm{SL}_g(\mathbb{H})$ and $N, N' \in \mathrm{SL}_g(\mathcal{O}_{\widehat{\mathbb{H}}})$. Thus $MN^{-1} = VM'N'^{-1}W^{-1}$ with $V \in \mathrm{GU}_g(\mathbb{H})$ and $W \in \mathrm{GU}_g(\mathcal{O}_{\widehat{\mathbb{H}}})$. Set $V^\dagger V = vI$ for $v \in \mathbb{Q}^\times$ and $W^\dagger W = wI$ for $w \in \widehat{\mathbb{Z}}^\times$. Let $U = M^{-1}VM' = N^{-1}WN'$ and observe that $U \in \mathrm{GL}_g(\mathbb{H}) \cap \mathrm{GL}_g(\mathcal{O}_{\widehat{\mathbb{H}}}) = \mathrm{SL}_g(\mathcal{O}_{\mathbb{H}})$. Now

$$H \cdot U = U^\dagger H U = (M^{-1}VM')^\dagger M^\dagger M M^{-1}VM' = M'^\dagger V^\dagger VM' = vH',$$

and a similar argument shows $H \cdot U = wH'$. Hence $v = w \in \mathbb{Q}^\times \cap \widehat{\mathbb{Z}}^\times = \mathbb{Z}^\times$. So $v = \pm 1$ and we can rule out -1 since $\mathbb{H}$ is definite. Thus $[H] = [H']$.

Surjectivity: Let

$$[V] \in \mathrm{GU}_g(\mathbb{H}) \backslash \mathrm{GU}_g(\widehat{\mathbb{H}}) / \mathrm{GU}_g(\mathcal{O}_{\widehat{\mathbb{H}}})$$

with $V \in \mathrm{GU}_g(\widehat{\mathbb{H}})$. Put $V^\dagger V = vI$ for $v \in \widehat{\mathbb{Q}}$. Put $v = ab$ with $a \in \mathbb{Q}_{>0}$ and $b \in \widehat{\mathbb{Z}}^\times$. Then by Lemma 6 there exist $\alpha \in \mathbb{H}$ with $N(\alpha) = a$ and $\beta \in \mathcal{O}_{\widehat{\mathbb{H}}}^\times$ with $N(\beta) = b$. After replacing V with $\alpha^{-1}V\beta^{-1}$ we may assume $V \in \mathrm{U}_g(\widehat{\mathbb{H}}) \subset \mathrm{SL}_g(\widehat{\mathbb{H}})$.

We will apply strong approximation to $G = \mathrm{SL}_g(\mathbb{H})$ with $S = \{\infty\}$. Note that G_∞ is not compact for $g > 1$ and hence the pair (G, S) satisfies the conditions of Theorem 4. The local conditions we will impose at each prime q will be $V^{-1}M \in \mathrm{SL}(\mathcal{O}_{\mathbb{H}} \otimes \mathbb{Z}_q)$. These are the standard conditions away from finitely many primes and are trivially nonempty since V always satisfies them.

Hence there exists $M \in \mathrm{SL}_g(\mathbb{H})$ such that $N = V^{-1}M \in \mathrm{SL}_g(\mathcal{O}_{\widehat{\mathbb{H}}})$. Thus $\iota([M^\dagger M]) = [V]$. $\square$

3. BRANDT MATRICES

3.1. Definition of Brandt matrices. Set $h_g := h_g(\mathbb{H})$ with $\mathcal{P}_g(\mathcal{O}_{\mathbb{H}}) = \{[L_1], \dots, [L_{h_g}]\}$ for principally polarized right $\mathcal{O}_{\mathbb{H}}$ -modules $L_1, \dots, L_{h_g} \subseteq \mathbb{H}^g$. We can now define the **Brandt matrix** $B_g(n) \in \mathrm{Mat}_{h_g \times h_g}(\mathbb{Z})$ for a natural number n .

Definition 13. Let $g \geq 1$ and $n \in \mathbb{N}$. For $1 \leq j \leq h_g(\mathbb{H}) =: h_g$, set

$$\begin{aligned} E_j(g) &:= \{U \in \mathrm{GU}_g(\mathbb{H}) \mid L_j = UL_j\}, \\ e_j(g) &:= \#E_j(g), \\ \widetilde{\mathbf{B}}_g(n)_{ij} &:= \{U \in \mathrm{GU}_g(\mathbb{H}) \mid [L_i : UL_j] = n^{2g}\}, \\ E(U) &:= \{V \in \mathrm{GU}_g(\mathbb{H}) \mid VL_i = L_i \text{ and } VUL_j = UL_j\} \text{ for } U \in \widetilde{\mathbf{B}}_g(n)_{ij}, \\ e(U) &:= \#E(U) \text{ for } U \in \widetilde{\mathbf{B}}_g(n)_{ij}. \end{aligned} \tag{15}$$

The sets $E_j(g)$, $\tilde{\mathbf{B}}_g(n)_{ij}$, $E(U)$ above depend on the choice of representatives $L_1, \dots, L_{h_g}$. However, they change by an explicit one-to-one correspondence if we change the representatives: if $\tilde{L}_j = W_j L_j$ for $W_j \in \mathrm{GU}_g(\mathbb{H})$, then in (15) the W_j can be absorbed into the U . In particular $\#\tilde{\mathbf{B}}_g(n)_{ij}$ and $\#E_j(g)$ do not depend on the choice of representatives for $\mathcal{P}_g(\mathcal{O}_{\mathbb{H}})$.

Note that $E_j(g) \leq \mathrm{GU}_g(\mathbb{H})$ and $E(U) \leq E_i(g)$ for $U \in \tilde{\mathbf{B}}_g(n)_{ij}$. Define the equivalence relation $\sim_b$ on $\tilde{\mathbf{B}}_g(n)_{ij}$ by $U \sim_b U'$ if $U = U'V$ for some $V \in E_j(g)$. Likewise define the equivalence relation $\sim_l$ on $\tilde{\mathbf{B}}_g(n)_{ij}$ by $U \sim_l U'$ if $U = V_i U' V_j$ for some $V_j \in E_j(g)$ and some $V_i \in E_i(g)$. Define the big quotient

$$\mathbf{B}_g(n)_{ij}^{\mathrm{big}} = \tilde{\mathbf{B}}_g(n)_{ij} / \sim_b \quad (16)$$

and the little quotient

$$\mathbf{B}_g(n)_{ij}^{\mathrm{little}} = \tilde{\mathbf{B}}_g(n)_{ij} / \sim_l. \quad (17)$$

Let $[U]_b \in \mathbf{B}_g(n)_{ij}^{\mathrm{big}}$, $[U]_l \in \mathbf{B}_g(n)_{ij}^{\mathrm{little}}$ be the equivalence classes of $U \in \tilde{\mathbf{B}}_g(n)_{ij}$. An equivalent definition is

$$\mathbf{B}_g(n)_{ij}^{\mathrm{big}} = \{L'_j \mid [L_i : L'_j] = n^{2g} \text{ and } UL_j = L'_j \text{ for some } U \in \mathrm{GU}_g(\mathbb{H})\}. \quad (18)$$

We define an equivalence relation $\sim$ on $\mathbf{B}_g(n)_{ij}^{\mathrm{big}}$ in (18) by $L'_{j_1} \sim L'_{j_2}$ if there exists $U \in \mathrm{GU}_g(\mathbb{H})$ such that $UL_i = L_i$ and $UL'_{j_1} = L'_{j_2}$; write $[L'_j]_l$ for the equivalence class of $L'_j \in \mathbf{B}_g(n)_{ij}^{\mathrm{big}}$. Then we equivalently have

$$\mathbf{B}_g(n)_{ij}^{\mathrm{little}} = \left(\mathbf{B}_g(n)_{ij}^{\mathrm{big}} / \sim \right) = \left\{ [L'_j]_l \mid L'_j \in \mathbf{B}_g(n)_{ij}^{\mathrm{big}} \right\}. \quad (19)$$

For $1 \leq i, j \leq h_g$, put

$$B_g(n)_{ij} = \#\mathbf{B}_g(n)_{ij}^{\mathrm{big}} = \frac{\#\tilde{\mathbf{B}}_g(n)_{ij}}{\#E_j(g)} \quad \text{and} \quad B_g(0)_{ij} = 1/e_j(g). \quad (20)$$

The matrices $B_g(n)$ do not depend on the choice of maximal order $\mathcal{O}_{\mathbb{H}}$ or on the choice of representatives for $\mathcal{P}_g(\mathcal{O}_{\mathbb{H}})$, up to the obvious indeterminacy of simultaneously permuting the rows and columns. Let $\mathbb{B}_g(\mathcal{O}_{\mathbb{H}}) \subseteq \mathrm{Mat}_{h_g \times h_g}(\mathbb{Z})$ be the $\mathbb{Z}$ -algebra generated by $B_g(n)$, $n \geq 1$. The $\mathbb{Z}$ -algebra $\mathbb{B}_g(\mathcal{O}_{\mathbb{H}})$ does not depend on the choice of maximal order $\mathcal{O}_{\mathbb{H}}$ and hence we can denote it as $\mathbb{B}_g = \mathbb{B}_g(\mathbb{H})$.

Remark 14. In the classical case $g = 1$, $h = h_1(\mathbb{H})$ is the class number of $\mathbb{H}$. Let $I_1, \dots, I_h$ be representatives for the right $\mathcal{O}_{\mathbb{H}}$ -ideal classes and let $\mathcal{O}_i$ be the left order of I_i , $1 \leq i \leq h$. We have $e_i = e_i(1) = \#\mathcal{O}_i^\times$. Definition 13 in the special case $g = 1$ gives

$$\begin{aligned} E_j(1) &= \mathcal{O}_j^\times, \\ e_j &:= e_j(1) = \#\mathcal{O}_j^\times, \\ \tilde{\mathbf{B}}_1(n)_{ij} &= \{\lambda \in I_i I_j^{-1} \mid \mathrm{Nm} \lambda = n \mathrm{Nm}(I_i I_j^{-1})\}, \\ B_1(n)_{ij} &= \frac{\#\{\lambda \in I_i I_j^{-1} \mid \mathrm{Nm} \lambda = n \mathrm{Nm}(I_i I_j^{-1})\}}{e_j}, \\ E(\lambda) &= \{u \in \mathcal{O}_i^\times \mid \lambda^{-1} u \lambda \in \mathcal{O}_j^\times\} \quad \text{for } \lambda \in \tilde{\mathbf{B}}_1(n)_{ij}, \\ e(\lambda) &= \#E(\lambda) \quad \text{for } \lambda \in \tilde{\mathbf{B}}_1(n)_{ij}. \end{aligned}$$

In particular, $B_1(1) = \text{Id}_{h \times h}$ and $B_1(n) \in \text{Mat}_{h \times h}(\mathbb{Z})$ for $n \geq 1$. The Brandt matrix $B_1(0)$ is $B_1(0)_{ij} = 1/e_j$ and $\mathbb{B}_1 = \mathbb{B}_1(\mathbb{H}) \subseteq \text{Mat}_{h \times h}(\mathbb{Z})$ is the $\mathbb{Z}$ -algebra generated by the Brandt matrices $B_1(n)$, $n \geq 1$.

By Theorem 9,

$$\#\overline{\mathcal{H}}_{g,1}(\mathcal{O}_{\mathbb{H}}) = h_g(\mathbb{H}) =: h_g = \#\mathcal{P}_g(\mathcal{O}_{\mathbb{H}}).$$

Write

$$\begin{aligned} \overline{\mathcal{H}}_{g,1}(\mathcal{O}_{\mathbb{H}}) &= \{[H_1], \dots, [H_{h_g}]\} \quad \text{for } H_i \in \mathcal{H}_{g,1}, 1 \leq i \leq h_g, \text{ and} \\ \mathcal{P}_g(\mathcal{O}_{\mathbb{H}}) &= \{[L_1], \dots, [L_{h_g}]\} \quad \text{with } L_i \text{ a principally polarized right } \mathcal{O}_{\mathbb{H}}\text{-submodule of } \mathbb{H}^g. \end{aligned} \quad (21)$$

First we give an equivalent definition of the Brandt matrix in terms of $\overline{\mathcal{H}}_{g,1}(\mathcal{O}_{\mathbb{H}})$ in case $g > 1$. It is convenient to make the following definition.

Definition 15. Suppose $H, H' \in \overline{\mathcal{H}}_{g,1}(\mathcal{O}_{\mathbb{H}})$. For a natural number n set

$$\begin{aligned} \mathbf{U}_n(H, H') &:= \{M \in \text{Mat}_{g \times g}(\mathcal{O}_{\mathbb{H}}) \mid M^\dagger H M = n H'\} \text{ and} \\ \mathbf{U}(H) &:= \mathbf{U}_1(H, H). \end{aligned}$$

Note that $\mathbf{U}(H)$ acts on $\mathbf{U}_n(H, H')$ by multiplication on the left and $\mathbf{U}(H')$ acts on $\mathbf{U}_n(H, H')$ by multiplication on the right. Define an equivalence relation $\sim_b$ on $\mathbf{U}_n(H, H')$ by $M \sim_b M U'$ for $U' \in \mathbf{U}(H')$ and set $\mathbf{U}_n(H, H')^{\text{big}} := \mathbf{U}_n(H, H') / \sim_b$ with $[M] \in \mathbf{U}_n(H, H')^{\text{big}}$ the class defined by $M \in \mathbf{U}_n(H, H')$. Define an equivalence relation $\sim_l$ on $\mathbf{U}_n(H, H')^{\text{big}}$ by $[M] \sim_l [UM]$ for $U \in \mathbf{U}(H)$. Set $\mathbf{U}_n(H, H')^{\text{little}} := \mathbf{U}_n(H, H')^{\text{big}} / \sim_l$.

Theorem 16. Let $g > 1$ with γ as in Theorem 9 and ι as in (14). If $[\gamma(\iota([H_i]))] = [L_i]$ and $[\gamma(\iota([H_j]))] = [L_j]$, then we have equivalently

$$\begin{aligned} \mathbf{B}_g(n)_{ij}^{\text{big}} &= \mathbf{U}_n(H_i, H_j)^{\text{big}} \text{ and} \\ \mathbf{B}_g(n)_{ij}^{\text{little}} &= \mathbf{U}_n(H_i, H_j)^{\text{little}}. \end{aligned}$$

In particular we have

$$\begin{aligned} e_j(g) &= \#\mathbf{U}(H_j) \text{ and} \\ B_g(n)_{ij} &= \mathbf{B}_g(n)_{ij}^{\text{big}} = \frac{\#\mathbf{U}_n(H_i, H_j)}{e_j(g)} \end{aligned}$$

for $n \geq 1$.

It clearly suffices prove the following lemma.

Lemma 17. Let $g > 1$. Choose any $[H_1], [H_2] \in \overline{\mathcal{H}}_{g,1}(\mathcal{O}_{\mathbb{H}})$. Let $[\gamma(\iota(H_k))] = [L_k]$ for $k \in \{1, 2\}$. There exists a bijective correspondence between $\{U \in \text{GU}_g(\mathbb{H}) \mid [L_1 : UL_2] = n^{2g}\}$ and $\{B \in \text{Mat}_{g \times g}(\mathcal{O}_{\mathbb{H}}) \mid B^\dagger H_1 B = n H_2\}$.

Proof. For $k \in \{1, 2\}$, let $[V_k] = \iota([H_k])$ with $L_k = \gamma(V_k)$. Let $H_k = M_k^\dagger M_k = N_k^\dagger N_k$, with $M_k \in \text{SL}_g(\mathbb{H})$, $N_k \in \text{SL}_g(\mathcal{O}_{\widehat{\mathbb{H}}})$, and $V_k = M_k N_k^{-1} \in \text{U}_g(\widehat{\mathbb{H}})$ as in (14).

For $B \in \text{Mat}_{g \times g}(\mathcal{O}_{\mathbb{H}})$ with $B^\dagger H_1 B = n H_2$, let $U_B = M_1 B M_2^{-1}$. Notice that $B^\dagger M_1^\dagger M_1 B = n M_2^\dagger M_2$ so $U_B^\dagger U_B = n \text{Id}_{g \times g}$ and $U_B \in \text{GU}_g(\mathbb{H})$. Similarly take $W_B = N_1 B N_2^{-1}$ and observe that $W_B \in \text{GU}_g(\widehat{\mathbb{H}})$ and $W_B \in \text{Mat}_{g \times g}(\mathcal{O}_{\widehat{\mathbb{H}}})$. Taking reduced norms, we get $\text{Nm}(W_B) = n^g$.

Therefore, $W_B \mathcal{O}_{\mathbb{H}}^g \subset \mathcal{O}_{\mathbb{H}}^g$ with

$$[\mathcal{O}_{\mathbb{H}}^g : W_B \mathcal{O}_{\mathbb{H}}^g] = n^{2g}. \quad (22)$$

Notice that $U_B V_2 = M_1 B N_2^{-1} = V_1 W_B$. Apply this to (22) gives $n^{2g} = [V_1 \mathcal{O}_{\mathbb{H}}^g : V_1 W_B \mathcal{O}_{\mathbb{H}}^g] = [V_1 \mathcal{O}_{\mathbb{H}}^g : U_B V_2 \mathcal{O}_{\mathbb{H}}^g]$. And intersecting with $\mathbb{H}^g$ gives $n^{2g} = [L_1 : U_B L_2]$.

The correspondence $B \mapsto U_B$ is clearly well-defined and injective. We will now show it is surjective. Given $U \in \text{GU}_g(\mathbb{H})$ with $[L_1 : U L_2] = n^{2g}$, hence tensoring with $\mathcal{O}_{\mathbb{H}}$ we see $[V_1 \mathcal{O}_{\mathbb{H}}^g : U V_2 \mathcal{O}_{\mathbb{H}}^g] = n^{2g}$. Let $B = M_1^{-1} U M_2$ and $W = N_1 B N_2^{-1}$, so $U V_2 = M_1 B N_2^{-1} = V_1 W$. Hence, $n^{2g} = [V_1 \mathcal{O}_{\mathbb{H}}^g : V_1 W \mathcal{O}_{\mathbb{H}}^g] = [\mathcal{O}_{\mathbb{H}}^g : W \mathcal{O}_{\mathbb{H}}^g]$. Thus, $W \in \text{Mat}_{g \times g}(\mathcal{O}_{\mathbb{H}})$ with $\text{Nm}(W) = n^g$. Since the M_k 's and N_k 's have reduced norm 1, U also has reduced norm n^g ; hence, $U^\dagger U = n \text{Id}_{g \times g}$ since $U \in \text{GU}_g(\mathbb{H})$. Also that means that $B \in \text{Mat}_{g \times g}(\mathbb{H})$. But also $B = N_1^{-1} W N_2$ with $N_1, N_2 \in \text{SL}_2(\mathcal{O}_{\mathbb{H}})$ and $W \in \text{Mat}_{g \times g}(\mathcal{O}_{\mathbb{H}})$, so $B \in \text{Mat}_{g \times g}(\mathcal{O}_{\mathbb{H}})$ and hence $B \in \text{Mat}_{g \times g}(\mathcal{O}_{\mathbb{H}})$. Straightforward algebra shows that $B^\dagger H_1 B = n H_2$, and we are done. $\square$

3.2. Brandt matrices: Examples. The Brandt matrices $B_g(n)$ for a maximal order $\mathcal{O}_{\mathbb{H}} \subseteq \mathbb{H}$ are amenable to machine computation, although the memory requirements rapidly grow with n and especially g so that few examples are accessible with $g = 3$. We had no computations finish for $g \geq 4$.

3.2.1. $\mathbb{H} = \mathbb{H}_7$. Take $\mathbb{H} = \mathbb{H}_7$, the rational definite quaternion algebra of discriminant 7. The first class numbers of $\mathbb{H}_7$ are: $h_1(\mathbb{H}_7) = 1$, $h_2(\mathbb{H}_7) = 2$, $h_3(\mathbb{H}_7) = 5$. The Brandt matrices $B_g(\ell)$ are given in Table 1 below for primes $\ell = 2, 3, 5, 11$ and $1 \leq g \leq 3$. Note that in all cases $B_g(\ell)$ has constant row-sum $N_g(\ell) = \prod_{k=1}^g (1 + \ell^k)$ in keeping with Theorem 19(a). A ? in the table below means that the computation did not finish.

	$B_g(2)$	$B_g(3)$	$B_g(5)$	$B_g(11)$
$g = 1$	[3]	[4]	[6]	[12]
$g = 2$	$\begin{bmatrix} 11 & 4 \\ 6 & 9 \end{bmatrix}$	$\begin{bmatrix} 28 & 12 \\ 18 & 22 \end{bmatrix}$	$\begin{bmatrix} 112 & 44 \\ 66 & 90 \end{bmatrix}$	$\begin{bmatrix} 928 & 536 \\ 804 & 660 \end{bmatrix}$
$g = 3$	$\begin{bmatrix} 45 & 36 & 8 & 32 & 14 \\ 18 & 27 & 6 & 60 & 24 \\ 14 & 21 & 30 & 14 & 56 \\ 4 & 15 & 1 & 101 & 14 \\ 7 & 24 & 16 & 56 & 32 \end{bmatrix}$	$\begin{bmatrix} 208 & 208 & 0 & 640 & 64 \\ 104 & 184 & 32 & 640 & 160 \\ 0 & 112 & 112 & 616 & 280 \\ 80 & 160 & 44 & 676 & 160 \\ 32 & 160 & 80 & 640 & 208 \end{bmatrix}$	?	?

TABLE 1. Brandt matrices $B_g(\ell)$ for $\mathbb{H}_7$

3.2.2. $\mathbb{H} = \mathbb{H}_{11}$. Now take $\mathbb{H} = \mathbb{H}_{11}$, the rational definite quaternion algebra of discriminant 11. The first class numbers of $\mathbb{H}_{11}$ are: $h_1(\mathbb{H}_{11}) = 2$, $h_2(\mathbb{H}_{11}) = 5$, $h_3(\mathbb{H}_{11}) = 19$. Table 2 below gives the Brandt matrices $B_g(\ell)$ for $\ell = 2, 3, 5, 7$ and $g = 1, 2$. Again in all examples $B_g(\ell)$ has constant row-sum $N_g(\ell) = \prod_{k=1}^g (1 + \ell^k)$.

	$B_g(2)$	$B_g(3)$	$B_g(5)$	$B_g(7)$
$g = 1$	$\begin{bmatrix} 1 & 2 \\ 3 & 0 \end{bmatrix}$	$\begin{bmatrix} 2 & 2 \\ 3 & 1 \end{bmatrix}$	$\begin{bmatrix} 4 & 2 \\ 3 & 3 \end{bmatrix}$	$\begin{bmatrix} 4 & 4 \\ 6 & 2 \end{bmatrix}$
$g = 2$	$\begin{bmatrix} 3 & 4 & 4 & 0 & 4 \\ 3 & 6 & 0 & 6 & 0 \\ 3 & 0 & 3 & 8 & 1 \\ 0 & 3 & 4 & 8 & 0 \\ 9 & 0 & 3 & 0 & 3 \end{bmatrix}$	$\begin{bmatrix} 8 & 8 & 4 & 16 & 4 \\ 6 & 20 & 0 & 12 & 2 \\ 3 & 0 & 9 & 22 & 6 \\ 6 & 6 & 11 & 16 & 1 \\ 9 & 6 & 18 & 6 & 1 \end{bmatrix}$	$\begin{bmatrix} 36 & 32 & 36 & 32 & 20 \\ 24 & 42 & 24 & 60 & 6 \\ 27 & 24 & 41 & 58 & 6 \\ 12 & 30 & 29 & 78 & 7 \\ 45 & 18 & 18 & 42 & 33 \end{bmatrix}$	$\begin{bmatrix} 80 & 80 & 72 & 128 & 40 \\ 60 & 128 & 48 & 144 & 20 \\ 54 & 48 & 94 & 172 & 32 \\ 48 & 72 & 86 & 176 & 18 \\ 90 & 60 & 96 & 108 & 46 \end{bmatrix}$

TABLE 2. Brandt matrices $B_g(\ell)$ for $\mathbb{H}_{11}$

3.3. First properties of Brandt matrices. To simplify the discussion, we restrict to the case of the definite quaternion algebra $\mathbb{H} = \mathbb{H}_p$ ramified at one finite prime p and choose a maximal order $\mathcal{O} = \mathcal{O}_{\mathbb{H}_p} \subseteq \mathbb{H}_p$.

3.3.1. *The classical case: $g = 1$.* We start by reviewing known properties of the classical Brandt matrices $B(n) = B_1(n)$ for $\mathcal{O} = \mathcal{O}_{\mathbb{H}_p}$, $n \geq 0$, largely following Gross [Gro87, §1, 2]. Set $h = h_1(\mathbb{H}_p)$. Almost all the results given are due to Eichler [Eic55].

Remark 18. (a) For $n \geq 0$ with $(n, p) = 1$ the row sums $\sum_j B(n)_{ij}$ are independent of i . For $n \geq 1$ and $\ell \neq p$ prime with $N_1(\ell)$ as in (3),

$$\sum_j B(\ell)_{ij} = N_1(\ell) := \ell + 1.$$

- (b) If $(m, n) = 1$, then $B(mn) = B(m)B(n)$.
- (c) $B(p)$ is a permutation matrix with $B(p)^2 = \text{Id}_{h \times h}$ and $B(p)^k = B(p^k)$.
- (d) For a prime $\ell \neq p$ and $k \geq 2$,

$$B(\ell^k) = B(\ell^{k-1})B(\ell) - \ell B(\ell^{k-2}).$$

- (e) Set $e_j = e_j(1)$ for $1 \leq j \leq h$. We have $e_j B(n)_{ij} = e_i B(n)_{ji}$ for $1 \leq i, j \leq h$. Equivalently, let $v_1, \dots, v_h$ be the standard basis of $\mathbb{Z}^h$. Define the inner product $\langle v_i, v_j \rangle = e_i \delta_{ij}$ on $\mathbb{Z}^h$. Then the Brandt matrices $B(n)$, $n \geq 1$, are self-adjoint with respect to $\langle \cdot, \cdot \rangle$.
- (f) (Eichler's mass formula) Let $\mathbb{H} = \mathbb{H}_p$. Then

$$\sum_{i=1}^h \frac{1}{e_i} = \frac{p-1}{24}.$$

Equivalently, the sum of any row of $B(0)$ is $(p-1)/24$ with $B(0) = B_1(0)$ as in (20).

- (g) For all m and n we have $B(m)B(n) = B(n)B(m)$.
- (h) The commutative $\mathbb{Q}$ -algebra $\mathbb{B} \otimes \mathbb{Q}$ is semi-simple, and isomorphic to the product of totally real number fields.

3.3.2. The general case $g \geq 1$. We now generalize the results of Remark 18 to the Brandt matrices $B_g(n)$ of Definition 13 with $\mathbb{H} = \mathbb{H}_p$. Put $h_g = h_g(\mathbb{H})$ and let $\mathbb{B}_g = \mathbb{B}_g(\mathbb{H})$ be the $\mathbb{Z}$ -subalgebra of $\text{Mat}_{h_g \times h_g}(\mathbb{Z})$ generated by the Brandt matrices $B_g(n)$ for $n \geq 1$ as in Definition 13.

Theorem 19. (a) For $n \geq 1$ with $(n, p) = 1$, $\sum_j B_g(n)_{ij} = N_g(n)$ as in (2). For $n = \ell \neq p$ prime this gives

$$\sum_j B_g(\ell)_{ij} = N_g(\ell) := \prod_{k=1}^g (1 + \ell^k)$$

with $N_g(\ell)$ as in (3). In particular, the row sums $\sum_j B_g(n)_{ij}$ are independent of i and in fact only depend on n and g (they do not depend on p).

- (b) If $(m, n) = 1$, then $B_g(mn) = B_g(m)B_g(n)$.
- (c) We have $e_j(g)B_g(n)_{ij} = e_i(g)B_g(n)_{ji}$ for $1 \leq i, j \leq h_g$. Equivalently, let $v_1, \dots, v_{h_g}$ be the standard basis of $\mathbb{Z}^{h_g}$. Define the inner product $\langle v_i, v_j \rangle_g = e_i(g)\delta_{ij}$ on $\mathbb{Z}^{h_g}$. Then the generalized Brandt matrices $B_g(n)$, $n \geq 1$, are self-adjoint with respect to $\langle \cdot, \cdot \rangle_g$.
- (d) (Mass formula of Ekedahl and Hashimoto/Ibukiyama)

$$M_g := \sum_{i=1}^{h_g} \frac{1}{e_i(g)} = \frac{(-1)^{g(g+1)/2}}{2^g} \left\{ \prod_{k=1}^g \zeta(1-2k) \right\} \cdot \prod_{k=1}^g \{p^k + (-1)^k\}.$$

Equivalently, the sum of any row of $B_g(0)$ as in (20) is M_g . Note that for $g = 1$ we have $M_1 = (p-1)/24$ and so recover Theorem 18(f).

- (e) For all m and n we have $B_g(m)B_g(n) = B_g(n)B_g(m)$.
- (f) The commutative $\mathbb{Q}$ -algebra $\mathbb{B}_g \otimes \mathbb{Q}$ is semi-simple, and isomorphic to the product of totally real number fields.

Proof. (b): It's not hard to see that

$$(B_g(m)B_g(n))_{ij} = \frac{\#\{U \in \text{GU}_g(\mathbb{H}) \text{ and } L_k \text{ p. p.} \mid [L_i : L_k] = m^{2g} \text{ and } [L_k : UL_j] = n^{2g}\}}{e_j(g)},$$

where p. p. denotes principally polarized. Since m and n are relatively prime given L_i , L_j , and U with $[L_i : UL_j] = (mn)^{2g}$ there exists a unique principally polarized L_k with $[L_i : L_k] = m^{2g}$ and $[L_k : UL_j] = n^{2g}$. Thus $(B_g(m)B_g(n))_{ij} = B_g(mn)_{ij}$.

(a): By (b) we may restrict to the case when $n = \ell^r$ is a prime power with $\ell \neq p$. Since each p. p. lattice belongs to precisely one equivalence class, we have using (18) and (20)

$$\begin{aligned} \sum_j B_g(\ell^r)_{ij} &= \sum_j \#\{L'_j \text{ p. p.} \mid [L_i : L'_j] = (\ell^r)^{2g} = \ell^{2rg} \text{ and } UL_j = L'_j \text{ for some } U \in \text{GU}_g(\mathbb{H})\} \\ &= \#\{L_j \text{ p. p.} \mid [L_i : L_j] = \ell^{2rg}\}. \end{aligned} \tag{23}$$

We now suppose $g > 1$ so that classes of $\mathrm{GU}_g(\mathcal{O}_{\mathbb{H}})$ can be described by Hermitian matrices as well as principally polarized lattices as in Theorem 12. The case $g = 1$ is covered by the classical results of Eichler in Remark 18.

Set $\mathcal{O}_{\ell} = \mathcal{O}_{\mathbb{H}} \otimes \mathbb{Z}_{\ell}$ for $\ell \neq p$ prime and $\mathbb{H}_{\ell} = \mathbb{H} \otimes \mathbb{Q}_{\ell}$. There is a well-known one-to-one correspondence $\leftrightarrow$ between $g \times g$ quaternionic Hermitian matrices and $2g \times 2g$ symplectic (= nondegenerate alternating) matrices; a reference is [Eke87, §1]. Let $e = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and identify $\mathcal{O}_{\ell}$ with $\mathrm{Mat}_{2 \times 2}(\mathbb{Z}_{\ell})$ so that the main involution on $\mathcal{O}_{\ell}$ becomes

$$\overline{\begin{bmatrix} a & b \\ c & d \end{bmatrix}} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = e^{-1} \begin{bmatrix} a & b \\ c & d \end{bmatrix}^t e. \quad (24)$$

Let E be the $2g \times 2g$ block matrix with e 's on the diagonal. The identification of $\mathcal{O}_{\ell}$ with $\mathrm{Mat}_{2 \times 2}(\mathbb{Z}_{\ell})$ gives an identification of $\mathrm{Mat}_{g \times g}(\mathcal{O}_{\ell})$ with $\mathrm{Mat}_{g \times g}(\mathrm{Mat}_{2 \times 2}(\mathbb{Z}_{\ell})) = \mathrm{Mat}_{2g \times 2g}(\mathbb{Z}_{\ell})$; as notation $A \in \mathrm{Mat}_{g \times g}(\mathcal{O}_{\ell})$ is identified with $\tilde{A} \in \mathrm{Mat}_{2g \times 2g}(\mathbb{Z}_{\ell})$ so $\mathrm{Nm}(A) = \det(\tilde{A})$. For a $A \in \mathrm{Mat}_{g \times g}(\mathcal{O}_{\ell})$ with $A^{\dagger} = \overline{A}^t \in \mathrm{Mat}_{g \times g}(\mathcal{O}_{\ell})$, (24) implies that

$$\widetilde{A^{\dagger}} = E^{-1} \tilde{A}^t E. \quad (25)$$

In case $A = H$ is Hermitian so that $H^{\dagger} = H$, (25) gives

$$E \tilde{H} = E \widetilde{H^{\dagger}} = \tilde{H}^t E,$$

so that

$$(E \tilde{H})^t = \tilde{H}^t E^t = \tilde{H}^t (-E) = -\tilde{H}^t E = -(E \tilde{H}). \quad (26)$$

This gives the one-to-one correspondence $\leftrightarrow$: to the Hermitian matrix $H \in \mathrm{Mat}_{g \times g}(\mathcal{O}_{\ell})$ we associate the symplectic matrix $S_H := E \tilde{H} \in \mathrm{Mat}_{2g \times 2g}(\mathbb{Z}_{\ell})$. With Pf denoting the Pfaffian of a symplectic matrix we have $\mathrm{HNm}(H) = \mathrm{Pf}(S_H)$.

We examine how this correspondence behaves with respect to sublattices. Let L be a nondegenerate Hermitian right $\mathcal{O}_{\ell}$ -module of rank g such that $L \otimes \mathbb{Q}_{\ell} \cong \mathbb{H}_{\ell}^g$ with Hermitian form given by $H \in \mathrm{Mat}_{g \times g}(\mathcal{O}_{\ell})$ (so $H^{\dagger} = H$). Let $L' = AL \subset L$ be an $\mathcal{O}_{\ell}$ -sublattice of finite index $i = [L : L']$ for $A \in \mathrm{Mat}_{g \times g}(\mathcal{O}_{\ell})$; then $(i) = (\mathrm{Nm}(A)^2)$ as ideals in $\mathbb{Z}_{\ell}$ and $i = \ell^{2 \mathrm{val}_{\ell}(\mathrm{Nm}(A))}$. Let $H' = A^{\dagger} H A$ be the restriction of H to L' . We have

$$\mathrm{Nm}(H') = \mathrm{Nm}(A)^2 \mathrm{Nm}(H) = i \mathrm{Nm}(H), \text{ or, } |\mathrm{HNm}(H')| = \sqrt{i} |\mathrm{HNm}(H)|. \quad (27)$$

Separately, let $\tilde{L}$ be a rank- $2g$ symplectic $\mathbb{Z}_{\ell}$ -lattice with symplectic form S . Let $\tilde{L}' := M \tilde{L} \subseteq \tilde{L}$ for $M \in \mathrm{Mat}_{2g \times 2g}(\mathbb{Z}_{\ell})$ be a sublattice of finite index $\tilde{i}$ so $(\tilde{i}) = (\det(M))$ as ideals in $\mathbb{Z}_{\ell}$ with symplectic form $S' = M^t S M$ given by restricting S to $\tilde{L}'$. Then $(\mathrm{Pf}(S')) = (\mathrm{Pf}(S) \tilde{i})$ as ideals in $\mathbb{Z}_{\ell}$. We have

$$\begin{aligned} (\tilde{i}) &= (\det(M)) \subseteq \mathbb{Z}_{\ell}, \quad (\det(S')) = (\det(M)^2 \det(S)), \text{ and} \\ (\mathrm{Pf}(S')) &= (\det(M) \mathrm{Pf}(S)) = (\tilde{i} \mathrm{Pf}(S)) \subseteq \mathbb{Z}_{\ell}. \end{aligned} \quad (28)$$

Now consider $\tilde{L} = \mathbb{Z}_{\ell}^{2g}$ with $S = S_H$ and $A \in \mathrm{Mat}_{g \times g}(\mathcal{O}_{\ell})$ with $H' = A^{\dagger} H A$ the restriction of H to the $\mathcal{O}_{\ell}$ -sublattice $L' = AL$, and take $M = \tilde{A} \in \mathrm{Mat}_{2g \times 2g}(\mathbb{Z}_{\ell})$. Then $S' = \tilde{A}^t S \tilde{A}$ the restriction of S' to the $\mathbb{Z}_{\ell}$ -sublattice $\tilde{L}' = \tilde{A} \tilde{L}$. Note that

$$S_{H'} = E \tilde{A}^{\dagger} \tilde{H} \tilde{A} = \tilde{A}^t E \tilde{H} \tilde{A} = \tilde{A}^t S_H \tilde{A} = S' \quad (29)$$

using (25). Using (27), the indices $\iota = [L : L']$ and $\tilde{i} = [\tilde{L} : \tilde{L}']$ are related by

$$\iota = \ell^{2 \mathrm{val}_{\ell}(\mathrm{Nm}(A))} = \ell^{2 \mathrm{val}_{\ell}(\det(\tilde{A}))} = (\ell^{\mathrm{val}_{\ell}(\det \tilde{A})})^2 = \tilde{i}^2. \quad (30)$$

The problem of computing a given row sum of the Brandt matrix $B(\ell^r)$ by (23) is the following: We are given $L = \mathcal{O}_\ell^g$ together with a unimodular Hermitian form $H \in \text{Mat}_{g \times g}(\mathcal{O}_\ell)$ (so $|\text{HNm}(H)| = 1$). We have to count the $\mathcal{O}_\ell$ -submodules $\ell^r L \subset L' \subset L$ with $[L : L'] = \ell^{2rg}$ such that the restriction H' of H to L' satisfies $H' = \ell^r \mathbf{H}'$ with $\mathbf{H}' \in \text{Mat}_{g \times g}(\mathcal{O}_\ell)$ unimodular. Applying the one-to-one correspondence $\leftrightarrow$ above induced by $H \leftrightarrow S = S_H$ and $H' \leftrightarrow S' = S_{H'}$ we see that this is equivalent to the following computation with symplectic $\mathbb{Z}_\ell$ -lattices of rank $2g$: given the lattice $\tilde{L} = \mathbb{Z}_\ell^{2g}$ together with a unimodular symplectic pairing S (unimodular in the sense that $\text{Pf}(S) \in \mathbb{Z}_\ell^\times$), count the $\mathbb{Z}_\ell$ -sublattices $\ell^r \tilde{L}' \subset \tilde{L}' \subset \tilde{L}$ with $[\tilde{L} : \tilde{L}'] = \ell^{rg}$ such that the restriction S' of S to $\tilde{L}'$ satisfies $S' = \ell^r \mathbf{S}'$ for a unimodular symplectic matrix $\mathbf{S}' \in \text{Mat}_{2g \times 2g}(\mathbb{Z}_\ell)$. (The indices $[L : L']$ and $[\tilde{L} : \tilde{L}']$ are related by (30).) It follows that $\tilde{L}'/\ell^r \tilde{L}$ is a maximal isotropic subspace of $\tilde{L}/\ell^r \tilde{L}$ with respect to the $\mathbb{Z}/\ell^r \mathbb{Z}$ -symplectic pairing on $\tilde{L}/\ell^r \tilde{L}$ induced by S . Moreover, given the maximal isotropic subspace $\tilde{L}'/\ell^r \tilde{L}$ we can recover $\tilde{L}' \subseteq \tilde{L}$. We now remark that all unimodular symplectic lattices over $\mathbb{Z}_\ell$ of the same dimension are isomorphic. Hence without loss of generality we can start with $\tilde{L} = \mathbb{Z}_\ell^{2g}$ and S the standard unimodular symplectic pairing. So the sum of the entries in any row of the Brandt matrix $B_g(\ell^r)$ is equal to $N_g(\ell^r)$ as in (2). In particular all the row sums of $B_g(\ell^r)$ are equal and (perhaps surprisingly) do not depend on p .

(c): By definition this is equivalent to proving that $\#\{U \in \text{GU}_g(\mathbb{H}) \mid [L_i : UL_j] = n^{2g}\}$ and $\#\{U \in \text{GU}_g(\mathbb{H}) \mid [L_j : UL_i] = n^{2g}\}$ are equal. By the comments following (20) we can replace the L 's with arbitrary representatives of their classes. By Remark 11 we can use their duals, so

$$\#\{U \in \text{GU}_g(\mathbb{H}) \mid [L_j : UL_i] = n^{2g}\} = \#\{U \in \text{GU}_g(\mathbb{H}) \mid [\widehat{L_j} : (\widehat{U^{-1}})^\dagger \widehat{L_i}] = n^{2g}\}.$$

But by Remark 8 the right hand side of the above is equal to

$$\#\{U \in \text{GU}_g(\mathbb{H}) \mid [(U^{-1})^\dagger L_i : L_j] = n^{2g}\} = \#\{U \in \text{GU}_g(\mathbb{H}) \mid [L_i : U^\dagger L_j] = n^{2g}\},$$

and we are done.

(d): See [Eke87, p. 159] and [HI80, Prop. 9], cf. [Yu06, Thm. 3.1].

(e): The Brandt matrices $B(n)$ are in image of the Hecke algebra for (G, K) with $G = \text{GU}_g(\widehat{\mathbb{H}})$, $K = \text{GU}_g(\mathcal{O}_{\widehat{\mathbb{H}}})$ acting on the lattice $\mathbb{Z}[\mathcal{P}_g(\mathcal{O}_{\widehat{\mathbb{H}}})]$ with basis $\mathcal{P}_g(\mathcal{O}_{\widehat{\mathbb{H}}})$, which is a space of algebraic modular forms in the sense of [Gro99]. In fact the Brandt matrices $B(n)$ are linear combinations of standard Hecke operators in the Hecke algebra.

By (b) we may restrict to the case where both m and n are powers of a prime ℓ . Commutativity here is implied by commutativity of the local Hecke algebra for

$$G = G_\ell = \text{GU}_g(\mathbb{H} \otimes \mathbb{Z}_\ell), \quad K = K_\ell = \text{GU}_g(\mathcal{O}_{\mathbb{H}} \otimes \mathbb{Z}_\ell) \quad (31)$$

Satake proves a structure theorem for this local algebra [Sat63, Thm. 8] which in particular shows that it is commutative.

Below we give a simple argument for commutativity, worked out in correspondence with Guy Henniart and Marie-France Vignéras. We use (G, K) as in (31). By Gelfand's trick [Lan85, IV, §1, Thm. 1] (see also [Shi94, Prop. 3.8]), it suffices to show that for all elements $M \in G$ we have $KMK = KM^\dagger K$.

In the case when $\ell = p$, by [Shi63, Prop. 3.10] we have that for every $M \in G$, $KMK = KdK$ for some diagonal matrix d over the quaternion algebra $\mathbb{H} \otimes \mathbb{Z}_\ell$. We also have $KdK = Kd^\dagger K$ since in the ramified case all ideals are two-sided and principal powers of the unique prime ideal.

When $\ell \neq p$, the group G is just the symplectic group and we can use [Shi63, Prop. 1.6] to show that for arbitrary $M \in G$ we have $KMK = KdK$, where d is now in a diagonal matrix over $\mathbb{Q}_\ell$, hence trivially preserved by transpose.

The only complication is making sure (conjugate-)transpose is in fact an anti-involution in the basis from [Shi63]. However if H is the matrix giving the Hermitian (or symplectic) form in Shimura's basis then we have $H^\dagger H H = H$, so H is itself an element of G . And since for any matrix $M \in G$ we have $M^\dagger = H M^{-1} H^{-1}$, (conjugate-)transpose is in fact an anti-involution.

(f): This follows trivially from (c), (e), and the fact that self-adjoint matrices are semi-simple with real eigenvalues. □

We do not know the analogue of Remark 18(d) for our generalized Brandt matrices $B_g(n)$. For a weak result see [And69, Thm. 3].

4. THE BIG AND LITTLE BRANDT GRAPHS

It is convenient to reformulate Section 3 on Brandt matrices in the broader context of Brandt graphs. We begin with a general discussion of graphs in order to be precise about the definitions. We will again use this in Section 6 when we consider the big, little, and enhanced isogeny graphs.

4.1. Graphs.

Definition 20. A graph Gr has a set of vertices $\text{Ver}(\text{Gr}) = \{v_1, \dots, v_s\}$ and a set of (directed) edges $\text{Ed}(\text{Gr})$. An edge $e \in \text{Ed}(\text{Gr})$ has initial vertex $o(e)$ and terminal vertex $t(e)$. For vertices $v_i, v_j \in \text{Ver}(\text{Gr})$, put

$$\text{Ed}(\text{Gr})_{ij} = \{e \in \text{Ed}(\text{Gr}) \mid o(e) = v_i \text{ and } t(e) = v_j\}.$$

The adjacency matrix $\text{Ad}(\text{Gr}) \in \text{Mat}_{s \times s}(\mathbb{Z})$ is the matrix with

$$\text{Ad}(\text{Gr})_{ij} = \# \text{Ed}(\text{Gr})_{ij}.$$

We place no further restrictions on our definition of a graph. Serre [Ser03] requires graphs to be **graphs with opposites**: every directed edge $e \in \text{Ed}(\text{Gr})$ has an **opposite** edge $\bar{e} \in \text{Ed}(\text{Gr})$. An edge e with $\bar{e} = e$ is called a **half-edge**. Serre forbids half-edges; we will call a graph satisfying his requirements a **graph without half-edges**. Kurihara [Kur79] relaxes Serre's definition to allow half-edges giving the notion of a **graph with half-edges**. (A graph with half-edges may have $\emptyset$ as its set of half-edges, so every graph without half-edges is a graph with half-edges.)

Definition 21. (a) A **graph with weights**, or a **weighted graph**, is a graph with opposites together with a **weight function** w mapping vertices and edges to positive integers such that for each edge e we have $w(e) = w(\bar{e})$ and $w(e) \mid w(o(e))$ (which implies $w(e) \mid w(t(e))$).
 (b) Following [Kur79, Defn. 3-1], a **graph with lengths** is a graph with opposites together with a **length function** f mapping edges to positive integers satisfying $f(e) = f(\bar{e})$. A graph

with weights defines a graph with lengths by setting the length of an edge equal to its weight and forgetting the weights of the vertices.

- (c) The **weighted adjacency matrix** $A_w := \text{Ad}_w(\text{Gr})$ of a weighted graph Gr with $\text{Ver}(\text{Gr}) = \{v_1, \dots, v_s\}$ is

$$(A_w)_{ij} = \sum_{e \in \text{Ed}(\text{Gr})_{ij}} \frac{w(v_i)}{w(e)}, \quad 1 \leq i, j \leq s.$$

- (d) Following [Kur79, §3], if Gr is a graph with half-edges, denote by Gr^* the graph obtained by removing the half-edges from Gr . If Gr is a graph with weights, then the graph Gr^* with half-edges removed is also a graph with weights—the weights are inherited from Gr . Likewise, if Gr is a graph with lengths, then Gr^* is a graph with inherited lengths.

Many authors (especially in computer science) call a graph with weights what we have called a graph with lengths, and accordingly have a different notion of a weighted adjacency matrix.

For the remainder of this section, we let $\mathbb{H}$ be a rational definite quaternion algebra with maximal order $\mathcal{O}_{\mathbb{H}} \subseteq \mathbb{H}$, main involution $x \mapsto \bar{x}$, and reduced norm $\text{Nm}_{\mathbb{H}/\mathbb{Q}}(x) = x\bar{x}$. Let $\hat{\mathbb{Z}}$ be the profinite completion of $\mathbb{Z}$ and $\hat{\mathbb{Q}} = \hat{\mathbb{Z}} \otimes \mathbb{Q}$ the finite adèles of $\mathbb{Q}$. Set $\mathcal{O}_{\hat{\mathbb{H}}} = \mathcal{O}_{\mathbb{H}} \otimes \hat{\mathbb{Z}}$ and let $\hat{\mathbb{H}} = \mathcal{O}_{\hat{\mathbb{H}}} \otimes \mathbb{Q}$ be the finite adèles of $\mathbb{H}$.

The classes of $\text{GU}_g(\mathcal{O}_{\mathbb{H}})$ are

$$\mathcal{P}_g(\mathcal{O}_{\mathbb{H}}) = \{[L_1], \dots, [L_h]\}$$

with L_i a principally polarized right $\mathcal{O}_{\mathbb{H}}$ -module and $h = h_g(\mathbb{H})$ as in Definition 10. In case $g = 1$ the principally polarized right $\mathcal{O}_{\mathbb{H}}$ -module L_i is just a right $\mathcal{O}_{\mathbb{H}}$ -ideal I_i with left order the maximal ideal $\mathcal{O}_i \subseteq \mathbb{H}$. We will freely use the notation in Definition 13 and Remark 14 of Section 3, which the reader is advised to review.

4.2. The big Brandt graph $Br_g(n, \mathcal{O}_{\mathbb{H}})$. The vertices of the big Brandt graph $Br_g(n) := Br_g(n, \mathcal{O}_{\mathbb{H}})$ are

$$\text{Ver}(Br_g(n)) = \mathcal{P}_g(\mathcal{O}_{\mathbb{H}}) = \{[L_1], \dots, [L_h]\}.$$

The directed edges connecting the vertex $[L_i]$ to the vertex $[L_j]$ are

$$\text{Ed}(Br_g(n))_{ij} = \mathbf{B}_g(n)_{ij}^{\text{big}}$$

as in (16) and (18). The graph $Br_g(n)$ is a graph without opposites. Moreover it is immediate from (20) that the adjacency matrix of $Br_g(n)$ is the Brandt matrix $B_g(n)$ for $\mathcal{O}_{\mathbb{H}} \subseteq \mathbb{H}$:

$$\text{Ad}(Br_g(n)) = B_g(n). \tag{32}$$

When $g = 1$ the big Brandt graph $Br_1(n)$ is the graph constructed by Pizer [Piz98], [Piz90] from the classical Brandt matrices.

4.3. The little Brandt graph $br_g(n, \mathcal{O}_{\mathbb{H}})$. The vertices of the little Brandt graph $br_g(n) := br_g(n, \mathcal{O}_{\mathbb{H}})$ are

$$\text{Ver}(br_g(n)) = \mathcal{P}_g(\mathcal{O}_{\mathbb{H}}) = \{[L_1], \dots, [L_h]\}.$$

The directed edges connecting the vertex $[L_i]$ to the vertex $[L_j]$ are

$$\text{Ed}(br_g(n))_{ij} = \mathbf{B}_g(n)_{ij}^{\text{little}}$$

as in (17) and (19).

Unlike the big Brandt graph, the little Brandt graph $br_g(n)$ is a graph with opposites: the opposite $\bar{e}$ of an edge $e \in \text{Ed}(br_g(n))_{ij}$ with $e = [L'_j]_l$ as in (18) is $\bar{e} = [V\widehat{L}_i]_l$, where V satisfies $V\widehat{L}'_j = L_j$ with the dual $\widehat{L}'$ of the principally polarized finitely generated right $\mathcal{O}_{\mathbb{H}}$ -module L' with $L' \otimes \mathbb{Q} = \mathbb{H}^g$ defined in (10). The little Brandt graph $br_g(n)$ is also a graph with weights: we set $w([L_i]) = e_i(g)$ for $[L_i] \in \mathcal{P}_g(\mathcal{O}_{\mathbb{H}}) = \text{Ver}(br_g(n))$ and $w([U]_l) = e(U)$ for $[U]_l \in \mathbf{B}_g(n)_{ij}^{\text{little}} = \text{Ed}(br_g(n))_{ij}$ in the notation (15). To see that this is well-defined, verify

- (a) $e(U) = e(U')$ if $[U]_l = [U']_l \in \mathbf{B}_g(n)_{ij}^{\text{little}} = \text{Ed}(br_g(n))_{ij}$ and
- (b) $w(e) = w(\bar{e})$ for $e \in \text{Ed}(br_g(n))_{ij}$.

It follows from the definitions that the weighted adjacency matrix of the little Brandt graph $br_g(n)$ is the usual Brandt matrix $B_g(n)$:

Proposition 22. *We have $\text{Ad}_w(br_g(n)) = \text{Ad}(B_g(n)) = B_g(n)$.*

Part 2. Applying the quaternion infrastructure to isogeny graphs

5. SUPERSPECIAL ABELIAN VARIETIES, THEIR PRINCIPAL AND $[\ell]$ -POLARIZATIONS, AND THEIR ISOGENIES

In this section X is an abelian variety defined over a field k (not necessarily algebraically closed) with dual abelian variety $\hat{X} = \text{Pic}^0(X)$; A will continue to denote a superspecial abelian variety. If $f: X \rightarrow Y$ is a morphism of abelian varieties over k , the dual morphism $\hat{f}: \hat{Y} \rightarrow \hat{X}$ is defined over k . For a point x of X , denote by t_x translation by x on X ; the isomorphism class of a line bundle L on X is denoted $[L]$. A homomorphism $\tau: X \rightarrow \hat{X}$ is symmetric if $\hat{\tau} = \tau$, where we identify $X = \hat{\hat{X}}$ via the canonical isomorphism

$$\kappa_X: X \xrightarrow{\sim} \hat{\hat{X}} \text{ of [vdGM, Thm. 7.9], for example.} \quad (33)$$

A line bundle L on X gives rise to a symmetric homomorphism $\varphi_L: X \rightarrow \hat{X}$ which maps points x of X to $[t_x^* L \otimes L^{-1}]$. The Poincaré line bundle on $X \times \hat{X}$ is denoted $\mathcal{P}$. Our standard reference for abelian varieties is [vdGM], whose modern treatment of polarizations is ideally suited to our needs here.

Definition 23. (cf. [vdGM, Cor. 11.5, Defn. 11.6].) A **polarization** of an abelian variety X over a field k is a homomorphism $\lambda: X \rightarrow \hat{X}$ over k satisfying the equivalent conditions

- (a) λ is a symmetric isogeny and the line bundle $(\text{id}_X, \lambda)^* \mathcal{P}$ is ample;
- (b) there exists a finite separable field extension $k \subseteq K$ and an ample line bundle L on X_K such that $\lambda_K = \varphi_L$.

If $\lambda: X \rightarrow \hat{X}$ is a polarization of the abelian variety X , following Mumford [MFK94, Defns. 7.2, 7.3] define the **degree** $\deg(\lambda)$ of the polarization λ to be the degree of the isogeny λ , i.e., $\#\ker(\lambda)$. The degree $\deg(\lambda)$ is always a square by the Riemann-Roch theorem: $\deg(\lambda) = d^2$ with $d = \chi(L)$ if $\lambda_{\bar{k}} = \varphi_L$, see [Mum08, §16]. It is convenient to define the **reduced degree** $\text{rdeg}(\lambda)$ of the polarization λ to be

$$\text{rdeg}(\lambda) = \sqrt{\deg(\lambda)}. \quad (34)$$

A polarization $\lambda: X \rightarrow \hat{X}$ which is an isomorphism is a **principal polarization**. If $\lambda: X \rightarrow \hat{X}$ is a polarization of the abelian variety X and $\phi: X' \rightarrow X$ is an isogeny, then

$$\phi^*(\lambda) := \hat{\phi} \circ \lambda \circ \phi: X' \rightarrow \hat{X}' \quad (35)$$

is a polarization of X' with

$$\deg(\phi^*(\lambda)) = \deg(\lambda) \deg(\phi)^2 \quad \text{and} \quad \text{rdeg}(\phi^*(\lambda)) = \text{rdeg}(\lambda) \deg(\phi). \quad (36)$$

Definition 24. Suppose the abelian variety X over the field k has dimension g and polarization $\lambda: X \rightarrow \hat{X}$ with kernel $\ker(\lambda)$. The polarization λ is an $[\ell]$ -**polarization** for a prime $\ell \neq \text{char } k$ if $\ker(\lambda) \subseteq X[\ell]$. An $[\ell]$ -polarization $\lambda: X \rightarrow \hat{X}$ has reduced degree $\text{rdeg}(\lambda) = \ell^r$ for $0 \leq r \leq g$. We say that λ is of **type** r and (X, λ) is an $[\ell]$ -polarized abelian variety of type r . An $[\ell]$ -polarization of type 0 is a principal polarization. If $\lambda: X \rightarrow \hat{X}$ is an $[\ell]$ -polarization of type r , then there is a homomorphism $[\lambda] = [\lambda]_\ell: \hat{X} \rightarrow X$ such that $[\lambda] \circ \lambda$ is multiplication by ℓ on X . We will see in Theorem 28 that $[\lambda]$ is an $[\ell]$ -polarization of type $\hat{r} := g - r$ on $\hat{X}$.

Remark 25. For an abelian variety X over a field k and $n \in \mathbb{N}$ prime to $\text{char } k$ there is a perfect pairing

$$\langle \cdot, \cdot \rangle_n := \langle \cdot, \cdot \rangle_{X,n}: X[n] \times \hat{X}[n] \rightarrow \mu_n.$$

A polarization λ on X gives rise to the Weil pairing

$$\langle \cdot, \cdot \rangle_{\lambda,n} := \langle \cdot, \cdot \rangle_{X,\lambda,n}: X[n] \times X[n] \longrightarrow X[n] \times \hat{X}[n] \xrightarrow{\langle \cdot, \cdot \rangle_n} \mu_n \text{ with } \langle u, v \rangle_{\lambda,n} = \langle u, \lambda(v) \rangle_n.$$

Proposition 26. Let X be an abelian variety over a field k with $\dim X = g$. Let $\mathcal{P}$ be the Poincaré line bundle on $X \times \hat{X}$.

(a) Let $\tau: X \rightarrow \hat{X}$ be a symmetric isogeny. The following are equivalent:

- (i) τ is a polarization.
- (ii) $(n \text{id}_X, \tau)^* \mathcal{P}$ is an ample line bundle on X for some $n \in \mathbb{N}$.
- (iii) $(n \text{id}_X, \tau)^* \mathcal{P}$ is an ample line bundle on X for all $n \in \mathbb{N}$.
- (iv) $n\tau$ is a polarization for some $n \in \mathbb{N}$.
- (v) $n\tau$ is a polarization for all $n \in \mathbb{N}$.

(b) Let $\ell \neq \text{char } k$ be a prime. If (X, λ) is an $[\ell]$ -polarized abelian variety of type g , then $\lambda = \ell\lambda'$ for a principal polarization λ' of X .

Proof. (a): As in Definition 23, the symmetric isogeny $\eta: X \rightarrow \hat{X}$ is a polarization if and only if the line bundle $(\text{id}_X, \eta)^* \mathcal{P}$ on X is ample. But

$$(n \text{id}_X, \eta)^* \mathcal{P} = (\text{id}_X, n\eta)^* \mathcal{P} = (\text{id}_X, \eta)^* \mathcal{P}^{\otimes n} = ((\text{id}_X, \eta)^* \mathcal{P})^{\otimes n}$$

by [vdGM, Exercise 7.4], and so $(n \text{id}_X, \eta)^* \mathcal{P} = (\text{id}_X, n\eta)^* \mathcal{P}$ is ample if and only if $(\text{id}_X, \eta)^* \mathcal{P}$ is ample.

(b): If (X, λ) is an $[\ell]$ -polarized abelian variety of type g , then $\lambda = \ell\lambda'$ for a symmetric isogeny $\lambda': X \rightarrow \hat{X}$. By (a) we have that λ' is a principal polarization of X . $\square$

Definition 27. Let $\mathcal{A} = (A, \lambda)$ be an $[\ell]$ -polarized g -dimensional superspecial abelian variety over $\overline{\mathbb{F}}_p$, $p \neq \ell$. We denote its $\overline{\mathbb{F}}_p$ -isomorphism class by $[\mathcal{A}]$.

(a) For $0 \leq r \leq g$, let $\text{SP}_g(\ell, p)_r$ be the set of $\overline{\mathbb{F}}_p$ -isomorphism classes $[\mathcal{A}]$ of g -dimensional $[\ell]$ -polarized superspecial abelian varieties over $\overline{\mathbb{F}}_p$ of type r . In particular $\text{SP}_g(p)_0 := \text{SP}_g(\ell, p)_0$ is the set of $\overline{\mathbb{F}}_p$ -isomorphism classes of principally polarized superspecial abelian varieties. The sets $\text{SP}_g(\ell, p)_r$ are finite.

- (b) For $[\mathcal{A} = (A, \lambda)] \in \mathbf{SP}_g(p)_0$, set $\ell\mathcal{A} = \ell(A, \lambda) = (A, \ell\lambda)$, so $[\ell\mathcal{A}] \in \mathbf{SP}_g(\ell, p)_g$. Suppose $\mathcal{A}' = (A, \lambda')$ with $[\mathcal{A}'] \in \mathbf{SP}_g(\ell, p)_g$. Then there is a principally polarized abelian variety $\mathcal{A} = (A, \lambda)$ with $[\mathcal{A}'] = [\ell\mathcal{A}]$ by Proposition 26(b). In particular $\mathbf{SP}_g(\ell, p)_g$ is the set of $\overline{\mathbb{F}}_p$ -isomorphism classes of g -dimensional superspecial abelian varieties over $\overline{\mathbb{F}}_p$ with ℓ times a principal polarization. There is a canonical bijection between $\mathbf{SP}_g(p)_0$ and $\mathbf{SP}_g(\ell, p)_g$ and $\#\mathbf{SP}_g(\ell, p)_g = h_g(p)$.

Theorem 28. *Suppose (X, λ) is a g -dimensional $[\ell]$ -polarized abelian variety of type r , $0 \leq r \leq g$, over a field k . Then $[\lambda] = [\lambda]_\ell$ as in Definition 24 is an $[\ell]$ -polarization of $\hat{X}$ of type $\hat{r} := g - r$.*

Proof. Firstly note that $[\lambda] : \hat{X} \rightarrow X$ is symmetric. Let $\mathcal{P}$ be the Poincaré bundle on $X \times \hat{X}$ and let $\mathcal{Q}$ be the Poincaré bundle on $\hat{X} \times X$, where we identify $\hat{\hat{X}} = X$ as in (33). If $s : X \times \hat{X} \rightarrow \hat{X} \times X$ is the switch factors map $s(x, y) = (y, x)$, then $s^*(\mathcal{Q}) = \mathcal{P}$. From this it follows that

$$([\lambda], \text{id}_{\hat{X}})^*\mathcal{P} = ([\lambda], \text{id}_{\hat{X}})^*s^*\mathcal{Q} = (s \circ ([\lambda], \text{id}_{\hat{X}}))^*\mathcal{Q} = (\text{id}_{\hat{X}}, [\lambda])^*\mathcal{Q} \quad (37)$$

as line bundles on $\hat{X}$. Now $[\lambda]$ is a polarization of $\hat{X}$ if and only if the line bundle $(\text{id}_{\hat{X}}, [\lambda])^*\mathcal{Q}$ on $\hat{X}$ is ample as in Definition 23. But since $\lambda : X \rightarrow \hat{X}$ is an isogeny, this is true if and only if

$$\lambda^*(\text{id}_{\hat{X}}, [\lambda])^*\mathcal{Q} = \lambda^*([\lambda], \text{id}_{\hat{X}})^*\mathcal{P} = (\ell \text{id}_X, \lambda)^*\mathcal{P}$$

is an ample line bundle on X , where we have used (37). But this is true since λ is a polarization by Proposition 26(a). Since $\deg([\lambda] \circ \lambda) = \ell^{2g}$ and $\deg(\lambda) = \ell^{2r}$, it follows that $\deg([\lambda]) = \ell^{2\hat{r}}$. Hence $[\lambda]$ is an $[\ell]$ -polarization of $\hat{X}$ of type $\hat{r}$. $\square$

Definition 29. Suppose $\mathcal{X} = (X, \lambda)$ is a g -dimensional $[\ell]$ -polarized abelian variety of type r , $0 \leq r \leq g$. The $[\ell]$ -dual of $\mathcal{X}$ is $\hat{\mathcal{X}} = (\hat{X}, [\lambda])$ with the $[\ell]$ -polarization $[\lambda]$ on $\hat{X}$ of type $\hat{r}$ as in Proposition 28. If $[\mathcal{A}] \in \mathbf{SP}_g(\ell, p)_r$, then $[\hat{\mathcal{A}}] \in \mathbf{SP}_g(\ell, p)_{\hat{r}}$. The association $[\mathcal{A}] \leftrightarrow [\hat{\mathcal{A}}]$ gives a one-to-one correspondence between $\mathbf{SP}_g(\ell, p)_r$ and $\mathbf{SP}_g(\ell, p)_{\hat{r}}$.

The $[\ell]$ -dual $\hat{\mathcal{A}}$ of $\mathcal{A} = (A, \lambda)$ with $[\mathcal{A}] \in \mathbf{SP}_g(p)_0$ is $\ell\mathcal{A}$ as in Definition 27(b) with $[\ell\mathcal{A}] \in \mathbf{SP}_g(\ell, p)_{\hat{0}} = \mathbf{SP}_g(\ell, p)_g$. Likewise the $[\ell]$ -dual $\widehat{\ell\mathcal{A}}$ of $\ell\mathcal{A} = (A, \ell\lambda)$ with $[\ell\mathcal{A}] \in \mathbf{SP}_g(\ell, p)_g$ is $[\mathcal{A}] \in \mathbf{SP}_g(p)_{\hat{g}} = \mathbf{SP}_g(p)_0$.

Now fix $n \in \mathbb{N}$ prime to $\text{char } k$. Let λ be a principal polarization on the abelian variety X over the field k . Then λ defines an alternating and nondegenerate Weil pairing on the n -torsion $X[n]$ of X

$$\langle \cdot, \cdot \rangle_{\lambda, n} : X[n] \times X[n] \rightarrow \mu_n; \quad (38)$$

$\#X[n] = n^{2g}$. A subgroup $C \subseteq X[n]$ is n -isotropic if the Weil pairing $\langle \cdot, \cdot \rangle_{\lambda, n}$ is trivial when restricted to C . An n -isotropic subgroup C is **maximal n -isotropic** if there is no n -isotropic subgroup of X properly containing C . The order of a maximal n -isotropic subgroup of X is n^g . Put

$$\text{Iso}_n(\mathcal{X}) = \{\text{maximal } n\text{-isotropic subgroups } C \subseteq X[n]\}. \quad (39)$$

For a prime $\ell \neq \text{char } k$ it is known that

$$\#\text{Iso}_\ell(\mathcal{X}) = N_g(\ell) := \prod_{k=1}^g (\ell^k + 1). \quad (40)$$

Define an equivalence relation $\sim$ on $\text{Iso}_n(\mathcal{X})$ by $C \sim C'$ if there exists $\alpha \in \text{Aut}(\mathcal{X})$ with $\alpha(C) = C'$ for $C, C' \in \text{Iso}_n(\mathcal{X})$. Put

$$\text{iso}_n(\mathcal{X}) = \text{Iso}_n(\mathcal{X}) / \sim \quad (41)$$

with $[C] \in \text{iso}_n(\mathcal{X})$ the equivalence class containing $C \in \text{Iso}_n(\mathcal{X})$.

A key fact is that quotienting a principally polarized abelian variety by a maximal isotropic subgroup gives an abelian variety which is again principally polarized:

Proposition 30. cf. [Mum08, §23, Cor. to Thm. 2] and [Oor74, p. 36]. *Suppose $\mathcal{X} = (X, \lambda)$ is a principally polarized abelian variety over an algebraically closed field k and $C \subseteq X[n]$ with n prime to $\text{char } k$. Let $\psi_C : X \rightarrow X/C =: X'$. Then there is a principal polarization λ' on X' so that $\psi_C^*(\lambda') = n\lambda$ if and only if $C \in \text{Iso}_n(\mathcal{X})$. In this case we write $\mathcal{X}' = (X', \lambda') = \mathcal{X}/C$. Furthermore, if $[\mathcal{A}] \in \text{SP}_g(p)_0$ and $(n, p) = 1$, then $[\mathcal{A}'] \in \text{SP}_g(p)_0$.*

Recall that we have fixed a supersingular elliptic curve $E = E/\overline{\mathbb{F}}_p$ with $\mathcal{O} = \mathcal{O}_{\mathbb{H}_p} = \mathcal{O}_E = \text{End}(E)$; $\mathcal{O}$ is a maximal order in the rational quaternion algebra $\mathbb{H}_p \cong \text{End}^0(E) := \text{End}(E) \otimes \mathbb{Q}$.

Remark 31. For $g > 1$ polarizations λ on g -dimensional superspecial abelian varieties $A = E^g$ in characteristic p with $\text{rdeg}(\lambda) = d$ as in (34) are in one-to-one correspondence with $\mathcal{H}_{g,d}(\mathcal{O})$ as in (7). Explicitly, let λ_0 be the product polarization on E^g . Then the polarization λ_H corresponding to $H \in \mathcal{H}_{g,d}(\mathcal{O})$ is

$$\lambda_H : A \xrightarrow{H} A \xrightarrow{\lambda_0} \hat{A}, \quad (42)$$

see [IKO86, Prop. 2.8]. Note that for $n \in \mathbb{N}$ and $H \in \mathcal{H}_{g,d}(\mathcal{O})$ we have $\lambda_{nH} = n\lambda_H$.

Proposition 32. *Let $\ell \neq p$ be prime. Let $A = E^g/\overline{\mathbb{F}}_p$ with polarizations $\lambda := \lambda_H, \lambda' := \lambda_{H'}$ corresponding to positive-definite Hermitian matrices $H, H' \in \mathcal{H}_{g,d}(\mathcal{O})$ as in (42). Let $\phi : A \rightarrow A$ be an isogeny of degree ℓ^{gm} given by $M \in \text{Mat}_{g \times g}(\mathcal{O})$. Then $\phi^*(\lambda') = \ell^m \lambda$ if and only if $M^\dagger H' M = \ell^m H$.*

Proof. By (35)

$$\phi^*(\lambda') = \hat{\phi} \circ \lambda' \circ \phi,$$

which by (42) equals

$$\hat{\phi} \circ \lambda_0 \circ H' \circ \phi = \widehat{M} \lambda_0 H' M = \lambda_0 \lambda_0^{-1} \widehat{M} \lambda_0 H' M.$$

Now $\lambda_0^{-1} \widehat{M} \lambda_0$ is the Rosati anti-involution applied to M by definition which equals $M^\dagger$ in the product polarization case. Thus we have

$$\phi^*(\lambda') = \lambda_0 M^\dagger H' M = \lambda_{M^\dagger H' M}.$$

Hence, $\phi^*(\lambda') = \lambda_{M^\dagger H' M}$ and since $\ell^m \lambda = \ell^m \lambda_H = \lambda_{\ell^m H}$, we are done by Remark 31. $\square$

This allows us to describe the set $\text{SP}_g(p)_0$ for $g > 1$ following [IKO86].

Proposition 33. *If $g > 1$ then the map*

$$\overline{\mathcal{H}}_{g,1}(\mathcal{O}) \ni [H] \mapsto [\mathcal{A}(H)], \text{ where } \mathcal{A}(H) = (A, \lambda_H),$$

with $\mathcal{O} = \mathcal{O}_{\mathbb{H}_p}$ is a bijection between $\overline{\mathcal{H}}_{g,1}(\mathcal{O})$ defined in (8) and $\text{SP}_g(p)_0$.

We thus obtain the following description of $\text{SP}_g(p)_0$.

Theorem 34. (Ibukiyama/Katsura/Oort, Serre) *There are one-to-one correspondences $\longleftrightarrow$ with $\mathcal{O} = \mathcal{O}_{\mathbb{H}_p}$:*

(a) *For $g \geq 1$,*

$$\mathrm{SP}_g(p)_0 \longleftrightarrow \mathcal{P}_g(\mathbb{H}_p) = \mathrm{GU}_g(\mathbb{H}_p) \backslash \mathrm{GU}_g(\widehat{\mathbb{H}}_p) / \mathrm{GU}_g(\mathcal{O}_{\widehat{\mathbb{H}}_p}).$$

(b) *For $g > 1$,*

$$\mathrm{SP}_g(p)_0 \longleftrightarrow \mathcal{P}_g(\mathbb{H}_p) = \mathrm{GU}_g(\mathbb{H}_p) \backslash \mathrm{GU}_g(\widehat{\mathbb{H}}_p) / \mathrm{GU}_g(\mathcal{O}_{\widehat{\mathbb{H}}_p}) \longleftrightarrow \overline{\mathcal{H}}_{g,1}(\mathcal{O}) = \mathcal{H}_{g,1}(\mathcal{O}) / \mathrm{GL}_g(\mathcal{O}),$$

where the second one-to-one correspondence is Theorem 12.

Theorem 35. *Let $\mathcal{A} = (A, \lambda)$ and $\mathcal{A}' = (A', \lambda')$ with $[\mathcal{A}], [\mathcal{A}'] \in \mathrm{SP}_g(p)_0$ for $g > 1$ and let $\ell \neq p$ be a prime. Suppose $\psi : A' \rightarrow A$ is an isogeny such that $\psi^*(\lambda) = \ell^m \lambda'$ for $m \geq 1$. Then there exist principally polarized superspecial abelian varieties*

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

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

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

Theorem 35 will follow from the purely algebraic Theorem 36 below.

Theorem 36. *Let V be a free $\mathbb{Z}/\ell^n\mathbb{Z}$ -module of rank $2g$ with a nondegenerate symplectic pairing*

$$\langle \ , \ \rangle_V : V \times V \longrightarrow \mathbb{Q}/\mathbb{Z}.$$

Note that there is an induced nondegenerate symplectic pairing on the ℓ -torsion $V[\ell] \subseteq V$

$$\langle \ , \ \rangle_{V[\ell]} : V[\ell] \times V[\ell] \longrightarrow \mathbb{Q}/\mathbb{Z} \quad \text{by} \quad \langle \bullet, \bullet \rangle_{V[\ell]} = \langle (1/\ell^{n-1})\bullet, \bullet \rangle_V.$$

Let $M \subseteq V$ be a maximal isotropic subspace. Then there exists $G \subseteq M[\ell]$ such that $G \subseteq V[\ell]$ is maximal isotropic with respect to $\langle \ , \ \rangle_{V[\ell]}$.

Proof. The proof is by induction on g . If $g = 1$, let G be any line in $M[\ell]$. Suppose the statement is true for $g - 1$.

Case 1. $V[\ell] \subseteq M$. In this case let G be any maximal isotropic subgroup of $V[\ell]$.

Case 2. $V[\ell] \not\subseteq M$. In this case there exists $N \subseteq V$, $N \cong (\mathbb{Z}/\ell^n\mathbb{Z})^{2g-1}$, such that $M \subseteq N$. To see this note that M has at most $2g - 1$ generators, lift them arbitrarily to ℓ^n -torsion to define N .

Note that $N^\perp \cong \mathbb{Z}/\ell^n\mathbb{Z}$ and $\langle N^\perp, M \rangle_V = 0$ since $M \subseteq N$. So $N^\perp \subseteq M$ by maximality. Apply the induction hypothesis to $M/N^\perp \subseteq N/N^\perp$: $N/N^\perp$ is rank $2g - 2$ over $\mathbb{Z}/\ell^n\mathbb{Z}$ with a nondegenerate symplectic pairing induced by $\langle \ , \ \rangle_V$. Also $M/N^\perp$ is isotropic; it is maximal isotropic since if it were contained in a bigger isotropic subgroup pulling back would contradict the maximality of M . Hence by the induction hypothesis there exists $\tilde{G} \subseteq M$ with $N^\perp \subseteq \tilde{G}$ such that $\tilde{G}/N^\perp \subseteq (M/N^\perp)[\ell]$ is maximal isotropic. Now take $G = \tilde{G}[\ell]$. $\square$

Proof of Theorem 35. The proof is by induction on m . For $m = 1$ the statement follows from Proposition 30. Suppose the statement is true for m and consider $\mathcal{A}' = (A, \lambda') := (A_1, \lambda_1)$, $\mathcal{A} = (A, \lambda) := \mathcal{A}_{m+2} = (A_{m+2}, \lambda_{m+2})$ with $[\mathcal{A}], [\mathcal{A}'] \in \mathrm{SP}_g(p)_0$ for $g > 1$ and an isogeny $\psi : A' \rightarrow A$ such that $\psi^*(\lambda) = \ell^{m+1} \lambda'$ for $m \geq 1$. By Proposition 30, the kernel $C \subseteq A'[\ell^{m+1}]$

of ψ is a maximal ℓ^{m+1} -isotropic subgroup. Now apply Theorem 36 to the free $\mathbb{Z}/\ell^{m+1}\mathbb{Z}$ -module $A'[\ell^{m+1}]$ with the nondegenerate symplectic pairing $\langle \cdot, \cdot \rangle_{\lambda', \ell^{m+1}}$. This shows there exists an ℓ -maximal isotropic subgroup $G \subseteq C[\ell] \subseteq A'[\ell]$ with respect to the nondegenerate symplectic pairing $\langle \cdot, \cdot \rangle_{\lambda', \ell}$.

Let $\mathcal{A}_2$ be the principally polarized abelian variety $\mathcal{A}_2 = (A_2, \lambda_2) := \mathcal{A}'/G$ with isogeny $\psi_1 = \psi_G: A_1 := A' \rightarrow A_2$. Since $G \subseteq C$, the isogeny $\psi: A' \rightarrow A$ factors as

$$\psi: A_1 = A' \xrightarrow{\psi_1} A_2 \xrightarrow{\psi'} A_{m+2} = A.$$

Note that both $\ell^m \lambda_2$ and $\psi'^*(\lambda_{m+2})$ are polarizations on A_2 which pull back under ψ_1 to $\ell^{m+1} \lambda_1$. Since the Néron-Severi group of an abelian variety is torsion-free, this implies that $\psi'^*(\lambda_{m+2}) = \ell^m \lambda_2$. Applying the induction hypothesis to $\psi': A_2 \rightarrow A_{m+2}$ with $\psi'^*(\lambda_{m+2}) = \ell^m \lambda_2$ now concludes the proof. $\square$

6. THE BIG, LITTLE, AND ENHANCED ISOGENY GRAPHS

6.1. The big isogeny graph $Gr_g(\ell, p)$. The big $(\ell)^g$ -isogeny graph $Gr = Gr_g(\ell, p)$ (often called simply “the isogeny graph”) is the directed graph with vertices $\text{Ver}(Gr) = \text{SP}_g(p)_0 = \{[\mathcal{A}_1 = (A, \lambda_1)], \dots, [\mathcal{A}_h = (A, \lambda_h)]\}$ with $\#\text{Ver}(Gr) = h = h_g(p)$ and $A = E^g/\overline{\mathbb{F}}_p$. Its edges are

$$\text{Ed}(Gr)_{ij} = \{C \in \text{Iso}_\ell(\mathcal{A}_i) \mid [\mathcal{A}_i/C] = [\mathcal{A}_j]\} \quad (43)$$

with $\text{Iso}_\ell(\mathcal{A})$ as in (39). A useful reformulation of (43) is the following: Set

$$\text{Hom}(\mathcal{A}_i, \mathcal{A}_j)_\ell = \{\text{isogenies } \phi: \mathcal{A}_i \rightarrow \mathcal{A}_j \text{ of degree } \ell^g \text{ such that } \phi^*(\lambda_j) = \ell \lambda_i\} \text{ and}$$

$$\text{Aut}(\mathcal{A}_j) = \{\text{automorphisms } \psi: A_i \rightarrow A_j\}.$$

Define the equivalence relation $\sim_b$ on $\text{Hom}(\mathcal{A}_i, \mathcal{A}_j)$ by $\phi \sim_b \phi'$ if there is an automorphism α of $\mathcal{A}_j$ such that $\phi' = \alpha \circ \phi$ and set $\overline{\text{Hom}}(\mathcal{A}_i, \mathcal{A}_j)_\ell = \text{Hom}(\mathcal{A}_i, \mathcal{A}_j)_\ell / \sim_b$. Then by Proposition 30 we have

$$\begin{aligned} \text{Ed}(Gr)_{ij} &= \overline{\text{Hom}}(\mathcal{A}_i, \mathcal{A}_j)_\ell \quad \text{and} \\ \#\text{Ed}(Gr)_{ij} &= \frac{\#\text{Hom}(\mathcal{A}_i, \mathcal{A}_j)_\ell}{\#\text{Aut}(\mathcal{A}_j)}. \end{aligned} \quad (44)$$

We have $\sum_{j=1}^h \#\text{Ed}(Gr)_{ij} = N_g(\ell) = \prod_{k=1}^g (\ell^k + 1)$; see (40).

Theorem 37. *Let $\mathcal{O} \subseteq \mathbb{H}_p$ be the maximal order $\text{End}(E)$ with $B_g(\ell)$ the Brandt matrix for the maximal order $\mathcal{O}$. Then*

- (a) $Gr_g(\ell, p) = Br_g(\ell, \mathcal{O})$,
- (b) $\text{Ad}(Gr_g(\ell, p)) = B_g(\ell)$, and
- (c) the big isogeny graph $Gr_g(\ell, p)$ is regular of degree $N_g(\ell) = \prod_{k=1}^g (\ell^k + 1)$.

Proof. The case $g = 1$ is classical and well-known: combine Remark 14 with the quaternionic-ideal description of isogenies of supersingular elliptic curves as in, for example, [Gro87, §2].

So suppose $g > 1$. (a): With $\mathcal{O} = \mathcal{O}_{\mathbb{H}_p}$, we have

$$\text{Ver}(Gr_g(\ell, p)) = \text{Ver}(Br_g(\ell, \mathcal{O})) = \text{SP}_g(p)_0 \leftrightarrow \mathcal{P}_g(\mathcal{O}) \leftrightarrow \overline{\mathcal{H}}_{g,1}(\mathcal{O}) := \mathcal{H}_{g,1}(\mathcal{O})/\text{SL}_g(\mathcal{O})$$

using Theorem 34(b) and the definitions in Sections 6.1 and 4.2. With $h = h_g$ and $\overline{\mathcal{H}}_{g,1}(\mathcal{O}) = \{[H_1], \dots, [H_h]\}$ for $H_i \in \mathcal{H}_{g,1}$, $1 \leq i \leq h$, as in (21) we have $\text{SP}_g(p)_0 =$

$\{[\mathcal{A}_1 := (A, \lambda_{H_1})], \dots, [\mathcal{A}_h := (A, \lambda_{H_h})]\}$ for $A = E^g/\overline{\mathbb{F}}_p$ by Proposition 33. But now using the notation of Definition 15 and Theorem 16 we have

$$\begin{aligned} \text{Ed}(Gr_g(\ell, p))_{ij} &= \overline{\text{Hom}}(\mathcal{A}_i, \mathcal{A}_j)_\ell \\ &= \mathbf{U}_\ell(H_i, H_j)^{\text{big}} \text{ by Prop. 32} \\ &= \text{Ed}(Br_g(\ell, p)) \text{ by Thm. 16} \end{aligned} \quad (45)$$

Since the edges and vertices of $Gr_g(\ell, p)$ and $Br_g(\ell, \mathcal{O})$ correspond, we have $Gr_g(\ell, p) \cong Br_g(\ell, \mathcal{O})$.

(b): This follows immediately from (a) using (32).

(c): This follows from (b) by Theorem 19 (a). $\square$

Taking the dual isogeny does *not* give a well-defined involution on $\text{Ed}(Gr)$, so the big isogeny graph $Gr_g(\ell, p)$ is not a graph with opposites.

6.2. The little isogeny graph $gr_g(\ell, p)$. The little $(\ell)^g$ -isogeny graph $gr = gr_g(\ell, p)$ has vertices $\text{Ver}(gr) = \mathbf{SP}_g(p)_0$, so the big graph Gr and the little graph gr have the same vertices. The edges of gr are

$$\text{Ed}(gr)_{ij} = \{[C] \in \text{iso}_\ell(\mathcal{A}_i) \mid [\mathcal{A}_i/C] = [\mathcal{A}_j]\} \quad (46)$$

with $\text{iso}_\ell(\mathcal{A}) = \text{Iso}_\ell(\mathcal{A})/\sim$ as in (41). Given an edge $e \in \text{Ed}(gr)_{ij}$ with $e = [C] \in \text{iso}_\ell(\mathcal{A}_i)$ we define its opposite edge $\bar{e} \in \text{Ed}(gr)_{ji}$ by $\bar{e} = [\widehat{C}] \in \text{iso}_\ell(\mathcal{A}_j)$ with $\widehat{C}$ the kernel of the dual isogeny $\mathcal{A}_j \rightarrow \mathcal{A}_i$. Note that this dual is only well-defined up to $\sim$; thus, it is an operation on gr (but not Gr). The little graph gr is therefore a graph with opposites. In general gr is a graph with half-edges.

Again we can reformulate (46) in terms of isogenies. Recall from Section 6.1 that

$$\text{Ed}(Gr)_{ij} = \overline{\text{Hom}}(\mathcal{A}_i, \mathcal{A}_j)_\ell; \quad (47)$$

an isogeny $\phi \in \text{Hom}(\mathcal{A}_i, \mathcal{A}_j)_\ell$ defines a class $[\phi] \in \overline{\text{Hom}}(\mathcal{A}_i, \mathcal{A}_j)$. Define an equivalence relation $\sim_l$ on $\overline{\text{Hom}}(\mathcal{A}_i, \mathcal{A}_j)_\ell$ by $[\phi] \sim_l [\phi']$ if $[\phi'] = [\phi \circ \beta]$ for $\beta \in \text{Aut}(\mathcal{A}_i)$ and set

$$\overline{\overline{\text{Hom}}}(\mathcal{A}_i, \mathcal{A}_j)_\ell = \overline{\text{Hom}}(\mathcal{A}_i, \mathcal{A}_j)_\ell / \sim_l.$$

Then

$$\text{Ed}(gr)_{ij} = \overline{\overline{\text{Hom}}}(\mathcal{A}_i, \mathcal{A}_j)_\ell. \quad (48)$$

Definition 38. Define a weight function w on the small graph $gr = gr_g(\ell, p)$ by $w([\mathcal{A}]) = \#\text{Aut}(\mathcal{A})$ and $w(C) = \#\text{Aut}(A, \lambda, C)$ for the vertex corresponding to $[\mathcal{A} = (A, \lambda)] \in \mathbf{SP}(g, p)$ and the edge corresponding to $[C] \in \text{iso}_\ell(\mathcal{A})$, respectively. Then gr is a weighted graph with half-edges.

Theorem 39. Let $\mathcal{O} = \text{End}(E) \subseteq \mathbb{H}_p$ and let $B_g(\ell)$ be the Brandt matrix for $\mathcal{O}$. Then

- (a) $gr_g(\ell, p) = br_g(\ell, \mathcal{O})$ and
- (b) $\text{Ad}_w(gr_g(\ell, p)) = \text{Ad}(Gr_g(\ell, p)) = B_g(\ell)$.

Proof. (a): Again the case $g = 1$ is classical and follows from Remark 14.

So suppose $g > 1$. We have

$$\text{Ver}(gr_g(\ell, p)) = \text{Ver}(Gr_g(\ell, p)) = \text{Ver}(Br_g(\ell, p)) = \text{Ver}(br_g(\ell, p))$$

from the proof of Theorem 37(a).

We have

$$\begin{aligned}
\text{Ed}(gr_g(\ell, p))_{ij} &= \overline{\overline{\text{Hom}}}(\mathcal{A}_i, \mathcal{A}_j)_\ell \text{ by (48)} \\
&= \mathbf{U}_\ell(H_i, H_j)^{\text{little}} \text{ by Prop. 32} \\
&= \text{Ed}(br_g(\ell, p))_{ij} \text{ by Thm. 16.}
\end{aligned} \tag{49}$$

Since the edges and vertices of $gr_g(\ell, p)$ and $br_g(\ell, \mathcal{O})$ correspond, we have $gr_g(\ell, p) \cong br_g(\ell, \mathcal{O})$.
(b): The equality of $\text{Ad}_w(gr_g(\ell, p))$ and $\text{Ad}(Gr_g(\ell, p))$ follows since each edge $[C] \in \text{Ed}(gr_g(\ell, p))$ corresponds to a number of edges of $\text{Ed}(Gr_g(\ell, p))_{ij}$ equal to the size of the orbit of C under $\text{Aut}(\mathcal{A}_i)$ which equals

$$\frac{\# \text{Aut}(\mathcal{A}_i)}{\# \text{Aut}(A_i, \lambda_i, C)} = \frac{w([\mathcal{A}_i])}{w([C])}.$$

Now apply Theorem 37(b). □

6.3. The enhanced isogeny graph $\tilde{gr}_g(\ell, p)$. In the notation of Definition 27, put $h = h_g(p)$ and

$$\begin{aligned}
\text{SP}_g(p)_0 &= \{[\mathcal{A}_1], \dots, [\mathcal{A}_h]\} = \{v_1, \dots, v_h\}, \\
\text{SP}_g(p)_g &= \{[\ell\mathcal{A}_1], \dots, [\ell\mathcal{A}_h]\} = \{v_{h+1}, \dots, v_{2h}\}.
\end{aligned}$$

The enhanced $(\ell)^g$ -isogeny graph $\tilde{gr} = \tilde{gr}_g(\ell, p)$ has vertices

$$\text{Ver}(\tilde{gr}) = \text{SP}_g(p)_0 \coprod \text{SP}_g(p)_g = \{v_1, \dots, v_h\} \coprod \{v_{h+1}, \dots, v_{2h}\}.$$

Polarizations of type g are just ℓ times a principal polarization, and thus there is a natural bijection between $\text{SP}_g(p)_0$ and $\text{SP}_g(p)_g$. Nevertheless, they correspond to distinct vertices of $\tilde{gr}$. For $\text{SP}_g(p)_g \ni [\hat{\mathcal{A}}_i] = [\ell\mathcal{A}_i] = v_{h+i} \in \text{Ver}(\tilde{gr})$ and $\text{SP}_g(p)_0 \ni [\mathcal{A}_j] = v_j \in \text{Ver}(\tilde{gr})$, the edges of $\tilde{gr}$ from v_{h+i} to v_j are

$$\text{Ed}(\tilde{gr})_{h+i,j} = \{[C] \in \text{iso}_\ell(\mathcal{A}_i) \mid [\mathcal{A}_i/C] = [\mathcal{A}_j]\}$$

with notation as in (41). For $\text{SP}_g(p)_0 \ni [\mathcal{A}_i] = v_i \in \text{Ver}(\tilde{gr})$ and $\text{SP}_g(p)_g \ni [\hat{\mathcal{A}}_j] = [\ell\mathcal{A}_j] = v_{h+j} \in \text{Ver}(\tilde{gr})$, the edges of $\tilde{gr}$ from $v_i \in \text{Ver}(\tilde{gr})$ to $v_{h+j} \in \text{Ver}(\tilde{gr})$ are

$$\text{Ed}(\tilde{gr})_{i,h+j} = \{[\hat{C}] \in \text{iso}_\ell(\hat{\mathcal{A}}_i) \mid [\hat{\mathcal{A}}_i/\hat{C}] = [\hat{\mathcal{A}}_j]\}$$

with $\hat{\mathcal{A}}$ denoting the $[\ell]$ -dual of $\mathcal{A}$ as in Definition 29. In case $1 \leq i, j \leq h$ or $h+1 \leq i, j \leq 2h$, $\text{Ed}(\tilde{gr})_{ij} = \emptyset$.

The enhanced isogeny graph $\tilde{gr}$ is a graph with opposites: If $e \in \text{Ed}(\tilde{gr})_{ij}$ the opposite edge $\bar{e} \in \text{Ed}(\tilde{gr})_{ji}$ is the equivalence class of the dual isogeny. We never have $\bar{e} = e$, so $\tilde{gr}$ is a graph without half-edges. The graph $\tilde{gr}$ is a graph with weights: define w as the order of the automorphism group as for gr .

Theorem 40. (a) *The enhanced isogeny graph $\tilde{gr} = \tilde{gr}_g(\ell, p)$ is the bipartite double cover of the little isogeny graph $gr = gr_g(\ell, p)$ with inherited weights.*

(b) *Let $A = \text{Ad}(gr)$ and $A_w = \text{Ad}_w(gr) = \text{Ad}(Gr_g(\ell, p))$. Then*

$$\text{Ad}(\tilde{gr}) = \begin{bmatrix} 0 & A \\ A & 0 \end{bmatrix} \quad \text{and} \quad \text{Ad}_w(\tilde{gr}) = \begin{bmatrix} 0 & A_w \\ A_w & 0 \end{bmatrix} = \begin{bmatrix} 0 & B_g(\ell) \\ B_g(\ell) & 0 \end{bmatrix}.$$

Proof. (a): Let $\iota : \tilde{gr} \rightarrow \tilde{gr}$ be the involution defined on vertices by $\iota([\mathcal{A}]) = [\hat{\mathcal{A}}]$ and on edges such that if $e \in \text{Ed}(\tilde{gr})_{ij}$ corresponds to the class $[C]$, then $\iota(e) \in \text{Ed}(\tilde{gr})_{i+h,j+h}$ (where

the indices are added mod $2h$) also corresponds to the class $[C]$. Then ι fixes no vertices and no edges of $\tilde{g}r$ and $\tilde{g}r/\iota = gr$. Thus the enhanced graph $\tilde{g}r$ is the bipartite double cover of the little graph gr .

(b): Given (a), the adjacency matrices for $\tilde{g}r$ now follow from Theorems 37 and 39. $\square$

7. CONNECTEDNESS RESULTS FOR ISOGENY GRAPHS

7.1. Connectedness for $g = 1$: supersingular elliptic curves. It is well known that the ℓ -isogeny graph for supersingular elliptic curves in characteristic p is connected. A standard proof of this result relies on the fact that integral primitive quaternary quadratic forms represent all sufficiently large integers. There is another proof by Serre [Mes86, p. 223] using that the space of Eisenstein series of weight 2 for the congruence subgroup $\Gamma_0(p)$ is 1-dimensional. In this section we give the proof using Theorem 4 on strong approximation. As a byproduct we get that $Gr_1(\ell, p)$ and $gr_1(\ell, p)$ are not bipartite. This in turn enables us to conclude that the enhanced isogeny graph $\tilde{g}r_1(\ell, p)$ is connected.

Let $E/\overline{\mathbb{F}}_p$, $E'/\overline{\mathbb{F}}_p$ be supersingular elliptic curves with $\mathcal{O} = \mathcal{O}_E = \text{End}(E)$ and $\mathcal{O}' = \mathcal{O}_{E'} = \text{End}(E')$ maximal orders in $\mathbb{H}_p$. Then $\text{Hom}(E, E')$ is an ideal in $\mathbb{H}_p$ with left order $\mathcal{O}'$ and right order $\mathcal{O}$.

Lemma 41. *If $\psi \in \text{Hom}(E', E)$ has degree $\deg \psi = x \neq 0$, then the right $\mathcal{O}$ -ideal*

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

has reduced norm x .

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

$$I = \{\alpha \in \text{End}(E) = \mathcal{O} \mid \hat{\alpha}(\ker \hat{\psi}) = 0\}.$$

Thus for each prime power $\ell^k \parallel x$, $I \otimes \mathbb{Z}_\ell$ is of index ℓ^{2k} in $\mathcal{O} \otimes \mathbb{Z}_\ell$. Combining these together we see that I has index x^2 in $\mathcal{O}$ and hence has reduced norm x .

Now suppose ψ is inseparable. Let ψ' be a separable map from E' to E of degree x' . Let $\beta = \psi \circ \hat{\psi}'$. Let

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

Then by the above case I' has reduced norm x' . Also $I = \frac{\beta}{x'} I'$ and taking norms of both sides we get that the reduced norm of I is x . $\square$

Theorem 42. *Let $\ell \neq p$ be prime.*

- (a) *The big isogeny graph $Gr_1(\ell, p)$ and the little isogeny graph $gr_1(\ell, p)$ for supersingular elliptic curves are connected.*
- (b) *The graphs $Gr_1(\ell, p)$ and $gr_1(\ell, p)$ are not bipartite, i.e., given any two supersingular elliptic curves E and E' in characteristic p , there exists an isogeny $\phi : E \rightarrow E'$ such that the degree of ϕ is an even power of ℓ .*
- (c) *The enhanced isogeny graph $\tilde{g}r_1(\ell, p)$ is connected.*

Proof. (a, b): Let $E = E/\overline{\mathbb{F}}_p$ and $E' = E'/\overline{\mathbb{F}}_p$ be any two supersingular elliptic curves. By Tate's theorem E and E' are isogenous. Hence there exists an isogeny $\psi \in \text{Hom}(E', E)$ with some degree $x \neq 0$. Consider the right ideal $I \subset \mathcal{O}_E$ defined by $I = \{\psi \circ \phi \mid \phi \in \text{Hom}(E, E')\}$; I has reduced norm x by Lemma 41. Let $\alpha \in \mathbb{H}_p$ be an element of norm x ; such an α exists by the Hasse-Minkowski theorem. Then the fractional right ideal $I_1 = \alpha^{-1}I$ has norm 1.

Now by Lemma 5, there exists an element $\beta \in I_1 \otimes \mathbb{Z}[1/\ell]$ of norm 1. Let ℓ^n be a sufficiently high power of ℓ so that $\ell^n \beta \in I_1$. Then $\alpha \ell^n \beta \in I$ and thus is equal to $\psi \circ \phi$ for some $\phi \in \text{Hom}(E, E')$.

Taking the equation $\alpha \ell^n \beta = \psi \circ \phi$ and computing norms/degrees, we obtain

$$\text{Nm}_{\mathbb{H}_p/\mathbb{Q}}(\alpha) \ell^{2n} \text{Nm}_{\mathbb{H}_p/\mathbb{Q}}(\beta) = \deg(\psi) \deg(\phi).$$

Since $\text{Nm}_{\mathbb{H}_p/\mathbb{Q}}(\alpha) = \deg(\psi) = x$ and $\text{Nm}_{\mathbb{H}_p/\mathbb{Q}}(\beta) = 1$, we see that the degree of ϕ is ℓ^{2n} . Hence $Gr_1(\ell, p)$ and $gr_1(\ell, p)$ are connected and not bipartite.

(c): Since $gr_1(\ell, p)$ is connected and not bipartite, its bipartite double cover $\tilde{gr}_1(\ell, p)$ (see Theorem 40(a)) is connected. $\square$

7.2. Connectedness for $g > 1$. We now consider the higher-dimensional case; henceforth suppose $g > 1$. Here we deduce the connectedness of the isogeny graphs from strong approximation for the quaternionic unitary group. Strong approximation in this context has previously been applied to questions of moduli of abelian varieties in characteristic p : applications to Hecke orbits are in Chai/Oort [CO11, Prop. 4.3] and applications to the geometry of stratifications are in Ekedahl/Oort [Oor01, §7]; see also Chai [Cha95, Prop. 1]. In particular, Theorem 43 below should be compared with Ekedahl/Oort's version of strong approximation in [Oor01, Lemma 7.9]. Combining strong approximation with Proposition 32 and Theorem 35 shows that the isogeny graphs $Gr_g(\ell, p)$ and $gr_g(\ell, p)$ are connected. Our strong approximation argument further implies that $Gr_g(\ell, p)$ and $gr_g(\ell, p)$ are not bipartite. This in turn is used to show that the enhanced isogeny graph $\tilde{gr}_g(\ell, p)$ is connected — analogously to the $g = 1$ argument of Theorem 42. Note that [Oor01, §7] treats inseparable isogenies of superspecial abelian varieties which we do not consider here.

Let $\mathbb{H}/\mathbb{Q}$ be an arbitrary rational definite quaternion algebra with maximal order $\mathcal{O}_{\mathbb{H}}$.

Theorem 43. (cf. [Oor01, Lemma 7.9]) *Let ℓ be a prime unramified in $\mathbb{H}$. Then given any two positive-definite Hermitian matrices $H, H' \in \text{Mat}_{g \times g}(\mathcal{O}_{\mathbb{H}})$ of reduced norm 1, there exists a matrix $M \in \text{Mat}_{g \times g}(\mathcal{O}_{\mathbb{H}})$ such that*

$$M^\dagger H M = \ell^{2n} H' \tag{50}$$

for some positive integer n .

Proof. Let $M_0 \in \text{Mat}_{g \times g}(\mathbb{H})$ satisfy $M_0^\dagger M_0 = H$; such an M_0 exists by Lemma 7. By the same lemma, we can assume that $H' = I$.

We are now ready to apply the strong approximation Theorem 4. Let $\mathbb{A}$ be the adèles of $\mathbb{Q}$ and G be the quaternionic unitary group

$$G = \text{U}_g(\mathbb{H}) = \{M \in \text{Mat}_{g \times g}(\mathbb{H}) \mid M^\dagger M = \text{Id}_{g \times g}\}.$$

The quaternionic unitary group G is the compact real form of Sp_{2g} , so is simple.

Let $S = \{\ell, \infty\}$ and set

$$U = \{M \in G(\mathbb{A}) \mid (M_0^{-1} M)_q \in \text{Mat}_{g \times g}(\mathcal{O}_{\mathbb{H}} \otimes \mathbb{Z}_q) \text{ for } q \neq \ell\}. \tag{51}$$

By Lemma 7 there exists $N_q \in \text{Mat}_{g \times g}(\mathcal{O}_{\mathbb{H}} \otimes \mathbb{Z}_{(q)})$ such that $H = N_q^\dagger N_q$. Then

$$M_0 N_q^{-1} \in \text{U}_g(\mathcal{O}_{\mathbb{H}} \otimes \mathbb{Q}_q) = G(\mathbb{Q}_q).$$

The set $U \subseteq G(\mathbb{A})$ in (51) is open and nonempty since $(M_0 N_q^{-1}, M_p)_{q \notin S, p \in S} \in U$ for M_p arbitrary.

Hence by strong approximation (Theorem 4) there exists $M' \in \text{Mat}_{g \times g}(\mathbb{H})$ such that $M'^\dagger M' = \text{Id}_{g \times g}$ and $M_0^{-1} M' \in \text{Mat}_{g \times g}(\mathcal{O}_{\mathbb{H}}[1/\ell])$. Let ℓ^n be a sufficiently high power of ℓ such that $\ell^n M_0^{-1} M' \in \text{Mat}_{g \times g}(\mathcal{O}_{\mathbb{H}})$. Let $M = \ell^n M_0^{-1} M'$. Then

$$M^\dagger H M = M^\dagger M_0^\dagger M_0 M = \ell^{2n} M'^\dagger M' = \ell^{2n} \text{Id}_{g \times g}.$$

□

Theorem 44. *Let $\ell \neq p$ be prime, $g > 1$, $A = E^g$, and $\mathcal{O} = \mathcal{O}_E = \text{End}(E)$.*

- (a) *The big isogeny graph $Gr_g(\ell, p)$ and the little isogeny graph $gr_g(\ell, p)$ are connected.*
- (b) *The graphs $Gr_g(\ell, p)$ and $gr_g(\ell, p)$ are not bipartite, i.e., given any two principal polarizations of A , λ_H and $\lambda_{H'}$ with $H, H' \in \text{SL}_g(\mathcal{O})$ positive-definite Hermitian matrices, there exists a path on each graph from the vertex $[\mathcal{A}' = (A, \lambda_{H'})]$ to the vertex $[\mathcal{A} = (A, \lambda_H)]$ of even length.*
- (c) *The enhanced isogeny graph $\tilde{gr}_g(\ell, p)$ is connected.*

Proof. Put $Gr = Gr_g(\ell, p)$ and $gr = gr_g(\ell, p)$.

(a, b): Let

$$[\mathcal{A} = (A, \lambda_H)], [\mathcal{A}' = (A, \lambda_{H'})] \in \text{Ver}(Gr) = \text{Ver}(gr)$$

with $H, H' \in \text{SL}_g(\mathcal{O})$ positive-definite Hermitian matrices. By Theorem 43, there exists $M \in \text{Mat}_{g \times g}(\mathcal{O})$ with $M^\dagger H M = \ell^{2n} H'$ for some positive integer n . Hence by Proposition 32, the isogeny $\psi \in \text{End}(A)$ given by M satisfies $\psi^*(\lambda_H) = \ell^{2n} \lambda_{H'}$. But then by Theorem 35 there exists a path of length $2n$ on both gr and Gr connecting the vertex $[\mathcal{A}']$ to the vertex $[\mathcal{A}]$.

(c): Since $gr_g(\ell, p)$ is connected and not bipartite, its bipartite double cover $\tilde{gr}_g(\ell, p)$ (see Theorem 40 (a)) is connected. □

8. THE ℓ -ADIC UNIFORMIZATION OF $gr_g(\ell, p)$ AND $\tilde{gr}_g(\ell, p)$

Through out this section X will be an arbitrary principally polarized, not necessarily supersingular, abelian variety.

It is well known that for $\ell \neq p$ the supersingular elliptic curves over $\overline{\mathbb{F}}_p$ are in bijective correspondence with the double cosets

$$\mathcal{O}_{\mathbb{H}_p}[1/\ell]^\times \backslash \text{GL}_2(\mathbb{Q}_\ell) / \mathbb{Q}_\ell^\times \text{GL}_2(\mathbb{Z}_\ell),$$

with $\text{GL}_2(\mathbb{Q}_\ell) / \mathbb{Q}_\ell^\times \text{GL}_2(\mathbb{Z}_\ell)$ corresponding to the vertices of the standard tree for $\text{GL}_2(\mathbb{Q}_\ell)$. We will generalize this form to higher dimension, starting with the definition below.

Definition 45. *Let R be a commutative ring and M an R -algebra with an anti-involution $x \mapsto x^\dagger$. We define the unitary group $U(M) = \{x \in M \mid x^\dagger x = 1\}$. We define the general unitary group $\text{GU}_R(M) = \{x \in M \mid x^\dagger x \in R^\times\}$.*

Remark 46. Let $\mathcal{B}_{2g}$ be the Bruhat-Tits building for GSp_{2g} over $\mathbb{Q}_\ell$. The special 1-skeleton $\mathcal{S}_{2g}$ of $\mathcal{B}_{2g}$ has vertices the special vertices of $\mathcal{B}_{2g}$ which are the vertices of type 0 or g – see, for example, [She07, Sect. 2,3], and edges the edges of the 1-skeleton of $\mathcal{B}_{2g}$ with both ends special vertices.

Note that the next theorem is true for all principally polarized abelian varieties whether superspecial or not. Specifically say that for a principally polarized abelian variety the anti-involution $x \mapsto x^\dagger$ on $\text{End}(A)$ is Rosati. On E^g we take the Rosati (anti-)involution

corresponding to the product polarization. Hence on $\text{Mat}_{g \times g}(\mathcal{O}_E)$ we take $M \mapsto M^\dagger := \overline{M}^t$, with $m \mapsto \overline{m}$ the main involution of the definite quaternion algebra $\text{End}(E) \otimes \mathbb{Q} := \text{End}^0(E)$.

Theorems similar to Theorem 47 can be found in the theory of Shimura varieties – see [Kot92], for example.

Theorem 47. *Let X be a principally polarized abelian variety of dimension g over an algebraically closed field k of characteristic $\text{char}(k)$ with $\ell \neq \text{char}(k)$ a prime. The principally polarized abelian varieties isogenous to X by ℓ -power isogenies (we require that the principal polarization be the one induced by the isogeny) are in bijective correspondence with the double cosets*

$$\text{GU}(\text{End}(X)[1/\ell]) \backslash \text{GSp}_{2g}(\mathbb{Q}_\ell) / \mathbb{Q}_\ell^\times \text{GSp}_{2g}(\mathbb{Z}_\ell), \quad (52)$$

with $\text{GSp}_{2g}(\mathbb{Q}_\ell) / \mathbb{Q}_\ell^\times \text{GSp}_{2g}(\mathbb{Z}_\ell)$ the vertices $\text{Ver}(\mathcal{S}_{2g})$ as in Remark 46. Furthermore, $(\ell)^g$ -isogenies correspond to the edges $\text{Ed}(\mathcal{S}_{2g})$. Specifically, two elements of

$$\text{GSp}_{2g}(\mathbb{Q}_\ell) / \mathbb{Q}_\ell^\times \text{GSp}_{2g}(\mathbb{Z}_\ell)$$

are adjacent if the corresponding homothety classes of unimodular symplectic lattices have representatives with one having index $(\ell)^g$ in the other. In particular, the principally polarized superspecial abelian varieties of dimension g are in bijective correspondence with

$$\text{GU}(\text{Mat}_{g \times g}(\mathcal{O}_E[1/\ell])) \backslash \text{GSp}_{2g}(\mathbb{Q}_\ell) / \mathbb{Q}_\ell^\times \text{GSp}_{2g}(\mathbb{Z}_\ell). \quad (53)$$

Proof. Let $T = \text{Ta}_\ell(X)$ be the Tate module of X , and let $V = \text{Ta}_\ell(X) \otimes \mathbb{Q}_\ell$, both equipped with the symplectic Weil pairing. Identify $\text{GSp}_{2g}(\mathbb{Q}_\ell) = \text{GSp}(V)$ and $\text{GSp}_{2g}(\mathbb{Z}_\ell) = \text{GSp}(T)$. Note that we have an exact sequence

$$0 \rightarrow T \rightarrow V \xrightarrow{\pi} X[\ell^\infty] \rightarrow 0.$$

Let $\phi : X \rightarrow X'$ be an ℓ -power isogeny to an abelian variety X' , principally polarized by the induced polarization. We will associate to the pair (ϕ, X') the homothety class of the $\mathbb{Z}_\ell$ -lattice $T' = \pi^{-1}(\ker \phi) \subset V$. Since the induced polarization on X' is principal, the symplectic pairing restricted to T' is a scalar multiple of a unimodular integral pairing. Conversely, if $[T']$ is a homothety class of full-rank $\mathbb{Z}_\ell$ -lattices in V such that symplectic pairing restricted to any representative is a scalar multiple of a unimodular integral pairing, pick a representative T' such that $T' \supset T$. Then $\pi(T')$ is the kernel of an ℓ -power isogeny whose image is principally polarized. Furthermore, picking a different representative corresponds to composing the ϕ with multiplication by a scalar power of ℓ .

Note that if $\psi : X' \rightarrow X''$ is an $(\ell)^g$ -isogeny, then $T'' = \pi^{-1}(\ker \psi \circ \phi)$ is an extension of T' of index $(\ell)^g$. Hence the corresponding vertices of the building are adjacent. Conversely, since both graphs have the same degree all special edges of the building come from $(\ell)^g$ -isogenies.

Now let Δ be the set of all homothety classes of full-rank $\mathbb{Z}_\ell$ -lattices in V such that the restriction of the symplectic pairing is a scalar multiple of a unimodular integral pairing. It is easy to see that $\Delta \cong \text{GSp}(V) / \mathbb{Q}_\ell^\times \text{GSp}(T)$ with $r\mathbb{Q}_\ell^\times \text{GSp}(T)$ corresponding to the class $[rT]$.

It suffices to show that $[rT]$ and $[sT]$ correspond to isomorphic principally polarized abelian varieties if and only if $[rT] = [\psi sT]$ for some $\psi \in \text{GU}(\text{End}(X)[1/\ell])$. After possibly scaling r , s , and ψ by powers of ℓ we may assume that $\psi \in \text{End}(X)$, $rT = \psi sT$, and $rT, sT \supset T$. Therefore $\pi(rT) = \psi(\pi(sT))$. Hence if $\ker \phi = \pi(rT)$ and $\ker \phi' = \pi(sT)$, then $\phi \circ \psi = \phi'$ and both have the same codomain.

Conversely, if ϕ and ϕ' have the same codomain, let $\psi = \widehat{\phi} \circ \phi'$. Note that $\psi \in \mathrm{GU}(\mathrm{End}(X)[1/\ell])$ since it preserves the polarization. Now $\phi \circ \psi = \deg(\phi)\phi'$. Now let $\pi(rT) = \ker \phi$ and $\pi(sT) = \ker(\deg(\phi)\phi')$. Then $rT = \psi sT$, and we are done with the main claim.

The final assertion with (53) now follows from Theorem 44. $\square$

We now apply Theorem 47 to derive the ℓ -adic uniformization of the isogeny graphs $gr_g(\ell, p)$ and $\widetilde{gr}_g(\ell, p)$.

8.1. The case $g = 1$: ℓ -adically uniformizing $gr_1(\ell, p)$ and $\widetilde{gr}_1(\ell, p)$. Let $\Delta = \Delta_\ell$ be the tree for $\mathrm{SL}_2(\mathbb{Q}_\ell)$. The rational definite quaternion algebra $\mathbb{H}_p$ with maximal order $\mathcal{O} = \mathcal{O}_{\mathbb{H}_p}$ is ramified at p and split at ℓ . Set

$$\Gamma_0 = \mathcal{O}[1/\ell]^\times \quad \text{and} \quad \Gamma_1 = \{\gamma \in \Gamma_0 \mid \mathrm{Nm}_{\mathbb{H}_p/\mathbb{Q}}(\gamma) = 1\}. \quad (54)$$

We have $\Gamma_0 = \mathcal{O}[1/\ell]^\times \hookrightarrow (\mathbb{H}_p \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)^\times = \mathrm{GL}_2(\mathbb{Q}_\ell)$ and likewise $\Gamma_1 \hookrightarrow \mathrm{GL}_2(\mathbb{Q}_\ell)$. Let $\bar{\Gamma}_i$ be the image of Γ_i in $\mathrm{PGL}_2(\mathbb{Q}_\ell)$ for $i = 0, 1$. The groups $\bar{\Gamma}_0, \bar{\Gamma}_1$ are discrete cocompact subgroups of $\mathrm{PGL}_2(\mathbb{Q}_\ell)$. The groups $\Gamma_i \subset \mathrm{GL}_2(\mathbb{Q}_\ell)$ act on Δ through their image $\bar{\Gamma}_i \subseteq \mathrm{PGL}_2(\mathbb{Q}_\ell)$, $i = 0, 1$. Hence the quotients $\mathbf{Gr}_1 := \Gamma_1 \backslash \Delta = \bar{\Gamma}_1 \backslash \Delta$ and $\mathbf{Gr}_0 := \Gamma_0 \backslash \Delta = \bar{\Gamma}_0 \backslash \Delta$ are finite graphs with weights. Kurihara [Kur79, p. 294] shows that the weighted adjacency matrix $\mathrm{Ad}_w(\mathbf{Gr}_0)$ is the Brandt matrix $B_1(\ell)$ for $\mathcal{O} \subseteq \mathbb{H}_p$; we know $\mathrm{Ad}_w(gr_1(\ell, p)) = B_1(\ell)$ by Theorem 39. In fact, to show $\mathrm{Ad}_w(\mathbf{Gr}_0) = B_1(\ell)$ Kurihara basically shows $\mathbf{Gr}_0 = br_1(\ell, p)$. In [Kur79, p. 296] it is shown that $\mathbf{Gr}_1$ (note that our $\bar{\Gamma}_1$ is Γ_+ in [Kur79]) is the bipartite double cover of $\mathbf{Gr}_0$. Hence we have

Theorem 48. (Kurihara)

- (a) $br_1(\ell, p) = \Gamma_0 \backslash \Delta_\ell = \bar{\Gamma}_0 \backslash \Delta_\ell$ as graphs with weights.
- (b) $\Gamma_1 \backslash \Delta_\ell = \bar{\Gamma}_1 \backslash \Delta_\ell$ is the bipartite double cover of $\Gamma_0 \backslash \Delta_\ell = \bar{\Gamma}_0 \backslash \Delta_\ell$.

Theorem 49. (a) $gr_1(\ell, p) = \Gamma_0 \backslash \Delta_\ell = \bar{\Gamma}_0 \backslash \Delta_\ell$ as graphs with weights.

- (b) $\widetilde{gr}_1(\ell, p) = \Gamma_1 \backslash \Delta_\ell = \bar{\Gamma}_1 \backslash \Delta_\ell$ as graphs with weights.

Proof. (a): Combine Theorem 39(a) with Theorem 48(a).

- (b): Combine Theorem 48(b) with Theorem 40(a). $\square$

Remark 50. (a) The big isogeny graph $Gr_1(\ell, p)$ is *not* ℓ -adically uniformized by Δ_ℓ since $Gr_1(\ell, p)$ is not a graph with opposites.

- (b) Theorem 49(a) obviously implies that the isogeny graph $gr_1(\ell, p)$ is connected. Note that in fact Kurihara [Kur79, p. 291] invokes strong approximation in the course of proving $br_1(\ell, p) = \bar{\Gamma}_0 \backslash \Delta_\ell$.

8.2. The isogeny graphs $gr_1(\ell, p)$, $\widetilde{gr}_1(\ell, p)$ and Shimura curves. Theorem 49 in turn will show that our isogeny graphs $gr_1(\ell, p)$ and $\widetilde{gr}_1(\ell, p)$ arise from the bad reduction of Shimura curves, which we now explain. Let B be the indefinite rational quaternion division algebra with $\mathrm{Disc} B = \ell p$. Let $V_B/\mathbb{Q}$ be the Shimura curve parametrizing principally polarized abelian surfaces with QM (quaternionic multiplication) by a maximal order $\mathcal{M} \subseteq B$. There is then a model $M_B/\mathbb{Z}$ of $V_B/\mathbb{Q}$ constructed as a coarse moduli scheme by Drinfeld [Dri76]; see also [JL85]. Let $\mathcal{L}/\mathbb{Z}_\ell$ be the ℓ -adic upper half-plane. The dual graph $G(\mathcal{L}/\mathbb{Z}_\ell)$ of its special fiber is canonically $\Delta = \Delta_\ell$. For $\bar{\Gamma} \subseteq \mathrm{PGL}_2(\mathbb{Q}_\ell)$ a discrete, cocompact subgroup, the quotient $\bar{\Gamma} \backslash \mathcal{L}$ is the formal completion of a scheme $\mathcal{L}_{\bar{\Gamma}}/\mathbb{Z}_\ell$ along its closed fiber. The

dual graph of its special fiber $G(\mathcal{L}_{\bar{\Gamma}}/\mathbb{Z}_\ell) \simeq (\bar{\Gamma} \setminus \Delta)^*$ as graphs with lengths in the notation of Definition 21(d), see [Kur79, Prop. 3.2].

For the formulation below, see [JL85, Theorems 4.3', 4.4].

Theorem 51. (Čerednik, Drinfeld) *Let w_ℓ be the Atkin-Lehner involution at ℓ of M_B . Let $\bar{\Gamma}_0$ be the image of $\Gamma_0 \subseteq \mathrm{GL}_2(\mathbb{Q}_\ell)$ in $\mathrm{PGL}_2(\mathbb{Q}_\ell)$ and similarly for $\bar{\Gamma}_1$. Let $\mathfrak{D}$ be the ring of integers in the unramified quadratic extension of $\mathbb{Q}_\ell$.*

(a) *The scheme $M_B \times \mathbb{Z}_\ell$ is the twist of $\mathcal{L}_{\bar{\Gamma}_1}/\mathbb{Z}_\ell$ given by the 1-cocycle*

$$\chi \in H^1(\mathrm{Gal}(\mathfrak{D}/\mathbb{Z}_\ell), \mathrm{Aut}(\mathcal{L}_{\bar{\Gamma}_1} \times_{\mathbb{Z}_\ell} \mathfrak{D}/\mathfrak{D})), \text{ where } \chi : \mathrm{Frob}_\ell \mapsto w_\ell : \\ M_B \times \mathbb{Z}_\ell = (\mathcal{L}_{\bar{\Gamma}_1})^\chi.$$

(b) $(M_B/w_\ell) \times \mathbb{Z}_\ell = \mathcal{L}_{\bar{\Gamma}_0}/\mathbb{Z}_\ell$.

The curve $M_B \times \mathbb{Z}_\ell/\mathbb{Z}_\ell$ is an *admissible curve* in the sense of [JL85, Defn. 3.1]. As such, the dual graph of its special fiber $G(M_B \times \mathbb{Z}_\ell/\mathbb{Z}_\ell)$ is a graph with lengths as in Definition 21(b) by [JL85, Defn. 3.2].

Corollary 52. (a) $G(M_B \times \mathbb{Z}_\ell/\mathbb{Z}_\ell) = \bar{\Gamma}_1 \setminus \Delta = \tilde{gr}_1(\ell, p)$ as graphs with lengths.

(b) $G((M_B/w_\ell) \times \mathbb{Z}_\ell/\mathbb{Z}_\ell) = (\bar{\Gamma}_0 \setminus \Delta)^* = gr_1(\ell, p)^*$ as graphs with lengths with $(\bar{\Gamma}_0 \setminus \Delta)^*$, $gr_1(\ell, p)^*$ as in Definition 21(d).

Proof. This follows from Theorem 51 by [JL85, Prop. 4.2], which in turn is extracted from [Kur79, §3]. □

8.3. The general case $g \geq 1$: ℓ -adically uniformizing $gr_g(\ell, p)$ and $\tilde{gr}_g(\ell, p)$. Recall $A = E^g$, $\mathcal{O} = \mathrm{End}(E) \subseteq \mathbb{H}_p$, and $\mathrm{End}(A) = \mathrm{Mat}_{g \times g}(\mathcal{O})$. Let $\mathcal{B}_{2g}$ be the Bruhat-Tits building for $\mathrm{Sp}_{2g}(\mathbb{Q}_\ell)$ and $\mathcal{S}_{2g}$ its special 1-skeleton as in Remark 46. Note that $\mathrm{GU}_g(\mathbb{H}_p \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)$ and $\mathrm{U}_g(\mathbb{H}_p \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)$ as in (9) act on $\mathcal{S}_{2g}$ with finite quotient.

Theorem 53. (a) $br_g(\ell, \mathcal{O}) = \mathrm{GU}_g(\mathcal{O}[1/\ell]) \backslash \mathcal{S}_{2g}$ as graphs with weights.

(b) $\mathrm{U}_g(\mathcal{O}[1/\ell]) \backslash \mathcal{S}_{2g}$ is the bipartite double cover of $\mathrm{GU}_g(\mathcal{O}[1/\ell]) \backslash \mathcal{S}_{2g}$.

Proof. (a) follows immediately from Theorem 47 since $\mathrm{GU}_g(\mathcal{O}[1/\ell]) \backslash \mathcal{S}_{2g}$ is the same as (53).

(b) follows from (1) since $\tilde{gr}_g$ is the bipartite double cover of gr_g and $\mathrm{PU}_g(\mathcal{O}[1/\ell])$ is the subgroup of $\mathrm{PGU}_g(\mathcal{O}[1/\ell])$ that preserves mod 2 distance. □

Theorem 54. (a) $gr_g(\ell, p) = \mathrm{GU}_g(\mathcal{O}[1/\ell]) \backslash \mathcal{S}_{2g}$ as graphs with weights.

(b) $\tilde{gr}_g(\ell, p) = \mathrm{U}_g(\mathcal{O}[1/\ell]) \backslash \mathcal{S}_{2g}$ as graphs with weights.

Proof. (a): Combine Theorem 39(a) with Theorem 53(a).

(b): Combine Theorem 53(b) with Theorem 40(a). □

Remark 55. (a) Theorem 54 once again immediately implies that the isogeny graphs $gr_g(\ell, p)$ and $\tilde{gr}_g(\ell, p)$ are connected. However, note that the proof of Theorem 54 uses Theorem 47, which in turn uses Theorem 44.

(b) In case $g = 1$ we have $\mathrm{Sp}_2(\mathbb{Q}_\ell) = \mathrm{SL}_2(\mathbb{Q}_\ell)$, $\mathcal{S}_2 = \Delta_\ell$, $\mathrm{U}_1(\mathcal{O}[1/\ell]) = \Gamma_1$, and $\mathrm{GU}_1(\mathcal{O}[1/\ell]) = \Gamma_0$. Hence for $g = 1$ we recover Theorem 49.

(c) The big isogeny graph $Gr_g(\ell, p)$ is *not* uniformized by $\mathcal{S}_{2g}$ as in the $g = 1$ case (Remark 50) since it is not a graph with opposites.

(d) There would be great interest in generalizing Theorem 51 and Corollary 52 to $g > 1$.

9. COMPUTATIONS: THE RAMANUJAN PROPERTY FOR $Gr_g(\ell, p)$ WITH $g > 1$

9.1. A non-Ramanujan example. To see that the isogeny graph $Gr_g(\ell, p)$ is in general non-Ramanujan, consider the case $\ell = 2$, $g = 2$, and $p = 11$. Here there are two supersingular elliptic curves: $E_1 : y^2 = x^3 + 1$ and $E_2 : y^2 = x^3 + x$. There are also two superspecial genus-2 curves: $C_1 : y^2 = x^6 + 1$ and $C_2 : y^2 = x^6 + 3x^3 + 1$. Hence there are five principally polarized superspecial abelian surfaces: $E_1 \times E_1$, $E_2 \times E_2$, $E_1 \times E_2$, and the jacobians $J(C_1)$, $J(C_2)$, the products taken with the product polarization and the jacobians with their canonical polarizations. A Richelot isogeny of a principally polarized abelian surface (A, λ) is quotienting by a maximal isotropic subgroup of $A[2]$. We computed the Richelot isogenies for these principally polarized abelian surfaces using Magma [BCP97]. The adjacency matrix for $Gr_2(2, 11)$ is

$$\text{Ad}(Gr_2(2, 11)) = \begin{bmatrix} 3 & 9 & 0 & 3 & 0 \\ 4 & 3 & 4 & 4 & 0 \\ 0 & 3 & 6 & 0 & 6 \\ 1 & 3 & 0 & 3 & 8 \\ 0 & 0 & 3 & 4 & 8 \end{bmatrix};$$

the row-sums of this matrix are all $15 = N_2(2) = (1 + 2)(1 + 2^2)$. The eigenvalues of this matrix are 15 , $7 \pm \sqrt{3}$, and $-3 \pm \sqrt{3}$. The second largest of these is $7 + \sqrt{3} > 2\sqrt{14}$. Hence the graph is not Ramanujan.

9.2. A Ramanujan example. To see that the isogeny graph $Gr_g(\ell, p)$ can (rarely) be Ramanujan, consider the case $\ell = 2$, $g = 2$, and $p = 7$. In characteristic 7 there is one supersingular elliptic curve $E : y^2 = x^3 - x$ and one superspecial genus-2 curve $C : y^2 = x^5 + x$. There are two principally polarized superspecial abelian surfaces: $E \times E$ with the product polarization and the jacobian $J(C)$ of C with its canonical polarization. The adjacency matrix for $Gr_2(2, 7)$ is

$$\text{Ad}(Gr_2(2, 7)) = \begin{bmatrix} 11 & 4 \\ 6 & 9 \end{bmatrix}.$$

Again, the graph $Gr_2(2, 7)$ is 15-regular and we see that the row sums of $\text{Ad}(Gr_2(2, 7))$ are all 15. The eigenvalues of this matrix are 15 and 5. Since $5 < 2\sqrt{14}$, the graph $Gr_2(2, 7)$ is Ramanujan.

9.3. A range of computations. We computed $Gr_g(\ell, p)$ using Theorem 37 by calculating the Brandt matrix $B_g(\ell)$ for the maximal order $\mathcal{O} = \text{End}(E) \subseteq \mathbb{H}_p$. We were able to do this for all primes $p \leq p_{\max}$ and $(g, \ell, p_{\max})$ one of $(2, 2, 311)$, $(2, 3, 257)$, $(2, 5, 173)$, $(3, 2, 41)$, $(3, 3, 23)$. Hence in these ranges we could determine whether the big isogeny graph $Gr_g(\ell, p)$ is Ramanujan.

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

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

ACKNOWLEDGMENTS

The proof of Theorem 19(e) using Gelfand’s trick was worked out with Guy Henniart and Marie-France Vignéras. Nicholas Shepherd-Barron suggested using [vdGM, Chap. 11] to prove our Theorem 28. Ching-Li Chai’s comments greatly improved our paper. We also benefited from conversations and correspondence with Tomoyoshi Ibukiyama and Frans Oort. The referee’s careful reading and suggestions went beyond the call of duty. It is a pleasure to thank them all.

REFERENCES

- [And69] A. N. Andrianov, *Rationality theorems for Hecke series and Zeta functions of the groups GL_n and Sp_n over local fields*, Izv. Akad. Nauk SSSR Ser. Mat. **33** (1969), 466–505. MR0262168
- [ATY24] Yusuke Aikawa, Ryokichi Tanaka, and Takuya Yamauchi, *Isogeny graphs on superspecial abelian varieties: eigenvalues and connection to Bruhat-Tits buildings*, Canad. J. Math. **76** (2024), no. 6, 1891–1916. MR4824554
- [BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265.
- [BK66] Hel Braun and Max Koecher, *Jordan-Algebren*, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen mit besonderer Berücksichtigung der Anwendungsgebiete, Band 128, Springer-Verlag, Berlin-New York, 1966. MR0204470
- [CDS20] Wouter Castryck, Thomas Decru, and Benjamin Smith, *Hash functions from superspecial genus-2 curves using Richelot isogenies*, J. Math. Cryptol. **14** (2020), no. 1, 268–292. MR4134760
- [Cha95] Ching-Li Chai, *Every ordinary symplectic isogeny class in positive characteristic is dense in the moduli*, Invent. Math. **121** (1995), no. 3, 439–479. MR1353306
- [CO11] Ching-Li Chai and Frans Oort, *Monodromy and irreducibility of leaves*, Ann. of Math. (2) **173** (2011), no. 3, 1359–1396. MR2800716
- [CS20] Craig Costello and Benjamin Smith, *The supersingular isogeny problem in genus 2 and beyond*, Post-quantum cryptography, 2020, pp. 151–168. MR4139650
- [Dri76] V. G. Drinfeld, *Coverings of p -adic symmetric domains*, Funkcional. Anal. i Priložen. **10** (1976), no. 2, 29–40. MR0422290
- [Eic55] Martin Eichler, *Zur Zahlentheorie der Quaternionen-Algebren*, J. Reine Angew. Math. **195** (1955), 127–151 (1956).
- [Eke87] Torsten Ekedahl, *On supersingular curves and abelian varieties*, Math. Scand. **60** (1987), no. 2, 151–178. MR914332
- [Gro87] Benedict H. Gross, *Heights and the special values of L -series*, Number theory (Montreal, Que., 1985), 1987, pp. 115–187.
- [Gro99] Benedict H. Gross, *Algebraic modular forms*, Israel J. Math. **113** (1999), 61–93. MR1729443
- [Has80] Ki-ichiro Hashimoto, *On Brandt matrices associated with the positive definite quaternion Hermitian forms*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **27** (1980), no. 1, 227–245. MR573338
- [HI80] Ki-ichiro Hashimoto and Tomoyoshi Ibukiyama, *On class numbers of positive definite binary quaternion Hermitian forms*, J. Fac. Sci. Univ. Tokyo Sect. 1A Math. **27** (1980), no. 3.
- [IKO86] Tomoyoshi Ibukiyama, Toshiyuki Katsura, and Frans Oort, *Supersingular curves of genus two and class numbers*, Compositio Math. **57** (1986), no. 2, 127–152. MR827350
- [JL85] Bruce W. Jordan and Ron A. Livné, *Local Diophantine properties of Shimura curves*, Math. Ann. **270** (1985), no. 2, 235–248. MR771981
- [JZ] Bruce W. Jordan and Yevgeny Zaytman, *Isogeny complexes of superspecial abelian varieties*. arXiv:2205.07383.
- [Kne66] Martin Kneser, *Strong approximation*, Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965), 1966, pp. 187–196.
- [Kot92] Robert E. Kottwitz, *Points on some Shimura varieties over finite fields*, J. Amer. Math. Soc. **5** (1992), no. 2, 373–444. MR1124982

- [KT20] Toshiyuki Katsura and Katsuyuki Takashima, *Counting Richelot isogenies between superspecial abelian surfaces*, ANTS XIV—Proceedings of the Fourteenth Algorithmic Number Theory Symposium, 2020, pp. 283–300. MR4235119
- [Kur79] Akira Kurihara, *On some examples of equations defining Shimura curves and the Mumford uniformization*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **25** (1979), no. 3, 277–300. MR523989
- [Lan85] Serge Lang, $SL_2(\mathbf{R})$, Graduate Texts in Mathematics, vol. 105, Springer-Verlag, New York, 1985. Reprint of the 1975 edition.
- [Mes86] J.-F. Mestre, *La méthode des graphes. Exemples et applications*, Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata 1986), 1986, pp. 217–242.
- [MFK94] D. Mumford, J. Fogarty, and F. Kirwan, *Geometric invariant theory*, Third Edition, Ergebnisse der Mathematik und ihrer Grenzgebiete (2) [Results in Mathematics and Related Areas (2)], vol. 34, Springer-Verlag, Berlin, 1994. MR1304906
- [Mum08] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition.
- [Ogu79] Arthur Ogus, *Supersingular $K3$ crystals*, Journées de Géométrie Algébrique de Rennes (Rennes, 1978), Vol. II, 1979, pp. 3–86. MR563467
- [Oor01] Frans Oort, *A stratification of a moduli space of abelian varieties*, Moduli of abelian varieties (Texel Island, 1999), 2001, pp. 345–416. MR1827027
- [Oor74] F. Oort, *Which abelian surfaces are products of elliptic curves?*, Invent. Math. **214** (1974), 35–47.
- [Piz90] Arnold K. Pizer, *Ramanujan graphs and Hecke operators*, Bull. Amer. Math. Soc. (N.S.) **23** (1990), no. 1, 127–137. MR1027904
- [Piz98] Arnold K. Pizer, *Ramanujan graphs*, Computational perspectives on number theory (Chicago, IL, 1995), 1998, pp. 159–178. MR1486836
- [Ple65] Vera Pless, *The number of isotropic subspaces in a finite geometry*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat. (8) **39** (1965), 418–421. MR199785
- [PR94] Vladimir Platonov and Andrei Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press, Inc., Boston, MA, 1994. Translated from the 1991 Russian original by Rachel Brown.
- [Rib90] K. A. Ribet, *On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms*, Invent. Math. **100** (1990), no. 2, 431–476. MR1047143
- [Sat63] Ichirô Satake, *Theory of spherical functions on reductive algebraic groups over p -adic fields*, Inst. Hautes Études Sci. Publ. Math. **18** (1963), 5–69. MR195863
- [Ser03] Jean-Pierre Serre, *Trees*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2003. Translated from the French original by John Stillwell, Corrected 2nd printing of the 1980 English translation. MR1954121
- [She07] Thomas R. Shemanske, *The arithmetic and combinatorics of buildings for Sp_n* , Trans. Amer. Math. Soc. **359** (2007), no. 7, 3409–3423. MR2299461
- [Shi63] Goro Shimura, *Arithmetic of alternating forms and quaternion hermitian forms*, J. Math. Soc. Japan **15** (1963), 33–65.
- [Shi79] Tetsuji Shioda, *Supersingular $K3$ surfaces*, Algebraic geometry (Proc. Summer Meeting, Univ. Copenhagen, Copenhagen, 1978), 1979, pp. 564–591. MR555718
- [Shi94] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1.
- [vdGM] Gerard van der Geer and Ben Moonen, *Abelian varieties*. <http://page.mi.fu-berlin.de/elenalavanda/BMoonen.pdf>, accessed 8 January, 2021.
- [Vig80] Marie-France Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics, vol. 800, Springer, Berlin, 1980.
- [Yu06] Chia-Fu Yu, *The supersingular loci and mass formulas on Siegel modular varieties*, Doc. Math. **11** (2006), 449–468.

DEPARTMENT OF MATHEMATICS, BARUCH COLLEGE, THE CITY UNIVERSITY OF NEW YORK, ONE
BERNARD BARUCH WAY, NEW YORK, NY 10010-5526, USA

Email address: `bruce.jordan@baruch.cuny.edu`

NEWTON, MA 02465, USA

Email address: `gzaytman@alum.mit.edu`