Centre de Recherches Mathématiques
CRM Proceedings and Lecture Notes
Volume **47**, 2008

Families of Ramanujan Graphs and Quaternion Algebras

Denis X. Charles, Eyal Z. Goren, and Kristin E. Lauter

1. Introduction

Expander graphs are graphs in which the neighbors of any given "not too large" set of vertices X form a large set relative to the size of X — rumors tend to spread very fast. Among those, the Ramanujan graphs are extremal in their expansion properties. To be precise, the eigenvalues of the adjacency matrix have an extremal property that guarantees good expansion properties. Expanders, and hence Ramanujan graphs, have many applications, practical and theoretical, to computer science, coding theory, cryptography and network construction, besides numerous purely mathematical applications. Some applications are briefly indicated in the last section of this paper; for a thorough overview see [14, 38] and the references therein.

Quaternion algebras make an appearance in many constructions of Ramanujan graphs. The constructions of Lubotzky – Phillips – Sarnak [24, 25] and Pizer [31] have used definite quaternion algebras over $\mathbb{Q}$, Pizer's construction allowing a more general setting, while making the arithmetic of quaternion algebras more dominant. The construction by Jordan – Livné [18, 23] makes use of quaternion algebras over totally real fields, but in essence is built out of the LPS (for Lubotzky, Phillips, Sarnak) graphs. In each of these cases the Ramanujan property follows from the Ramanujan conjecture for a suitable space of automorphic representations. This much is true also for a related construction by Li [21]. In hindsight, given recent research into Ramanujan complexes (see, e.g., [4, 26]), the reason for the appearance of quaternion algebras is that they supply one with discrete co-compact subgroups of $\mathrm{PGL}_2(F)$, where F is a finite extension of $\mathbb{Q}_p$. The combinatorial properties of the graphs, or, more generally, complexes, constructed from the Bruhat – Tits buildings associated $\mathrm{PGL}_n(F)$, are intimately related to automorphic forms on the appropriate group.

The construction presented in this paper generalizes some of Pizer's work from definite quaternion algebras over $\mathbb{Q}$ to totally definite quaternion algebras over totally real fields. It is, in essence, a special case of the construction by Jordan – Livné (JL), though our main examples are different from theirs as our emphasis

2000 *Mathematics Subject Classification.* Primary 05C25, 05C50, 14K02; Secondary 05C12, 11G10.

This is the final form of the paper.

©2008 American Mathematical Society

is either on the case where the class number of the quaternion algebra is large, or on the case when the order is not a maximal order in the quaternion algebra. A particular feature of these graphs, which indeed was our initial motivation for their construction, is that for a chain of totally real fields $L_1 \subset L_2 \subset \cdots \subset L_n$ of strict class number one, and for distinct primes p and l, where p is unramified in all the fields L_i, one gets a chain (or "nested family") of Ramanujan graphs $G(L_1; p, l) \to G(L_2; p, l) \to \cdots \to G(L_n; p, l)$, where the arrows are morphisms of graphs in either the strict sense or in a modified sense that we define below. (We expect that the class number one assumption can be removed.) We can guarantee that the ratio of the size of the graph to the degree goes to infinity with n. We remark that this is a feature that can be obtained for LPS graphs (using the work of [18]) in great generality. See Section 5.3. At this point we are not able to decide if the maps are injective (perhaps under suitable additional hypotheses). We remark that having a nested family of Ramanujan graphs is appealing for certain applications where one desires to *augment* pre-existing graphs to construct larger graphs while retaining the Ramanujan property, and it raises many new questions we hope others will also find appealing, among them determining the situation for the family $G(L_1; p, l) \to G(L_2; p, l) \to \cdots \to G(L_n; p, l)$.

One of the main reasons for discussing such particular cases of the LPS or JL graphs is that, as in Pizer's work, the arithmetic of quaternion algebras is more prevalent. In addition, for such a totally real field L, the graph $G(L; p, l)$ is associated to a very interesting set of points on the Hilbert modular variety of L in characteristic p—the superspecial points. Thus, the connection between graphs and supersingular elliptic curves appearing in Pizer's work is generalized to a connection between graphs and superspecial abelian varieties with real multiplication. The Ramanujan property, appearing in an abstract representation theory language in the general construction, now takes the pleasant face of estimates for Fourier coefficients of theta series of quadratic forms valued in a totally real field L. To make these connections we make essential use of the thesis of Nicole [27]. We remark that this connection is appealing from the point of view of arithmetic geometry, but is not essential to the construction of the graphs. The whole construction can be done for any totally definite quaternion algebra B over a totally real field L, not necessarily of class number one, and very possibly for a larger family of orders than considered in this paper.

To our knowledge, families of "nested" Ramanujan graphs were not studied systematically before and many questions arise. For example, for any family of connected k-regular graphs (necessarily not nested) the second largest eigenvalue of the adjacency matrix is, by a theorem of Alon and Boppana, asymptomatically at least $2\sqrt{k-1} - \epsilon$ for any $\epsilon > 0$. The bound $2\sqrt{k-1}$ is called the *Ramanujan bound*. However, since for a particular graph the Ramanujan bound can be broken, it raises the question whether one can construct a nested family of Ramanujan graphs all breaking the Ramanujan bound, where the degree is always small relative to the size of the graph. (Without this proviso the answer is easily "yes," see Section 5.) Other constructions of Ramanujan graphs also lend themselves to creating nested families of graphs. Examples include the Paley graphs and the Terras graphs. We discuss those examples, and explain the relation between our construction and [18, 25] in Section 5.

There are other nice features of the constructions discussed in this paper. For one, it is a general feature of the JL graphs that they allow the construction of essentially different Ramanujan graphs of the same degree on the same vertex set. Indeed, for example, for a prime l we can can get $l+1$-regular graphs from any totally real field of class number one in which l splits completely. The number of vertices of such a graph is the class number of a specific quaternion algebra over L and, if p splits completely in L, is of the order of magnitude $(p-1)^{[L:\mathbb{Q}]}\zeta_L(-1)$. By varying L and p we expect graphs of the same number of vertices to appear many times, while there is no reason to expect all such graphs to even have the same spectrum.

On the other hand, one can also fix the field L and the prime p, and varying l one obtains different graphs on the same vertex set. In that case, one can ask how likely it is that two vertices which are close to each other in one of the graphs are also close in the other graph. In Section 7 we introduce a notion of independence of graphs in this setting, and argue why in many cases the Pizer graphs arising from a fixed p and different l should be independent.

Another interesting feature of the graphs we construct is that one can study the number of closed walks of length n in the graphs we construct as sums of class numbers. Since the characteristic polynomial of the adjacency matrix A is determined by the sequence $\mathrm{tr}(A^n), n=1,2,3,\ldots$, either through Newton's formula or through the identity $\exp(\sum_{n=1}^{\infty}\mathrm{tr}(A^n)t^n/n)=\det(1-tA)^{-1}$, we are getting in that way information on the spectrum of the adjacency matrix.

2. Quaternion algebras and superspecial points

2.1. Elliptic curves and the quaternion algebra $B_{p,\infty}$. Let p be a prime. This section contains no original material; it recalls the well-known connection between supersingular elliptic curves over $\overline{\mathbb{F}}_p$ and orders in the quaternion algebra $B_{p,\infty}$ — the rational quaternion algebra ramified precisely at p and ∞. Good references for this section are [13, 42]. It prepares the ground for a more general theory to follow. Explicit descriptions of $B_{p,\infty}$ and a maximal order in it can be found in [31, Section 4].

Let $E=E_1,\ldots,E_h$ be representatives for the isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$. We fix an identification $\mathrm{End}(E)\otimes\mathbb{Q}=B_{p,\infty}$ and let $\mathcal{O}_i=\mathrm{End}(E_i)$. Then, every order $\mathcal{O}_i$ is isomorphic to a maximal order of $B_{p,\infty}$ and each maximal order of $B_{p,\infty}$ is isomorphic to some $\mathcal{O}_i$. The class number of any maximal order of $B_{p,\infty}$ is h, where h is given by the following formula: $h=[p/12]+\epsilon(p)$, where $\epsilon(2),\epsilon(3)$ are equal to 1 and for $p\geq 5$, $\epsilon(p)=0,1,1,2$ if $p\equiv 1,5,7,11 \pmod{12}$, respectively. See [34, Chapter 5, Theorem 4.1]]. Moreover, fix representatives $I_1,\ldots,I_h$ for the right ideal classes of $\mathcal{O}=\mathcal{O}_1$ with $I_1=\mathcal{O}$. We can choose the ideals I_i in such a way so that $\mathrm{Hom}(E,E_i)\cong I_i$ as projective $\mathcal{O}$-modules. Furthermore, the two quadratic forms

$$\deg\colon \mathrm{Hom}(E,E_i)\to\mathbb{Z},\quad f\mapsto \deg(f)=f^t\circ f,$$

(the degree) and

$$\mathrm{Norm}_c\colon I_i\to\mathbb{Z},\quad f\mapsto\frac{\mathrm{Norm}(f)}{\mathrm{Norm}(I_i)},$$

(the calibrated norm) agree under that isomorphism. In fact, one may define E_i as $I_i\otimes_{\mathcal{O}}E$. We then have that $\mathcal{O}_i$ is the left order of I_i and $\mathrm{Hom}(E_i,E_j)=I_jI_i^{-1}$.

Let n be an integer. We define the *Brandt matrix* $\mathrm{B}(n)$, whose ijth entry $\mathrm{B}(n)_{ij}$ is the number of subgroup schemes H of order n of E_i with $E_i/H \cong E_j$. We note that $\mathrm{B}(n)$ has the following properties:

(1) The sum of every row of $\mathrm{B}(n)$ is equal to $\sigma'(n) := \sum_{d|n,(d,p)=1} d$.
(2) Let $w_i = \frac{1}{2}|\mathrm{Aut}(E_i)|$ then $w_j\,\mathrm{B}(n)_{ij} = w_i\,\mathrm{B}(n)_{ji}$.

Let l be a prime different from p. The matrix $\mathrm{B}(l)$ defines the adjacency matrix of a directed $l+1$ regular graph $G(\mathbb{Q}; p, l)$. Here and throughout the paper "graph" is taken in the loose sense: loops and multiple edges are allowed. If we want to emphasize that there are no loops or multiple edges we say "simple graph."

2.1.1. *Connectedness.* To prove that the graph is connected one can appeal to a theorem on definite quadratic forms in 4 variables. If such a form represents each integer locally at every completion of $\mathbb{Q}$ then it represents any large enough integer. Once the local conditions are verified, one can thus conclude that l^n is represented by the degree map on I_i for every i, provided $n \gg 0$, and so the graph is connected. Other proofs could be given using strong approximation (cf. § 5.3), or by decomposing the associated theta series, which is of weight 2 and level $\Gamma_0(p)$, into a nontrivial Eisenstein component, say $\sum b_n q^n$, and a cusp form and using a "Ramanujan type bound" to show that the coefficients $b_n, (n,p) = 1$, of the Eisenstein series component grow faster than those of the cusp form component. In particular, for n large enough, the coefficients, say c_n, of the associated theta series, which are the representation numbers for the norm forms for the ideal classes, will be nonzero at least of $(n,p) \neq 0, n \gg 0$. Elements of the ideal class of a given norm correspond to isogenies of that same degree and so one concludes that any two supersingular elliptic curves admit isogenies of degree l^n for any prime $l \neq p$ and any large enough n. The Ramanujan type bound referred to here says that if $f(q) = q + \sum_{n>1} a_n q^n$ is a normalized weight two eigenform of level $\Gamma_0(p)$, then $|a_l| \leq 2\sqrt{l}$. In fact, in the case at hand, the bound on the eigenvalues of Hecke operators, equivalently, on the Fourier coefficients of cusp forms, follows from the Eichler – Shimura isomorphism and Weil's own work on the Weil conjectures in the case of curves and abelian varieties.

Let $p \equiv 1 \pmod{12}$. Then each $w_i = 1$ and so the matrices $\mathrm{B}(n)$ are symmetric. In particular, we can pass to the $l+1$-regular undirected graph defined by $\mathrm{B}(l)$. In [31, Proposition 4.7] Pizer proves that this graph is Ramanujan. This *also* implies that the graph is connected. Pizer's work is more general than the case we consider, and in our case it can be simply explained: by classical work of Eichler, the spectrum of the Brandt matrix $\mathrm{B}(l)$ is equal to the spectrum of the Hecke operator T_l in its action on the weight two modular forms of level $\Gamma_0(p)$. The Ramanujan type bound for cusp forms thus gives that every eigenvalue λ of $\mathrm{B}(l)$, apart from $l+1$, satisfies $|\lambda| \leq 2\sqrt{l}$ and so that the graph is Ramanujan. Note, incidently, that this implies that the graphs are not bipartite, because a bipartite k-regular graph has $-k$ as an eigenvalue.

2.2. Abelian varieties with real multiplication and superspecial points. Let L be a totally real field of degree g over $\mathbb{Q}$ of strict class number 1. The moduli problem of classifying triples $(A, \iota\colon \mathcal{O}_L \to \mathrm{End}(A), \lambda)$, where A is a g-dimensional abelian variety, ι is a ring embedding (inducing a ring embedding $\mathcal{O}_L \to \mathrm{End}(A^t)$, where A^t is the dual abelian variety) and λ is an $\mathcal{O}_L$-equivariant

principal polarization, has a coarse moduli scheme $\mathscr{M} \to \mathrm{Spec}(\mathbb{Z})$ of relative dimension g. One has $\mathscr{M}(\mathbb{C}) \cong \mathrm{SL}_2(\mathcal{O}_L)\backslash\mathfrak{H}^g$, where $\mathfrak{H}$ is the upper half plane $\{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. We let $\mathscr{M}_p = \mathscr{M} \times_{\mathrm{Spec}(\mathbb{Z})} \mathrm{Spec}(\overline{\mathbb{F}}_p)$. The principal polarization λ on (A, ι) is determined uniquely by (A, ι) up to $\mathcal{O}_L$-automorphism. Indeed, the set of $\mathcal{O}_L$-linear symmetric homomorphisms $A \to A^t$ is a projective rank 1 $\mathcal{O}_L$-module and the polarizations are a positive cone in it. The strict class number being one, this module is isomorphic to $\mathcal{O}_L$ and the polarizations to $\mathcal{O}_L^+$. In particular, the principal polarizations are now given by $\mathcal{O}_L^{\times,+}$. Under this identification, the principally polarized abelian variety with real multiplication $(A, \iota, 1)$ is isomorphic to $(A, \iota, \epsilon^*1) = (A, \iota, \epsilon^2)$ for any $\epsilon \in \mathcal{O}_L^\times$. Strict class number one implies that any totally positive unit is a square of a unit thus proving our claim.

A *superspecial abelian variety* A of dimension g over an algebraically closed field of positive characteristic is equivalently:

(1) an abelian variety A isomorphic to a product of g supersingular elliptic curves;
(2) an abelian variety A isomorphic to E^g, where E is a supersingular elliptic curve;
(3) an abelian variety A such that the absolute Frobenius acts as zero on $H^1(A, \mathcal{O}_A)$.

The implications (2) $\Rightarrow$ (1) $\Rightarrow$ (3) are obvious but the full equivalence is far from obvious. The equivalence of (1) and (2) is a theorem of Deligne (see [33]) and the equivalence with (3) is a theorem of Oort [29]. If $g > 1$ then Deligne's theorem also says that $E^g \cong E'^g$ for any two supersingular elliptic curves over an algebraically closed field.

Definition 2.1. We call a superspecial principally polarized abelian variety with RM by L an L-superspecial variety.

2.2.1. Assume henceforth that L has strict class number one and fix a supersingular elliptic curve E over $\overline{\mathbb{F}}_p$ with endomorphism ring $\mathcal{O}$; we identify once and for all $B_{p,\infty}$ with $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q}$. A general reference for what follows is Nicole's thesis [27]. See also [28]. We assume that p is unramified in L.

A concrete example of an L-superspecial variety is given by $E \otimes_{\mathbb{Z}} \mathcal{O}_L$. Its dual is naturally $E^t \otimes D_{L/\mathbb{Q}}^{-1}$ but since $D_{L/\mathbb{Q}}^{-1}$ has a totally positive generator α, $E \otimes_{\mathbb{Z}} \mathcal{O}_L$ has a principal $\mathcal{O}_L$-linear polarization $\lambda \otimes \alpha$, where λ is the canonical principal polarization $\lambda : E \to E^t$. One can prove that $R := \mathrm{End}_{\mathcal{O}_L}(E \otimes \mathcal{O}_L)$ is equal to $\mathcal{O} \otimes_{\mathbb{Z}} \mathcal{O}_L$. This is an order of discriminant $p\mathcal{O}_L$ in the quaternion algebra $B_{p,L} := B_{p,\infty} \otimes_{\mathbb{Q}} L$. Let $p = \mathfrak{p}_1 \ldots \mathfrak{p}_a$ be the decomposition of p into prime ideals in $\mathcal{O}_L$. Then $B_{p,L}$ is ramified precisely at the infinite places of L and at the primes $\mathfrak{p}_i$ such that $f(\mathfrak{p}_i/p) \equiv 1 \pmod 2$, where $f(\mathfrak{p}_i/p)$ is the residue degree $\dim_{\mathbb{F}_p}(\mathcal{O}_L/\mathfrak{p}_i)$.

Example 2.2. Let L be a real quadratic field. If p is inert then $B_{p,L}$ is ramified exactly at the infinite places and the order R is not maximal. On the other hand, if p is split then $B_{p,L}$ is ramified at the infinite places and at the two places above p and the order R is maximal.

The order R is not always maximal and so some care has to be taken with its ideal theory. Our main reference is Brzezinski [3]. The order R is an Eichler order of square-free level, though, and so is a hereditary order. An ideal of $B_{p,L}$ is by definition a finitely generated $\mathcal{O}_L$-module that contains a basis for $B_{p,L}$. An ideal I

is called a right R-ideal (or a right ideal of R) if $R = \{f \in B_{p,L} : If \subseteq I\}$. For such an ideal I, the properties projective, locally principal, invertible (in the sense that $II^{-1}, I^{-1}I$ are the trivial ideals, where $I^{-1} := \{f \in B_{p,L} : IfI \subseteq I\}$) or satisfying $[R : I] = \mathrm{Norm}(I)^2$, are all equivalent. For a hereditary order one has that every ideal is projective. See *loc. cit.* for all this.

Let $R = I_1, \ldots, I_h$ be representatives for the right ideal classes of R. The isomorphism classes of L-superspecial varieties are in bijection with the abelian varieties $A_i := I_i \otimes_R (E \otimes_{\mathbb{Z}} \mathcal{O}_L)$, $A = A_1$. One has $\mathrm{Hom}_{\mathcal{O}_L}(A, A_i) = I_i$ and, more generally, $\mathrm{Hom}_{\mathcal{O}_L}(A_i, A_j) = I_j I_i^{-1}$. The left order R_i of I_i is thus naturally isomorphic to $\mathrm{End}(A_i)$. Every order that is everywhere locally conjugate to R is isomorphic to one of the orders R_i and each order R_i is everywhere locally conjugate to R. One can characterize the orders that are everywhere locally conjugate to R simply as Eichler orders of level $p\mathcal{O}_L$. See [27, 28]. Following *loc. cit.* we call such orders *superspecial orders*.

For completeness, we indicate the key point that goes into proving some of these assertions. If $A/\mathbb{F}_{p^r}$ is L-superspecial, then over some $\mathbb{F}_{p^{r'}}$ the abelian variety A is isomorphic to E^g, where E is a supersingular elliptic curve over $\mathbb{F}_p$. In particular, the Weil number of E is $\sqrt{-p}$. It follows that the characteristic polynomial of Frobenius on E (acting on any Tate module and also as an endomorphism) is just $x^2 + p$. Thus, the relative Frobenius over $\mathbb{F}_{p^{2r'}}$ is nothing else than multiplication by $p^{r'}$ on "anything in sight". It is not hard to conclude then that after a finite field extension $T_l(A) \cong \mathcal{O}_L^{2g}$ as $\mathcal{O}_L$-modules where the Galois action is given as above (and is independent of A). The proof that the same holds for the Dieudonné modules appears in [12]. To determine the local structure of homomorphisms, one uses now a variant of Tate's theorem: for abelian varieties A, B with RM by $\mathcal{O}_L$, defined over a finite field $\mathbb{F}_q$, $\mathrm{Hom}_{\mathcal{O}_L}(A, B) \otimes \mathbb{Z}_l \cong \mathrm{Hom}_{\mathcal{O}_L \otimes \mathbb{Z}_l}(T_l(A), T_l(B))^{\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)}$ and the similar statement for Dieudonné modules (see [43]).

On the ideals I_i we have *calibrated norm* maps. Choose a totally positive generator α of $\mathrm{Norm}(I_i)$ and define

$$\mathrm{Norm}_c \colon I_i \to \mathcal{O}_L, \quad \mathrm{Norm}_c(f) = \mathrm{Norm}(f)/\alpha.$$

This is a positive definite quarternary $\mathcal{O}_L$-valued quadratic form, well defined up to a totally positive unit. On the other hand, choose principal $\mathcal{O}_L$-linear polarizations λ, λ_i on A, A_i and define

$$\deg_L \colon \mathrm{Hom}(A, A_i) \to \mathcal{O}_L, \quad \deg_L(f) = \lambda^{-1} f^t \lambda_i f.$$

This is also a positive definite quarternary $\mathcal{O}_L$-valued quadratic form, well defined up to a totally positive unit. As defined, $\deg(f)$ is clearly an element of R. It takes values in $\mathcal{O}_L$ because it is fixed by the Rosati involution. The projective R-modules I_i and $\mathrm{Hom}(A, A_i)$ are isomorphic. Moreover, the isomorphism can be chosen as to take Norm_c to $\deg_L$. Note that if $A_i = A$ there are canonical choices for both Norm_c and $\deg_L$ and they are equal. The above generalizes in the expected manner to $\mathrm{Hom}_{\mathcal{O}_L}(A_i, A_j)$ and $I_j I_i^{-1}$.

2.2.2. Let $H \subseteq A$ be a finite $\mathcal{O}_L$-invariant group scheme, where A is an abelian variety with RM, and assume that H is étale. Thus, over an algebraic closure we can write a composition series $0 \subsetneqq H_1 \subsetneqq H_2 \subsetneqq \cdots \subsetneqq H_n = H$ for H as an $\mathcal{O}_L$-module; the quotients H_i/H_{i-1} are $\mathcal{O}_L$-modules of the form $\mathcal{O}_L/\mathfrak{l}_i$, where $\mathfrak{l}_i$ is a prime ideal of $\mathcal{O}_L$ which is prime to p.

Definition 2.3. In the notation above, define the $\mathcal{O}_L$-degree of H, $\deg_L(H)$, to be $\mathfrak{l}_1\mathfrak{l}_2\cdots\mathfrak{l}_n$.

Lemma 2.4. *Let A be an L-superspecial variety, $R = \mathrm{End}(A)$ and $J \lhd R$ a left ideal whose norm is relatively prime to p. Let $A[J] = \bigcap_{f\in J}\mathrm{Ker}(f)$ then*

$$\deg_L(A[J]) = \mathrm{Norm}(J).$$

Proof. Let $\mathfrak{l}$ be a prime ideal of $\mathcal{O}_L$ not dividing p. We have the primary decomposition $A[J] = \bigoplus_{(\mathfrak{l},p)=1} A[J]_{\mathfrak{l}}$ and $\deg_L(A[J]) = \prod_{(\mathfrak{l},p)=1}\deg_L(A[J]_{\mathfrak{l}})$. On the other hand, the group $A[J]_{\mathfrak{l}}$ is isomorphic over an algebraic closure to $T_{\mathfrak{l}}(A)/\sum_{f\in J} fT_{\mathfrak{l}}(A) = T_{\mathfrak{l}}(A)/\sum_{f\in J_{\mathfrak{l}}} fT_{\mathfrak{l}}(A)$, where, using that $T_l(A)$ is a free $\mathcal{O}_L\otimes_{\mathbb{Z}}\mathbb{Z}_l$-module of rank 2 [32], we have decomposed the Tate module $T_l(A)$ as $\bigoplus_{\mathfrak{l}|l} T_{\mathfrak{l}}(A) \cong \oplus_{\mathfrak{l}|l}\mathcal{O}_{L\mathfrak{l}}^2$. Since all ideals are locally principal, we have $J_{\mathfrak{l}} = M_2(\mathcal{O}_{L\mathfrak{l}})j_{\mathfrak{l}}$ for a matrix $j_{\mathfrak{l}} \in M_2(\mathcal{O}_{L\mathfrak{l}})$, and $A[J]_{\mathfrak{l}}$ is isomorphic to $(\mathcal{O}_{L\mathfrak{l}})^2/j_{\mathfrak{l}}(\mathcal{O}_{L\mathfrak{l}})^2$. The product of the composition factors of this cokernel as an $\mathcal{O}_{L\mathfrak{l}}$-module is precisely $\det(j_{\mathfrak{l}})$, which is just the component at $\mathfrak{l}$ of $\mathrm{Norm}(J)$ (the local norm *is* the determinant). □

2.2.3. A very useful tool is the notion of kernel ideals studied in the context of general abelian varieties by Waterhouse in [42, Section 3.2]. Let A be a principally polarized superspecial abelian variety with RM over an algebraically closed field, $R = \mathrm{End}(A)$. For a subgroup scheme $H \subset A$ let $I(H) = \{f \in R : f(H) = 0\}$. One always has $J \subseteq I(A[J])$ and we call J a *kernel ideal* if $J = I(A[J])$. If A is a superspecial abelian variety with RM, p unramified in L, $R = \mathrm{End}(A)$ and H is étale then $I(H)$ is a left R-ideal; indeed it is easy to check that it is everywhere a locally principal ideal. It is proved in [27], following the proof of [42, Theorem 3.15], that every ideal of R is a kernel ideal. In particular, the map $J \mapsto A[J]$, taking ideals of norm prime-to-p contained in R to $\mathcal{O}_L$-subgroup schemes, is injective. More is true. This map is bijective when restricted to group schemes of order prime-to-p. To show that one needs only show that if $H_1 \subsetneqq H_2$ are two distinct $\mathcal{O}_L$-invariant group schemes of order prime-to-p then there is an endomorphism of A that vanishes on H_1 but not on H_2 (it then follows that $I(H_1) \neq I(H_2)$ and one concludes that we must have $A[I(H)] = H$ for every finite $\mathcal{O}_L$-subgroup scheme). We can thus consider only the case where both H_i are $\mathfrak{l}$-primary for some prime ideal $\mathfrak{l} \lhd \mathcal{O}_L$, $(\mathfrak{l}, p) = 1$. We have then that $R\otimes_{\mathcal{O}_L}\mathcal{O}_{L\mathfrak{l}} \cong \mathrm{End}_{\mathcal{O}_{L\mathfrak{l}}}(T_{\mathfrak{l}}(A)) \cong M_2(\mathcal{O}_{L\mathfrak{l}})$. Using the correspondence between $\mathfrak{l}$-primary finite groups schemes $H \subset A$ and lattices $\Lambda \supset T_{\mathfrak{l}}(A) \cong \mathcal{O}_{L_{\mathfrak{l}}}^2$, $H \mapsto \Lambda(H) = \pi_H^*(T_{\mathfrak{l}}(A/H))$, we see that it is enough to prove that if $\Lambda_2 \supsetneqq \Lambda_1 \supsetneqq \mathcal{O}_{L_{\mathfrak{l}}}^2$ then there is a matrix $\gamma \in M_2(\mathcal{O}_{L_{\mathfrak{l}}})$ such that $\gamma(\Lambda_1) = \mathcal{O}_{L_{\mathfrak{l}}}^2$. This is of course immediate using, say, elementary divisors. One then approximates γ well enough $\mathfrak{l}$-adically, using the isomorphism $R\otimes_{\mathcal{O}_L}\mathcal{O}_{L_{\mathfrak{l}}} \cong \mathrm{End}_{\mathcal{O}_{L_{\mathfrak{l}}}} T_{\mathfrak{l}}(A) = M_2(\mathcal{O}_{L_{\mathfrak{l}}})$.

2.3. The situation at p. The subtle point in defining the analog at p is that we want the quotient A/H to have a principal $\mathcal{O}_L$-polarization and be superspecial. An abelian variety A/k with RM and principal polarization satisfies the Rapoport condition: the tangent space to A at the origin is a free $\mathcal{O}_L\otimes_{\mathbb{Z}}k$-module of rank 1. In our case, since the class number of L is one, every abelian variety satisfying the Rapoport condition has a principal $\mathcal{O}_L$-linear polarization.

If H is étale then A/H satisfies the Rapoport condition, because $A \to A/H$ induces an $\mathcal{O}_L$-equivariant isomorphism on tangent spaces at the origin. Thus A/H will also have a principal $\mathcal{O}_L$-polarization and be superspecial; in general, one can

give examples of $\mathcal{O}_L$-invariant subgroup schemes $H \subset A[p]$ such that A/H does not satisfy the Rapoport condition and so will not have a principal $\mathcal{O}_L$-polarization. Therefore, the situation is more subtle when H is not étale.

Consider the following diagram

$$\begin{array}{ccc} A & \xrightarrow{f^*\mu} & A^t \\ \downarrow{\scriptstyle f} & & \uparrow{\scriptstyle f^t} \\ A/H & \xrightarrow{\mu} & (A/H)^t \end{array}$$

where $f\colon A \to A/H$ is the canonical projection. We are seeking a principal $\mathcal{O}_L$-polarization μ such that $f^*\mu := f^t \circ \mu \circ f$ has kernel in which H is maximal isotropic with respect to the Mumford pairing induced by $f^*\mu$. Let λ be a principal $\mathcal{O}_L$-polarization of A then any $\mathcal{O}_L$-polarization, in particular $f^*\mu$, is of the form $a\lambda$, where $a \in \mathcal{O}_L$ is a totally positive element. The kernel is just $A[a]$, which fits into an exact sequence of $\mathcal{O}_L$ group schemes $1 \to H \to A[a] \to H^t \to 1$. There is an additional condition: we want A/H to be superspecial.

Since our wish is to maintain the correspondence between ideals and subgroup schemes, we first examine "the situation at p" for superspecial orders. Let $\mathfrak{p} \mid p$ be a prime of $\mathcal{O}_L$. There are two cases:

(1) *The quaternion algebra $B_{p,L}$ is ramified at $\mathfrak{p}$.* In this case the completion at $\mathfrak{p}$ of $B_{p,L}$ is the unique quaternion algebra over $L_{\mathfrak{p}}$. If R is a superspecial order then R is a maximal order at $\mathfrak{p}$ and its completion at $\mathfrak{p}$ is uniquely determined. One can give a model for $R_{\mathfrak{p}}$. Let Q be an unramified extension of degree two of $L_{\mathfrak{p}}$, V its valuation ring and σ the nontrivial automorphism of Q/L. Let π be a uniformizer of $\mathcal{O}_{L_{\mathfrak{p}}}$. Then $B_{p,L} \otimes_L L_{\mathfrak{p}} \cong \left\{ \left(\begin{smallmatrix} a & b \\ -\pi b^\sigma & a^\sigma \end{smallmatrix}\right) : a, b \in Q \right\}$ and $R_{\mathfrak{p}} = \left\{ \left(\begin{smallmatrix} a & b \\ -\pi b^\sigma & a^\sigma \end{smallmatrix}\right) : a, b \in V \right\}$ with the trace and norm given by the trace and determinant of matrices. It has a unique maximal ideal, given by the matrices $\left\{ \left(\begin{smallmatrix} \pi a & b \\ -\pi b^\sigma & \pi a^\sigma \end{smallmatrix}\right) : a, b \in V \right\} = R_{\mathfrak{p}} \left(\begin{smallmatrix} \pi & 1 \\ -\pi & \pi \end{smallmatrix}\right)$, which has norm equal to $\mathfrak{p}\mathcal{O}_{L_{\mathfrak{p}}}$. In fact, all ideals are two-sided and every ideal is a power of the maximal ideal [40, [Chapter II, §1]]. We thus conclude that there is a unique ideal $J \lhd R$ such that $\mathrm{Norm}(J) = \mathfrak{p}$. Clearly $A[J] \subset A[p]$; we claim that $A[J] = (\mathrm{Ker}(\mathrm{Fr}\colon A \to A^{(p)}))_{\mathfrak{p}}$. Indeed, the uniqueness of the principally polarized superspecial crystal with RM [12] allows us to assume that the action of $B_{p,L} \otimes_{\mathbb{Q}} \mathbb{Q}_p$ on $H^1_{\mathrm{crys}}(A/W(\overline{\mathbb{F}}_p))$ is induced from the action of $B_{p,\infty}$ on a supersingular elliptic curve E. Thus, in essence we are working with the abelian variety $E \otimes \mathcal{O}_L$ and our assertion follows from the case of elliptic curves, where the uniqueness of a subgroup scheme of order p makes the claim straightforward.

In this case it is clear that the only subgroups H should have as component at $\mathfrak{p}$ are of the form, $\mathrm{Ker}(\mathrm{Fr}^n\colon A \to A^{(p^n)})_{\mathfrak{p}}$ for some n.

We can take $\pi \in \mathcal{O}_L$ such that $(\pi) = \mathfrak{p}$. Then we take $a = \pi^n$. It is a direct verification that $H \subset A[a]$ is totally isotropic with respect to the pairing defined by the polarization $a\lambda$. Moreover the $\mathfrak{p}$-primary part of the tangent space $T_{A/H,0}$ of A/H at the origin is naturally isomorphic to the $\mathfrak{p}$-primary part of $T_{A^{(p^n)},0}$ as an $\mathcal{O}_L$-module and so is a locally free $\mathcal{O}_{L_{\mathfrak{p}}} \otimes \overline{\mathbb{F}}_p$-module of rank 1, while the $\mathfrak{q}$-primary part of $T_{A/H,0}$ for every other prime $\mathfrak{q} \mid p$ of $\mathcal{O}_L$ is naturally isomorphic to the $\mathfrak{q}$-primary part of $T_{A,0}$. Those isomorphisms commute with the action of Fr and Ver and so A/H is also superspecial.

(2) *The quaternion algebra $B_{p,L}$ is split at $\mathfrak{p}$.* In this case the completion at $\mathfrak{p}$ of $B_{p,L}$ is isomorphic to $M_2(L_{\mathfrak{p}})$. If R is a superspecial order then R is an Eichler

order of level $p\mathcal{O}_L$ and under a suitable isomorphism its completion $R_\mathfrak{p}$ at $\mathfrak{p}$ is $\left\{\left(\begin{smallmatrix} a & b \\ \pi c & d\end{smallmatrix}\right) : a,b,c,d \in O_{L_\mathfrak{p}}\right\}$, where π is a uniformizer of $O_{L_\mathfrak{p}}$. The Jacobson radical $J(R_\mathfrak{p})$ is of finite index in $R_\mathfrak{p}$ and one thus concludes that it contains the matrices $\left(\begin{smallmatrix}\pi & 0\\ 0 & 0\end{smallmatrix}\right), \left(\begin{smallmatrix}0 & 0\\ 0 & \pi\end{smallmatrix}\right)$ and the nilpotent elements $\left(\begin{smallmatrix}0 & 1\\ 0 & 0\end{smallmatrix}\right), \left(\begin{smallmatrix}0 & 0\\ \pi & 0\end{smallmatrix}\right)$ and so

$$J(R_\mathfrak{p}) = \left\{\begin{pmatrix}\pi a & b\\ \pi c & \pi d\end{pmatrix} : a,b,c,d \in \mathcal{O}_{L_\mathfrak{p}}\right\}.$$

Since $R_\mathfrak{p}$ is an Eichler order it has Eichler symbol 1 at $\mathfrak{p}$ which means that $R_\mathfrak{p}/J(R_\mathfrak{p})$ is isomorphic to $\mathcal{O}_L/\mathfrak{p} \oplus \mathcal{O}_L/\mathfrak{p}$ and indeed this isomorphism is visibly induced from $\left(\begin{smallmatrix} a & b \\ \pi c & d\end{smallmatrix}\right) \mapsto (a,d) \mod \pi$. Thus, $R_\mathfrak{p}$ has two maximal left lattices that are

$$J_1 = \left\{\begin{pmatrix} a & b\\ \pi c & \pi d\end{pmatrix} : a,b,c,d \in \mathcal{O}_{L_\mathfrak{p}}\right\}, \quad J_2 = \left\{\begin{pmatrix}\pi a & b\\ \pi c & d\end{pmatrix} : a,b,c,d \in \mathcal{O}_{L_\mathfrak{p}}\right\}.$$

Those lattices are *not* $R_\mathfrak{p}$-ideals; J_1 is an ideal for the order $\left\{\left(\begin{smallmatrix} a & \pi^{-1}b \\ \pi c & d\end{smallmatrix}\right) : a,b,c,d \in \mathcal{O}_{L_\mathfrak{p}}\right\}$ and J_2 is an ideal for $M_2(\mathcal{O}_{L_\mathfrak{p}})$, and indeed one can verify that they are not locally principal for the order $R_\mathfrak{p}$. However, $J(R_\mathfrak{p})$ also has norm $\mathfrak{p}$ and is locally principal, equal to $R_\mathfrak{p}\left(\begin{smallmatrix}\pi & 1\\ \pi & \pi\end{smallmatrix}\right)$. We find again that there is a unique R-ideal J of norm $\mathfrak{p}$, whose kernel, as before, is equal to $\mathrm{Ker}(\mathrm{Fr})_\mathfrak{p}$. It should be noted that there are other principal ideals of $R_\mathfrak{p}$ of norm $\mathfrak{p}$. Indeed, any matrix M with $(\det(M)) = \mathfrak{p}$ provides such an ideal $R_\mathfrak{p}M$ and this constitutes all such examples. The ideal $J(R)$ can be characterized in two different ways: (i) It is the collection of matrices M such that $M^2 \equiv 0 \pmod{\pi}$; (ii) If $J(\mathfrak{O}_p)$ is the maximal ideal of a maximal order $\mathcal{O}$ of $B_{p,\infty}$ then, choosing an isomorphism $\mathcal{O}_p \otimes_{\mathbb{Z}_p} \mathcal{O}_{L_\mathfrak{p}} \cong R_\mathfrak{p}$, we have $J(R_\mathfrak{p}) = J(\mathcal{O}) \otimes_\mathbb{Z} \mathcal{O}_{L_\mathfrak{p}}$. To see that, note that $J(\mathcal{O}) \otimes_\mathbb{Z} \mathcal{O}_{L_\mathfrak{p}}$ is an ideal of $R_\mathfrak{p}$ containing $\pi R_\mathfrak{p} = pR_\mathfrak{p}$ and the quotient $R_\mathfrak{p}/J(\mathcal{O}) \otimes_\mathbb{Z} \mathcal{O}_{L_\mathfrak{p}}$ is isomorphic to $\mathcal{O}/J(\mathcal{O}) \otimes \mathcal{O}_{L_\mathfrak{p}} \cong \mathbb{F}_{p^2} \otimes \mathcal{O}_{L_\mathfrak{p}} \cong (\mathcal{O}_L/\mathfrak{p})^2$. Here we have used that p is unramified in $\mathcal{O}_L$ and that $B_{p,L}$ splits at $\mathfrak{p}$ if and only if $2 \mid f(\mathfrak{p}/p)$.

Let E be a supersingular elliptic curve with $\mathrm{End}(E) = \mathcal{O}$. The isomorphism $\mathcal{O}_p \otimes_{\mathbb{Z}_p} \mathcal{O}_{L_\mathfrak{p}} \cong R_\mathfrak{p}$ can be chosen so that the action of $R_\mathfrak{p}$ on $H^1_{\mathrm{crys}}(A/W(\overline{\mathbb{F}}_p))$ is the action of $\mathcal{O}_p \otimes_{\mathbb{Z}_p} \mathcal{O}_{L_\mathfrak{p}}$ on $H^1_{\mathrm{crys}}(E/W(\overline{\mathbb{F}}_p)) \otimes_{\mathbb{Z}_p} \mathcal{O}_{L_\mathfrak{p}}$, by the uniqueness of the superspecial crystal with RM. This shows that $J(R_\mathfrak{p})$ kills the $\mathfrak{p}$-part of the kernel of Frobenius. In the same way as in the first case one concludes that A/H is superspecial and satisfies the Rapoport condition.

We summarize our discussion.

Definition 2.5. Call an $\mathcal{O}_L$-invariant subgroup scheme *admissible* if for every $\mathfrak{p} \mid p$ the $\mathfrak{p}$-primary component of H is equal to the $\mathfrak{p}$-primary component of $\mathrm{Ker}(\mathrm{Fr}^{(n)}\colon A \to A^{(p^n)})$ for some $n = n(\mathfrak{p}) \geq 0$. Call a left ideal I *admissible* if for every prime $\mathfrak{p} \mid p$ the local component $I_\mathfrak{p}$ is a power of the Jacobson ideal.

Writing $p = \mathfrak{p}_1 \cdots \mathfrak{p}_a$, the p-primary part of admissible subgroups is in bijection with vectors $(b_1, \ldots, b_a)$ with $b_i \in \mathbb{Z}_{\geq 0}$. Given an admissible subgroup H, we write $H = H' \oplus H''$, where H' is the prime-to-p part of H and H'' is classified by a vector $(b_1, \ldots, b_a)$. We then let $\deg_L(H) = \deg_L(H') \cdot \prod_{i=1}^a \mathfrak{p}_i^{b_i}$.

Proposition 2.6. *Let A be a superspecial abelian variety with RM by L and having a principal $\mathcal{O}_L$-polarization. The admissible subgroups H correspond bijectively to admissible locally principal ideals $I \lhd R$, by $J \mapsto A[J]$, $H \mapsto I(H)$ and* $\deg_L(H) = \mathrm{Norm}\big(I(H)\big)$.

Example 2.7. Let L be a real quadratic field. Let A be a superspecial abelian surface with RM by L. Let p be inert in L, then there is a unique admissible $\mathcal{O}_L$-invariant group scheme in $A[p]$; it is equal to the kernel of $\mathrm{Fr}\colon A \to A^{(p)}$.

If, on the other hand, $p = \mathfrak{p}_1\mathfrak{p}_2$ is split in L, then there are precisely two admissible $\mathcal{O}_L$-invariant subgroup schemes of order p in A. These are the $\mathfrak{p}_i$-primary subgroups of the kernel of Frobenius.

3. Hecke operators, Brandt matrices and superspecial graphs

We keep our assumption that L is a totally real field of degree g of strict class number 1. The prime p is unramified in L and decomposes as $p = \mathfrak{p}_1 \cdots \mathfrak{p}_a$.

3.1. Brandt matrices. Let R be a superspecial order in $B_{p,L} = B_{p,\infty} \otimes_{\mathbb{Q}} L$ and let h be its class number. Let A be a superspecial abelian variety with an identification $\mathrm{End}(A) \cong R$. Index the right ideal classes of R as before by $R = I_1, \ldots, I_h$. We denote equivalence in the class group by $\sim$. Let R_i be the left order of I_i and let $A_i = I_i \otimes_R A$ be the corresponding superspecial abelian variety.

Definition 3.1. Let $\mathfrak{n}$ be an ideal of $\mathcal{O}_L$. We define the Brandt matrix $\mathrm{B}(\mathfrak{n})$ to be the $h \times h$ matrix whose ijth entry is the number of admissible integral left ideals $J \lhd R_i$ such that $\mathrm{Norm}(J) = \mathfrak{n}$ and $J \sim I_i I_j^{-1}$.

Proposition 3.2. *The Brandt matrices* $\mathrm{B}(\mathfrak{n})$ *have the following properties*:

1. *The entry* $\mathrm{B}(\mathfrak{n})_{ij}$ *is equal to the number of admissible* $\mathcal{O}_L$*-invariant subgroup schemes* H *of* A_i *with* $\deg_L(H) = \mathfrak{n}$ *and* $A_i/H \cong A_j$.
2. *We have* $\sum_j \mathrm{B}(\mathfrak{n})_{ij} = \sigma'(\mathfrak{n})$, *where* $\sigma'(\mathfrak{n}) = \sum_{\mathfrak{d}|\mathfrak{n},(\mathfrak{d},p)=1} \mathrm{Norm}_{L/\mathbb{Q}}\,\mathfrak{d}$
3. *Let* $w_i = |R_i^\times/\mathcal{O}_L^\times|$. *Then* w_i *is finite and* $w_j\,\mathrm{B}(\mathfrak{n})_{ij} = w_i\,\mathrm{B}(\mathfrak{n})_{ji}$.
4. *The matrices* $\mathrm{B}(\mathfrak{n})$ *commute. If* $(\mathfrak{n},\mathfrak{m}) = 1$ *then* $\mathrm{B}(\mathfrak{m})\,\mathrm{B}(\mathfrak{n}) = \mathrm{B}(\mathfrak{m}\mathfrak{n})$.
5. *For a prime ideal* $\mathfrak{p}$ *above* p *we have* $\mathrm{B}(\mathfrak{p})^n = \mathrm{B}(\mathfrak{p}^n)$. *The matrix* $\mathrm{B}(\mathfrak{p})$ *is a permutation matrix of order* 2.
6. *For a prime ideal* $\mathfrak{l}$ *not above* p *we have*

$$\mathrm{B}(\mathfrak{l})\,\mathrm{B}(\mathfrak{l}^n) = \mathrm{B}(\mathfrak{l}^{n+1}) + \mathrm{Norm}\,\mathfrak{l} \cdot \mathrm{B}(\mathfrak{l}^{n-2}).$$

Proof. By symmetry it is enough to consider the case of $i = 1$, and so $R = R_1$. Every such right ideal $J \lhd R$ defines a subgroup scheme $A[J]$, giving a bijection between admissible ideals of norm $\mathfrak{n}$ and admissible subgroup schemes H such that $\deg_L(H) = \mathfrak{n}$. The abelian variety $A/A[J]$ is isomorphic to the abelian variety $\mathrm{Hom}_R(J, A) \cong J^{-1} \otimes A$, which is isomorphic to $I_j \otimes A = A_j$ if J is in the class of I_j^{-1} [42, Corollary A.4]. Since we have a bijection between admissible ideals and admissible group schemes, we conclude the first statement.

The number of admissible $\mathcal{O}_L$-invariant group schemes of degree $\mathfrak{n}$ is a multiplicative function in $\mathfrak{n}$ and so is σ'. We may therefore assume that $\mathfrak{n} = \mathfrak{l}^k$ is a power of a prime ideal. The case of $\mathfrak{l} \mid p$ is trivial and we assume thus that $\mathfrak{l} \nmid p$. We now argue by induction on k. Since the number of $\mathcal{O}_L$-group schemes of $\deg_L = \mathfrak{l}$ is the number of lines in the $\mathbb{F}_\mathfrak{l} := \mathcal{O}_L/\mathfrak{l}$-vector space $A[\mathfrak{l}] \cong \mathbb{F}_\mathfrak{l}^2$, which is equal to $\sharp\mathbb{P}^1(\mathbb{F}_\mathfrak{l}) = \mathrm{Norm}(\mathfrak{l}) + 1$, we see that the cases $k = 0, 1$ hold. We have $\sigma'(\mathfrak{l}^k) - \sigma'(\mathfrak{l}^{k-2}) = \mathrm{Norm}\,\mathfrak{l}^k + \mathrm{Norm}\,\mathfrak{l}^{k-1} = l^{kf(\mathfrak{l})} + l^{(k-1)f(\mathfrak{l})}$. On the other hand, $\sum_j(\mathrm{B}(\mathfrak{l}^k)_{ij} - \mathrm{B}(\mathfrak{l}^{k-2})_{ij})$ is exactly the number of $\mathcal{O}_L$-subgroup schemes H of A_i such that $\deg_L(H) = \mathfrak{l}^k$ and $H \not\supseteq A_i[\mathfrak{l}]$. Passing to $T_\mathfrak{l}(A)/(\mathfrak{l}^k)$, we see that this is the number of cyclic $\mathcal{O}_L$-modules of $(\mathcal{O}_L/\mathfrak{l}^k)^2$ isomorphic to $\mathcal{O}_L/\mathfrak{l}^k$. This number

is just the number of elements (a,b) of $(\mathcal{O}_L/\mathfrak{l}^k)^2$ such that at least one of a,b is not divisible by $\mathfrak{l}$, taken modulo $(\mathcal{O}_L/\mathfrak{l}^k)^\times$, a group of order $(l^{f(\mathfrak{l})}-1)l^{(k-1)f(\mathfrak{l})}$. On the other hand the number of such generators (a,b) is clearly $l^{2kf(\mathfrak{l})}-l^{2(k-1)f(\mathfrak{l})}$. We conclude that there are $\left(l^{2kf(\mathfrak{l})}-l^{2(k-1)f(\mathfrak{l})}\right)/\left((l^{f(\mathfrak{l})}-1)l^{(k-1)f(\mathfrak{l})}\right) = l^{kf(\mathfrak{l})}+l^{(k-1)f(\mathfrak{l})}$ such $\mathcal{O}_L$-modules and we are done.

To show finiteness of $R^\times/\mathcal{O}_L^\times$, let R^1 be the elements of norm 1 in R and consider the injective group homomorphism $R^\times/\mathcal{O}_L^\times \to R^1$ given by $z \mapsto z/\bar{z}$. The positive definiteness of the norm map implies that R^1 is finite. To get the symmetry property consider $\mathrm{Hom}(A_i,A_j)$ and $\mathrm{Hom}(A_j,A_i)$ and the $\deg_L$ map on both, viewed as taking values in $\mathcal{O}_L/\mathcal{O}_L^\times$. If $\phi \in \mathrm{Hom}(A_i,A_j)$ is of degree prime to p and $\deg(\phi)=\mathfrak{n}$ then $\phi^t \in \mathrm{Hom}(A_j^t,A_i^t)=\mathrm{Hom}(A_j,A_i)$ has the same degree. The map from $\mathrm{Hom}(A_i,A_j)$ to group schemes $\phi \mapsto \mathrm{Ker}(\phi)$ has fibers that are principal homogeneous spaces under $R_j^\times$ and the result follows.

If $(\mathfrak{m},\mathfrak{n})=1$ then the identity $\mathrm{B}(\mathfrak{m})\,\mathrm{B}(\mathfrak{n})=\mathrm{B}(\mathfrak{mn})$ is just the decomposition of $\mathcal{O}_L$-group schemes of $\deg_L$ equal $\mathfrak{mn}$ into their $\mathfrak{m}$-primary and $\mathfrak{n}$-primary components. This also implies that such matrices commute. The formula $\mathrm{B}(\mathfrak{p}^n)=\mathrm{B}(\mathfrak{p})^n$ is immediate from the definition. We have $\mathrm{B}(\mathfrak{p}^2)_{ii}=1$, because the subgroup $A[p]_\mathfrak{p}=\mathrm{Ker}(\pi)$, where $(\pi)=\mathfrak{p}$ and $A/\mathrm{Ker}(\pi)\cong A$. It follows that $\mathrm{B}(\mathfrak{p})^2=\mathrm{Id}$. The formula $\mathrm{B}(\mathfrak{l})\,\mathrm{B}(\mathfrak{l}^n)=\mathrm{B}(\mathfrak{l}^{n+1})+\mathrm{Norm}\,\mathfrak{l}\cdot\mathrm{B}(\mathfrak{l}^{n-2})$ is the usual dévissage argument, similar to the counting arguments we did above. Note that now the commutativity of all the matrices follows. □

3.1.1. *Symmetry.* Our next goal is to find conditions that guarantee the symmetry of the Brandt matrices. This will later allow us to pass from a directed graph to an undirected graph.

Proposition 3.3. *Let $L_1,L_2,\ldots,L_n$ be totally real fields. There is a positive density of rational primes p such that for every superspecial order R of B_{p,L_i} we have $R^\times=\mathcal{O}_L^\times$.*

Proof. Let L be a totally real field. Let R be a maximal order of $B_{p,L}$ and suppose that $R^\times \supsetneq \mathcal{O}_L^\times$. Let $\alpha \in R^\times-\mathcal{O}_L^\times$. Then α defines a CM field $L(\alpha)=L[x]/(x^2-(\alpha+\bar{\alpha})x+\alpha\bar{\alpha})$ with an embedding into $B_{p,L}$. Note that α is an algebraic integer.

Let us now consider CM fields $M \supset L$ and the group of units $\mathcal{O}_M^\times \supset \mathcal{O}_L^\times$. There is an exact sequence

$$1 \to \mathcal{O}_L^\times \to \mathcal{O}_M^\times \to W_M,$$

where W_M is the roots of unity in M. The map $\mathcal{O}_M^\times \to W_M$ is given by $\alpha \mapsto \alpha/\bar{\alpha}$. According to [41, Theorem 4.12], we have

$$[\mathcal{O}_M^\times : W_M\mathcal{O}_L^\times] = \begin{cases} 2 & \text{if } \mathcal{O}_M^\times \twoheadrightarrow W_M, \\ 1 & \text{otherwise.} \end{cases}$$

We need the following lemma:

Lemma 3.4. *There are finitely many such CM extensions M of L with $W_M=\{\pm 1\}$ and $[\mathcal{O}_M^\times:\mathcal{O}_L^\times]=2$. These extensions can be effectively enumerated.*

Proof of Lemma 3.4. If M is such an extension then there is a unit α in M such that $\alpha/\bar{\alpha}=-1$ and so $M=L(\alpha)$ and α has minimal polynomial over L given

by $x^2+\alpha\bar{\alpha}$. The discriminant of M is thus bounded by $\mathrm{Norm}\big(\mathrm{disc}(\alpha)\big)\,\mathrm{disc}(L/\mathbb{Q})^2 = 4^{[L:\mathbb{Q}]}\,\mathrm{disc}(L/\mathbb{Q})^2$. By Hermite – Minkowski (which is effective) there are only finitely many such fields M. □

We return to the proof of the proposition. Let us now consider all CM fields M containing L such that $\mathcal{O}_M^\times \supsetneq \mathcal{O}_L^\times$. If $W_M \neq \{\pm 1\}$ then $M = L\cdot\mathbb{Q}(W_M)$ and $\varphi(|W_M|)$ divides $2[L:\mathbb{Q}]$. This shows that there are only finitely many such fields M (that can be effectively enumerated). If $W_M = \{\pm 1\}$ then by Lemma 3.4 there are only finitely many fields M such that $[\mathcal{O}_M^\times : \mathcal{O}_L^\times] = 2$.

Now, there is a positive density of prime ideals p such that p splits completely in the finitely many CM fields M such that $[M{:}L_i] = 2$ for some $1 \leq i \leq n$ and $\mathcal{O}_M^\times \supsetneq \mathcal{O}_{L_i}^\times$. If A is an abelian variety with CM by an order of such a field M then A is ordinary. Indeed, by passing to an isogenous abelian variety we may assume that $\mathcal{O}_M \subseteq \mathrm{End}(A)$ and that A is obtained as a reduction from characteristic 0, hence that $H^1_{\mathrm{crys}}(A/W(\overline{\mathbb{F}}_p))$ is a free $\mathcal{O}_M \otimes_{\mathbb{Z}} W(\overline{\mathbb{F}}_p)$-module of rank 1. Let σ be the Frobenius homomorphism on $\overline{\mathbb{F}}_p$ and consider the corresponding decomposition of $H^1_{\mathrm{dR}}(A/\overline{\mathbb{F}}_p)$ as $\bigoplus H^1_{\mathrm{dR}}(A/\overline{\mathbb{F}}_p)^\chi$, where χ runs over all ring homomorphisms $\mathcal{O}_M \to \overline{\mathbb{F}}_p$ and $\mathcal{O}_M$ acts on $H^1_{\mathrm{dR}}(A/\overline{\mathbb{F}}_p)^\chi$ by χ. The absolute Frobenius Fr induces a σ-linear map on $H^1_{dR}(A/\overline{\mathbb{F}}_p)$ taking $H^1_{\mathrm{dR}}(A/\overline{\mathbb{F}}_p)^\chi$ to $H^1_{\mathrm{dR}}(A/\overline{\mathbb{F}}_p)^{\sigma\circ\chi}$. The information on $H^1_{\mathrm{crys}}(A/W(\overline{\mathbb{F}}_p))$ implies that each $H^1_{\mathrm{dR}}(A/\overline{\mathbb{F}}_p)^\chi$ is one dimensional. Since p is split completely we get in our case that $\sigma\circ\chi = \chi$ for every χ. One concludes that on a subset Φ of g homomorphisms χ (the "CM-type") the map Fr is the zero map and that it is an isomorphism on each χ-typical component for $\chi \notin \Phi$. Moreover, the same considerations applied to the Verschiebung map show that we have a corresponding decomposition of group schemes $A[p] = \bigoplus_\chi A[p]^\chi$, where each $A[p]^\chi$ is a group scheme of rank p. It follows that the group schemes $A[p]^\chi$ for $\chi \notin \Phi$ are étale and so that A is ordinary.

We conclude that for such primes, for every superspecial order R in B_{p,L_i} we have $R^\times = \mathcal{O}_L^\times$. □

Remark 3.5. If in Proposition 3.3 the list of fields consists only of the field $\mathbb{Q}$, then the fields arising in its proof are the cyclotomic field $\mathbb{Q}(i)$ and $\mathbb{Q}(\omega)$, and the primes guaranteed in the Proposition are just the primes p congruent to 1 modulo 12, which is the condition for p to split in both $\mathbb{Q}(i)$ and $\mathbb{Q}(\omega)$.

3.2. Superspecial graphs. Let $\mathfrak{l}$ be a prime ideal of L not dividing p. Let h be the class number of a superspecial order R in $B_{p,L}$. The Brandt matrix $\mathrm{B}(\mathfrak{l})$ defines a directed graph on h vertices indexed by ideal classes $I_1, \ldots, I_h$ of R. We denote this graph by $G(L; p, \mathfrak{l})$ and call it a *superspecial graph*. By our previous results it can be viewed as the graph of isogenies between L-superspecial abelian varieties in characteristic p (modulo a suitable equivalence relation) and that explains our choice of terminology.

Proposition 3.6. *The graph $G(L; p, \mathfrak{l})$ has the following properties*:
(1) *It is a directed graph which is regular of degree $l^{f(\mathfrak{l}/l)} + 1$.*
(2) *For fixed g, the number of vertices h is approximately of the order*

$$2^{1-g} p^g \cdot |\zeta_L(-1)|.$$

More precisely, let

$$H = 2^{1-g} \cdot |\zeta_L(-1)| \cdot \prod_{\substack{\mathfrak{p}|p \\ f(\mathfrak{p}) \text{ odd}}} (\mathrm{Norm}(\mathfrak{p}) - 1) \prod_{\substack{\mathfrak{p}|p \\ f(\mathfrak{p}) \text{ even}}} (\mathrm{Norm}(\mathfrak{p}) + 1).$$

Then

$$H \leq h \leq C(g)H,$$

where

$$C(g) = \begin{cases} 2^{g+3}g^2 & g \geq 3 \\ 240 & g = 2 \\ 48 & g = 1. \end{cases}$$

(*In fact, for* $g = 1$ *we have* $h = [p/12] + \epsilon_p$ *where* ϵ_p, *where* $\epsilon_2 = \epsilon_3 = 1$ *and for* $p \geq 5$ *we have* $\epsilon_p = 0, 1, 1, 2$ *if* $p \equiv 1, 5, 7, 11 \pmod{12}$.)

(3) *The number of edges from* I_i *to* I_j *is the number of integral ideals* J *of* $\mathcal{O}_i$ *such that* $\mathrm{Norm}(J) = l$ *and* $J \sim I_i I_j^{-1}$.

(4) *There is a positive density of primes* p *such that the Brandt matrices* $\mathrm{B}(\mathfrak{n})$ (*relative to* p *and* L) *are symmetric for every* $\mathfrak{n}$.

Proof. This follows immediately from Propositions 3.2, 3.3, except for the estimate for the class number, which we proceed to explain. The order R is an Eichler order of discriminant p, which we write as $D \cdot N$, where D is the discriminant of $B_{p,L}$ (so $D = \prod_{\{i: f(\mathfrak{p}_i/p) \text{ is odd}\}} \mathfrak{p}_i$). Using [40, Chapter V, Corollary 2.3], we find the following mass formula:

$$\sum_{i=1}^{h} \frac{1}{[\mathcal{O}_i^* : \mathcal{O}_L^*]} = 2^{1-g} \cdot |\zeta_L(-1)| \cdot \prod_{\mathfrak{p}|D} (\mathrm{Norm}(\mathfrak{p}) - 1) \prod_{\mathfrak{p}|N} (\mathrm{Norm}(\mathfrak{p}) + 1).$$

The right-hand side is of the order $2^{1-g} p^g \cdot |\zeta_L(-1)|$. To analyze the left hand side we let $\mu(R)$ denote the torsion subgroup of $R^\times$. If $u \in \mu(R)$ then, viewed as an element of the field $L(u)$, u is a root of unity. One has an exact sequence

$$1 \to \mu(R) \to R^\times \xrightarrow{\mathrm{Norm}} \mathcal{O}_L^\times,$$

which induces an inclusion $R^\times/\mathcal{O}_L^\times \mu(R) \subseteq \mathcal{O}_L^\times/\mathcal{O}_L^{\times,2}$. Thus, $|R^\times/\mathcal{O}_L^\times| \leq 2^{g-1}|\mu(R)|$. By the discussion in Section 3.1, any element of $\mu(R)$ is a root of unity of order r with $\phi(r) \mid 2g$. Since $\phi(r) \geq \sqrt{r}/2$, this implies that r is less than $8g^2$ (it is easy to improve on that for any given g). Now, since the quaternion algebra is ramified at infinity, $\mu(R)/\pm 1 \subseteq \mathbb{H}_{\mathbb{R}}/\pm 1 \cong \mathrm{SO}_3(\mathbb{R})$. If the image is dihedral of order $2n$ or cyclic of order n then $\mu(R)$ will contain an element of order $2n$ and so in this case $|\mu(R)| \leq 4n \leq 16g^2$. Else, the image is isomorphic to A_4, S_4 or A_5 and so of order at most 60 and $|\mu(R)| \leq 120$. One can now deduce the upper bound for $g \geq 3$.

The case $g = 1$ is classical and the formula is in [34, Section V.4.1]. However, in the spirit of the argument above, we get the bound 48 for the size of $\mu(R)$, though the correct bound is 24, using that every root of unity must have order $1, 2, 3, 4$ or 6 in this case, thus ruling out the A_5 case. For $g = 2$, roots of unity can have order r with $\phi(r) \mid 4$ implying $r = 1, 2, 3, 4, 5, 6, 8, 10$. Our methods give only the bound $|\mu(R)| \leq 120$. □

3.3. Hecke operators for $B_{p,L}$. The Ramanujan conjecture is often phrased and proven in the language of automorphic representations. To use this literature we connect the Hecke operator at $\mathfrak{l}$ defined in the language of Brandt matrices as $\mathrm{B}(\mathfrak{l})$ with a Hecke operator at $\mathfrak{l}$ defined in adelic language.

Let $\mathfrak{l}$ be a prime of L. We define another $h \times h$ matrix $C(\mathfrak{l})$ by the following data. Fix a superspecial order R. Let $\mathscr{B}$ be the algebraic group over $\mathcal{O}_L$ such that for every $\mathcal{O}_L$-algebra S we have $\mathscr{B}(S) = (R \otimes_{\mathcal{O}_L} S)^\times$. Thus, for example, $\mathscr{B}(\mathcal{O}_L) = R^\times$ and $\mathscr{B}(L) = B_{p,L}^\times$. The right ideal classes for R are in natural correspondence with $\mathscr{B}(L)\backslash\mathscr{B}(\mathbb{A}_{L,f})/\mathscr{B}(\widehat{\mathcal{O}_L})$, where $\mathbb{A}_{L,f}$ is the ring of finite adèles of L and $\widehat{\mathcal{O}_L}$ is its maximal open-compact subring, the profinite completion of $\mathcal{O}_L$.

We may therefore view the complex valued functions on the superspecial points as functions on the double cosets space $\mathscr{B}(L)\backslash\mathscr{B}(\mathbb{A}_{L,f})/\mathscr{B}(\widehat{\mathcal{O}_L})$. Let $\mathfrak{l} = (\pi_\mathfrak{l})$, $a_\mathfrak{l}$ the adèle of $\mathscr{B}(\mathbb{A}_{L,f})$ whose components are 1 at every place different from $\mathfrak{l}$ and $\left(\begin{smallmatrix} \pi_\mathfrak{l} & \\ & 1 \end{smallmatrix}\right)$ at $\mathfrak{l}$. Consider the double coset $Ua_\mathfrak{l}U = \coprod x_i U$, where $U = \mathscr{B}(\widehat{\mathcal{O}_L})$. The Hecke operator $T_\mathfrak{l}$ is now defined as the averaging operator

$$f \mapsto T_\mathfrak{l}(f), \quad T_\mathfrak{l}(f)(x) = \sum_i f(xx_i).$$

Lemma 3.7. *The operator $T_\mathfrak{l}$ with respect to the basis consisting of δ functions is equal to the Brandt matrix* $\mathrm{B}(\mathfrak{l})$.

Proof. We choose representatives $x_1, \ldots, x_h$ for $\mathscr{B}(L)\backslash\mathscr{B}(\mathbb{A}_{L,f})/\mathscr{B}(\widehat{\mathcal{O}_L})$ corresponding to the right ideal classes $I_1, \ldots, I_h$. The component at a place $\mathfrak{q}$ of I_i is $(x_i)_\mathfrak{q} R_\mathfrak{q}$. Identifying a function f with the column vector ${}^t(f(x_1), \ldots, f(x_h))$, the operator defined by $Ua_\mathfrak{l}U$ is given by the matrix $C(\mathfrak{l})$ whose ijth entry is the number of x_n such that the ideal associated to $x_i x_n$ is in the same ideal class as x_j.

The elementary divisors theorem implies that the decomposition $Ua_\mathfrak{l}U = \coprod x_i U$ can be done so that the representatives x_i are the image of the $l^{f(\mathfrak{l})} + 1$ matrices in $\mathrm{GL}_2(L_\mathfrak{l})$ given by $\left(\begin{smallmatrix} 1 & \\ & \pi_\mathfrak{l} \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} \pi_\mathfrak{l} & i \\ & 1 \end{smallmatrix}\right)$, where i runs over a set of representatives for $\mathcal{O}_L/\mathfrak{l}$. Note that this gives us the set of all left ideals $J \lhd R$ of norm $\mathfrak{l}$. Let us denote the ideal corresponding to J_i by x_i. Since all superspecial orders are locally conjugate, this also produces such a set for any superspecial order. We may therefore concern ourselves just with the order R, i.e., just with the point x corresponding to the trivial ideal class R. The effect of passing from x to xx_i is passing to the ideal class of J_i. The number of times we get the ideal class I_j is the number of ideals J_i such that $J_i \sim I_j$, which is exactly the $1i$ entry in the Brandt matrix $\mathrm{B}(\mathfrak{l})$. □

4. Properties of superspecial graphs

In this section we investigate the properties of the graphs $G(L; p, \mathfrak{l})$ we have constructed. In particular, we prove that they are Ramanujan graphs and that they are "nested" in a suitable sense. In proving the Ramanujan property we use what has become a common technique: we deduce it from the Ramanujan conjecture for a suitable class of automorphic representations.

4.1. Connectivity.

Theorem 4.1. *The graph $G(L; p, \mathfrak{l})$ is connected.*[1]

[1]This also follows from the Ramanujan property in a straight-forward manner; one just looks at the expansion of the set of vertices of a connected component of minimal size.

PROOF. We fix a maximal order and describe the vertices of the graph as the right ideal classes $I_1, \ldots, I_h$ for this order. The problem translates into showing that the quadratic form Norm_c on $I_j I_i^{-1}$ represents λ^n for some $n \gg 0$, where λ is a totally positive generator of $\mathfrak{l}$. To see why, we find it convenient to think geometrically. Using Propositions 2.6, 3.2, we conclude that to show that for every i, j there is a path from I_i to I_j in the graph it is enough to show that the entry $\mathrm{B}(\mathfrak{l}^n)_{ij}$ is not zero. That is, it is enough to show that for every i, j there is an isogeny between the abelian varieties corresponding to I_i, I_j, whose kernel H satisfies $\deg_L(H) = \mathfrak{l}^n$. Such an isogeny corresponds to an element of $I_j I_i^{-1}$ with Norm_c a totally positive generator of $\mathfrak{l}^n$.

One possible proof is to consider the associated theta series, writing it as a sum of Eisenstein series and cusp forms to deduce that eventually all its coefficients are positive integers. Another proof can be obtained using the strong approximation theorem. See Section 5.3. We choose to appeal to a theorem of quadratic modular forms in 4 variables over $\mathcal{O}_L$. The theorem states that if such a quadratic form locally represents every element of $\mathcal{O}_{L\mathfrak{q}}$ for every prime ideal $\mathfrak{q}$ of $\mathcal{O}_L$ then it represents every totally positive element of $\mathcal{O}_L$ that is large enough.

We now verify the local conditions (cf. [11]) — that there are no local obstructions. The ideal $I_i I_j^{-1}$ is locally principal everywhere and in fact an isomorphism with the trivial local ideal can be chosen such that the function Norm_c becomes the norm form on $R_{\mathfrak{q}}$. All superspecial orders being locally conjugate, we may moreover assume that $R = \mathcal{O} \otimes \mathcal{O}_L$, where $\mathcal{O}$ is a maximal order in $B_{p,\infty}$. If $\mathfrak{q}$ doesn't divide p then $R_{\mathfrak{q}} \cong M_2(\mathcal{O}_{L\mathfrak{q}})$ with the norm being the determinant and we are done. If $\mathfrak{q}$ divides p then either we are dealing with an Eichler order of conductor $\mathfrak{q}$ in $M_2(\mathcal{O}_{L\mathfrak{q}})$, or with the maximal order of the unique division quaternion algebra over $\mathcal{O}_{L\mathfrak{q}}$. In the first case, the order is conjugate to $\left\{ \left(\begin{smallmatrix} a & b \\ \pi c & d \end{smallmatrix}\right) : a, b, c, d \in \mathcal{O}_{L\mathfrak{q}} \right\}$, where π is a uniformizer of $\mathcal{O}_{L_{\mathfrak{q}}}$. The norm form is just the determinant and clearly there are no local obstructions. In the second case, we can represent $\mathcal{O}_{\mathfrak{q}}$ as the ring $\left\{ \left(\begin{smallmatrix} a & b \\ -qb^\sigma & a^\sigma \end{smallmatrix}\right) : a, b \in W(\mathbb{F}_{q^2}) \right\}$, where q is the rational prime below $\mathfrak{q}$ and σ is the Frobenius automorphism. Note that being in this case implies that $f(\mathfrak{q}/q)$ is odd and so $W(\mathbb{F}_{q^2}) \otimes \mathcal{O}_{L\mathfrak{q}} \cong W(\mathbb{F}_{q^{2f}})$, where $f = f(\mathfrak{q}/q)$, and $\mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q) = \mathrm{Gal}(\mathbb{F}_{q^{2f}}/\mathbb{F}_{q^f}) = \{1, \sigma\}$. We conclude that we need to deal with the order $\left\{ \left(\begin{smallmatrix} a & b \\ -qb^\sigma & a^\sigma \end{smallmatrix}\right) : a, b \in W(\mathbb{F}_{q^{2f}}) \right\}$. Again, the norm form is just the determinant and we need to show that one can write $\lambda \in W(\mathbb{F}_{q^f})^\times$ as $aa^\sigma - qbb^\sigma$. In fact, one can take $b = 0$ by local class field theory. We see that there are no local obstructions. □

4.2. The Ramanujan property. We assume now that the suitable conditions as in Proposition 3.6(4) hold so that in particular the Brandt matrix $\mathrm{B}(\mathfrak{l})$ is symmetric for every $\mathfrak{l}$ and the units of every superspecial order are just $\mathcal{O}_L^\times$. The superspecial graphs $G(L; p, \mathfrak{l})$ (associated to a totally real field L of strict class number one, a rational prime p unramified in L and a prime $\mathfrak{l}$ of L) are then well-defined.

Theorem 4.2. *The graphs $G(L; p, \mathfrak{l})$ are (connected) Ramanujan graphs of degree $\sharp\mathbb{P}^1(\mathcal{O}_L/\mathfrak{l})$. Let l be a rational prime and let $\mathfrak{l}_1, \ldots, \mathfrak{l}_a$ be prime ideals dividing l in $\mathcal{O}_L$. Let $G(L; p, \mathfrak{l}_1, \ldots, \mathfrak{l}_a)$ be the graph whose adjacency matrix is $\mathrm{B}(\mathfrak{l}_1) + \mathrm{B}(\mathfrak{l}_2) + \cdots + \mathrm{B}(\mathfrak{l}_a)$ then $G(L; p, l)$ is a (connected) graph of degree $d = \sum_{i=1}^a (l^{f(\mathfrak{l}_i)} + 1)$ whose eigenvalues are d and the rest are bounded in absolute value by $2\sum_{i=1}^a \sqrt{l^{f(\mathfrak{l}_i)}}$.*

PROOF. There are two ways to argue. The first approach uses the Jacquet – Langlands correspondence to connect the Brandt matrices with Hecke operators on a Hilbert modular group. The second approach, which is historically a precursor of the first, uses theta series to do the same. Eventually, the Ramanujan property follows from the Ramanujan property for a suitable space of Hilbert modular forms and is due, in the case we need, to Livné [23].

FIRST PROOF. Let R be a maximal order of $B_{p,L}$. Consider the space S_R of complex functions on the double coset space $\mathscr{B}(L)\backslash\mathscr{B}(\mathbb{A}_{L,f})/\mathscr{B}(\widehat{\mathcal{O}_L})$ in the notation of Section 3.3, endowed with the action of the prime-to-p Brandt matrices. The Brandt matrices act either via the identification of the double coset space with the L-superspecial abelian varieties in characteristic p, or, equivalently, through the identification of the Brandt matrix $\mathrm{B}(\mathfrak{l})$ with the adelic Hecke operator $T_{\mathfrak{l}}$ defined by the double coset $Ua_{\mathfrak{l}}U$ (*loc. cit.*).

The argument now is as in [16–18]; see also [7, 8, 35]. Consider the subspace of S_R consisting of functions f such that, for $x \in B(L \otimes_{\mathbb{Q}} \mathbb{A}_f)$, $f(x)$ depends only on $\mathrm{Norm}(x) \in \mathbb{A}_{L,f}^{\times}/(\mathcal{O}_L \otimes \widehat{\mathbb{Z}_f})^{\times}$. Since $\mathrm{Norm}\colon B_{p,L}^{\times} \to L^{\times,+}$ is surjective and $\mathbb{A}_{L,f}^{\times} = L^{\times,+}(\mathcal{O}_L \otimes \widehat{\mathbb{Z}_f})^{\times}$ (due to strict class number 1) we conclude that such a function f is constant. On the other hand, consider the space S_L of Hilbert modular newforms of level $\Gamma_0(p)$ on $\mathrm{PSL}_2(L)$ of weight 2. The Jacquet – Langlands correspondence (see [10, 15]) gives an isomorphism $S_R/\mathbb{C} \to S_L$, which is Hecke-equivariant. In particular, the eigenvalues of $\mathrm{B}(\mathfrak{l})$, besides the eigenvector $(1, \ldots, 1)$ are precisely those of the Hecke operator $T_{\mathfrak{l}}$. By the Ramanujan conjecture for such Hilbert modular forms (see [23]), we conclude that the graph defined by $\mathrm{B}(\mathfrak{l})$ is Ramanujan.

SECOND PROOF. The second proof makes use of Eichler's result on theta series and Hecke operators [9]. L.c. assumes that the order is maximal, however the results carry through with the obvious modifications (the level of the theta series changes of course, however as long as one avoids the Hecke operators at primes dividing p everything goes through). The Brandt matrices appearing in l.c. §7 (25)-(26) agree with the Brandt matrices as defined in this paper. The theta functions of l.c. §9 (for the constant function 1 as a spherical polynomial) are now holomorphic weight 2 Hilbert modular forms of level $\Gamma_0(p)$ (we note that since the strict class number is 1 we also have that the groups $\mathrm{SL}_2(\mathcal{O}_L)$ and $\mathrm{SL}(\mathcal{O}_L \oplus \mathfrak{d}^{-1}) = \left\{ \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) : \alpha, \delta \in \mathcal{O}_L, \beta \in \mathfrak{d}^{-1}, \gamma \in \mathfrak{d} \right\}$ are conjugate in $\mathrm{SL}_2(L)$). Theorem 7 of l.c. implies that the spectrum of $\mathrm{B}(\mathfrak{l})$ in its action on the theta series thus constructed is that of $V_2(\mathfrak{l}^{-1})T_2(\mathfrak{l})$ in the notation of that reference. Here $T_2(\mathfrak{l})$ is the Hecke operator $T_2(\mathfrak{l}, \mathfrak{I}/\mathfrak{I}\mathfrak{l}^{-1})$ defined there in (14) and $V_2(\mathfrak{l}^{-1})$ is $V_2(\mathfrak{l}, \mathfrak{I}/\mathfrak{I}\mathfrak{l}^{-2})$ of (17), which by l.c., Proposition 3, is trivial in the case of strict class number one. It remains to verify that the Hecke operators used in l.c. have the correct normalization (see, e.g., [39, Section VI.1]) leading to an Euler product associated to a normalized eigenform, and that is a simple matter of comparing definitions. □

4.3. "Cleaner" Ramanujan graphs. Following Pizer, for a given field L, we shall explain here how to get simple undirected graphs $G(L; p, l)$ by posing conditions on the prime p. In Proposition 3.6 we saw that if p splits in finitely many quadratic CM extensions of L then the Brandt matrices are symmetric. We shall find below conditions that guarantee that there are no loops or multiple edges;

those conditions are the requirement that p splits in finitely many number fields M_i that depend on l. It will thus follow that there are infinitely many primes $\mathfrak{l} \lhd \mathcal{O}_L$ such that the graphs defined by the Brandt matrix $\mathrm{B}(\mathfrak{l})$ relative to $B_{p,L}$ are simple Ramanujan graphs.

Instead of developing a criterion in the greatest generality, we take a particular example where $l = 2$ is inert in L and L is quadratic . The reader will readily see that the argument generalizes for any prime $\mathfrak{l} \nmid p$, where l may have any splitting behavior and L need not be quadratic.

We consider the Brandt matrix $\mathrm{B}(2)$. We assume p already satisfies congruences so that $\mathrm{B}(2)$ is symmetric and we thus get a $5 = 2^2 + 1$ regular graph. To say that there are no self loops is to say that there are no isogenies $f\colon A \to A$ of degree 4, for any L-superspecial abelian surface A in characteristic p. If f is such an isogeny then $f \notin \mathcal{O}_L$ and so f induces an embedding of a CM order $\mathcal{O}_L[x]/(x^2 - (f + \bar{f}) + 2\epsilon) \hookrightarrow \mathrm{End}(A)$. Note that $\epsilon \in \mathcal{O}_L^{\times,+}$ and that we may replace f by uf for $u \in \mathcal{O}_L^\times$. We may thus assume that we have the orders $\mathcal{O}_L[x]/(x^2 - (f + \bar{f}) + 2) \hookrightarrow \mathrm{End}(A)$, whose field of quotients are CM fields, quadratic over L. This implies that $(f + \bar{f})^2 - 8$ is totally negative and so the element $a(f) = (f + \bar{f})^2$ is a totally positive element of $\mathcal{O}_L$ which is bounded by 8 under any embedding into $\mathbb{R}$. It follows that, given L, there are only finitely many such orders arising, regardless of p. Let K_i be their fields of quotients.

Multiple edges, say $f_1, f_2\colon A \to A'$ of degree 4, imply an endomorphism $f_2^t f_1 \in \mathrm{End}(A)$ of degree $16 = 2^4$, which is verified to be not multiplication by 2. The same argument as above gives a finite list of CM orders that may arise out of $f_2^t f_1$ and we let N_i be their field of quotients.

Fixing L, we have a positive density of primes splitting in all the finitely many fields $\{M_i\}, \{K_i\}, \{N_i\}$. For such a prime p we get a simple undirected 5-regular graph $G(L; p, 2)$.

4.4. Sequences of Ramanujan graphs. An interesting feature of our construction is the existence of natural maps between the graphs we have constructed. For every inclusion of totally real fields $L \subset M$, a rational prime p and prime ideals $\mathfrak{m}_1\mathfrak{m}_2 \cdots \mathfrak{m}_a = \mathfrak{l}$, where $\mathfrak{l}$ is a prime of L and $\mathfrak{m}_i$ of M, there is a natural "map"

$$G(L; p, \mathfrak{l}) \to G(M; p, \mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_a).$$

The map is canonical on vertices. If A is an abelian variety with RM by L then $A \otimes_{\mathcal{O}_L} \mathcal{O}_M$ is an abelian variety with RM by M. In the language of quaternion algebras, once we have fixed a superspecial order R of $B_{p,L}$ and a right ideal I of R, we get a superspecial order $R' = R \otimes_{\mathcal{O}_L} \mathcal{O}_M$ and an ideal $I' = I \otimes_{\mathcal{O}_L} \mathcal{O}_M$ of R'. This process is compatible with calculating left orders. If $\phi : A \to A'$ is an $\mathcal{O}_L$-isogeny with $(\deg_L(\phi)) = \mathfrak{l}$ then $\phi \otimes 1 : A \otimes_{\mathcal{O}_L} \mathcal{O}_M \to A \otimes_{\mathcal{O}_L} \mathcal{O}_M$ is an $\mathcal{O}_M$-isogeny with $(\deg_M(\phi)) = \mathfrak{l}\mathcal{O}_M$. We can decompose this isogeny into a sequence of $\mathcal{O}_M$-isogenies $\psi_1 \circ \cdots \circ \psi_a$ so that $(\deg_M \psi_i) = \mathfrak{m}_i$. Thus, the single edge from A to A' is replaced by a path of length a from $A \otimes_{\mathcal{O}_L} \mathcal{O}_M$ to $A' \otimes_{\mathcal{O}_L} \mathcal{O}_M$. In that sense we have a map of graphs $G(L; p, \mathfrak{l}) \to G(M; p, \mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_a)$. Note that if $a = 1$, that is, if $\mathfrak{l}$ is inert in M, then this is a map of graphs in the usual sense.

The question of whether these maps of graphs are *injective* on vertices is more subtle. Consider such an extension of totally real fields $L \subset M$ and two L-superspecial abelian varieties A, A'. One approach could be to consider $\mathrm{Hom}_{O_M}(A \otimes_{O_L} O_M, A' \otimes_{O_L} O_M)$ with the O_M-valued degree map. This module

is isomorphic to $\mathrm{Hom}_{O_L}(A, A') \otimes_{O_L} O_M$ with the degree map being the O_M-linear extension of the O_L degree map on $\mathrm{Hom}_{O_L}(A, A')$. If $A \otimes_{O_L} O_M \cong A' \otimes_{O_L} O_M$, then the lattices $\mathrm{End}_{O_L}(A)$ and $\mathrm{Hom}_{O_L}(A, A')$ become isomorphic after extension to O_M. Such issues are considered in [20] in detail for the case $L = \mathbb{Q}$. Based on the discussion there (see also the remarks in the end of the book), it doesn't seem far-fetched to ask whether such an isomorphism implies that $\mathrm{End}_{O_L}(A)$ is isomorphic to $\mathrm{Hom}_{O_L}(A, A')$. If so, this implies that 1 is represented by the degree map on $\mathrm{Hom}_{O_L}(A, A')$ and so that A and A' are isomorphic as L-superspecial abelian varieties. This, in turn, implies that the map of superspecial graphs $G(L; p, l) \to G(M; p, l)$ is injective on vertices. This question, though interesting and relevant to our topic, is a subject for independent research, as the discussion in [20] (which only deals with $L = \mathbb{Q}$) indicates.

5. Families of nested Ramanujan graphs

Our discussion in this section does not claim to be exhaustive. Our purpose is to discuss certain nested families of Ramanujan graphs, in particular we consider our superspecial graphs from another point of view, and pose questions that we find intriguing.

5.1. Paley graphs. Let $\mathbb{F}_q$ be a finite field of order $q \equiv 1 \pmod 4$. The vertices of the Paley graph $P(q)$ are the elements of $\mathbb{F}_q$, and $x \neq y$ are connected if $x - y$ is a square in $\mathbb{F}_q$. This is a $(q-1)/2$ regular graph on q vertices. Recall that a graph is strongly regular with parameters (k, a, b) if it is a k-regular incomplete graph, any two adjacent vertices have $a \geq 0$ common neighbors and any two nonadjacent vertices have $b \geq 1$ common neighbors. One can show that a Paley graph is a strongly regular graph with q vertices and parameters $((q-1)/2, (q-5)/4, (q-1)/4)$. Cf. [24, Section 8.3]. The eigenvalues of the adjacency matrix are therefore $(q-1)/2$ and the roots of $x^2 + x - (q-1)/4$, namely $(-1 \pm \sqrt{q})/2$. Note that these graphs beat the bound $2\sqrt{(q-1)/2 - 1}$; for $q \gg 0$ their ratio is about $2\sqrt{2}$.

We have an inclusion $P(q) \hookrightarrow P(q^n)$ for any n and so, for concreteness, we can take the chain of Ramanujan graphs $P(p) \to P(p^3) \to P(p^9) \to \cdots$. We make three remarks:

(1) The degree is very large compared to the size of the graph, a fact which renders this graph inappropriate for most applications.

(2) The possible advantage of the sequence $P(p) \to P(p^3) \to P(p^9) \to \cdots$ over, say, the sequence $P(p) \to P(p^2) \to P(p^4) \to \cdots$ is that any two vertices of $P(p^{2^i})$ become adjacent in $P(p^{2^{i+1}})$, while in $P(p) \to P(p^3) \to P(p^9) \to \cdots$ nonadjacent vertices remain nonadjacent. Since the diameter of all these graphs is 2 we conclude that the arrows in $P(p) \to P(p^3) \to P(p^9) \to \cdots$ are isometries.

(3) An even simpler construction can be made with the complete graphs K_n. There are (noncanonical) inclusions $K_1 \hookrightarrow K_2 \hookrightarrow K_3 \hookrightarrow \cdots$. Trivially, those inclusions are isometries. The graph K_n has eigenvalues $n-1$ and -1 with multiplicities 1 and $n-1$ respectively and so is Ramanujan for $n \geq 2$. The same comments as to the interest in those examples apply.

5.2. Terras graphs. We discuss the graphs defined by Terras. See [36, 37] and the references therein.

Consider a finite field $\mathbb{F}_q$ with q elements, q odd. Let $\delta \in \mathbb{F}_q$ be a nonsquare. Then $\mathbb{F}_{q^2} = \mathbb{F}_q \oplus \mathbb{F}_q\sqrt{\delta}$ as an $\mathbb{F}_q$-vector space. Terras defines the finite upper half

plane $\mathfrak{H}_q$ as

$$\mathfrak{H}_q = \{x + y\sqrt{\delta} : x, y \in \mathbb{F}_q, y \neq 0\} = \mathbb{F}_{q^2} - \mathbb{F}_q.$$

The group $\mathrm{PGL}_2(\mathbb{F}_q)$ acts transitively on $\mathfrak{H}_q$ by $z \mapsto (az+b)/(cz+d)$ for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$. Note that the action does not depend on δ. The stabilizer of $\sqrt{\delta}$ is $K_q = \left\{\left(\begin{smallmatrix} a & b\delta \\ b & a \end{smallmatrix}\right) : a, b \in \mathbb{F}_q, a^2 - b^2\delta \neq 0\right\}$. Thus $\mathfrak{H}_q = \mathrm{GL}_2(\mathbb{F}_q)/K_q$. The elements of $\mathfrak{H}_q$ are the vertices $V(T(q))$ of the Terras graph $T(q)$.

Define a function,

$$d\colon V(T(q)) \to \mathbb{F}_q, \quad d(z,w) = \frac{N(z-w)}{\mathrm{Im}(z)\,\mathrm{Im}(w)},$$

where $\mathrm{Im}(x + y\sqrt{\delta}) = y$, $\overline{x + y\sqrt{\delta}} = x - y\sqrt{\delta}$ and $N(z) = z\bar{z}$. Choose an element $a \in \mathbb{F}_q$, $a \neq 0, 4\delta$ (in characteristic different from 3, a canonical choice could be $a = \delta$). Define z, w to be adjacent if $d(z,w) = a$. One can show that this gives a $q+1$-regular graph $T(q) = T(q, \delta, a)$ on $q^2 - q$ vertices. The group $\mathrm{GL}_2(\mathbb{F}_q)$ acts as isometries on this graph. Such graphs were proven to be Ramanujan by Katz.

The neighbors of $\sqrt{\delta}$ are the set $S = \{x + y\sqrt{\delta} : x^2 = ay + \delta(y-1)^2\}$. One can show that $T(q)$ is the Cayley graph of the group $\left\{\left(\begin{smallmatrix} y & x \\ 0 & 1 \end{smallmatrix}\right) : x, y \in \mathbb{F}_q, y \neq 0\right\}$ with respect to the set of generators S. In [2, Theorems 1 and 2] the diameter of the graph $T(q, \delta, a)$ is determined: *If $a \notin \{0, 2\delta, 4\delta\}$ then the diameter is 3 if $\delta - a$ is a square in $\mathbb{F}_q$ and 4 otherwise. If $a = 2\delta$ then the diameter is 3 unless $q = 3, 5$ in which case the diameter is 2.*

Consider the question of which vertices in $T(q)$ are at distance 2 from a given vertex. Since $\mathrm{GL}_2(\mathbb{F}_q)$ acts transitively on the set of vertices, we may consider the question just for the vertex $\sqrt{\delta}$. Given a point $x_0 + y_0\delta$ we are interested in the set of points $x + y\sqrt{\delta}$ that solve the two equations:

$$(x - x_0)^2 - (y - y_0)^2\delta = ayy_0, \quad x^2 - (y-1)^2\delta = ay.$$

The number of such points is the number of distinct paths of length 2 from $x_0 + y_0\delta$ to $\sqrt{\delta}$.

Viewing x_0, y_0 as fixed and x, y as variables and homogenizing we get two quadratic curves in $\mathbb{P}^2$:

$$(x - x_0 z)^2 - (y - y_0 z)^2\delta = ay_0 yz, \quad x^2 - (y - z)^2\delta = ayz.$$

By Bezout's theorem they intersect at 4 points (counted with multiplicity) on which $\mathrm{Gal}(\mathbb{F}_q^{\mathrm{alg}}/\mathbb{F}_q)$ act. At infinity, the curves intersect at the two points $\{(x : y : 0) : x^2 - \delta y^2 = 0\}$ which form a Galois orbit for $\mathrm{Gal}(\mathbb{F}_q^{\mathrm{alg}}/\mathbb{F}_q)$. It follows that there are the following possibilities for the intersection points that lie in $\mathbb{A}^2$ (i.e., solutions to the original system of equations) and no others:

(1) The intersection points in $\mathbb{A}^2$ are not defined over $\mathbb{F}_q$. In that case, there are two of them and they form a single $\mathrm{Gal}(\mathbb{F}_q^{\mathrm{alg}}/\mathbb{F}_q)$-orbit and are defined over $\mathbb{F}_{q^2}$.

(2) The intersection points in $\mathbb{A}^2$ are defined over $\mathbb{F}_q$. In this case, there are two different paths of length two from $x_0 + y_0\sqrt{\delta}$ to $\sqrt{\delta}$ if the intersection points are distinct, and one path if they are the same.

To fix ideas, assume now that $p > 3$. We may then choose $a = \delta \in \mathbb{F}_p$ a nonsquare and get a directed system of Terras graphs

$$T(p) \to T(p^3) \to T(p^9) \to \cdots.$$

The maps are injective on vertices and are isometries locally in the sense that if two vertices in $T(p^{3^n})$ are adjacent in $T(p^{3^{n+1}})$ then they are already adjacent in $T(p^{3^n})$. Since the diameter of all the graphs is 3 the maps are globally isometries. Indeed, if two points of $T(q)$, $q = p^{3^n}$, are in distance 2 they stay in distance 2 since the distance function d on $T(q^3)$ extends the one on $T(q)$. If they are at distance 3 in $T(q)$ they cannot be in distance 1 in $T(q^3)$ (for the same reason) and also cannot be in distance 2 in $T(q^3)$, because that would mean that the solutions $x+y\sqrt{\delta}$ appearing in the first conclusion above, are only defined over $\mathbb{F}_{q^2}$ (because the points are not in distance 2 in $T(q)$) yet belong to $\mathbb{F}(q^3)$, which is absurd.

Question. What is the limit distribution of the eigenvalues of $T(p^n)$ for fixed p and $n \to \infty$?

To the best of our knowledge this question is open. See [37] for some discussion of this and [19] for the failure of the "naive conjecture."

5.3. LPS graphs. The graphs defined by Lubotzky – Phillips – Sarnak [24,25] and Jordan – Livné [18], that we call *LPS graphs*, can be described conceptually as follows.

Let l be a prime and consider the Bruhat – Tits tree $\mathscr{T}_K$ of $\mathrm{PGL}_2(K)$, where K is a finite extension of $\mathbb{Q}_l$. Let $\mathcal{O}_K$ be its valuation ring, π_K a uniformizer and κ the residue field. The tree has vertices corresponding to lattices in K^2 modulo homothety. To describe a lattice up-to-homothety is to give a basis, modulo change of basis and then modulo re-scaling, and so the vertices correspond to $K^\times \backslash \mathrm{GL}_2(K)/\mathrm{GL}_2(\mathcal{O}_K) = \mathrm{PGL}_2(K)/\mathrm{PGL}_2(\mathcal{O}_K)$. We say that two classes of lattices are adjacent if we can find representatives L_0, L_1 such that $L_1 \subset L_0$ and $[L_0/L_1] \cong \kappa$ as $\mathcal{O}_K$ modules. If κ has l^f elements, since the lattices adjacent to L_0 are parameterized by $\mathbb{P}^1(\kappa)$, the tree is l^f+1-regular. Also, to give an edge is to give a lattice L_0 together with a cyclic $\mathcal{O}_K$-module of order l^f in L_0/lL_0 and thus the edges are parameterized by $\mathrm{PGL}_2(K)/\overline{I(K)}$, where $I(K) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : a,b,c,d \in \mathcal{O}_K, c \in (\pi_K) \right\}$ is the standard Iwahori subgroup and $\overline{I(K)}$ its projection to $\mathrm{PGL}_2(K)$.

Trees are the best expanders one can hope for. They are infinite, though. One therefore looks for a subgroup $\Gamma \subset \mathrm{Aut}(\mathscr{T}_K)$ such that the quotient $\Gamma\backslash\mathscr{T}_K$ is a finite graph (and conversely, the universal covering space of any l^f+1-regular tree is isomorphic to $\mathscr{T}_K$); to get a finite graph, Γ needs to be a discrete co-compact subgroup and there is an art to finding such groups. One method is to use quaternion algebras.

Let L be a number field, l a rational prime and $\mathfrak{l}|l$ an unramified prime factor of l in $\mathcal{O}_L$. For simplicity of exposition we assume L is totally real. Let B be a definite quaternion algebra over L, split at $\mathfrak{l}$, $K = L_\mathfrak{l}$. Let $\mathcal{O}$ be an order (over $\mathcal{O}_L$) of B and let $\Gamma = (\mathcal{O}[l^{-1}])^\times$. Let $\mathcal{O}^\dagger$ be a maximal order of B containing $\mathcal{O}$. Through an identification $B(L_\mathfrak{l}) \cong \mathrm{GL}_2(K)$, such that $\mathcal{O}^\dagger \otimes \mathcal{O}_{L_\mathfrak{l}} = \mathrm{GL}_2(\mathcal{O}_K)$, Γ is a discrete co-compact subgroup of $\mathrm{GL}_2(O_K)$ and one obtains a finite graph (possibly with multiple edges and self-loops) $\Gamma\backslash\mathscr{T}_K$. See [24, Section 7.3].

To illustrate the construction of *nested families* of LPS graphs, we make the simplifying assumption that $\mathcal{O}$ is a maximal order in $B_{p,\infty}$ — the rational quaternion algebra B ramified at p and ∞; the construction works for any definite quaternion algebra over $\mathbb{Q}$. For every field $L \supseteq \mathbb{Q}$, let $B_{p,L} = B_{p,\infty} \otimes_{\mathbb{Q}} L$. Choose a sequence of totally real fields $\mathbb{Q} \subset L_1 \subset L_2 \subset \cdots$ and a sequence of compatible

primes $\cdots \mathfrak{l}_3 \mid \mathfrak{l}_2 \mid \mathfrak{l}_1 \mid l$ and assume that p is split and l is unramified in each of the fields L_i. Then the discriminant of B_{p,L_i} is $p\mathcal{O}_{L_i}$ and hence $\mathcal{O} \otimes_{\mathbb{Z}} \mathcal{O}_{L_i}$ is a maximal order of B_{p,L_i}. We let $\Gamma_i = (\mathcal{O} \otimes_{\mathbb{Z}} \mathcal{O}_{L_i}[l^{-1}])^\times$. Let $K_i = (L_i)_{\mathfrak{l}_i}$ then $\mathbb{Q}_l \subset K_1 \subset K_2 \subset \cdots$ is a sequence of unramified l-adic fields. There are canonical injections of trees $\mathscr{T}_{\mathbb{Q}} \hookrightarrow \mathscr{T}_{K_1} \hookrightarrow \mathscr{T}_{K_2} \hookrightarrow \cdots$, corresponding to the natural map of lattices $\Lambda \subset K_i^2 \mapsto \Lambda \otimes_{\mathcal{O}_{K_i}} \mathcal{O}_{K_{i+1}} \subset K_{i+1}^2$. In terms of double cosets, this is the map taking $K_i^\times \gamma \,\mathrm{GL}_2(\mathcal{O}_{K_i})$ to $K_{i+1}^\times \gamma \,\mathrm{GL}_2(\mathcal{O}_{K_{i+1}})$. If $K_{i+1}^\times \gamma_1 \,\mathrm{GL}_2(\mathcal{O}_{K_{i+1}}) = K_{i+1}^\times \gamma_2 \,\mathrm{GL}_2(\mathcal{O}_{K_{i+1}})$ then $\gamma_2^{-1}\gamma_1 = l\delta$ for some $l \in K_{i+1}^\times, \delta \in \mathrm{GL}_2(\mathcal{O}_{K_{i+1}})$. If $\gamma_1, \gamma_2 \in \mathrm{GL}_2(K_i)$ then $l\delta \in K_{i+1}^\times \,\mathrm{GL}_2(\mathcal{O}_{K_{i+1}}) \cap \mathrm{GL}_2(K_i)$. However, $K_{i+1}^\times \,\mathrm{GL}_2(\mathcal{O}_{K_{i+1}}) \cap \mathrm{GL}_2(K_i) = K_i^\times \,\mathrm{GL}_2(\mathcal{O}_{K_i})$. First, the inclusion $\supseteq$ is obvious. To see the other inclusion, write an element $l\delta$ as above in the form $\pi^n l'\delta$, where π is a uniformizer of K_i and $l' \in \mathcal{O}_{K_{i+1}}^\times$. It is enough to show that $l'\delta \in \mathrm{GL}_2(\mathcal{O}_{K_i})$, but $l'\delta \in \mathrm{GL}_2(\mathcal{O}_{K_{i+1}}) \cap \mathrm{GL}_2(K_i) = \mathrm{GL}_2(\mathcal{O}_{K_i})$. We therefore conclude that $K_i^\times \gamma_1 \,\mathrm{GL}_2(\mathcal{O}_{K_i}) = K_i^\times \gamma_2 \,\mathrm{GL}_2(\mathcal{O}_{K_i})$. Note that the map of trees that we get are not just injection on vertices. It is an isometry (namely, it is truly a map of graphs), because the extensions are unramified.

To get a map of graphs $\Gamma\backslash\mathscr{T}_{\mathbb{Q}} \hookrightarrow \Gamma_1\backslash\mathscr{T}_{K_1} \hookrightarrow \Gamma_2\backslash\mathscr{T}_{K_2} \hookrightarrow \cdots$, we first need that $\Gamma_{i+1} \cap \mathrm{GL}_2(K_i) \supseteq \Gamma_i$ and that is clear. Next note that if two vertices of $\mathscr{T}_{K_i}$ (i.e., two lattices in K_i^2, up to homothety) are equivalent under an element γ of Γ_{i+1} then we may suppose $\gamma \in \mathrm{GL}_2(K_i)$. To get actual injections $\Gamma_i\backslash\mathscr{T}_{K_i} \hookrightarrow \Gamma_{i+1}\backslash\mathscr{T}_{K_{i+1}}$, we at least need $(\mathcal{O} \otimes_{\mathbb{Z}} \mathcal{O}_{L_{i+1}}[l^{-1}])^\times \cap B_{L_i} = (\mathcal{O} \otimes_{\mathbb{Z}} \mathcal{O}_{L_i}[l^{-1}])^\times$, which is not hard to verify. This is not sufficient for injectivity, however, as pointed out in Section 4.4 above. Whatever the case may be, this construction gives a direct family of graphs $\Gamma\backslash\mathscr{T}_{\mathbb{Q}} \to \Gamma_1\backslash\mathscr{T}_{K_1} \to \Gamma_2\backslash\mathscr{T}_{K_2} \to \cdots$ that are all Ramanujan; The Ramanujan property follows from the deep results [23, Theorem 2.4; 24, *loc. cit.* and Corollary 5.5.3], using the fact that the fields are totally real. Finally, we remark that the assumption that p splits in all the fields L_i is not essential. One can simply assume that p is not ramified; the same arguments apply, the only difference being that the orders $\mathcal{O} \otimes \mathcal{O}_{L_i}$ are not necessarily maximal.

5.3.1. *The connection between the work of Lubotzky – Phillips – Sarnak and Pizer.* In this section we explain the relation between the work of Lubotzky – Phillips – Sarnak and the work of Pizer. This is well understood by the experts, though only cryptic remarks appear in the literature. We thus find it worthwhile to explain that, and in so doing to explain the relation between the constructions appearing in this paper and the work of Jordan – Livné.

Let L be a totally real field of strict class number 1, B a totally definite quaternion algebra over L and $\mathcal{O}$ a hereditary $\mathcal{O}_L$-order of B contained in a maximal order $\mathcal{O}^\dagger$. The order $\mathcal{O}$ gives us a ring scheme over $\mathcal{O}_L$ whose value for every $\mathcal{O}_L$-algebra S is $\mathcal{O} \otimes S$, and a group scheme $\mathscr{B}$ over $\mathcal{O}_L$ which is the units in the ring scheme. Let $\mathfrak{l}|l$ be a prime of L such that $(l, \mathrm{disc}_L) = 1$ and which splits B.

Since $\mathcal{O}$ is hereditary, every $\mathcal{O}$-ideal is locally principal and therefore the class group of $\mathcal{O}$ is given by $\mathscr{B}(L)\backslash\mathscr{B}(\mathbb{A}_{L,f})/\mathscr{B}(\mathcal{O}_L \otimes \widehat{\mathbb{Z}})$, where $\mathbb{A}_{L,f}$ are the finite adèles of L. The inclusion $L_{\mathfrak{l}} \to \mathbb{A}_{L,f}$ induces inclusions $\mathscr{B}(L_{\mathfrak{l}}) \hookrightarrow \mathscr{B}(\mathbb{A}_{L,f})$ and $\mathscr{B}(\mathcal{O}_L[l^{-1}])\backslash\mathscr{B}(L_{\mathfrak{l}})/\mathscr{B}(\mathcal{O}_{L_{\mathfrak{l}}}) \hookrightarrow \mathscr{B}(L)\backslash\mathscr{B}(\mathbb{A}_{L,f})/\mathscr{B}(\mathcal{O}_L \otimes \widehat{\mathbb{Z}})$. The last map is in fact a surjection. We need to show that $\mathscr{B}(\mathbb{A}_{L,f}) = \mathscr{B}(L)\mathscr{B}(L_{\mathfrak{l}})\mathscr{B}(\mathcal{O}_L \otimes \widehat{\mathbb{Z}})$. This follows from strong approximation. (This only requires that B is ramified at least

in one place at infinity.) Recalling that B is split at $\mathfrak{l}$ we conclude a bijection

$$\mathcal{O}[l^{-1}]^\times \backslash \operatorname{GL}_2(L_\mathfrak{l}) / \operatorname{GL}_2(\mathcal{O}_{L_\mathfrak{l}}) \cong \mathscr{B}(L) \backslash \mathscr{B}(\mathbb{A}_{L,f}) / \mathscr{B}(\mathcal{O}_L \otimes \widehat{\mathbb{Z}}) = \operatorname{Cl}(\mathcal{O}). \tag{1}$$

If $B = B_{p,\infty}$ is the rational quaternion algebra ramified at p and ∞ alone, $\mathcal{O}$ a maximal order, then $\operatorname{Cl}(\mathcal{O})$ is in bijection with supersingular elliptic curves. Taking a nonmaximal order gives the cases considered by Pizer (only that his orders are not necessarily hereditary). For L a totally real field of class number one and a prime p unramified in L, and the order $\mathcal{O} \otimes \mathcal{O}_L$ in $B_{p,L} := B_{p,\infty} \otimes_{\mathbb{Q}} L$, we have $\operatorname{Cl}(\mathcal{O} \otimes \mathcal{O}_L)$ is in bijection with the superspecial abelian varieties with real multiplication by $\mathcal{O}_L$. The bijection (1) is not only connecting the constructions of [18, 25] with ours, but also shows the connectivity of the graph of $\mathfrak{l}$-isogenies.

5.4. A question. The above examples motivate the following problem. Construct a long or infinite series of Ramanujan graphs $G_0 \to G_1 \to G_2 \to \cdots$, where G_i has n_i vertices and degree d_i, and the maps, if not injective, should at least be "nondegenerate" in some well-quantified sense. We are particularly interested in a construction meeting one or more of the following extra requirements:

- That d_i be bounded from above by $\log(n_i)^r$ for some positive r.
- That $n_i = o(i^{1+\epsilon})$ for some $\epsilon < 1$.
- That the morphisms $G_i \to G_{i+1}$ be isometries.
- That each G_i be a Cayley graph.
- That each G_i beat the Ramanujan bound, e.g., in the sense that we have $\lambda(G_i) < 2\sqrt{d_i - 1} - \epsilon$ for some $\epsilon > 0$ independent of i (or an even stronger requirement). We remark that for every d-regular simple graph G we have $\lambda(G) \geq \sqrt{d} \cdot \sqrt{(n-d)/(n-1)}$, which puts a bound on by how much one can beat the Ramanujan bound.

6. Applications and implementation

There are many interesting and well-known applications of Ramanujan graphs. Due to the fact that random walks on expanders (and hence on Ramanujan graphs) mix very rapidly, expanders are used as pseudo-random number generators, for approximating the average value of a function, and in the design of low-density parity check codes in coding theory. See [14] for a comprehensive exposition of the many applications in different branches of mathematics and computer science. Here we point out some new applications that are enabled by our construction, and raise some related questions.

6.1. Reliable networked storage. One (possibly new) application of graphs with good expansion properties is to use the graph to build a network of users who share storage of files and content on each others' machines, for example using network coding (see for example [6]). In this scenario, a network of participants is built by modeling the participants as nodes of a graph, and forming a participant's neighbor set (with whom it shares storage) as the set of neighbors of that node in the graph. Given an existing network of participants, one may wish to add a new collection of participants to the network while preserving the existing connections. For this purpose, a nested family of Ramanujan graphs could be used. Any user's files are then distributed to its neighbors via network coding, and subsequently stored. If a node fails, the data can be reconstructed from some subset of the participants through the error correcting capacity of network coding.

6.2. Cryptographic hash functions. In [5], the idea was proposed that Ramanujan graphs can also be used to construct cryptographic hash functions. Hash functions used in cryptographic protocols need to be efficiently computable and collision resistant, at a minimum. A hash function can be constructed from a graph by specifying a starting vertex, using the input to the hash function as directions for walking around the graph (without backtracking), and then returning the final vertex of the walk as the output of the hash function. If the graph has good expansion properties, the output of the hash function will appear random, since walks on expander graphs quickly approximate the uniform distribution. Given a graph with suitable labels for its edges and vertices, finding collisions in such a hash function is equivalent to finding cycles in the graph. Thus this construction can be applied to construct collision-resistant hash functions from any expander graph in which finding cycles is a hard problem. For more details see [5]. We give there two families of Ramanujan graphs, constructed by Pizer and Lubotzky-Phillips-Sarnak, and report the efficiency and collision resistance properties further.

When constructing a hash function from the Ramanujan graph of supersingular elliptic curves over $\mathbb{F}_{p^2}$ with l-isogenies, l a prime different from p, finding collisions is at least as hard as computing isogenies between supersingular elliptic curves. This is believed to be a hard problem, and the best algorithm currently known solves the problem in $O(\sqrt{p}\log^2 p)$ time ([5]). Thus the prime p can be taken to be a 256-bit prime, to get 128 bits of security from the resulting hash function. To compute the hash function from Pizer's graph when $l = 2$ requires roughly $2\log(p)$ field multiplications per bit of input to the hash function. This is roughly the same efficiency as a provable hash based on the Elliptic Curve Discrete Logarithm Problem.

The Pizer graph is the $g = 1$ case of our general construction of superspecial graphs. One feature of such graphs is that the same vertex set (fixing p) can give rise to many different graphs by varying l, the degree of the isogenies. One can ask, given two different edge sets on the same vertex set, whether there is any correlation of distances between vertices in the two graphs. This question is relevant to attacks on the hash function. Indeed, starting at two vertices which are at distance one from each other in one graph, and taking a walk from each vertex using the same directions in the two different graphs, it should not happen with high probability that the two ending vertices are close to each other in the other graph. This application raises an interesting question about the independence of graphs which will be considered in Section 7.

7. Metrics and independence of graphs

Fix L and p, where L is a totally real field of strict class number 1, and p is an unramified prime in L. Taking various prime ideals $\mathfrak{l}$ (not above p) we get a collection of Ramanujan graphs $G(L; p, \mathfrak{l})$. Let V be the vertex set of the graphs $G(L; p, \mathfrak{l})$. As $\mathfrak{l}$ varies, one can view these graphs as defining a sequence of metrics $d_{\mathfrak{l}} \colon V \times V \to \mathbb{N}$, where $d_{\mathfrak{l}}(u, v)$ is the length of the shortest path between the vertices u and v in $G(L; p, \mathfrak{l})$. It is natural to wonder what, if any, relations exist between these various metrics. It turns out that even for the Pizer graphs this question is already difficult to investigate. In this section we treat these metrics as defining random variables on $V \times V$ and study some properties of these random variables.

Let V be a set with N elements. Given two connected graphs $G_1 = (V, E_1)$ and $G_2 = (V, E_2)$ that are k_1 and k_2 regular, respectively, our goal for this section is to study some properties of the random variables d_1 and d_2 that define the distance metric on these graphs. In the cases of interest (to us) G_1 and G_2 will be Ramanujan graphs and hence we may specialize our results to this situation. We begin with a discussion on the average distance between two vertices in a graph.

7.1. Average distance. Let G be a connected k-regular graph on N vertices. Define a random variable $d\colon V \times V \to \mathbb{N}$ as follows: Pick two vertices u, v uniformly (and independently) from V and set $d(u, v)$ to be the length of the shortest path in G between u and v. We study the expectation of this random variable in this section.

Proposition 7.1. *Suppose $G = (V, E)$ is a k-regular graph ($k > 2$) that is a Ramanujan graph and let $|V| = N$. Then $d(u, v) \leq 2\lceil \log_{1+c} N/2 \rceil + 1$ for any pair of vertices u and v, where $c = (1 - 2\sqrt{(k-1)/k^2})/2$.*

Proof. Let $U \subseteq V$, $\overline{U}$ be the complement of U in V, and let $\Gamma(U) := \{v : v \notin U \text{ and } (u, v) \in E \text{ for some } u \in U\}$. Since G is a Ramanujan graph $E(U, \overline{U}) = \{(u, v) \in E : u \in U, v \notin U\}$ satisfies

$$|E(U, \overline{U})| \geq \frac{k - 2\sqrt{k-1}}{2} \min\{|U|, N - |U|\}$$

(see [1]). Since the graph is k-regular, this means that

$$|\Gamma(U)| \geq c|U| \quad \text{if } |U| \leq \frac{N}{2}, \tag{2}$$

where $c = (1 - 2\sqrt{(k-1)/k^2})/2$ in the following discussion. Let u and v be any two vertices in the graph. We start with the sets $U_0 = \{u\}$ and $V_0 = \{v\}$ and define $U_i := U_{i-1} \cup \Gamma(U_{i-1})$ and $V_i := V_{i-1} \cup \Gamma(V_{i-1})$ for $i > 0$. Let $\tilde{\imath}$ and $\tilde{\jmath}$ be a pair (i, j) such that $|U_i| + |V_j| > N$ and that the sum $i + j$ is minimal, then $\tilde{\imath} + \tilde{\jmath}$ is the distance between the vertices u and v. From (2), we find that $|U_i| \geq (1+c)^i$ as long as $|U_i| \leq N/2$ and similarly for $|V_i|$. In any case, $|U_i| > N/2$ if $i \geq \lceil \log_{1+c} N/2 \rceil + 1$. Thus,

$$d(u, v) \leq 2\lceil \log_{1+c} N/2 \rceil + 1. \qquad \square$$

The following corollary is immediate:

Corollary 7.2. *Let G_n be a family of connected k-regular Ramanujan graphs ($k > 2$). Let $\mathrm{E}[d_n]$ be the expectation of the random variable d_n that gives the distance between vertices in G_n. Then $\mathrm{E}[d_n] \leq 2\lceil \log_{1+c} |V(G_n)|/2 \rceil + 1$ where $c = (1 - 2\sqrt{(k-1)/k^2})/2$.*

The next result shows that the above upper bound is quite close to the truth.

Proposition 7.3. *Let G_n be a family of connected k-regular ($k > 2$) graphs such that $|V(G_n)|$ is unbounded and let d_n be the random variable giving the distance between vertices in G_n. Then*

$$\liminf_{n \to \infty} \frac{\mathrm{E}[d_n]}{\log_{k-1} |V(G_n)|} \geq 1.$$

PROOF. For a k-regular graph, one can find an upper bound on the probability $\Pr_{u,v}[d(u,v) \leq i]$ as follows. Define, for any vertex u, the set $\Gamma^{\leq i}(u) := \{v \mid d(u,v) \leq i\}$. One sees that

$$\Pr_{u,v}[d(u,v) \leq i] \leq \max_w \frac{|\Gamma^{\leq i}(w)|}{N},$$

where N is the number of vertices in the graph. For a k-regular graph one has

$$|\Gamma^{\leq i}(w)| \leq 1 + \sum_{1 \leq j \leq i} k(k-1)^{j-1}.$$

Consequently, one has

$$\Pr_{u,v}[d(u,v) \leq i] \leq \frac{k((k-1)^i - 1) + (k-2)}{(k-2)N}.$$

Let $a < 1$, then

$$\begin{aligned}
\Pr_{u,v}[d(u,v) \leq a \log_{k-1} N] &\leq \frac{k((k-1)^{a \log_{k-1} N} - 1) + (k-2)}{(k-2)N} \\
&\leq \frac{k(N^a - 1) + (k-2)}{(k-2)N} \\
&\leq \frac{kN^a}{(k-2)N} + \frac{1}{N} \\
&\leq \frac{k}{k-2}(N^{a-1} + N^{-1}).
\end{aligned}$$

In particular, $\lim_{N \to \infty} \Pr_{u,v}[d(u,v) \leq a \log_{k-1} N] = 0$.

Suppose $\mathrm{E}[d] \leq b \log_{k-1} N$ where $b < a$. Then by Markov's inequality

$$\Pr_{u,v}[d(u,v) > a \log_{k-1} N] \leq \frac{b \log_{k-1} N}{a \log_{k-1} N} = \frac{b}{a}$$

and b/a is bounded away from 1. On the other hand, we showed earlier that if N is large enough $\Pr_{u,v}[d(u,v) > a \log_{k-1} N] > b/a$, a contradiction.

Thus, for large enough graphs, G_n, $\mathrm{E}[d] > b \log_{k-1} |V(G_n)|$ for any $b < 1$. □

7.2. Independence of graphs. Let $G_1 = (V, E_1)$ and $G_2 = (V, E_2)$ be two graphs on the same vertex set that are k_1 and k_2 regular respectively. Define d_i, for $i = 1, 2$, to be the random variable giving the distance in the graph G_i. One natural definition of independence of graphs relates to the independence of these random variables, more precisely:

Definition 7.4. We call the graphs G_1 and G_2 *independent* if for each $i \leq \mathrm{Diam}(G_1)$ and $j \leq \mathrm{Diam}(G_2)$ we have that

$$\Pr_{u,v}[d_1(u,v) = i \text{ and } d_2(u,v) = j] = \Pr_{u,v}[d_1(u,v) = i] \cdot \Pr_{u,v}[d_2(u,v) = j].$$

We note that it is perhaps unreasonable to expect independence of graphs under this strong notion of independence. The definition, however, allows one to quantify "approximate independence" in terms of the size of the difference between the two quantities. In the following we investigate the Pizer graphs to see how closely the above condition holds.

7.2.1. *Independence of Pizer graphs.* Let l_1 and l_2 be two different primes and consider the Pizer graphs $G_1 = G(p, l_1)$ and $G_2 = G(p, l_2)$. For simplicity, we will assume $p \equiv 1 \mod 12$ so that edges on the graphs correspond to isogenies, up to a sign. We first analyze the case where $i = 1$ and j is allowed to be any positive integer less than the diameter of G_2. To say that $d_1(u, v) = 1$ and $d_2(u, v) = j$ means that there are two isogenies $\phi : E_u \to E_v$ and $\psi : E_u \to E_v$ such that $\deg(\phi) = l_1$ and $\deg(\psi) = l_2^j$. Taking $\hat{\psi} \circ \phi$ we get an endomorphism in $\mathrm{End}(E_u)$ of degree $l_1 l_2^j$ while taking $\psi \circ \hat{\phi}$ we get an endomorphism of degree $l_1 l_2^j$ in $\mathrm{End}(E_v)$ (here $\hat{\phi}$ and $\hat{\psi}$ refer to the dual isogeny of ϕ and ψ respectively); both endomorphisms are well-defined up to a sign. In this way we get embeddings of a quadratic imaginary order $\mathbb{Z}[x]/(x^2 - ax + l_1 l_2^j)$ into $B_{p,\infty}$. Now

$$\begin{aligned}\sharp\{(u, v) \mid d_1(u, v) = 1 \text{ and } d_2(u, v) = j\} &= \frac{1}{2} \sum_E \sharp\{\phi \in \mathrm{End}(E) \mid \deg(\phi) = l_1 l_2^j\} \\ &= \sum_{\substack{0 \le a \le 2\sqrt{l_1 l_2^j} \\ p \text{ inert or ramified in } \mathbb{Q}(\sqrt{a^2 - 4 l_1 l_2^j})}} H(a^2 - 4 l_1 l_2^j)\end{aligned}$$

where $H(m)$ is the Hurwitz class number of the order of discriminant m in $\mathbb{Q}(\sqrt{m})$. Using the estimate $H(m) \le |m|^{\frac{1}{2}+\epsilon}$ (for every $\epsilon > 0$) we get

$$\begin{aligned}\sharp\{(u, v) \mid d_1(u, v) = 1 \text{ and } d_2(u, v) = j\} &\le \sum_{0 \le a \le 2\sqrt{l_1 l_2^j}} (4 l_1 l_2^j - a^2)^{\frac{1}{2}+\epsilon} \\ &\le \frac{\pi}{4} (l_1 l_2^j)^{1+\epsilon},\end{aligned}$$

where we have used approximation of the sum by an integral in the second step. Finally, we get the bound

$$\Pr_{u,v}[d_1(u, v) = 1 \text{ and } d_2(u, v) = j] \le \frac{(l_1 l_2^j)^{1+\epsilon}}{N^2}. \tag{3}$$

One can obtain a lower bound for this probability for many primes p. Indeed, if p remains inert or ramified in at least a constant proportion of the fields $\mathbb{Q}\big(\sqrt{a^2 - 4 l_1 l_2^j}\big)$, we can use the Brauer–Siegel ineffective lower bound for the class number to get

$$\Pr_{u,v}[d_1(u, v) = 1 \text{ and } d_2(u, v) = j] \gg \frac{(l_1 l_2^j)^{1-\epsilon}}{N^2}. \tag{4}$$

The Chebotarev density theorem implies that the lower bound holds for at least a constant proportion of the primes p for fixed l_1, l_2 and j. On the other hand there are also a constant proportion of primes for which the lower bound does not hold.

Meanwhile, $\Pr_{u,v}[d_1(u, v) = 1] = (l_1 + 1)/N$. Since G_2 is $l_2 + 1$ regular we have that $\Pr_{u,v}[d_2(u, v) = j] \le (l_2 + 1) l_2^{j-1}/N$. On the other hand, the expansion property shows us that for any u, $\sharp\{v \mid d(u, v) = j\} = \Gamma(\Gamma^{\le j-1}(\{u\})) \ge c(1 + c)^{j-1}$ for small j (adopting the notation introduced in Section 7.1). Thus we get the bounds

$$\begin{aligned}\frac{(l_1 + 1) c (1 + c)^{j-1}}{N^2} &\le \Pr_{u,v}[d_1(u, v) = 1] \cdot \Pr_{u,v}[d_2(u, v) = 1] \\ &\le \frac{(l_1 + 1)(l_2 + 1) l_2^{j-1}}{N^2}.\end{aligned} \tag{5}$$

Equations (3) – (5) together imply that the graphs are close to being independent (for many primes p). We expect that a similar result holds for $\Pr_{u,v}[d_1(u,v) = i$ and $d_2(u,v) = j]$ for $i > 1$.

References

1. N. Alon and V. D. Milman, λ_1 *isoperimetric inequalities for graphs, and superconcentrators*, J. Combin. Theory Ser. B **38** (1985), no. 1, 73 – 88.
2. J. Angel and R. Evans, *Diameters of finite upper half plane graphs*, J. Graph Theory **23** (1996), no. 2, 129 – 137.
3. J. Brzeziński, *On orders in quaternion algebras*, Comm. Algebra **11** (1983), no. 5, 501 – 522.
4. D. I. Cartwright, P. Solé, and A. Żuk, *Ramanujan geometries of type* $\tilde{\mathrm{A}}_n$, Discrete Math. **269** (2003), no. 1-3, 35 – 43.
5. D. X. Charles, E. Z. Goren, and K. E. Lauter, *Cryptographic hash functions from expander graphs*, J. Cryptology, to appear. DOI: 10.1007/s00145-007-9002-x.
6. D. X. Charles, K. Jain, and K. E. Lauter, *Signatures for network coding*, CISS 2006, 40th Conference on Information Sciences and Systems, available at `http://www288.pair.com/ciss/ciss/numbered/340.pdf`.
7. C. Consani and J. Scholten, *Arithmetic on a quintic threefold*, Internat. J. Math. **12** (2001), no. 8, 943 – 972.
8. L. Dembélé, *Quaternionic Manin symbols, Brandt matrices, and Hilbert modular forms*, Math. Comp. **76** (2007), no. 258, 1039 – 1057.
9. M. Eichler, *On theta functions of real algebraic number fields*, Acta Arith. **33** (1977), no. 3, 269 – 292.
10. S. S. Gelbart, *Automorphic forms on adèle groups*, Ann. of Math. Stud., vol. 83, Princeton Univ. Press, Princeton, NJ, 1975.
11. E. Z. Goren and K. E. Lauter, *Evil primes and superspecial moduli*, Int. Math. Res. Not. **2006**, Art. ID 53864.
12. E. Z. Goren and F. Oort, *Stratifications of Hilbert modular varieties*, J. Algebraic Geom. **9** (2000), 111 – 154.
13. B. H. Gross, *Heights and the special values of L-series*, Number Theory (Montréal, 1985) (H. Kisilevsky and J. Labute, eds.), CMS Conf. Proc., vol. 7, Amer. Math. Soc., Providence, RI, 1987, pp. 115 – 187.
14. S. Hoory, N. Linial, and A. Wigderson, *Expander graphs and their applications*, Bull. Amer. Math. Soc. (N.S.) **43** (2006), no. 4, 439 – 561.
15. H. Jacquet and R. P. Langlands, *Automorphic forms on* GL(2), Lecture Notes in Math., vol. 114, Springer, Berlin, 1970.
16. B. W. Jordan and R. Livné, *Integral Hodge theory and congruences between modular forms*, Duke Math. J. **80** (1995), no. 2, 419 – 484.
17. ———, *Ramanujan local systems on graphs*, Topology **36** (1997), no. 5, 1007 – 1024.
18. ———, *The Ramanujan property for regular cubical complexes*, Duke Math. J. **105** (2000), no. 1, 85 – 103.
19. A. Katamoto, *On 3rd and 4th moments of finite upper half plane graphs*, Finite Fields Appl. **13** (2007), no. 2, 249 – 258.
20. Y. Kitaoka, *Arithmetic of quadratic forms*, Cambridge Tracts in Math., vol. 106, Cambridge Univ. Press, Cambridge, 1993.
21. W.-C. W. Li, *Character sums and abelian Ramanujan graphs*, J. Number Theory **41** (1992), no. 2, 199 – 217.
22. ———, *Ramanujan hypergraphs*, Geom. Funct. Anal. **14** (2004), no. 2, 380 – 399.
23. R. Livné, *Communication networks and Hilbert modular forms*, Applications of Algebraic Geometry to Coding Theory, Physics and Computation (Eilat, 2001) (C. Ciliberto, F. Hirzebruch, R. Miranda, and M. Teicher, eds.), NATO Sci. Ser. II Math. Phys. Chem., vol. 36, Kluwer Acad. Publ., Dordrecht, 2001, pp. 255 – 270.
24. A. Lubotzky, *Discrete groups, expanding graphs and invariant measures*, with an appendix by J. D. Rogawski, Progr. Math., vol. 125, Birkhäuser, Basel, 1994.
25. A. Lubotzky, R. S. Phillips, and P. Sarnak, *Ramanujan graphs*, Combinatorica **8** (1988), no. 3, 261 – 277.

26. A. Lubotzky, B. Samuels, and U. Vishne, *Ramanujan complexes of type* $\tilde{\mathrm{A}}_d$, Israel J. Math. **149** (2005), 267 – 299.
27. M.-H. Nicole, *Superspecial abelian varieties, Theta series and the Jacquet – Langlands correspondence*, Ph.D. thesis, McGill University, 2005.
28. ———, *Superspecial abelian varieties and the Eichler basis problem for Hilbert modular forms*, J. Number Theory, to appear.
29. F. Oort, *Which abelian surfaces are products of elliptic curves*?, Math. Ann. **214** (1975), 35 – 47.
30. A. K. Pizer, *An algorithm for computing modular forms on* $\Gamma_0(N)$, J. Algebra **64** (1980), no. 2, 340 – 390.
31. ———, *Ramanujan graphs*, Computational Perspectives on Number Theory (Chicago, IL, 1995) (D. A. Buell and J. T. Teitelbaum, eds.), AMS/IP Stud. Adv. Math., vol. 7, Amer. Math. Soc., Providence, RI, 1998, pp. 159 – 178.
32. M. Rapoport, *Compactifications de l'espace de modules de Hilbert-Blumenthal*, Compositio Math. **36** (1978), no. 3, 255 – 335.
33. T. Shioda, *Supersingular* $K3$ *surfaces*, Algebraic Geometry (Copenhagen, 1978) (K. Lønsted, ed.), Lecture Notes in Math., vol. 732, Springer, Berlin, 1979, pp. 564 – 591.
34. J. H. Silverman, *The arithmetic of elliptic curves*, Grad. Texts in Math., vol. 106, Springer, New York, 1986.
35. J. Socrates and D. Whitehouse, *Unramified Hilbert modular forms, with examples relating to elliptic curves*, Pacific J. Math. **219** (2005), no. 2, 333 – 364.
36. A. Terras, *Are finite upper half plane graphs Ramanujan*?, Expanding Graphs (Princeton, NJ, 1992) (J. Friedman, ed.), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 10, Amer. Math. Soc., Providence, RI, 1993, pp. 125 – 142.
37. ———, *Survey of spectra of Laplacians on finite symmetric spaces*, Experiment. Math. **5** (1996), no. 1, 15 – 32.
38. A. Valette, *Graphes de Ramanujan et applications*, Séminaire Bourbaki, Vol. 1996/97, Astérisque, vol. 245, Exp. No. 829, 4, Soc. Math. France, Paris, 1997, pp. 247 – 276.
39. G. van der Geer, *Hilbert modular surfaces*, Ergeb. Math. Grenzgeb. (3), vol. 16, Springer, Berlin, 1988.
40. M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Math., vol. 800, Springer, Berlin, 1980.
41. L. C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Grad. Texts in Math., vol. 83, Springer, New York, 1997.
42. W. C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521 – 560.
43. W. C. Waterhouse and J. S. Milne, *Abelian varieties over finite fields*, 1969 Number Theory Institute (Stony Brook, 1969) (D. J. Lewius, ed.), Proc. Sympos. Pure Math., vol. 20, Amer. Math. Soc., Providence, RI, 1971, pp. 53 – 64.

Microsoft Live Labs, One Microsoft Way, Redmond, WA 98052, USA
E-mail address: cdx@microsoft.com

Department of Mathematics and Statistics, McGill University, 805 Sherbrooke St. W, Montreal, QC H3A 2K6, Canada
E-mail address: goren@math.mcgill.ca

Microsoft Research, One Microsoft Way, Redmond, WA 98052, USA
E-mail address: klauter@microsoft.com