MS/IP Studies in Advanced Mathematics
Volume 7, 1998

Ramanujan Graphs

Arnold K. Pizer

1 Introduction

The purpose of this paper is to give an explicit construction of a large class of Ramanujan graphs. A Ramanujan graph G is a finite, connected, k-regular graph with the property that the largest nontrivial eigenvalue of the adjacency matrix of G is as small as possible in an asymptotic sense. The precise definition is given in section 3 below. The eigenvalue bound forces such graphs to have high "magnification" (or "expansion" when they are bipartite) and as such they have many applications to the construction of networks and explicit algorithms. Intuitively, they are sparse graphs (in the sense that they have few edges) with the property that subsets of vertices always have many distinct neighbors. In addition to being Ramanujan, the graphs we construct also have large girth. The first constructions of Ramanujan graphs were given by Lubotzky, Phillips, and Sarnak [LPS86, LPS88] and independently by Margulis [Mar88]. Bien [Bie89] has written an excellent survey article on the subject. Our construction is based on the arithmetic of quaternion algebras and depends on the theory of Hecke operators and modular forms. Before giving the construction in sections 4 and 5, we develop some results on graph theory in section 2 and discuss general Ramanujan graphs in section 3.

It is a pleasure to dedicate this paper on Ramanujan Graphs to Oliver Atkin on the occasion of his retirement. Atkin's contribution to this area is explained in the paragraph preceding Theorem 5.2 below.

2 Graph Theory

A fundamental concept for us will be a *walk without backtracking* in a graph. In order to make this concept explicit, we follow Serre [Ser80].

Definition 2.1 A finite multigraph G consists of a finite set V of vertices of G, a finite set E of edges of G, and two maps

$$E \to V \times V, \quad e \mapsto (o(e), t(e))$$

and

$$E \to E, \quad e \mapsto \bar{e}$$

which satisfy the following conditions: for each $e \in E$, we have $\bar{\bar{e}} = e$, $\bar{e} \neq e$, and $o(e) = t(\bar{e})$.

An element e of E is called an (*oriented*) *edge* with $\bar{e}$ being it's *inverse* edge. The vertex $o(e)$ is the *origin* of e and $t(e)$ is the *terminus* of e. Two vertices v_0 and v_1 are *adjacent* if there exists an edge e with $o(e) = v_0$ and $t(e) = v_1$. An *orientation* of a

multigraph G is a subset E_+ of the edges E of G such that E is the disjoint union of E_+ and $\overline{E_+}$. The *order* of G is the number of vertices in G and is denoted by $|G|$.

Thus our multigraphs are undirected, but may have "multiple edges" and/or "loops". In an obvious manner we can represent a graph as a diagram. The diagram in Figure

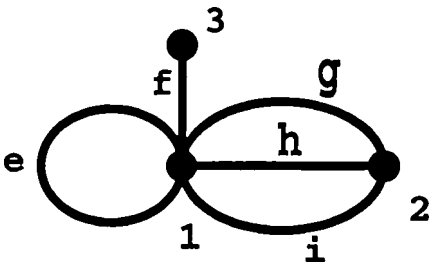

Figure 1:

1 represents a multigraph with vertices 1,2,3 and edges $e,\bar{e},f,\bar{f},g,\bar{g},h,\bar{h},i$, and $\bar{i}$. This diagram does not tell us e.g. whether 1 is the origin or terminus of f, but if necessary we could assign "directions" to the edges which would give an orientation and provide the information on origins and termini. A *walk* W in a multigraph G is a sequence of (oriented) edges $e_1,\ldots,e_r$ such that $t(e_i) = o(e_{i+1})$ for $1 \leq i \leq r-1$. If $v_0 = o(e_1)$ and $v_r = t(e_r)$, we say W is a walk from v_0 to v_r of *length* r. If for any i, $1 \leq i \leq r-1$, $e_{i+1} = \bar{e}_i$, we say that W contains a *backtracking*. A *walk without backtracking (a w.b. walk)* is a walk that does not contain any backtracking.

Let G be a finite multigraph of order n with vertices $v_1,\ldots,v_n$. We denote by $a_{ij}^{(r)}$ the number of w.b. walks of length r from v_i to v_j in G and put $A_r = (a_{ij}^{(r)})$. The A_r are symmetric n by n matrices with nonnegative integer entries and even diagonal entries. A_1 is the *adjacency* matrix of G. G is determined by A_1 and conversely every symmetric n by n matrix with nonnegative integer entries and even diagonal entries determines a multigraph. It is clear that G has no loops if and only if $\operatorname{tr} A_1 = 0$ and that G has neither loops nor multiple edges if and only if $\operatorname{tr} A_2 = 0$. We call a multigraph with neither loops nor multiple edges a *graph* or a *simple graph* if we want to emphasize the point. The *diameter* of G is the least d such that there is a walk of length less than or equal to d from any vertex to any other vertex of G, i.e. such that $I + A_1 + \cdots + A_d$ has all nonzero entries. A multigraph with a finite diameter is said to be *connected*. The *girth* of G is the length of the shortest "cycle" of G, i.e. the least positive g such that $\operatorname{tr} A_g \neq 0$. The *degree* of a vertex v_i, $\deg(v_i)$, is the number of edges originating at v_i, i.e. the sum of the i^{th} row of A_1. For example if G is the multigraph in Figure 1, then $\deg(v_1) = 6$. Denote by D the (diagonal) degree matrix with diagonal entries $\deg(v_1),\ldots,\deg(v_n)$ and by I the n by n identity matrix. The A_r are determined recursively by

Proposition 2.1 *Let G be a finite multigraph of order n with vertices $v_1,\ldots,v_n$.*

Then

$$\begin{aligned} A_1A_1 &= A_2 + D \\ A_rA_1 &= A_{r+1} + A_{r-1}(D - I) \qquad \textit{for} \quad r \geq 2. \end{aligned} \tag{1}$$

Proof Let $d_i = \deg(v_i)$. First consider the case $r \geq 2$. Let v_i and v_j be two (not necessarily distinct) vertices of G and let $e_1, e_2, \ldots, e_{r+1}$ be any w.b. walk of length $r+1$ from v_i to v_j. Then $e_1, e_2, \ldots, e_r$ is a w.b. walk of length r from v_i to $v_k = o(e_{r+1})$ for some $k = 1, 2, \ldots, n$ and e_{r+1} is a w.b. walk of length 1 from v_k to v_j. Thus all possible w.b. walks of length $r+1$ are counted in the sum $\sum_{k=1}^{n} a_{ik}^{(r)} a_{kj}^{(1)}$ and clearly all counted walks are distinct. The only question is how many of the counted walks have backtracking. Let $f_1, \ldots, f_r$ denote a w.b. walk counted in $a_{ik}^{(r)}$ and f_{r+1} a w.b. walk counted in $a_{kj}^{(1)}$. Then if $f_1, f_2, \ldots, f_{r+1}$ has a backtracking, we must have $f_r = \bar{f}_{r+1}$. Thus $f_1, \ldots, f_{r-1}$ is a w.b. walk of length $r-1$ from v_i to v_j. If g_r is any of the d_j edges originating from v_j *except* $\bar{f}_{r-1}$, then $f_1, \ldots, f_{r-1}, g_r$ is a w.b. walk and $f_1, \ldots, f_{r-1}, g_r, \bar{g}_r$ is a walk counted in $\sum_{k=1}^{n} a_{ik}^{(r)} a_{kj}^{(1)}$ which contains a backtracking and all such walks are of this form. Thus $\sum_{k=1}^{n} a_{ik}^{(r)} a_{kj}^{(1)} = a_{ij}^{(r+1)} + a_{ij}^{(r-1)}(d_j - 1)$ if $r \geq 2$. Note that if $d_j = 0$ so that there is no possible edge of the type $\bar{f}_{r-1}$, the equation $(\sum_{k=1}^{n} a_{ik}^{(r)} 0 = 0 + 0(0-1))$ still holds. If $r = 1$, the analysis is identical except that since there is no f_{r-1}, there is no restriction on g_r being equal to $\bar{f}_{r-1}$. □

Example 1 If G is the graph in Figure 1, then D has diagonal entries 6, 3, and 1 and

$$A_1 = \begin{pmatrix} 2 & 3 & 1 \\ 3 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \quad A_2 = \begin{pmatrix} 8 & 6 & 2 \\ 6 & 6 & 3 \\ 2 & 3 & 0 \end{pmatrix} \quad A_3 = \begin{pmatrix} 26 & 18 & 8 \\ 18 & 18 & 6 \\ 8 & 6 & 2 \end{pmatrix}$$

More simply, if G is the graph given in Figure 2 below, then

$$D = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix} \quad A_1 = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} \quad A_2 = \begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix} \quad \text{and} \quad A_r = \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}$$

for all $r \geq 3$.

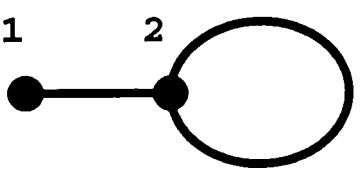

Figure 2:

In order to simplify the recursion relation (1), we define matrices B_r as follows:

$$\begin{aligned} B_{-1} = 0, \quad B_0 = I, \quad B_1 = A_1 \qquad &\text{and} \\ B_rB_1 = B_{r+1} + B_{r-1}(D - I) \qquad &\text{for} \quad r \geq 0. \end{aligned} \tag{2}$$

The relation between the A_r and B_r is given by

Proposition 2.2

$$A_r = B_r - B_{r-2} \qquad \text{for all } r \geq 1 \tag{3}$$

$$\begin{aligned} B_r &= A_r + A_{r-2} + \cdots + A_1 \qquad \text{if } r \text{ is odd} \quad \text{and} \\ B_r &= A_r + A_{r-2} + \cdots + I \qquad \text{if } r \text{ is even.} \end{aligned} \tag{4}$$

Proof (3) follows easily by induction and (4) is a consequence of (3). □

Remark 2.1 Assume G is a k-regular multigraph (i.e. the degree of each vertex is k) with $k = p + 1$ for some prime p. Then (2) becomes

$$B_r B_1 = B_{r+1} + pB_{r-1} \qquad \text{for} \quad r \geq 0. \tag{5}$$

This is exactly the recursion relation satisfied by the Hecke operators $B_r = T_{p^r}$ acting on a space of modular forms of weight 2 on $\Gamma_0(N)$ when $p \nmid N$. Thus if we are able to associate a $p+1$ regular graph G to the Hecke operator T_p by giving a suitable matrix representation $B_1 = A_1$ of T_p, the action of the Hecke operators T_{p^r} will, by (3), determine the A_r and hence give information about G. For example a trace formula for T_{p^r} immediately yields information on the girth of G. This is precisely what we do in section 5 below by showing that Brandt matrices associated to certain orders in quaternion algebras provide a suitable representation. By varying the spaces (of theta series) on which the Hecke operators act we will obtain a large family of interesting (e.g. Ramanujan with relatively large girth) graphs. The Petersson Ramanujan Conjecture implies that the graphs we obtain are in fact Ramanujan graphs. If m is not prime, we will also be able to associate a graph to T_m. These graphs will in general be "almost Ramanujan".

3 Ramanujan and Magnifying Graphs

In this section we assume that all graphs G are simple, finite, connected, and k-regular. For any subset X of the vertices V of G, we denote by $\partial X = \{v \in V, v \notin X \mid v \text{ is adjacent to some } x \in X\}$ the *boundary* of X.

Definition 3.1 G is an (n,k,c)-*magnifier* if $|G| = n$ and for every subset X of V with $|X| \leq n/2$, we have $|\partial X| \geq c|X|$. The largest c for which G is an (n,k,c)-magnifier is called the *magnification* of G.

Obviously $0 \leq c \leq 1$ or $\frac{n+1}{n-1}$ depending on whether n is even or odd. If G is bipartite, we have the closely related concept of *expansion*.

Definition 3.2 G is an (n,k,c)-*expander* if G is a bipartite graph on the set of vertices I (inputs) and O (outputs) where $|I| = |O| = n$ and for every subset X of I, we have

$$|\partial X| \geq \left(1 + c\left(1 - \frac{|X|}{n}\right)\right)|X|.$$

The largest c for which G is an (n,k,c)-expander is called the *expansion* of G.

The double cover of an (n,k,c)-magnifier is an $(n,k+1,c)$-expander (see Alon [Alo86]). Note that there are several different definitions of expansion and magnification in the literature. They all measure essentially the same thing.

A well known problem is to fix k and $c > 0$ and then to construct an infinite family of (n,k,c)-expanders G_i with $n_i = |G_i| \to \infty$ and $n_i/n_{i+1} \to 1$ as $i \to \infty$. The larger the c, the better. For example, such a construction is used in the parallel sorting algorithm of Ajtai, Komlos, and Szemereci [AKS83]. One can prove the existence of such families by probabilistic means but explicit constructions are more difficult. Margulis in [Mar75] was the first to give an explicit construction with $c > 0$, but undetermined. Using a related construction, Gabber and Galil [GG81] gave a family of $(n_i, 5, c)$-expanders with $c = \frac{2-\sqrt{3}}{4} \approx .067$.

The magnification or expansion of a graph G is related to the eigenvalues of the adjacency matrix A_1 of G. If G is a k-regular connected graph of order n, then k is an eigenvalue of G of multiplicity one and the other eigenvalues $\mu_1, \ldots, \mu_{n-1}$ satisfy $k > \mu_1 \geq \mu_2 \geq \cdots \geq \mu_{n-1} \geq -k$. $-k$ is an eigenvalue if and only if G is bipartite in which case the eigenvalues are symmetric about 0 (see e.g. [Bol79]).

Theorem 3.1 *Let the notation be as above.*

1. *G is an (n,k,c)-magnifier with $c = \frac{2(k-\mu_1)}{3k-2\mu_1}$*
2. *If G is an (n,k,c)-magnifier, then $\mu_1 \leq k - \frac{c^2}{4+2c^2}$*

Proof Both of the above results are due to Alon [Alo86]. A result similar to (1) was first proved by Tanner [Tan84]. □

This result says very roughly that G has high magnification if and only if μ_1 is small. A_1 can be viewed as an averaging operator on functions on G and $\Delta = kI - A_1$ is analogous to the Laplacian operator. Thus μ_1 corresponds to the smallest positive eigenvalue $\lambda_1 = k - \mu_1$ of Δ and the relations between μ_1 and the magnification of a graph are analogous to isoperimetric inequalities in differential geometry (see Bien [Bie89]and Alon [Alo86]).

By Theorem 3.1, we want to construct families of k-regular graphs with μ_1 small. The question arises as to how small μ_1 can be. This is answered by the following result of Alon and Boppana. First let $\mu = \mu(G) = \max(|\mu_i|)$ where μ_i runs over all μ_i with $|\mu_i| \neq k$. μ small implies μ_1 is small and $\mu = \mu_1$ if G is bipartite.

Theorem 3.2 *If G_i is a family of k-regular connected multigraphs with k fixed and $n_i = |G_i| \to \infty$, then* $\liminf_{n_i \to \infty} \mu(G_i) \geq 2\sqrt{k-1}$.

This was proved by Alon and Boppana [Alo86]. The first published proof appeared in [LPS88]. Another proof, using random walks on graphs, appears in [Lob94]. Still another proof can be found in [Nil91]. Here we present a simple proof based on the theory of the A_r matrices.

Proof Let $\ell = k - 1$ and let G denote any k-regular connected multigraph of order n with adjacency matrix $A_1 = B_1$. Using (2), a straight forward induction argument shows that

$$B_1^m = \sum_{0 \le r \le m/2} \left[\binom{m}{r} - \binom{m}{r-1} \right] \ell^r B_{m-2r} \tag{6}$$

for all positive integers m. Here $\binom{m}{r}$ is the binomial coefficient. In fact (6) is Exercise 3.27′ on page 65 of [Shi71] when $B_1 = T(p)$. From (4), we see that all entries of the B_s are nonnegative. Letting $m = 2s$, we see from (6) that

$$\operatorname{tr} B_1^{2s} \ge \left[\binom{2s}{s} - \binom{2s}{s-1} \right] \ell^s \operatorname{tr} B_0 = \frac{(2s)!}{s!(s+1)!} \ell^s n$$

Except for k and possibly $-k$, all eigenvalues of B_1 have absolute value less than or equal to $\mu(G) = \mu_n < k$. Hence $2k^{2s} + (n-2)\mu_n^{2s} \ge \operatorname{tr} B_1^{2s}$ so that

$$\mu_n^{2s} \ge \frac{(2s)!}{s!(s+1)!} \ell^s \frac{n}{n-2} - \frac{2k^{2s}}{n-2} = \binom{2s}{s} \ell^s \frac{n}{n-2} \frac{1}{s+1} - \frac{2k^{2s}}{n-2}.$$

Now $(2s+1)\binom{2s}{s} \ge (1+1)^{2s} \ge \binom{2s}{s}$ so that $\lim_{s\to\infty} \binom{2s}{s}^{\frac{1}{2s}} = 2$ and the result follows. □

Remark 3.1 Suppose we fix p and are able to associate to the Hecke operator T_p a family of $p+1$ regular graphs G_i as indicated in Remark 2.1 above. Further suppose that except for the eigenvalues $k = p+1$ and possibly $-k = -p-1$, all other eigenvalues μ_j of T_p arise from eigenforms which are cuspforms of weight 2. Then the Ramanujan Petersson Conjecture implies that $|\mu_j| \le 2\sqrt{p} = 2\sqrt{k-1}$ so that the family of graphs G_i would be optimal in having $\mu(G_i)$ asymptotically as small as possible.

This leads us to the definition of Ramanujan graphs. The name comes from the fact that the first constructions, given independently by Lubotzky-Phillips-Sarnak [LPS86, LPS88] and Margulis [Mar88], used the Ramanujan Conjecture to prove that the graphs constructed were in fact Ramanujan. The interest in them comes from the fact that a family of k-regular Ramanujan graphs G_i is optimal with respect to the size of $\mu(G_i)$ and consequences of this property for the magnification, diameter, and independence number of the graphs (see [LPS88]).

Definition 3.3 A k-regular connected graph G is said to be *Ramanujan* if $\mu(G) \le 2\sqrt{k-1}$

4 Quaternion Algebras and Brandt Matrices

We need to review some well known facts about quaternion algebras. Let $\mathbb{A}$ be a *quaternion algebra* over $\mathbb{Q}$. Then $\mathbb{A}$ has a standard basis 1, I, J, K over $\mathbb{Q}$ where the

multiplication in $\mathbb{A}$ is given in terms of the basis as follows: 1 is the identity, $I^2 = a$, $J^2 = b$, and $IJ = K = -JI$ where a and b are some nonzero elements of $\mathbb{Q}$. Conversely, given such a and b, the above basis and relations determine a quaternion algebra over $\mathbb{Q}$. We denote this quaternion algebra by (a, b). A *lattice* on $\mathbb{A}$ is a free $\mathbb{Z}$-submodule of $\mathbb{A}$ of rank 4 and an *order* $\mathcal{O}$ of $\mathbb{A}$ is lattice which is also a subring containing the identity. If ℓ is a finite prime, then $\mathcal{O}_\ell = \mathcal{O} \otimes_Z \mathbb{Z}_\ell$ is an order of the quaternion algebra $\mathbb{A}_\ell = \mathbb{A} \otimes_Q \mathbb{Q}_\ell$ over $\mathbb{Q}_\ell$. For purposes of simplicity and easy computability, we will henceforth restrict our attention in this paper to quaternion algebras $\mathbb{A}$ over $\mathbb{Q}$ which ramify precisely at a single finite prime q and ∞. This means that $\mathbb{A}_q$ and $\mathbb{A}_\infty = \mathbb{A} \otimes_Q \mathbb{R}$ are division algebras and $\mathbb{A}_\ell$ is a (split) matrix algebra for all finite primes $\ell \neq q$. Let M be a positive integer prime to q. We need to consider orders of *level* qM and q^2M of $\mathbb{A}$. Before we begin, things will be clearer for the reader if one realizes that from an arithmetic point of view the (unique) maximal order in the (division) quaternion algebra $\mathbb{A}_q$ is really analogous to the nonmaximal order

$$\begin{pmatrix} \mathbb{Z}_q & \mathbb{Z}_q \\ q\mathbb{Z}_q & \mathbb{Z}_q \end{pmatrix}$$

of the (split) quaternion algebra $\mathrm{Mat}(2, \mathbb{Q}_q)$ (see e.g. [Piz80b]).

Definition 4.1 Let $\mathbb{A}$ be a quaternion algebra ramified precisely at a single finite prime q and ∞ and let M be a positive integer prime to q. An order $\mathcal{O}$ of $\mathbb{A}$ is said to have level qM if $\mathcal{O}_q$ is maximal in $\mathbb{A}_q$ and for all finite primes $\ell \neq q$, $\mathcal{O}_\ell$ is isomorphic to the order

$$\begin{pmatrix} \mathbb{Z}_\ell & \mathbb{Z}_\ell \\ M\mathbb{Z}_\ell & \mathbb{Z}_\ell \end{pmatrix}$$

of $\mathbb{A}_\ell$. For an odd prime q, $\mathcal{O}$ is said to have level q^2M if $\mathcal{O}_q$ has index q in the maximal order of $\mathbb{A}_q$ and $\mathcal{O}_\ell$ satisfies the same conditions as above for all finite primes $\ell \neq q$.

Remark 4.1 Orders of level q are maximal orders and orders of level qM with M squarefree are known as Eichler orders. Orders of level qM and q^2M are part of the much larger classes of special and primitive orders (see [HPS89], [Brz90], [Jun91]) all of which could be used in the construction of Ramanujan graphs (see Remark 2 in [Piz90]).

The following three propositions give explicit constructions of quaternion algebras and orders of level q and q^2.

Proposition 4.1 *The (unique) quaternion algebra* $\mathbb{A}$ *over* $\mathbb{Q}$ *ramified precisely at* q *and* ∞ *is given by*

$$\begin{aligned} \mathbb{A} &= (-1, -1) \quad \text{if} \quad q = 2 \\ \mathbb{A} &= (-1, -q) \quad \text{if} \quad q \equiv 3 \pmod 4 \\ \mathbb{A} &= (-2, -q) \quad \text{if} \quad q \equiv 5 \pmod 8 \\ \mathbb{A} &= (-q, -r) \quad \text{if} \quad q \equiv 1 \pmod 8 \end{aligned}$$

where r *is a prime with* $r \equiv 3 \pmod 4$ *and the Legendre symbol* $\left(\frac{q}{r}\right) = -1$.

Proposition 4.2 *Let $\mathbb{A} = (a, b)$ be the quaternion algebra given by Proposition 4.1 above. Then an order of level q (i.e. a maximal order) of $\mathbb{A}$ is given by the $\mathbb{Z}$-basis:*

$$\begin{aligned}
&\frac{1}{2}(1+I+J+K), I, J, K && \text{if } q = 2 \\
&\frac{1}{2}(1+J), \frac{1}{2}(I+K), J, K && \text{if } q \equiv 3 \pmod 4 \\
&\frac{1}{2}(1+J+K), \frac{1}{4}(I+2J+K), J, K && \text{if } q \equiv 5 \pmod 8 \\
&\frac{1}{2}(1+J), \frac{1}{2}(I+K), \frac{1}{r}(J+aK), K && \text{if } q \equiv 1 \pmod 8
\end{aligned}$$

where a is some integer such that $r|(a^2q+1)$.

Proposition 4.3 *Let $\mathbb{A} = (a, b)$ be the quaternion algebra given by Proposition 4.1 above. Then for $q > 2$ an order of level q^2 of $\mathbb{A}$ is given in by the $\mathbb{Z}$-basis:*

$$\begin{aligned}
&\frac{1}{2}(1+J), \frac{1}{2}(qI+K), J, K && \text{if } q \equiv 3 \pmod 4 \\
&\frac{1}{2}(1+J+K), \frac{q}{4}(I+2J+K), J, K && \text{if } q \equiv 5 \pmod 8 \\
&\frac{1}{2}(1+qJ), \frac{1}{2}(I+K), \frac{q}{r}(J+aK), K && \text{if } q \equiv 1 \pmod 8
\end{aligned}$$

where a is some integer such that $r|(a^2q+1)$.

Proofs Once discovered (with the aid of a computer), proving these results is straight forward. Propositions 4.1 and 4.2 are proved in section 5 of [Piz80b] and Proposition 4.3 can be checked by similar methods.

□

Note that starting with an order of level q or q^2, orders of level qM and q^2M can be constructed by the method given in section 5 of [Piz80b].

Let $\mathcal{O}$ be an order of level $N = qM$ or q^2M and let m be a positive integer relatively prime to N. Then the Hecke operator T_m acts on a space of theta series (which are modular forms of weight 2 on $\Gamma_0(N)$) associated to $\mathcal{O}$ and this action has an explicit matrix representation given by the Brandt matrix $B(m) = B(N; m)$ ([Eic73, HS73, Piz80a, Piz80b, HPS89b]). We recall the definition here (see [Piz80b] for more details). Let $I_1, \ldots, I_H$ be representatives of all the distinct left $\mathcal{O}$-ideal classes. Here $H = H(N)$, the class number of $\mathcal{O}$, is given by

Proposition 4.4 *The class number H of $\mathcal{O}$ is given by*

$$\begin{aligned} H(qM) = &\frac{q-1}{12} M \prod_{\ell \mid M} (1 + 1/\ell) \\ &+ \begin{cases} \frac{1}{4}\left(1 - \left(\frac{-4}{q}\right)\right) \prod_{\ell \mid M} \left(1 + \left(\frac{-4}{\ell}\right)\right) & \text{if } 4 \nmid M \\ 0 & \text{if } 4 \mid M \end{cases} \\ &+ \begin{cases} \frac{1}{3}\left(1 - \left(\frac{-3}{q}\right)\right) \prod_{\ell \mid M} \left(1 + \left(\frac{-3}{\ell}\right)\right) & \text{if } 9 \nmid M \\ 0 & \text{if } 9 \mid M \end{cases} \end{aligned} \tag{7}$$

if $\mathcal{O}$ has level qM and by

$$H(q^2 M) = \frac{q^2-1}{12} M \prod_{\ell \mid M} (1 + 1/\ell) + \begin{cases} 0 & \text{if } q \geq 5 \\ \frac{4}{3} \prod_{\ell \mid M} \left(1 + \left(\frac{-3}{\ell}\right)\right) & \text{if } q = 3 \end{cases} \tag{8}$$

if $\mathcal{O}$ has level $q^2 M$ where $q \geq 3$. Here the product is over all primes ℓ dividing M and $\left(\frac{*}{*}\right)$ is the Kronecker symbol. In particular $\left(\frac{-4}{2}\right) = \left(\frac{-3}{3}\right) = 0$ and $\left(\frac{-3}{2}\right) = -1$.

Proof For (7) see Theorem 1.12 of [Piz80b] and for (8) see Theorem 4.18 of [Piz80a]. □

Let $b_{ij}(m)$ denote e_j^{-1} times the number of α in $I_j^{-1} I_i$ with $\mathrm{N}(\alpha) = m\,\mathrm{N}(I_i)/\mathrm{N}(I_j)$. Here e_j is the number of units in the right order of I_j and N( ) denotes the reduced norm of $\mathbb{A}$. It is clear that the $b_{ij}(m)$ are integers. The Brandt matrix $B(m)$ is the H by H matrix with $b_{ij}(m)$ as the $i^{\text{th}}, j^{\text{th}}$ entry. Up to conjugation by a permutation matrix, the Brandt matrices $B(m) = B(N; m)$ depend only on the level N of $\mathcal{O}$, not on the order $\mathcal{O}$ nor the ideal class representatives $I_1, \ldots, I_H$ used in the definition (see Propositions 4.2 and 4.3 in [Piz80a]).

Once an order of level qM or $q^2 M$ is constructed as above, ideal class representatives $I_1, \ldots, I_H$ and the associated Brandt matrices $B(m)$ can be constructed by the algorithm given in [Piz80b].

Proposition 4.5 *Let $B(m) = (b_{ij}(m))$ be a Brandt matrix as above. Then*

$$e_j b_{ij}(m) = e_i b_{ji}(m) \qquad \text{for all } i, j \quad 1 \leq i, j \leq H \text{ and} \tag{9}$$

$$\sum_{j=1}^{H} b_{ij}(m) = b(m) \text{ (say) is independent of } i. \tag{10}$$

Further, if m is relatively prime to qM, then $b(m) = \sigma_1(m)$ where $\sigma_r(m) = \sum_{d \mid m} d^r$, the sum being over all positive divisors of m.

Proof See Lemma 2.18 of [Piz80b]. $b(m)$ is just the number of integral left $\mathcal{O}$-ideals of norm m and calculating $b(m)$ reduces to local calculations. If ℓ is relatively prime to qM, then $\mathcal{O}_\ell \cong \mathrm{Mat}(2, \mathbb{Z}_\ell)$ and the number of left $\mathcal{O}_\ell$-ideals of norm ℓ^r is easily seen to

be $1+\ell+\cdots+\ell^r = \sigma_1(\ell^r)$. Thus if m is relatively prime to qM, we have $b(m) = \sigma_1(m)$. □

Our aim is to show that certain Brandt matrices $B(m)$ are adjacency matrices of Ramanujan graphs. (9) says that if all e_j are equal, then $B(m)$ is a symmetric matrix and so is a candidate for an adjacency matrix. (10) says that, assuming all other conditions are satisfied, $B(m)$ is the adjacency matrix of a $b(m)$-regular graph. The following proposition tells us when the $B(m)$ are symmetric.

Proposition 4.6 *A Brandt matrix $B(qM;m)$ associated to an order of level qM is symmetric if*

$$E(qM) = \begin{cases} \frac{1}{4}\left(1-\left(\frac{-4}{q}\right)\right)\prod_{\ell|M}\left(1+\left(\frac{-4}{\ell}\right)\right) & \text{if } 4\nmid M \\ 0 & \text{if } 4|M \end{cases} + \begin{cases} \frac{1}{3}\left(1-\left(\frac{-3}{q}\right)\right)\prod_{\ell|M}\left(1+\left(\frac{-3}{\ell}\right)\right) & \text{if } 9\nmid M \\ 0 & \text{if } 9|M \end{cases} \tag{11}$$

is equal to 0. A Brandt matrix $B(q^2M;m)$ associated to an order of level q^2M is symmetric if

$$E(q^2M) = \begin{cases} 0 & \text{if } q \geq 5 \\ \frac{4}{3}\prod_{\ell|M}\left(1+\left(\frac{-3}{\ell}\right)\right) & \text{if } q = 3 \end{cases} \tag{12}$$

is equal to 0. In particular, all Brandt matrices $B(qM;m)$ associated to orders of level qM are symmetric if $q \equiv 1 \pmod{12}$ and all Brandt matrices $B(q^2M;m)$ associated to orders of level q^2M are symmetric if $q \geq 5$.

Proof First we recall that the *Mass* of an order is defined by $M = M(N) = \sum_{i=1}^{H} \frac{2}{e_i}$ and depends only on the level N of the order. Also note that all $e_i \geq 2$ since certainly ± 1 are units in all orders. Now first consider the case of orders of level qM. From Propositions 25 of [Piz76a] and (7) above, we see that $H(qM) = M(qM) + E(qM)$. Hence all $e_i = 2$ if and only if $H(qM) = M(qM)$ if and only if $E(qM) = 0$. The proof for orders of level q^2M is identical except that the formula for the mass is given by Theorem 3.4 of [Piz80a]. □

Proposition 4.7 *Denote by $B(m) = B(qM;m)$ the Brandt matrices associated to an order of level $qM = N$. Assume m, m', and p are relatively prime to N. Further, assume $E(qM) = 0$. Then*

1. $\sum_{j=1}^{H} b_{ij}(m) = \sigma_1(m)$ *for all* i, $1 \leq i \leq H$
2. *The $B(m)$ form a commuting family of symmetric diagonalizable matrices which satisfy the following relations:*

$$B(m)B(m') = \sum_{d|(m,m')} dB(mm'/d^2) \qquad \textit{in particular}$$

$$B(m)B(m') = B(mm') \qquad \text{if } (m,m') = 1$$

$$B(p^r)B(p^s) = \sum_{k=0}^{\min\{r,s\}} p^k B(p^{r+s-2k}) \qquad \text{if } p \text{ is prime}$$

3. *$\mu_0 = \sigma_1(m)$ is an eigenvalue of $B(m)$ and the other eigenvalues μ_i, $1 \le i \le H-1$ satisfy $|\mu_i| \le \sigma_0(m)\sqrt{m}$.*

Proof Proposition 4.5 shows that the row sums for $B(m)$ are $\sigma_1(m)$ and Proposition 4.6 implies the $B(m)$ are symmetric matrices. Also the relations in part 2. show that the Brandt matrices satisfy the same recursion relations as the Hecke operators. For a proof, see Theorem 2 of Eichler [Eic73]. This brings us to the critical part 3. Let $\mu_0 = \sigma_1(m)$. Then μ_0 is an eigenvalue of $B(m)$ and Theorem 2.21 of [Piz80b] shows that all other eigenvalues of $B(m)$ arise from the action of the Hecke operator T_m on cuspforms of weight 2, and thus by the Ramanujan Petersson Conjecture (proved by Deligne [Del74] and Eichler [Eic54]) all other eigenvalues satisfy the Ramanujan bound $|\mu_i| \le \sigma_0(m)\sqrt{m}$ (see e.g. [Kob84], p.164).

□

Proposition 4.8 *Denote by $B(m) = B(q^2M; m)$ the Brandt matrices associated to an order of level $q^2M = N$. Assume m, m', and p are relatively prime to N. Further, assume $E(q^2M) = 0$, i.e. $q \ge 5$ or M is divisible by 2 or by a prime $\ell \equiv 2 \pmod 3$. Then the ideals $I_1, \ldots, I_H$ can be ordered so that, simultaneously for all m,*

$$B(m) = \begin{pmatrix} C(m) & 0 \\ 0 & C(m) \end{pmatrix} \qquad \left(\text{resp. } \begin{pmatrix} 0 & D(m) \\ D(m) & 0 \end{pmatrix}\right)$$

if m is a quadratic residue (resp. nonresidue) mod q. Further

1. *$C(m) = (c_{ij}(m))$ and $D(m) = (d_{ij}(m))$ are $H/2$ by $H/2$ symmetric matrices.*
2. *If m is a quadratic residue mod q then $\sum_{j=1}^{H/2} c_{ij}(m) = \sigma_1(m)$ for all i, $1 \le i \le H/2$ while if m is a quadratic nonresidue mod q then $\sum_{j=1}^{H/2} d_{ij}(m) = \sigma_1(m)$ for all i, $1 \le i \le H/2$.*
3. *The $B(m)$ form a commuting family of diagonalizable matrices which satisfy the following relations:*

$$B(m)B(m') = \sum_{d|(m,m')} dB(mm'/d^2) \qquad \text{in particular}$$

$$B(m)B(m') = B(mm') \qquad \text{if } (m,m') = 1$$

$$B(p^r)B(p^s) = \sum_{k=0}^{\min\{r,s\}} p^k B(p^{r+s-2k}) \qquad \text{if } p \text{ is prime}$$

4. *If m is a quadratic residue mod q then $\mu_0 = \sigma_1(m)$ is an eigenvalue of $C(m)$ and the other eigenvalues μ_i, $1 \leq i \leq H/2 - 1$ satisfy $|\mu_i| \leq \sigma_0(m)\sqrt{m}$. If m is a quadratic nonresidue mod q then $\mu_0 = \sigma_1(m)$ and $\mu_{H-1} = -\sigma_1(m)$ are eigenvalues of $B(m)$ and the other eigenvalues μ_i, $1 \leq i \leq H - 2$ satisfy $|\mu_i| \leq \sigma_0(m)\sqrt{m}$.*

Proof That the ideals $I_1, \ldots, I_H$ can be ordered so that, simultaneously for all m,

$$B(m) = \begin{pmatrix} C(m) & 0 \\ 0 & C(m) \end{pmatrix} \qquad (\text{resp. } \begin{pmatrix} 0 & D(m) \\ D(m) & 0 \end{pmatrix} \ )$$

if m is a quadratic residue (resp. nonresidue) mod q is proved in Theorems 5.15 and 5.18 of [Piz80a]. From the proof of Proposition 4.6, under the given hypotheses, we see that all $e_i = 2$. It follows from Lemma 5.23 of [Piz80a] that $C(m)$ and $D(m)$ are symmetric matrices. We already know that the row sums for $B(m)$ are $\sigma_1(m)$ and this establishes part 2. Part 3. follows as in the proof of Proposition 4.7 above. This brings us to part 4. Let $\mu_0 = \sigma_1(m)$. Then Lemma 5.24 of [Piz80a] shows that μ_0 is an eigenvalue of both $C(m)$ and $D(m)$. Hence $\pm\sigma_1(m)$ are both eigenvalues of $B(m)$ when m is a quadratic nonresidue mod q. By Theorem 5.34 of [Piz80a], all other eigenvalues of $B(m)$ arise from the action of the Hecke operator T_m on cuspforms of weight 2, and thus by the Ramanujan Petersson Conjecture satisfy the bound $|\mu_i| \leq \sigma_0(m)\sqrt{m}$ as above.

□

Let us introduce the following

Notation Let $B(m) = B(qM; m)$ be as in Proposition 4.7 and further assume all diagonal entries of $B(m)$ are even. Then $B(m)$ is the adjacency matrix of a $\sigma_1(m)$-regular nonbipartite multigraph of order $H(qM)$ which we denote by $G(qM; m)$. Assume m is a quadratic residue mod q, $C(m)$ is as in Proposition 4.8, and all diagonal entries of $C(m)$ are even. Then $C(m)$ is the adjacency matrix of a $\sigma_1(m)$-regular nonbipartite multigraph of order $H(q^2M)/2$ which we denote by $G(q^2M; m)$. Finally assume m is a quadratic nonresidue mod q and $B(m) = B(q^2M; m)$ is as in Proposition 4.8. Then $B(m)$ is the adjacency matrix of a $\sigma_1(m)$-regular bipartite multigraph of order $H(q^2M)$ which we also denote by $G(q^2M; m)$.

The final tool we require for the construction of Ramanujan graphs is a trace formula for the Brandt matrices $B(m)$.

Proposition 4.9 *The trace of a Brandt matrix $B(m)$ associated to an order $\mathcal{O}$ of level $N = qM$ or q^2M is given by*

$$\begin{aligned} \operatorname{tr} B(m) = &\sum_s a(s) \sum_f b(s,f) \prod_{\ell | N} c(s,f,\ell) \\ &+ \delta(\sqrt{m}) Mass(\mathcal{O}) \end{aligned} \tag{13}$$

where

$$\delta(\sqrt{m}) = \begin{cases} 1 & \text{if } m \text{ is a perfect square} \\ 0 & \text{otherwise} \end{cases}$$

$$Mass(\mathcal{O}) = \begin{cases} \frac{q-1}{12} M \prod_{\ell | M}(1+1/\ell) & \\ & \text{if } \mathcal{O} \text{ has level } qM \\ \frac{q^2-1}{12} M \prod_{\ell | M}(1+1/\ell) & \\ & \text{if } \mathcal{O} \text{ has level } q^2 M \end{cases}$$

The meaning of s, $a(s)$, $b(s,f)$, and $c(s,f,\ell)$ are given as follows:

Let s run over all integers such that $s^2 - 4m$ is negative. Hence with some positive *integer t and* squarefree negative *integer r, $s^2 - 4m$ has one of the following forms:*

$$s^2 - 4m = \begin{cases} t^2 r & 0 > r \equiv 1 \pmod 4) \\ t^2 4r & 0 > r \equiv 2,3 \pmod 4) \end{cases}.$$

Put $a(s) = \frac{1}{2}$.

For each fixed s let f run over all positive divisors of t.

$$b(s,f) = h((s^2 - 4m)/f^2)/\omega((s^2 - 4m)/f^2)$$

where $h(d)$ (resp. $\omega(d)$) denotes the class number of locally principal ideals (resp. 1/2 the cardinality of the unit group) of the order o^d (say) of $Q(\sqrt{d})$ with discriminant d.

Finally, $c(s,f,\ell)$ is the number of inequivalent mod $U(\mathcal{O}_\ell)$ optimal embeddings of o_ℓ^d into $\mathcal{O}_\ell$ where $d = (s^2 - 4m)/f^2$.

Proof See Theorem 26 of [Piz76a] for the case of orders of level qM and Theorem 4.12 of [Piz80a] for the case of orders of level $q^2 M$. □

Remark 4.2 The key to evaluating the above trace formula is determining the numbers $c(s,f,\ell)$ of optimal embeddings. These are given in the tables in [Piz76b] in the case of orders of level qM and in Theorem 2.7 of [Piz80a] for orders of level q^2. Note that if $\ell | M$, $c(s,f,\ell)$ is the number of optimal embeddings of o_ℓ^d, $d = (s^2 - 4n)/f^2$, into the split order $\mathcal{O}_\ell \equiv \begin{pmatrix} Z_\ell & Z_\ell \\ \ell^\nu Z_\ell & Z_\ell \end{pmatrix}$ where $\nu = \mathrm{ord}_\ell(M)$. These numbers were first determined by Hijikata [Hij74] and can be found explicitly in the tables of [Piz76a] where they are denoted by $c'(s,f,\ell)$ to distinguish the split case from the ramified case. Also see [HPS89a] for a much more general trace formula.

5 Construction of Ramanujan Graphs

Once one realizes that Brandt matrices can be used to construct interesting graphs, the most natural idea is to consider Brandt matrices associated to maximal orders or Eichler orders or more generally to orders of level qM. We consider this case first. Before we begin, we have the following general

Proposition 5.1 *Let p be a prime with $(p, qM) = 1$ and let $N = qM$ or $q^2 M$. Assume, as in Propositions* 4.7 *and* 4.8, *that $E(N) = 0$. Then $G(N;p)$ is a $p+1$ regular simple Ramanujan graph if and only if* $\mathrm{tr}\, B(N;p) = 0$ *and* $\mathrm{tr}\, B(N;p^2) = H$. *Further $G(qM;p)$ is nonbipartite of order $H(qM)$, $G(q^2 M;p)$ is nonbipartite of order*

$H(q^2M)/2$ if p is a residue mod q, and $G(q^2M;p)$ is bipartite of order $H(q^2M)$ if p is a nonresidue mod q.

Proof Proposition 4.7 shows that $A_1 = B_1 = B(qM;p)$ is the adjacency matrix of a nonbipartite $p+1$ regular Ramanujan multigraph of order H *provided* that $B(p)$ has all even diagonal entries and $\operatorname{tr} B(p) = 0$ certainly implies this. Note that since the eigenvalue $p+1$ occurs with multiplicity one, the graph is connected and since $-p-1$ is not an eigenvalue, it is nonbipartite. Further, this graph is a *simple graph* with neither loops nor multiple edges if and only if $\operatorname{tr} A_2 = \operatorname{tr}(B_2 - B_0) = \operatorname{tr}(B(qM;p^2) - I) = 0$, that is if and only if $\operatorname{tr} B(qM;p^2) = H$. We remark that if all diagonal entries of $B(qM;p)$ are even, then it follows from graph theory (see section 2) that $\operatorname{tr} B(qM;p^2) = H$ implies $\operatorname{tr} B(qM;p) = 0$. The proof for the case of level q^2M is similar. □

In the examples below we construct an infinite family of 3-regular Ramanujan graphs associated to maximal orders (i.e. orders of level q) and a larger family associated to orders of level qM. Analogous methods can be used to construct families of $p+1$ regular Ramanujan graphs associated to orders of level qM for primes p. These graphs will in general not have large girth. We then show how it is much easier to construct families of Ramanujan graphs (which also have large girth) using orders of level q^2M.

Example 2 Our aim is to find primes q such that the Brandt matrix $B(2) = B(q;2)$ associated to an order of level q in Proposition 4.7 is the adjacency matrix of a Ramanujan graph. $E(q) = 0$ if and only if $q \equiv 1 \pmod{12}$ so we assume $q \equiv 1 \pmod{12}$. Next by Proposition 5.1, we need that $\operatorname{tr} B(2) = 0$. From Proposition 4.9 we see that this holds if and only if all $c(s,f,q)$ occuring in (13) equal 0. Now $s^2 - 4 \cdot 2 = \Delta$ takes on the negative values -8, -7, and -4. These are all primitive discriminants so that $t = 1$ and $f = 1$ in all cases in the trace formula (13). From the tables on p.692-3 in [Piz76b], we see that $c(s,f,q) = 0$ only if $\Delta = 1$ (i.e. only if Δ is the square of a unit in $\mathbb{Z}_q$) or $q|\Delta$. Note that what we denote by $c(s,f,q)$ is denoted by $c(s,f,q)_q$ in the tables of [Piz76b]. Since $q|\Delta$ can not hold, we require that -8, -7, and -4 are all quadratic residues mod q. By quadratic reciprocity, taking into account that $q \equiv 1 \pmod{12}$, we see that $q \equiv 1$, 25, or 121 (mod 168). The first prime satisfying this requirement is 193. Now by Proposition 5.1, we also need that $\operatorname{tr} B(2^2) = H = \frac{q-1}{12}$. From Proposition 4.9 we again see that this holds if and only if all $c(s,f,q)$ occuring in (13) equal 0. Now $s^2 - 4 \cdot 4 = \Delta$ takes on the negative values -16, -15, -12 and -7. As above we require that these all be quadratic residues mod q. It is easily checked that the only additional requirement is that $q \equiv 1$ or 4 (mod 5) so that the final requirement is that

$$q \equiv 1,\ 121,\ 169,\ 289,\ 361,\ \text{or } 529 \pmod{840}. \tag{14}$$

The first prime satisfying this requirement is 1009. Thus for all primes q satisfying (14) (which have density $6/\phi(840) = 1/32$), the Brandt matrix $B(q;2)$ associated to a maximal order in the quaternion algebra over $\mathbb{Q}$ ramified precisely at q and ∞ is the adjacency matrix of a nonbipartite 3-regular Ramanujan graph $G(q;2)$ of order $\frac{q-1}{12}$.

If more generally, we want to consider 3-regular graphs associated to orders of level qM, where M is any positive odd integer prime to q, we would only need to require that all products $c(s,f,q)\prod_{\ell|M} c(s,f,\ell)$ occuring in the trace formulas (13) for the

trace of $B(2)$ and $B(4)$ be 0. This is easy to check in any particular case (see e.g. Example 4 below), but giving general results is tedious. Certainly if $c(s,f,q)=0$, the whole product is zero, so that we have

Example 3 For all primes q satisfying (14) the Brandt matrix $B(qM;2)$ associated to an order of level qM, where M is any positive odd integer prime to q, is the adjacency matrix of a nonbipartite 3-regular Ramanujan graph $G(qM;2)$ of order $\frac{q-1}{12}M\prod_{\ell|M}(1+1/\ell)$.

Now we finally come to the construction which is the main aim of this paper. First, as this volume honors Oliver Atkin on the occasion of his retirement, it is especially appropriate and a distinct pleasure to explain Atkin's contribution to this subject. In the late 70's W. Parry, a student of Ogg, wrote a thesis [Par79] in which he considered the following question. Do all newforms of weight 2 on $\Gamma_0(q^2)$ come from theta series? The answer is yes if the level is not a perfect square (see [Piz76b]). Parry obtained a negative answer by explicitly constructing a basis for the subspace of cuspforms that do come from theta series in the case $q=13$ and then comparing dimensions. Simultaneously, Pizer was studying orders of level q^2 in order to construct, in analogy with [Piz76b], newforms of level q^2 but he realized that not all newforms could be constructed in that manner (as was clear from representation theory). Atkin, using Parry's calculations, was able to determine that the missing newforms, i.e. those not obtained from theta series, in the case $q=13$ where the forms obtained by taking forms on $\Gamma_0(13)$ with character ψ^2 and twisting them by $\bar{\psi}$ where ψ ran over all characters of $(\mathbb{Z}/13\mathbb{Z})^\times$ with $\psi^2\neq 1$. This and other calculations led Atkin to the obvious conjecture as to what the missing forms where in general for the case of level q^2. His questions to Pizer concerning this led to [Piz80a] where orders of level q^2M are studied and these are precisely the orders we use in the construction of Ramanujan graphs in the following Theorems. For a real number x denote by $\lceil x\rceil$ the smallest integer greater than or equal to x.

Theorem 5.2 *Fix a prime p. Let q be any prime with $q>4p$ and let M be any positive integer prime to pq. Then $G(p)=G(q^2M;p)$ is a $p+1$ regular connected (simple) Ramanujan graph. $G(p)$ has no even cycles of length $r<2\lceil\log_p q-\log_p 4\rceil$ and no odd cycles of length $r<\lceil\log_p q-\log_p 4\rceil$. Further*

1. *Assume p is a quadratic residue mod q. Then $G(p)$ is nonbipartite of order $n=H(q^2M)/2$ with girth g and diameter d satisfying $g\geq\lceil\log_p q-\log_p 4\rceil$ and $d\leq 2\log_p n+2$*
2. *Assume p is a quadratic nonresidue mod q. Then $G(p)$ is bipartite of order $n=H(q^2M)$ with girth g and diameter d satisfying $g\geq 2\lceil\log_p q-\log_p 4\rceil$ and $d\leq 2\log_p n+2\log_p 2+1$.*

Here $H(q^2M)=\frac{q^2-1}{12}M\prod_{\ell|M}(1+1/\ell)$.

Proof Consider the Brandt matrices $B(p^r)=B(q^2M;p^r)$. By Proposition 5.1 we have to check that $\operatorname{tr}B(p)=0$ and $\operatorname{tr}B(p^2)=H$. Let us consider the trace of $B(p^r)$ in general, especially the terms $c(s,f,q)$ occuring in (13). Letting $m=p^r$, $c(s,f,q)$ denotes the number of (equivalence classes of) optimal embeddings of an order of

discriminant $\Delta = (s^2 - 4m)/f^2$ into $\mathcal{O}_q$ where $\mathcal{O}$ is an order of level q^2M. From Theorem 2.7 of [Piz80a], we see that $c(s, f, q) = 0$ if $q \nmid \Delta$. Now for r odd, q does not divide the negative numbers $s^2 - 4p^r$ if $4p^r < q$, i.e. if $r < \log_p q - \log_p 4$. Thus by (13), $\operatorname{tr} B(p^r) = 0$ if r is odd and $r < \log_p q - \log_p 4$. Recall that $A_r = B_r - B_{r-2}$ and that from Proposition 4.8 $B_r = B(p^r)$ if p is a quadratic nonresidue mod q and $B_r = C(p^r)$ if p is a quadratic residue mod q. Since $\operatorname{tr} C(m) = \frac{1}{2} \operatorname{tr} B(m)$, in all cases we have $\operatorname{tr} A_r = 0$ if r is odd and $r < \log_p q - \log_p 4$ so that $G(p)$ has no odd cycles of length $r < \lceil \log_p q - \log_p 4 \rceil$. If $r = 2t$ is even, then q does not divide the negative numbers $s^2 - 4p^{2t} = (s - 2p^t)(s + 2p^t)$ if $r < 2\lceil \log_p q - \log_p 4 \rceil$. Then by (13), $\operatorname{tr} B(p^r) = H$ if r is even and $r < 2\lceil \log_p q - \log_p 4 \rceil$. As above it follows that $G(p)$ has no even cycles of length $r < 2\lceil \log_p q - \log_p 4 \rceil$. In particular, if $q > 4p$, $\operatorname{tr} A_1 = \operatorname{tr} A_2 = 0$, so $G(p)$ is a simple graph. If p is a nonresidue mod q, then $G(p)$ is bipartite and so has no odd cycles at all so the bounds on the girth follow from the results on cycles. Finally, the diameter bounds are a consequence of the Ramanujan property (see Theorem 5.1 of [LPS88]).

□

Remark 5.1 If we denote by $g(G)$ the girth of a graph G, then it is easy to see that there is an (asymptotic) upper bound on the size of $g(G)$ given by $g(G) < 2 \log_{k-1} n$ for k-regular graphs of order n (see e.g. [Bol79]). If $G = G(q^2; p)$ is bipartite, we see from the above Theorem that $g(G) > \log_{k-1} n$ while if $G = G(q^2; p)$ is nonbipartite, then $g(G) > \frac{1}{2} \log_{k-1} n$. In the bipartite case, these bounds are equal to the existence bounds proved by Erdős and Sachs [ES63] using counting arguments. However, these bounds are not as good as those obtained by Lubotzky, Phillips, and Sarnak [LPS88] where they construct bipartite G with $g(G) > \frac{4}{3} \log_{k-1} n$ and nonbipartite G with $g(G) > \frac{2}{3} \log_{k-1} n$.

Theorem 5.3 *Fix a positive nonsquare integer m. Let q be any prime with $q > 4m$ and let M be any positive integer prime to mq. Then $G(m) = G(q^2M; m)$ is a $\sigma_1(m)$-regular connected (simple) almost Ramanujan graph. Almost Ramanujan means that all eigenvalues λ of the adjacency matrix B_1 of $G(m)$ not equal to $\pm\sigma_1(m)$ satisfy the Ramanujan bound $|\lambda| \leq \sigma_0(m)\sqrt{m}$. If $q > 4m^3$, then $G(m)$ has no cycles of length 3. Further*

1. *Assume m is a quadratic residue mod q. Then $G(m)$ is nonbipartite of order $n = H(q^2M)/2$*
2. *Assume m is a quadratic nonresidue mod q. Then $G(m)$ is bipartite order $n = H(q^2M)$*

Here $H(q^2M) = \frac{q^2-1}{12} M \prod_{\ell \mid M} (1 + 1/\ell)$.

Proof We need to consider the matrices $B_1, B_2, \ldots$, especially their traces. Since

$$B(m) = \begin{pmatrix} B_1 & 0 \\ 0 & B_1 \end{pmatrix} \qquad \text{or} \qquad B(m) = B_1$$

depending on whether m is or is not a quadratic residue mod q, we will assume $B_1 = B(m)$ as the argument is almost identical in the other case. If $q > 4m$, then $q \nmid s^2 - 4m$

for any s such that $s^2 - 4m < 0$. By Proposition 4.9 and the proof of Theorem 5.2, we see that $\operatorname{tr} B_1 = 0$ and so $G(m)$ contains no loops. In order to show that $G(m)$ does not contain multiple edges, we must show that $\operatorname{tr} B_2 = \operatorname{tr} B_0$. Now by (2)

$$B_2 = B_1 B_1 - (\sigma_1(m) - 1)B_0$$

and by Proposition 4.8

$$B_1 B_1 = B(m)B(m) = \sum_{d|m} dB(m^2/d^2).$$

Now $q > 4m$ implies $q \nmid s^2 - 4\frac{m^2}{d^2}$ for any s such that $s^2 - 4\frac{m^2}{d^2} < 0$. Thus by Proposition 4.9 and the proof of Theorem 5.2, we see that $\operatorname{tr} B(m^2/d^2) = Mass(\mathcal{O}) = H$ for all $d|m$. Hence

$$\operatorname{tr} B_2 = \sigma_1(m)H - (\sigma_1(m) - 1)H = H = \operatorname{tr} B_0$$

so that $\operatorname{tr} A_2 = 0$ and $G(m)$ is a simple graph. If $q > 4m^3$, similar calculations show that $\operatorname{tr} B_3 = 0$, so that $G(m)$ contains no three cycles. Finally all other claims follow from Proposition 4.8.

□

6 Examples

In this section we present several examples taken from [Piz90].

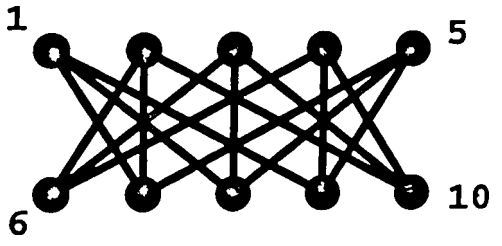

Figure 3: $G(11^2; 2)$

The graph $G = G(11^2; 2)$ given in Figure 3 below is a $(5, 3, 5/6)$-expander with diameter 3 and girth 4. The automorphism group of G has order 48 and is generated by the reflections about the horizontal and vertical axes, the transposition $(1, 5)$ and the element $(2, 3, 4)(7, 8, 9)$ of order 3. In particular, G is not a Cayley graph.

The graph $G = G(13^2; 2)$ given in figure 4 below is a $(7, 3, 7/6)$-expander with diameter 4 and girth 4. The automorphism group of G has order 28 and is generated by the reflections R_H and R_V about the horizontal and vertical axes and the translation (or rotation) $(1, 2, 3, 4, 5, 6, 7)(8, 9, 10, 11, 12, 13, 14)$ which we denote by T. Note that TR_H has order 14 and that the automorphism group is also generated by TR_H and R_V.

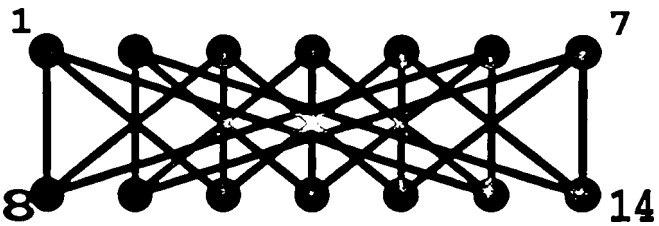

Figure 4: $G(13^2;2)$

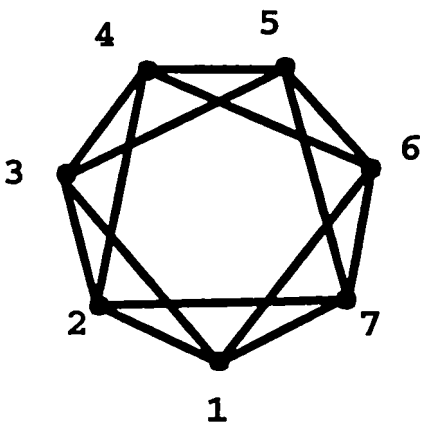

Figure 5: $G(13^2;3)$

The graph $G = G(13^2;3)$ given in Figure 5 is a $(7,4,4/3)$-magnifier which is best possible. It has diameter 2 and girth 3. The automorphism group of G has order 14 and is generated by a reflection and a rotation.

Example 4 Bien in [Bie89] states that one is interested in graphs of order about $1,000,000$ and degree about $1,000$. As our final example we determine such a graph. In the process we demonstrate how a particular graph or multigraph can be easily modified to obtain another graph with enhanced properties. Let $q = 2003$ and $p = 991$ and note that p is a nonresidue mod q. Thus, if r is odd, $q \nmid (s^2 - 4p^r)$ for any s. It follows as in the proof of Theorem 5.2 that $\operatorname{tr} B(q^2;p^r) = 0$ for r odd. Hence we can associate the multigraph $G' = G(q^2;p)$ of order $H(q^2) = 334,334$ to $B(q^2;p)$. Now $q|(s^2 - 4p^2)$ where $s^2 - 4p^2 < 0$ if and only if $s = 21$. It follows that $c(21,1,q) > 0$ so that $\operatorname{tr} B(q^2;p^2) > H(q^2)$ and thus G' has girth 2. Now consider level q^2M with $M = 2$. By the calculations above $\operatorname{tr} B(q^2 2;p^r) = 0$ for r odd. Also $21^2 - 4p^2 \equiv 5 \mod 8$ so by the tables in [Piz76b], $c(21,f,2) = 0$ so that $\operatorname{tr} B(q^2 2;p^2) = H(q^2 2) = 1,003,002$. Thus the girth of $G = G(q^2 2;p)$ is at least 4 and a trivial calculation shows it is 4. Note that (see e.g. [Bol79]) for a bipartite 992-regular graph to have girth greater than 4, it would have to have order at least 1,966,146 so the girth of G is best possible for a bipartite graph of order approximately $1,000,000$ and degree approximately $1,000$.

References

[1] N. Alon, *Eigenvalues and expanders*, Combinatorica, **6** (1986), 83-96.

[2] M. Ajtai, J. Komlos and E. Szemereci, *Sorting in $c \log n$ steps*, Combinatorica, **3** (1983), 1-19.

[3] F. Bien, *Constructions of telephone networks by group*, Notices of the AMS, **36** (1989), 5-22.

[4] B. Bollobas, *Graph Theory*, Springer-Verlag, New York, 1979.

[5] J. Brzezinski, *On automorphisms of quaternion algebras*, J. reine angew. Math., **403** (1990), 166-186.

[6] P. Deligne, *La Conjecture de Weil I*, Publ. Math. I.H.E.S., **43** (1974), 273-308.

[7] M. Eichler, *Quaternare quadratische Formen und die Riemannsche Vermutung fur die Kongruenz Zetafunktion*, Arch. der Math., **5** (1954), 355-366.

[8] M. Eichler, *The Basis Problem for modular forms and the traces of the Hecke operators*, Lecture notes in Math., **320**, Springer, 1973.

[9] P. Erdős and H. Sachs, *Regulare Graphen gegenebener Teillenweite mit Minimaler Knotenzahl*, Wiss. Z. Univ. Halle-Wittenberg, Math. Nat. R., **12** (1963), 251-258.

[10] O. Gabber and Z. Galil, *Explicit construction of linear sized superconcentrators*, Comput. System. Sci., **22** (1981), 407-420.

[11] H. Hijikata, *Explicit formula of the traces of the Hecke operators for $\Gamma_0(N)$*, Math. Soc. Japan, **26** (1974), 56-82.

[12] H. Hijikata, A. Pize and T. Shemanske, *Orders in Quaternion Algebras*, J. reine angew. Math., **394** (1989), 59-106.

[13] H. Hijikata, A. Pizer and T. Shemanske, *The Basis Problem for Modular Forms on $\Gamma_0(N)$*, Memoirs of the AMS, **82(418)** (1989).

[14] Y. Ihara, *Discrete subgroups of $PL(2, k_p)$*, Proc. Symp. in Pure Math., **IX**, AMS, (1966), 272-278.

[15] S. Jun, *Optimal Embeddings in Quaternion Algebras and Applications*, thesis, Univ. of Rochester, 1991.

[16] N. Koblitz, *Introduction to elliptic curves and modular forms*, Springer-Verlag, New York, 1984.

[17] W. Li, *Abelian Ramanujan Graphs*, 1989, preprint.

[18] A. Lubotzky, *Discrete Groups, Expanding Graphs and Invariant Measures*, Prog. in Math., **125**, Birkhauser-Verlag, 1994.

[19] A. Lubotzky, R. Phillips and P. Sarnak, *Explicit expanders and the Ramanujan conjectures*, Proc. of the Eighteenth Annual ACM Sym. on Theory of Computing, **18** (1986), 240-246.

[20] A. Lubotzky, R. Phillips and P. Sarnak, *Ramanujan graphs*, Combinatorica, **8** (1988), 261-277.

[21] G. Margulis, *Explicit group theoretic constructions of combinatorical schemes and their applications for the construction of expanders and concentrators*, J. of Problems of Information Transmission, **9** (1975), 325-332.

[22] G. Margulis, *Explicit construction of concentrators*, J. of Problems of Information Transmission, **24** (1988), 39-46.

[23] A. Nilli, *On the second eigenvalue of a graph*, Discrete Math., **91** (1991), 207-210.

[24] R. Parry, *A negative result on the representation of modular forms by theta series*, J. reine angew. Math., **310** (1979), 151-170.

[25] A. Pizer, *On the arithmetic of quaternion algebras II*, J. Math. Soc. Japan, **28** (1976), 676-688.

[26] A. Pizer, *The representability of modular forms by theta series*, J. Math. Soc. Japan, **28** (1976), 689-698.

[27] A. Pizer, *Theta series and modular forms of level p^2M*, Compositio Math., **40** (1980), 177-241.

[28] A. Pizer, *An algorithm for computing modular forms on $\Gamma_0(N)$*, J. of Algebra, **64** (1980), 340-390.

[29] A. Pizer, *Ramanujan graphs and Hecke operators*, Bulletin of the Am. Math. Soc., **23** (1990), 127-137.

[30] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton Univ. Press, 1971.

[31] R. Tanner, *Explicit concentratorrs from generalized N-gons*, SIAM J. of Alg. Dis. Math., **5** (1984), 278-285.

address: *Department of Mathematics*
University of Rochester
Rochester, NY 14627