COMBINATORICA
Akadémiai Kiadó — Springer-Verlag

COMBINATORICA 8 (3) (1988) 261—277

RAMANUJAN GRAPHS

A. LUBOTZKY, R. PHILLIPS* and P. SARNAK*

Received June 25, 1986
Revised August 5, 1987

A large family of explicit k-regular Cayley graphs X is presented. These graphs satisfy a number of extremal combinatorial properties.

(i) For eigenvalues λ of X either $\lambda=\pm k$ or $|\lambda|\leqq 2\sqrt{k-1}$. This property is optimal and leads to the best known explicit expander graphs.

(ii) The girth of X is asymptotically $\geqq 4/3 \log_{k-1}|X|$ which gives larger girth than was previously known by explicit or non-explicit constructions.

1. Introduction

Let $X=X_{n,k}$ be a k-regular graph on n vertices. If A is its adjacency matrix and $\lambda_0\geqq\lambda_1\geqq\ldots\geqq\lambda_{n-1}$ its eigenvalues then $|\lambda_j|\leqq k$. In fact $\lambda_0=k$ and X is bipartite if and only if $\lambda_{n-1}=-k$. If X is connected, which we assume, then $\lambda_0=k$ and $\lambda_{n-1}=-k$ (in the bipartite case) are both simple eigenvalues as is easily verified. Denote by $\lambda(X)$ the absolute value of the largest eigenvalue (in absolute value) of A which is distinct from $\pm k$; in other words $\lambda^2(X)$ is the next to largest eigenvalue of A^2.

Definition 1.1. A graph $X_{n,k}$ will be called a *Ramanujan graph* if

$$\lambda(X)\leqq 2\sqrt{k-1}.$$

The importance of the number $2\sqrt{k-1}$ in the above definition lies in the following lower bound due to Alon and Boppana; see [3] and Proposition 4.2 below:

$$\varliminf_{n\to\infty}\lambda(X_{n,k})\geqq 2\sqrt{k-1}. \tag{1.1}$$

Thus if one wants graphs with λ_1 as small as possible, $2\sqrt{k-1}$ serves as the lower limit of what can be done. Ramanujan graphs are optimal in this sense. Graphs with λ_1 small make good expander graphs and indeed the Ramanujan graphs introduced in this paper give the best known explicit expanders. This and their importance in many explicit algorithms in computer science are discussed in our announcement [17].

* The work of the second author was supported in part by the NSF under the Grant No. DMS-85-03297 and the third by NSF Grant No. DMS-85-04329.

AMS subject classification (1980): 05C35

Let p and q be unequal primes congruent to 1 mod 4. Our Ramanujan graphs $X^{p,q}$ will be $(p+1)$-regular Cayley graphs of the group $\mathrm{PSL}(2, \mathbf{Z}/q\mathbf{Z})$ if the Legendre symbol $\left(\frac{p}{q}\right)=1$ and of $\mathrm{PGL}(2, \mathbf{Z}/q\mathbf{Z})$ if $\left(\frac{p}{q}\right)=-1$. In both cases the Cayley graph is constructed from $p+1$ generators which are chosen according to the $p+1$ ways of representing p as a sum $p=a_0^2+a_1^2+a_2^2+a_3^2$ with $a_0>0$ and odd, and a_j even for $j=1, 2, 3$. That there are $p+1$ such solutions follows from the well known theorem of Jacobi which states that the number of representations of a positive integer as a sum of 4 squares is

$$r_4(n) = 8 \sum_{\substack{d|n \\ 4\nmid d}} d. \tag{1.2}$$

Jacobi's theorem and more generally the representation of integers by certain quaternary quadratic forms are needed in the construction of our graphs as well as in the proofs. Let $Q=Q_q(x_1, x_2, x_3, x_4)$ be the quadratic form

$$Q(x_1, x_2, x_3, x_4) = x_1^2+4q^2x_2^2+4q^2x_3^2+4q^2x_4^2 \tag{1.3}$$

and let $r_Q(n)$ be the number of representations of n by Q, i.e. the number of solutions to

$$Q(v) = n \quad \text{with} \quad v\in\mathbf{Z}^4. \tag{1.4}$$

In this generality there is no explicit formula for $r_Q(n)$ as in (1.2). However the Ramanujan conjecture (see Ramanujan [22]) and its proof in the above cases by Eichler [6] and Igusa [12], lead to a good approximation to $r_Q(n)$. (Eichler's results are not complete enough for our purposes here as they ignore a finite unspecified set of primes. Igusa's work fills in this gap.) Thus for the case $n=p^k$, $k\geqq 0$

$$r_Q(p^k) = C(p^k)+O_\varepsilon(p^{k(1/2+\varepsilon)}) \quad \text{as} \quad k\to\infty \quad \forall\varepsilon>0 \tag{1.5}$$

where

$$C(p^k) = \begin{cases} c_1 \sum_{d|p^k} d & \text{if } \left(\frac{p}{q}\right)=1 \\ c_2 \sum_{d|p^k} d & \text{if } \left(\frac{p}{q}\right)=-1 \text{ and } k \text{ is even} \\ 0 & \text{if } \left(\frac{p}{q}\right)=-1 \text{ and } k \text{ is odd.} \end{cases}$$

The constants c_1 and c_2 are determined during the course of the discussion in Section 4. That our graphs are Ramanujan graphs will be a consequence of (1.5).

The explicit Cayley graphs $X^{p,q}$ also satisfy a number of other extremal combinatorial properties. Let $g(X)$ denote the girth of a graph X (i.e. the length of the shortest circuit), $i(X)$ the independence number (i.e. the maximal number of independent vertices), $\chi(X)$ the chromatic number and $\mathrm{diam}(X)$ the diameter of X. See [4] for the definitions. The graph $X^{p,q}$ is regular of degree $k=p+1$. We will prove the following inequalities:

Case i. $\left(\frac{q}{p}\right)=-1$; $X^{p,q}$ is bipartite of order $n=|X^{p,q}|=q(q^2-1)$,

(a) $g(X^{p,q}) \geqq 4\log_p q-\log_p 4$,

(b) $\operatorname{diam}(X^{p,q}) \leqq 2\log_p n+2\log_p 2+1$.

Case ii. $\left(\frac{q}{p}\right)=1$; $n=|X^{p,q}|=q(q^2-1)/2$ and $X^{p,q}$ is not bipartite,

(a) $g(X^{p,q}) \geqq 2\log_p q$,

(b) $\operatorname{diam}(X^{p,q}) \leqq 2\log_p n+2\log_p 2+1$,

(c) $i(X^{p,q}) \leqq \dfrac{2\sqrt{p}}{p+1}\, n$,

(d) $\chi(X^{p,q}) \geqq \dfrac{p+1}{2\sqrt{p}}$.

Some comments concerning these inequalities are in order. First we note that the main results, which we establish for $X^{p,q}$, are the Ramanujan property and the bounds for the girth. The bounds on the diameter and independence number are consequences of the Ramanujan property, while the bound on the chromatic number is a simple consequence of the bound on $i(X)$. Second (i) (a) shows that the $X^{p,q}$ are k-regular bipartite graphs of order n which asymptotically satisfy $g(X)\geqq$ $\geqq 4\log_{k-1} n/3$. The problem of exhibiting regular graphs with large girth is non-trivial [4]. Erdős and Sachs [7] proved, using counting arguments, the existence of graphs with $g(X)>\log_{k-1} n$ (k fixed $n\to\infty$). The result of Margulis [19] was followed by an improvement by Imrich [14] which gave explicit examples with $g\geqq 4\log_{k-1} n/9$. Thus our explicit graphs give an improvement even over "the known random one". This should be compared with the easily derived asymptotic upper bound of $g(X_{n,k})\leqq 2\log_{k-1} n$. In the case $k=3$ Weiss [27] gave explicit examples which have the same lower bound as ours.

Equalities (ii) (c) and (d) were pointed out to us by N. Alon [1, 2]. Indeed his Proposition 5.2 below shows in general that for a nonbipartite Ramanujan graph, $i(X)$ has such a bound. (ii) (a) and (c) show that these $X^{p,q}$ furnish a rich explicit family of graphs with arbitrary large girth and $i(X)/n$ arbitrary small. It appears that this is the first such explicit family. In particular we have an explicit family with arbitrarily large girth and chromatic number; see [4] for a history and discussion of this problem. Precisely, given g we have graphs of girth $\geqq g$ order n and independence number $\leqq n^{1-1/3g}$.

Finally we remark that we may view our graphs in the following way: the homogeneous tree of degree $p+1$ may be realized as the coset space $\mathrm{PGL}(2, Q_p)/\mathrm{PGL}(2, \hat{\mathbf{Z}}_p)$ (where Q_p is the field of p-adic numbers and $\hat{\mathbf{Z}}_p$ is the ring of p-adic integers; see Serre [23]). Then by choosing suitable arithmetic discrete subgroups Γ of $\mathrm{GL}(2, Q_p)$ (see for example Serre 23] or Vignéras [24]) one may form the double coset space $\Gamma\backslash\mathrm{PGL}(2, Q_p)/\mathrm{PGL}(2, \mathbf{Z}_p)$ which is a finite graph if Γ is torsion free. By using the theory of automorphic forms one can prove (see

Ihara [13] and [18*II*, Theorem 4.1]) that these are Ramanujan graphs. In fact the graphs of this paper are explicit versions of these, where Γ is taken to be an appropriate congruence subgroup of $H(\mathbf{Z}[1/p])^*$, H being the Hamiltonian quaternions. In general these graphs are not Cayley graphs but if the class number of the quaternion algebra is one they may be presented as such.

The paper is organized as follows: In Section 2 we give the construction of $X^{p,q}$; in Section 3 we realize the graphs as quotients of a "quaternion group" and estimate the girth. In Section 4 we prove the graphs are Ramanujan graphs and in fact determine their spectral densities. The diameter and related quantities are estimated in Section 5.

2. Construction of $X^{p,q}$

In this short section we describe the graphs $X^{p,q}$. Let p, q be unequal primes congruent to 1 mod 4. Let i be an integer satisfying $i^2 \equiv -1 \pmod{q}$. By (1.2) there are $8(p+1)$ solutions $\alpha=(a_0, a_1, a_2, a_3)$ to $a_0^2+a_1^2+a_2^2+a_3^2=p$. Among them (see the next section) there are $p+1$ with $a_0>0$ and odd and a_j even for $j=1, 2, 3$. To each such solution α associate the matrix $\tilde{\alpha}$ in PGL $(2, \mathbf{Z}/q\mathbf{Z})$

$$\tilde{\alpha} = \begin{pmatrix} a_0+ia_1 & a_2+ia_3 \\ -a_2+ia_3 & a_0-ia_1 \end{pmatrix}. \tag{2.1}$$

Form the Cayley graph of PGL $(2, \mathbf{Z}/q\mathbf{Z})$ relative to the above $p+1$ elements (the Cayley graph of a group G relative to a symmetric set of elements S is the graph whose vertices are the elements of G and whose edges are (x, y) if $x=sy$ for some $s \in S$). This is a $(p+1)$-regular graph with $n=q(q^2-1)$ vertices. If $\left(\frac{p}{q}\right)=1$ then this graph is not connected since the generators all lie in the index two subgroup PSL $(2, \mathbf{Z}/q\mathbf{Z})$ (their determinant is a square). We therefore define the Cayley graph $X^{p,q}$ to be the above Cayley graph if $\left(\frac{p}{q}\right)=-1$, and to be the Cayley graph of PSL $(2, \mathbf{Z}/q\mathbf{Z})$ relative to these generators if $\left(\frac{p}{q}\right)=1$. We will see that $X^{p,q}$ is connected. These are the graphs referred to in Section 1. If $\left(\frac{p}{q}\right)=-1$, $X^{p,q}$ is bipartite, the bipartition corresponding to the subsets PSL $(2, \mathbf{Z}/q\mathbf{Z})$ and its complement. When $\left(\frac{p}{q}\right)=1$ we will see that it is definitely not bipartite. Thus $X^{p,q}$ is a $k=p+1$ regular graph of order $n=q(q^2-1)$ or $q(q^2-1)/2$ depending on the sign of $\left(\frac{p}{q}\right)$.

3. Quaternions

Let $H(\mathbf{Z})$ denote the integral quaternions

$$H(\mathbf{Z}) = \{\alpha = a_0+a_1\mathbf{i}+a_2\mathbf{j}+a_3\mathbf{k} | a_j \in \mathbf{Z}\}, \quad \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$$

$\mathbf{ij}=-\mathbf{ji}=\mathbf{k}$ etc. Set $\bar{\alpha}=a_0-a_1\mathbf{i}-a_2\mathbf{j}-a_3\mathbf{k}$ and let $N(\alpha)$ be the integer $\alpha\bar{\alpha}$. The units of the ring $H(\mathbf{Z})$ are $\pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}$. As before take $p\equiv 1(4)$ to be a prime and consider the set of $\alpha \in H(\mathbf{Z})$ with $N(\alpha)=p$. Since $p\equiv 1(4)$ only one of the a_i's of α will be odd. As in the introduction the number of such α's is $8(p+1)$. The units act on this set and it is clear that each solution has exactly one associate $\varepsilon\alpha$, ε a unit, with $\varepsilon\alpha \equiv 1(2)$ and $a_0>0$. Let S be the set of these $p+1$ elements with $N(\alpha)=p$, $\alpha\equiv 1(2)$ and $a_0>0$. This set splits into distinct conjugate pairs $\{\alpha_1, \bar{\alpha}_1, \alpha_2, \bar{\alpha}_2, \ldots, \alpha_s, \bar{\alpha}_s\}$ where $s=(p+1)/2$. By a reduced word of length m in the elements $s\in S$ we mean a word of length m in the α_j, $\bar{\alpha}_j$'s in which no expression of the form $\alpha_j\bar{\alpha}_j$ or $\bar{\alpha}_j\alpha_j$ appears.

Lemma 3.1. ([8].) *Every $\alpha \in H(\mathbf{Z})$ with $N(\alpha)=p^k$ can be expressed uniquely in the form*

$$\alpha = \varepsilon p^r R_m(\alpha_1, \ldots, \bar{\alpha}_s)$$

where ε is a unit, $2r+m=k$, and R_m is a reduced word in the α_i's of length m.

Proof. To obtain the existence of such an expression we use the results of Dickson [5] which show that for odd quaternions (i.e. those of odd norm) one has a theory of g.c.d's and the usual factorization (on the left and right). Since α is odd and a quaternion is prime if and only if its norm is prime we may write $\alpha=\gamma\beta$ with $N(\gamma)=p^{k-1}$, $N(\beta)=p$.

Now by the choice of S we can find a unit ε such that $\alpha=\gamma\varepsilon s_1$ with $s_1\in S$. Now repeat this for $\gamma\varepsilon$, etc. We eventually get $\alpha=\varepsilon s_1 s_2 \ldots s_k$ with $s_j\in S$. After performing cancellations we arrive at $\alpha=\varepsilon p^r R_m$ for some r and m. This proves the existence of such a decomposition.

We show the uniqueness by a counting argument. First, the number of reduced words $R_m(\alpha_1, \ldots, \bar{\alpha}_s)$ is $(p+1)p^{m-1}$ for $m\geqq 1$ and is 1 if $m=0$. Hence the number of expressions $\varepsilon p^r R_m(\alpha_1, \ldots, \bar{\alpha}_s)$ with $2r+m=k$ is

$$8\Big(\sum_{0\leqq r<k/2} (p+1)p^{k-2r-1} + \delta(k)\Big)$$

where

$$\delta(k) = \begin{cases} 1 & \text{if } k \text{ is even} \\ 0 & \text{if } k \text{ is odd.} \end{cases}$$

Hence the number of such expressions is

$$8\left(\frac{p^{k-1}-1}{p-1}\right) = 8\sum_{d|p^k} d.$$

This is the number of $\alpha\in H(\mathbf{Z})$ with $N(\alpha)=p^k$. It follows that each such expression represents a distinct element. ∎

Corollary 3.2. *If* $\alpha \equiv 1(2)$ *and* $N(\alpha)=p^k$ *then*

$$\alpha = \pm p^r R_m(\alpha_1, \ldots, \bar{\alpha}_s) \quad \text{with} \quad 2r+m=k,$$

and this representation is unique.

Consider the set $\Lambda'(2)$ of all $\alpha \in H(\mathbf{Z})$, $\alpha \equiv 1(2)$ and $N(\alpha)=p^v$ for some $v \in \mathbf{Z}$. $\Lambda'(2)$ is closed under multiplication and if we identify α and β in $\Lambda'(2)$ whenever $\pm p^{v_1}\alpha = p^{v_2}\beta$, $v_1, v_2 \in \mathbf{Z}$ then the classes so obtained form a group with

$$[\alpha][\beta] = [\alpha\beta] \quad \text{and} \quad [\alpha][\bar{\alpha}] = [1].$$

Corollary 3.2 implies that this group which we denote by $\Lambda(2)$ is free on $[\alpha_1], [\alpha_2], \ldots, [\alpha_s]$. The Cayley graph of $\Lambda(2)$ with respect to the set S is therefore a tree of degree $p+1$. This tree will be denoted by $\Lambda(2)$ as well. We have thus realized this free group or tree in a suitable number theoretic way. In order to form finite graphs we choose a normal subgroup Γ of $\Lambda(2)$ of finite index. Then Γ acts on $\Lambda(2)$ by multiplication on the right and the quotient graph (or group) $\Lambda(2)/\Gamma$ is finite. This is of course a Cayley graph of $\Lambda(2)/\Gamma$ with respect to the generators $\alpha_1\Gamma, \alpha_2\Gamma, \ldots, \bar{\alpha}_s\Gamma$.

In order to have any number theoretic significance we must choose Γ in an appropriate way. Let $(m, p)=1$ and consider all $[\alpha] \in \Lambda(2)$ such that $2m | a_j$, $j=1, 2, 3$, where $\alpha = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$. This defines a subgroup $\Lambda(2m)$ of $\Lambda(2)$. It is in fact a normal subgroup of finite index in $\Lambda(2)$ since it may be viewed as follows:

Let $H(\mathbf{Z}/2m\mathbf{Z})$ be the quaternions with entries in $\mathbf{Z}/2m\mathbf{Z}$ and let $H(\mathbf{Z}/2m\mathbf{Z})^*$ be the invertible elements of this ring. Let $Z \leqq H(\mathbf{Z}/2m\mathbf{Z})^*$ be the central subgroup: $Z=\{a_0 | a_0 \neq 0\}$. The homomorphism $\pi: \Lambda(2) \to H(\mathbf{Z}/2m\mathbf{Z})^*/Z$ defined by $[\alpha] \to (\alpha \bmod 2m)Z$ is well defined. Its kernel is $\Lambda(2m)$.

We next show that the graphs presented in Section 2 can be identified with the Cayley graphs of the group $\Lambda(2)/\Lambda(2q)$ with respect to the generators $\alpha_1, \ldots, \bar{\alpha}_s$. From now on $m=q$.

Define the homomorphism $\varphi: \Lambda(2) \to \mathrm{PGL}(2, \mathbf{Z}/q\mathbf{Z})$ by

$$[\alpha] \xrightarrow{\pi} \alpha \bmod q \xrightarrow[\varphi]{\sigma} \begin{bmatrix} a_0+ia_1 & a_2+ia_3 \\ -a_2+ia_3 & a_0-ia_1 \end{bmatrix}$$

where i is a fixed integer satisfying $i^2 \equiv -1 \pmod{q}$. It is easily verified that φ is well defined and is a homomorphism.

Proposition 3.3.

$$\text{Image } \varphi = \begin{cases} \mathrm{PGL}(2, \mathbf{Z}/q\mathbf{Z}) & \text{if } \left(\frac{p}{q}\right) = -1 \\ \mathrm{PSL}(2, \mathbf{Z}/q\mathbf{Z}) & \text{if } \left(\frac{p}{q}\right) = 1. \end{cases}$$

Proof. If $\alpha_i \in H(\mathbf{Z})$ is of norm p then $\varphi(\alpha_i)$ is in $\mathrm{PSL}(2, \mathbf{Z}/q\mathbf{Z})$ if and only if $\left(\frac{p}{q}\right)=1$. Since $[\mathrm{PGL}(2, \mathbf{Z}/q\mathbf{Z}): \mathrm{PSL}(2, \mathbf{Z}/q\mathbf{Z})]=2$, it suffices to show that $\varphi(\Lambda(2)) \supseteq$

$\supseteq \mathrm{PSL}(2, \mathbf{Z}/q\mathbf{Z})$. Now φ factors as

$$\Lambda(2) \xrightarrow{\pi_1} H(\mathbf{Z}/2q\mathbf{Z})^*/Z \xrightarrow{\pi_2} H(\mathbf{Z}/q\dot{\mathbf{Z}})^*/Z \xrightarrow{\pi_3} \mathrm{PGL}(2, \mathbf{Z}/q\mathbf{Z}).$$

π_3 is clearly an isomorphism so that the point to check is: What is the image of $\pi_2 \circ \pi_1$? To prove the Proposition it suffices to show that if $\beta = b_0 + b_1\mathbf{i} + b_2\mathbf{j} + b_3\mathbf{k}$ is in $H(\mathbf{Z}/q\mathbf{Z})$ and is of norm 1 (mod q) then there is $\alpha \in H(\mathbf{Z})$ satisfying $N(\alpha) = p^k$ for some k, $\alpha \equiv 1\,(2)$ and $\alpha \equiv \beta\,(q)$. So let such a β be given; set $\gamma = \gamma_0 + \gamma_1\mathbf{i} + \gamma_2\mathbf{j} + \gamma_3\mathbf{k}$ where $\gamma_0 = b_0 \pmod q$, $2\gamma_j \equiv b_j \pmod q$ for $j = 1, 2, 3$. Then

$$\gamma_0^2 + 4\gamma_1^2 + 4\gamma_2^2 + 4\gamma_3^2 \equiv 1\,(q).$$

We will use some results from the theory of quadratic diophantine equations and in particular the theory of singular series of Hardy and Littlewood. Mališev [20] obtained the following from this theory: Let $f(x_1, \ldots, x_n)$ be a quadratic form in $n \geqq 4$ variables with integral coefficients and discriminant d. Let g be an integer prime to $2d$ then if m is sufficiently large (depending on f and g) with $(g, 2md) = 1$, m generic for f, and if $(b_1, \ldots, b_n, g) = 1$, $f(b_1, \ldots, b_n) \equiv m \pmod g$ then there are integers $(a_1, \ldots, a_n) \equiv (b_1, \ldots, b_n) \pmod g$ with $f(a_1, \ldots, a_n) = m$. Indeed he obtains an asymptotic formula for the number of such $(a_1, \ldots, a_n)$ as $m \to \infty$ (the singular series).

We apply this to

$$f(x_1, x_2, x_3, x_4) = x_1^2 + 4x_2^2 + 4x_2^3 + 4x_4^2,$$

$m = p^k$, $g = q$ and $(b_0, b_1, b_2, b_3) = (\gamma_0, \gamma_1, \gamma_2, \gamma_3)$. If k is large enough and $p^k \equiv 1\,(q)$ then we have $f(\gamma_0, \gamma_1, \gamma_2, \gamma_3) \equiv p^k\,(q)$ and p^k is generic so there is $(a_0, a_1, a_2, a_3) \equiv (\gamma_0, \gamma_1, \gamma_2, \gamma_3)(q)$ satisfying $a_0^2 + 4a_1^2 + 4a_2^2 + 4a_3^2 = p^k$. Hence if

$$\alpha = a_0 + 2a\,\mathbf{i} + 2a\,\mathbf{j} + 2a_3 k$$

then $N(\alpha) = p^k$, $\alpha \equiv 1\,(2)$ and $\alpha \equiv \beta \pmod q$ as needed.

Remark 1. Proposition 3.3 may also be deduced from the strong approximation theorem for arithmetic groups see ([16]).

From Proposition 3.3 it follows that $\Lambda(2)/\Lambda(2q) \cong \mathrm{PGL}(2, \mathbf{Z}/q\mathbf{Z})$ or $\mathrm{PSL}(2, \mathbf{Z}/q\mathbf{Z})$ depending on $\left(\frac{p}{q}\right)$. Furthermore the homomorphism takes the generators $\alpha_1, \ldots, \bar{\alpha}_s$ to the matrices in (2.1) hence the graphs $X^{p,q}$ may be identified with $\Lambda(2)/\Lambda(2q)$. For theoretical purposes this latter realization is more useful. For example it is now clear that the graphs $X^{p,q}$ are connected. We now examine the girth,

Theorem 3.4. *If* $\left(\frac{p}{q}\right) = -1$

$$g(X^{p,q}) \geqq 4\log_p q - \log_p 4, \quad |X^{p,q}| = q(q^2-1)$$

while if $\left(\frac{p}{q}\right) = 1$

$$g(X^{p,q}) \geqq 2\log_p q \quad \text{and} \quad |X^{p,q}| = q(q^2-1)/2.$$

Proof. $X=X^{p,q}$ is a Cayley graph and hence is homogeneous. The shortest circuit may therefore be assumed to run from the identity to itself. On the tree $\Lambda(2)$ this corresponds to the length of the smallest nontrivial member of $\Lambda(2q)$. If $\gamma\in\Lambda(2q)$, $\gamma\neq e$ is of length t then we can find an integral quaternion $\tilde{\gamma}\in\Lambda'(2)$ such that

$$\tilde{\gamma}=\beta_1\beta_2\ldots\beta_t \quad \text{with} \quad \beta_j\in\{\alpha_1,\ldots,\bar{\alpha}_s\}$$

and $\tilde{\gamma}\in\Lambda'(2q)$. Thus $N(\tilde{\gamma})=p^t$ and $\tilde{\gamma}=a_0+2qa_1\mathbf{i}+2qa_2\mathbf{j}+2qa_3\mathbf{k}$, $a_0, a_1, a_2, a_3\in\mathbf{Z}$. Since $\gamma\neq e$ at least one of a_1, a_2, a_3 is non-zero. Thus we have

$$p^t=a_0^2+4q^2a_1^2+4q^2a_2^2+4q^2a_3^2. \tag{3.1}$$

In the case $\left(\frac{p}{q}\right)=1$ we simply observe that since one of a_1, a_2, a_3 is $\neq 0$

$$p^t\geqq 4q^2$$

or $t\geqq 2\log_p q$ as claimed. In the case $\left(\frac{p}{q}\right)=-1$ we first note that t must be even, for if not we would have on reducing mod q

$$\left(\frac{p^t}{q}\right)=1 \quad \text{or} \quad \left(\frac{p}{q}\right)=1.$$

Thus t is even and we may write $t=2r$. In this case (3.1) has the trivial solutions $a_0=\pm p^r$. The congruence

$$X_0^2\equiv p^t \pmod{q^2} \tag{3.2}$$

has only solutions

$$X_0\equiv\pm p^r \pmod{q^2} \tag{3.2}'$$

since $(\mathbf{Z}/q^2\mathbf{Z})^*$ is cyclic. If we assume that (3.1) has a non-trivial solution with

$$p^t<q^4/4 \tag{3.3}$$

then $p^r<q^2/2$ and so any solution X_0 of the congruence (3.2) which is not $\pm p^r$ will by (3.2)′ satisfy

$$|X_0|\geqq q^2/2$$

and hence $X_0^2\geqq q^4/4$. But then from (3.1) $p^t>q^4/4$ contradicting (3.3). It follows that $p^t\geqq q^4/4$ or

$$t\geqq\frac{4\log q-\log 4}{\log p}.$$

We end this section by showing that when $\left(\frac{p}{q}\right)=1$, $X^{p,q}$ is not bipartite. If this were so we would have $X=\mathrm{PSL}(2,\mathbf{Z}/q\mathbf{Z})$ partitioned into two sets A and B such that $\alpha_jA=B$ and $\alpha_jB=A$ for each of the generators $\alpha_1,\ldots,\bar{\alpha}_s$. If the

identity is in A then it is clear that A is a subgroup of $G=\mathrm{PSL}(2,\mathbf{Z}/q\mathbf{Z})$; in fact, it is the subgroup of all those elements of G which are expressible as a product of an even number of the generators. However for $q>3$, $\mathrm{PSL}(2,\mathbf{Z}/q\mathbf{Z})$ is a simple group and since A would be an index two subgroup this is a contradiction.

4. Spectrum of $X^{p,q}$

We investigate the spectrum of the $X^{p,q}$ and in particular prove the main result

Theorem 4.1. *$X^{p,q}$ is a Ramanujan graph.*

Before proving this theorem we study the general behavior of the spectrum of an $X_{n,k}$ as $n\to\infty$. In particular we begin by proving (1.1).

Proposition 4.2. $\overline{\lim_{n\to\infty}}\,\lambda(X_{n,k})\geqq 2\sqrt{k-1}$.

Proof. Let Δ be the adjacency matrix of $X_{n,k}$. Then $\Delta^l=(\delta_{ij}^{(l)})$ where $\delta_{ij}^{(l)}$ is the number of paths of length l joining i to j in $X_{n,k}$. Let $\lambda_0=k\geqq\lambda_1\geqq\ldots\geqq\lambda_{n-1}$ be the eigenvalues of Δ. Since trace is independent of basis we have

$$\sum_{j=0}^{n-1}\lambda_j^l=\sum_j\delta_{jj}^{(l)}. \tag{4.1}$$

Now it is clear that since T^k, the k-regular tree, is the universal cover of $X_{n,k}$ we have $\delta_{jj}^{(l)}\geqq\varrho(l)$, where $\varrho(l)$ is the number of paths of length l in T^k joining x to x (which is independent of x). Hence

$$\sum_{j=0}^{n-1}\lambda_j^l\geqq n\varrho(l). \tag{4.2}$$

It follows after removing the eigenvalues $\pm k$ that

$$\lambda(X)^{2l}\geqq\varrho(2l)-\frac{2k^{2l}}{n-2}. \tag{4.3}$$

Now $\varrho(2l)\geqq\varrho'(2l)$ where $\varrho'(2l)$ is the number paths of length $2l$ beginning at x and ending at x for the first time (in T^k). One checks that

$$\varrho'(2l)=\frac{1}{l}\binom{2l-2}{l-1}k(k-1)^{l-1}.$$

Thus

$$\lambda(X)^{2l}\geqq\frac{1}{l}\binom{2l-2}{l-1}(\sqrt{k-1})^{2l})-\frac{2k^{2l}}{n-2}.$$

The Proposition follows from this since

$$\binom{2l-2}{l-1}^{1/2l}\to 2\quad\text{as}\quad l\to\infty.$$

We can be more precise if girth $(X_{n,k}) \to \infty$ as $n \to \infty$. Associate to the graph $X_{n,k}$ a measure μ_X supported on $[-k, k]$ which puts point masses $\frac{1}{n}$ at the eigenvalues of Δ.

Proposition 4.3.

$$\lim_{\substack{n\to\infty \\ g(X_{n,k})\to\infty}} \mu_{X_{n,k}} = \mu_k$$

where

$$d\mu_k(t) = \begin{cases} \dfrac{\sqrt{k-1-t^2/4}}{\pi k(1-(t/k)^2)}\,dt & \text{if } |t| \leqq 2\sqrt{k-1} \\ 0 & \text{otherwise.} \end{cases}$$

The limit in Proposition 4.3 is the weak* limit i.e.

$$\lim_{n\to\infty} \int f(t)\, d\mu_{X_{n,k}}(t) = \int f(t)\, d\mu(t)$$

for all continuous f.

Proof. It suffices to show that

$$\int t^l\, d\mu_{n,k}(t) \to \int t^l\, d\mu_k(t) \tag{4.4}$$

for each $l \geqq 0$. Now for l fixed and n large enough $g(X_{n,k}) > 2l$. Hence locally up to distances of length l, $X_{n,k}$ looks like T^k. In particular $\delta_{ii}^{(l)} = \varrho(l)$ for each vertex i of X. Thus as in the previous proof

$$\frac{1}{n}\sum_{j=0}^{n-1} \lambda_j^l = \int t^l\, d\mu_{n,k}(t) = \varrho(l).$$

Hence the left hand side of (4.4) converges to $\varrho(l)$ as $n \to \infty$. It remains to chack that $\varrho(l)$ is the sequence of moments of the measure μ_k in Proposition 4.3. This is a simple calculation and is carried out in Kesten [15] for example.

As was proved in Section 3 the girth $g(X^{p,q})$ of our graphs $\to \infty$ as q (and hence n) $\to \infty$. Thus the spectrum of the graphs $X^{p,q}$ lies in $[-2\sqrt{p}, 2\sqrt{p}]$ (besides $\pm(p+1)$) and it is distributed in this interval according to the density $d\mu_{p+1}$ as $q \to \infty$.

We turn to the proof of Theorem 4.1. We begin with some remarks concerning harmonic analysis on the tree T^k. Let Γ be a discrete group of isometries acting freely on $T = T^k$ and such that $n = |T/\Gamma| < \infty$. Consider the space of Γ periodic (or automorphic) complex valued functions on T such that

$$f(\gamma x) = f(x) \quad \text{for} \quad x \in T, \quad \gamma \in \Gamma.$$

This space is finite dimensional and is denoted by $L^2(T/\Gamma)$. The Laplacian on the tree leaves $L^2(T/\Gamma)$ invariant and so may be spectrally decomposed. This gives an orthonormal basis $u_j(x)$ of $L^2(T/\Gamma)$ satisfying

$$\begin{cases} \Delta u_j = \lambda_j u_j \\ u_0(x) = \dfrac{1}{\sqrt{n}}, \quad \lambda_0 = p+1 = k. \end{cases} \tag{4.5}$$

For $l \geqq 0$, an integer, define the point pair function $k_l: T \times T \to \mathbf{C}$ by (see Remark 2 at the end of this proof for a different approach)

$$k_l(x, y) = \begin{cases} 1 & \text{if } d(x, y) = l \\ 0 & \text{otherwise.} \end{cases} \tag{4.6}$$

Set

$$K_l(x, y) = \sum_{\gamma \in \Gamma} k_l(\gamma x, y) \tag{4.7}$$

$K_l(x, y)$ counts the number of elements in the orbit Γx which are at distance l from y in T. It is clearly symmetric in x and y and as a function of each is in $L^2(T/\Gamma)$. We may therefore expand it

$$K_l(x, y) = \sum_{j=0}^{n-1} h_j(l) u_j(x) u_j(y). \tag{4.8}$$

The reason we obtain only diagonal terms in this expansion is that Δ commutes with the 'integral' operator k_l and hence

$$\sum_{y \in T/\Gamma} K_l(x, y) u_j(y) = \sum_{y \in T} k_l(x, y) u_j(y) = h_j(l) u_j(x)$$

for a suitable $h_j(l)$. If $t \geqq 0$ is an integer we form

$$L_t(x, y) = \sum_{0 \leqq r \leqq t/2} K_{t-2r}(x, y) \tag{4.9}$$

which counts the number of elements in the orbit Γx in alternate shells about y at distances $\leqq t$. It is not difficult to compute the dependence of $h_j(l)$ on λ_j and l, see [18] and in fact

$$L_t(x, y) = p^{t/2} \sum_{j=0}^{n-1} \frac{\sin(t+1)\theta_j}{\sin \theta_j} u_j(x) u_j(y) \tag{4.10}$$

where θ_j is complex valued and defined by

$$\lambda_j = 2\sqrt{p} \cos \theta_j. \tag{4.11}$$

Here θ_j is real if $|\lambda_j| \leqq 2\sqrt{p}$ otherwise it is purely imaginary with $\mathrm{Im}(\theta_j) > 0$ if $\lambda_j > 2\sqrt{p}$ or it is of the form $\pi + i\mu$, $\mu \in \mathbf{R}$ if $\lambda_j < -2\sqrt{p}$. For example $\theta_0 = i \log \sqrt{p}$ and $\theta_{n-1} = \pi + i \log \sqrt{p}$ if $\lambda_{n-1} = -(p+1)$. We apply the above considerations to the case where $T = \Lambda(2)$ and $\Gamma = \Lambda(2q)$ as in Section 3. For $x \in \Lambda(2)$

$$K_l(x, x) = \left|\{\gamma \in \Lambda(2q): d(\gamma x, x) = l\}\right| = \left|\{\gamma \in \Lambda(2q): d(x^{-1}\gamma x, e) = l\}\right|.$$

Since $\Lambda(2q)$ is normal in $\Lambda(2)$, this can be rewritten as

$$K_l(x, x) = \left|\{\gamma \in \Lambda(2q): d(\gamma e, e) = l\}\right|. \tag{4.12}$$

Hence $K_l(x, x) = K_l(e, e)$ for all $x \in \Lambda(2)$, $l \geqq 0$ and also

$$L_t(x, x) = L_t(e, e), \quad \text{for all} \quad x \in \Lambda(2), \quad t \geqq 0. \tag{4.13}$$

We now relate this count to the problem of representing a number by a quadratic form. Let Q be the quadratic form

$$Q(x_1, x_2, x_3, x_4) = x_1^2+(2q)^2x_2^2+(2q)^2x_3^2+(2q)^2 x_4^2.$$

Then $r_Q(p^k)$ is the number of $\alpha\in H(\mathbf{Z})$ such that $2q|\alpha-a_0$ and $N(\alpha)=p^k$. Now by Corollary 3.2 every such α is of the form $\pm p^r R_t(\alpha_1, \ldots, \bar{\alpha}_s)$ where $2r+t=k$ and where $[\alpha]\in\Lambda(2q)$. It follows from this and the uniqueness (Corollary 3.2) that

$$r_Q(p^k) = 2\sum_{r<k/2} |\{\alpha\in\Lambda(2q)|d(\alpha, e) = k-2r\}|.$$

In other words

$$r_Q(p^k) = 2L_k(e, e) = 2L_k(x, x). \tag{4.14}$$

Inserting (4.10) into the right hand side of this last equation and summing over $x\in T/\Lambda(2q)$ gives

$$r_Q(p^k) = \frac{2p^{k/2}}{n}\sum_{j=0}^{n-1}\frac{\sin(k+1)\theta_j}{\sin\theta_j}. \tag{4.15}$$

This is the key relation relating (1.5) and the spectrum of $\Lambda(2)/\Lambda(2q)=X^{p,q}$ (notice the automorphic spectrum of Δ is the same as the spectrum of Δ on the quotient graph!). Combining (1.5) with (4.15) gives

$$C(p^k)+O_\varepsilon(p^{k(1/2+\varepsilon)}) = \frac{2p^{k/2}}{n}\sum_{j=0}^{n-1}\frac{\sin(k+1)\theta_j}{\sin\theta_j} \quad \forall\varepsilon>0. \tag{4.16}$$

$C(p^k)$ is the "singular series" and it comes from the contribution of the Eisenstein series when expressing the "θ-function"

$$\theta(z) = \sum_{v\in\mathbf{Z}^4} e^{2\pi iQ(v)z}$$

as a combination of Eisenstein series and a cusp form — see Hecke [10]. That is, $C(p^k)$ is the p^k-th Fourier coefficient of a combination of the Einsenstein series of weight two for $\Gamma(16q^2)$. From the known Fourier expansions of Eisenstein series [10, 21] one easily shows that C is of the form

$$C(n) = \sum_{d|n} dF(d)$$

where F: $\mathbf{N}\to\mathbf{C}$ is periodic of period $4q^2$.

Lemma 4.4. *Let* G: $\mathbf{N}\to\mathbf{C}$ *be periodic and satisfy*

$$\sum_{d|p^k} dG(d) = o(p^k) \quad as \quad k\to\infty$$

then

$$\sum_{d|p^k} dG(d) = 0 \quad for\ all \quad k.$$

Proof. Let $\alpha_k=\sum_{d|p^k} dG(d)$ then

$$\frac{\alpha_k}{p^k}-\frac{\alpha_{k-1}}{p^{k-1}p} = G(p^k). \tag{4.17}$$

The left hand side of (4.17) $\to 0$ as $k \to \infty$. Since G is periodic it follows that $G(p^k)=0$ for all k proving the lemma.

Returning to (4.16) we may write

$$\sum_{d|p^k} dF(d)+O_\varepsilon(p^{k(1/2+\varepsilon)} = \frac{2p^{k/2}}{n} \sum_{j=0}^{n-1} \frac{\sin(k+1)\theta_j}{\sin\theta_j} \quad \forall \varepsilon > 0. \tag{4.18}$$

We must now distinguish two cases:

Case i. $\left(\frac{p}{q}\right)=-1$. In this case $X^{p,q}$ is bipartite as we saw in Section 3. The eigenvalues λ_j appear in pairs $\pm(p+1), \pm\lambda_1, \ldots$ etc. Furthermore as was observed at the beginning of this paper in this case $\pm(p+1)$ are simple eigenvalues hence $|\lambda_j|<p+1$ for $j\neq 0, j=n-1$. Therefore the right hand side of (4.18) is clearly 0 if k is odd, while for k even it is of the form

$$\frac{4(p^{k+1}-1)}{n(p-1)}+o(p^k) = \frac{4}{n}\sum_{d|p^k} d+o(p^k)$$

as $k\to\infty$. We apply Lemma 4.4 and conclude that

$$C(p^k) = \begin{cases} 0 & \text{if } k \text{ is odd} \\ \dfrac{4(p^{k+1}-1)}{n(p-1)} & \text{if } k \text{ is even.} \end{cases} \tag{4.19}$$

We may now eliminate the leading terms on both sides of (4.18) since they are identical and conclude that

$$\frac{2p^{k/2}}{n} \sum_{j=1}^{n-2} \frac{\sin(k+1)\theta_j}{\sin\theta_j} = O_\varepsilon(p^{k(1/2+\varepsilon)}) \quad \forall \varepsilon > 0$$

Hence as $k\to\infty$, k even

$$\sum_{j=2}^{n-2} \frac{\sin(k+1)\theta_j}{\sin\theta_j} = O_\varepsilon(p^{\varepsilon k}) \quad \forall \varepsilon > 0.$$

This clearly implies that all the θ_j, $2\leqq j\leqq n-2$ are real, that is that $|\lambda_j|\leqq \leqq 2\sqrt{p}$ for $2\leqq j\leqq n-2$. Thus we have shown that $X^{p,q}$ when $\left(\frac{p}{q}\right)=-1$ is a bipartite Ramanujan graph.

Case ii. $\left(\frac{p}{q}\right)=1$. In this case as we showed at the end of Section 3, $X^{p,q}$ is not bipartite. Hence $|\lambda_j|<p+1$ for $j\neq 0$. This time (4.16) reads

$$C(p^k)+O_\varepsilon(p^{k(1/2+\varepsilon)}) = \frac{2(p^{k+1}-1)}{n(p-1)}+o(p^k).$$

Hence by the Lemma

$$C(p^k) = \frac{2(p^{k+1}-1)}{n(p-1)} \tag{4.20}$$

and this time

$$\sum_{j=1}^{n-1} \frac{\sin(k+1)\theta_j}{\sin\theta_j} = O_\varepsilon(p^{k\varepsilon}) \quad \forall \varepsilon > 0.$$

Hence θ_j is real for $j=1, \ldots, n-1$ and $X^{p,q}$ is Ramanujan. This completes the proof of Theorem 4.1. ∎

Remark 2. As pointed out to us by a referee the initial part of the proof of Theorem 4.1 (as well as the proof of Theorem 5.1) can be made a little more direct and self-contained by avoiding the use of the harmonic analysis of point pair functions as follows. Let $H_0(x), H_1(x), \ldots$ be the Čebyšev polynomials defined by

$$H_0(x) = 1 \quad H_1(x) = x$$
$$H_t(x) = xH_{t-1}(x) - pH_{t-2}(x) \quad \text{for} \quad t \geqq 2.$$

Define the operator L_t by

$$L_t = H_t(\Delta).$$

Computing the trace of L_t on $L^2(T/\Gamma)$ as in the argument leading to (4.14) one finds that $\mathrm{TR}(L_t) = nr_Q(p^t)/2$. On the other hand on computing this trace spectrally

$$\mathrm{TR}(L_t) = \sum_{0 \leqq j \leqq n-1} H_t(\lambda_j).$$

This, when expressed in terms of the θ_j's defined in (4.11), yields

$$\mathrm{TR}(L_t) = \sum_{0 \leqq j \leqq n-1} \frac{p^{t/2}\sin(t+1)\theta_j}{\sin\theta_j}$$

(4.15) follows on equating these expressions for $\mathrm{TR}(L_t)$.

The graphs $X^{p,q}$ may be used to construct a somewhat richer family of Ramanujan bipartite graphs as follows:

$\mathrm{PGL}(2, \mathbf{Z}/q\mathbf{Z})$ acts on $\mathbf{P}^1(F_q) = \{0, 1, \ldots, q-1, \infty\}$ in the usual linear fractional way. We turn $\mathbf{P}^1(F_q)$ into a $p+1$ regular graph by joining $\xi \in \mathbf{P}^1$ to $\gamma\xi$ for each generator $\gamma \in \{\alpha_1, \ldots, \bar{\alpha}_s\}$. Call this graph $Y^{p,q}$. It has order $q+1$. It is clear that any eigenfunction f of Δ for $Y^{p,q}$ gives rise to one F on $X^{p,q}$ with the same eigenvalue. In fact

$$F(g) = f(g(0))$$

supplies this correspondence. Thus to show $Y^{p,q}$ is Ramanujan non-bipartite all we need show is that $-(p+1)$ is not an eigenvalue of $Y^{p,q}$. If it were we clearly must be in the case $\left(\frac{p}{q}\right) = -1$ and we can assume that $F(g) = f(g(0))$ is 1 on $\mathrm{PSL}(2, \mathbf{Z}/q\mathbf{Z})$ and -1 on $\mathrm{PSL}(2, \mathbf{Z}/q\mathbf{Z})^{\mathrm{comp}}$. Now F is constant on the subgroup $\left\{\begin{pmatrix}\alpha & 0\\ \gamma & \delta\end{pmatrix} | \alpha\delta \neq 0\right\}$. This subgroup clearly contains members of $\mathrm{PSL}(2, \mathbf{Z}/q\mathbf{Z})$ as well as its complement which is a contradiction. We have shown

Theorem 4.4. *The graphs $Y^{p,q}$ are non-bipartite Ramanujan graphs of order $q+1$ and degree $p+1$.*

5. Diameter and other quantities

We conclude by estimating some other graph theoretic quantities for the graphs $X^{p,q}$. Since $X^{p,q} \cong \Lambda(2)/\Lambda(2q) = T/\Lambda(2q)$, the diameter may be realized as

$$\operatorname{diam}(X^{p,q}) = \sup_{x,y \in T} \inf_{\gamma \in \Lambda(2q)} d(x, \gamma y). \tag{5.1}$$

Let $k_m(x, y)$ be the function on T defined in (4.4) along with $K_m(x, y)$ defined in (4.5). If $d(x, y) > l$ then $K_m(x, y) = 0$ for all $m \leqq l$. Hence

$$\sum_{m<l} a_m K_m(x, y) = 0 \tag{5.2}$$

for any choice of coefficients a_m. We choose these to be the coefficients of the l^{th} Čebyšev polynomial $H_l(x)$;

$$H_l(x) = \cos(l \arccos(x)) = \sum_{m=0}^{l} a_m x^m. \tag{5.3}$$

By the analysis similar to that carried out in Section 4 we find

$$\sum_{m<l} a_m K_m(x, y) = p^{l/2} \sum_{j=0}^{n-1} \cos(l\theta_j) u_j(x) u_j(y), \tag{5.4}$$

where as before $\lambda_j = 2\sqrt{p} \cos \theta_j$. Thus if $d_X(x, y) > l$

$$0 = p^{l/2} \sum_{j=0}^{n-1} \cos(l\theta_j) u_j(x) u_j(y).$$

If l is even this gives

$$\frac{p^l + 1}{2n} \leqq p^{l/2} \sum_{j=1}^{n-2} |u_j(x) u_j(y)| \leqq p^{l/2} \sum_{j=2}^{n-2} (|u_j(x)|^2 + |u_j(y)|^2)/2 \leqq p^{l/2}$$

since $\sum_{j=1}^{n-1} |u_j(x)|^2 = 1$ for any x. Hence $p^{l/2} \leqq 2n$ or $l \leqq 2 \log_p (2n)$. We conclude

Theorem 5.1. *If* $n = |X^{p,q}|$ *then*

$$\operatorname{diam}(X^{p,q}) \leqq 2 \log_p n + 2 \log_p 2 + 1.$$

It is easy to see on the other hand, that $\operatorname{diam}(X^{p,q}) \geqq \log_p n$.

For the rest of this section we assume $\left(\frac{p}{q}\right) = 1$. In this case we can give an upper bound to the independence number of $X^{p,q}$ and hence a lower bound to the chromatic number. That this is so, follows from the following proposition due to Alon [1]; see also [2].

Proposition 5.2. (Alon) *Let* $X_{n,k}$ *be a non-bipartite Ramanujan graph; then*

$$i(X) \leqq \frac{2\sqrt{k-1}}{k} n.$$

Proof. Suppose that A is an independent set of vertices with $|A| = r$. Define a function $f(x)$ on X by

$$f(x) = \begin{cases} 1 & \text{on } A \\ -c & \text{on } A^c \end{cases} \tag{5.5}$$

where $r-(n-r)c=0$. Then $f \perp 1$ and hence by the Ramanujan (non-bipartite) condition

$$\|\Delta f\|_2^2 \leqq 4(k-1)\|f\|_2^2. \tag{5.6}$$

On the other hand clearly by the independence property of A, $\Delta f(x)=-ck$ for $x \in A$. Thus

$$\|\Delta f\|_2^2 \geqq c^2 k^2 r. \tag{5.7}$$

Now $c=r/(n-r)=v/(1-v)$ where $v=r/n$. (5.6) and (5.7) yield.

$$c^2 k^2 r \leqq 4(k-1)\|f\|_2^2 = 4(k-1)(r+c^2(n-r)) \tag{5.8}$$

or

$$c^2 k^2 \leqq 4(k-1)\left(1+c^2\left(\frac{1}{v}-1\right)\right).$$

Hence

$$\frac{v^2}{(1-v)^2} k^2 \leqq 4(k-1)\left(1+\frac{v^2}{(1-v)^2}\left(\frac{1-v}{v}\right)\right)$$

$$v^2 k^2 \leqq 4(k-1)(1-v) \Rightarrow v^2 k^2 \leqq 4(k-1)$$

or

$$v \leqq \frac{2\sqrt{k-1}}{k}$$

proving the proposition.

An upper bound on $i(X)$ clearly implies a lower bound on $\chi(X)$. We have shown: $X_{n,k}$ non-bipartite Ramanujan implies

$$\chi(X_{n,k}) \geqq \frac{k}{2\sqrt{k-1}}. \tag{5.9}$$

Remark 3. The bound (5.9) may also be obtained directly from Hofmann [11] using the Ramanujan property.

In conclusion we remark that the results of this paper show that the explicit graphs $X^{p,q}$ share many of the extremal properties of random graphs.

Remark 4. We recently learned from Professor Margulis that he has obtained results similar to those in this paper, see:

G. A. Margulis, Arithmetic groups and graphs without short cycles, *6th Internat. Symp. on Information Theory, Tashkent* 1984, *Abstracts, Vol. 1,* pp. 123—125 (in Russian).

G. A. Margulis, Some new constructions of low-density paritycheck codes. *3rd Internat. Seminar on Information Theory, convolution codes and multi-user communication, Sochi* 1987, pp. 275—279 (in Russian).

G. A. Margulis, Explicit group theoretic constructions of combinatorial schemes and their applications for the construction of expanders and concentrators, *Journal of Problems of Information Transmission,* 1988 (to appear in Russian).

Acknowledgements. We would like to thank N. Alon and N. Pippenger for many illuminating discussions concerning this paper.

References

[1] N. Alon, *Private communication* 1986.
[2] N. Alon, Eigenvalues, geometric expanders, sorting in rounds and Ramsey theory, *Combinatorica,* **6** (1986), 207—219.
[3] N. Alon, Eigenvalues and expanders, *Combinatorica,* **6** (1986), 83—96.
[4] B. Bollobás, *Extremal graph theory,* Academic Press, London 1978.
[5] L. E. Dickson, Arithmetic of quaternions, *Proc. London Math. Soc.* (2) **20** (1922), 225—232.
[6] M. Eichler, Quaternäre quadratische Formen und die Riemannsche Vermutung für die kongruentz Zeta Funktion, *Archiv. der Math.* Vol. V, (1954), 355—366.
[7] P. Erdős and H. Sachs, Reguläre Graphen gegenebener Teillenweite mit Minimaler Knotenzahl, Wiss. Z. Univ. Halle—Wittenberg, *Math. Nat. R.* **12** (1963), 251—258.
[8] L. Gerritzen and N. Van der Put, *Schottky groups and Mumford curves,* Springer-Verlag, L. N. in Math. 817 (1980).
[9] G. Hardy and E. Wright, *An introduction to number theory,* Oxford University Press 1978 (Fifth Edition).
[10] E. Hecke, Analytische arithmetik der positiven quadratic formen, *Collected works* pp. 789—898, Göttingen, 1959.
[11] A. Hofmann, On eigenvalues and colorings of graphs, *in Graph theory and its applications (ed. B. Harris)* Academic Press (1970), 79—91.
[12] J. Igusa, Fibre systems of Jacobian varieties III, *American Jnl. of Math.* **81** (1959), 453—476.
[13] Y. Ihara, Discrete subgroups of PL $(2, k_p)$, *Proc. Symp. in Pure Math.* IX, AMS (1968), 272—278.
[14] W. Imrich, Explicit construction of regular graphs with no small cycles, *Combinatorica* **4** (1984), 53—59.
[15] H. Kesten, Symmetric random walks on groups, *Trans. AMS* **92** (1959), 336—354.
[16] M. Knesser, Strong approximation in: *Algebraic Groups and Discontinuous Subgroups, Proc. Symp. Pure Math.* Vol. IX, (1966), 187—196.
[17] A. Lubotzky, R. Phillips, P. Sarnak, Ramanujan conjecture and explicit construction of expanders, *Proc. Stoc.* **86** (1986), 240—246.
[18] A. Lubotzky, R. Phillips, P. Sarnak, Hecke operators and distributing points on S^2 I, II *Comm. Pure and Applied Math.* **39** (1986), 149—186, **40** (1987), 401—420.
[19] G. A. Margulis, Graphs without short cycles, *Combinatorica* **2** (1982), 71—78.
[20] Mališev, On the representation of integers by positive definite forms, *Mat. Steklov* **65** (1962).
[21] A. Ogg, *Modular forms and Dirichlet series,* W. A. Benjamin Inc., New York 1969.
[22] S. Ramanujan, On certain arithmetical functions, *Trans. Camb. Phil. Soc.* **22** (1916), 159—184.
[23] J. P. Serre, *Trees,* Springer Verlag, Berlin—Heidelberg—New York, (1980).
[24] M. F. Vignéras, *Arithmetique dè Algebras de Quaternions,* Springer Lecture Notes; V. 800, (1980).
[25] G. L. Watson, Quadratic diophantine equations, *Royal Soc. of London, Phil. Trans.,* A 253, 227—2 (1960).
[26] A. Weil, Sur les courbes algébriques et les varétés qui s'en déduisent, *Actualites Sci. Et ind.* No. 1041 (1948).
[27] A. Weiss, Girths of bipartite sextet graphs, *Combinatorica* **4** (1984), 241—245.

A. Lubotzky

Institute of Mathematics
and Computer Science
Hebrew University
Jerusalem, Israel

R. Phillips

Department of Mathematics
Stanford University
Stanford, California 94305, U.S.A.

P. Sarnak

Department of Mathematics
Stanford University
Stanford, California 94305, U.S.A.