Pacific Journal of Mathematics

EIGENVALUE BOUNDS AND GIRTHS OF GRAPHS OF FINITE, UPPER HALF-PLANES

NANCY JEANNE CELNIKER

Volume 166 No. 1 November 1994

PACIFIC JOURNAL OF MATHEMATICS
Vol. 166, No. 1, 1994

EIGENVALUE BOUNDS AND GIRTHS OF GRAPHS OF FINITE, UPPER HALF-PLANES

NANCY CELNIKER

For each odd prime power $q = p^r$ we will investigate $q-2$ different Cayley graphs called finite, upper half planes over F_q. We define a finite, upper half-plane by

$$H_q = \{x + y\sqrt{d} | x, y \in F_q, y \neq 0\}$$

where F_q is the finite field with q elements and d is not a square in F_q. We define a distance k between points z and w $\in H_q$ by

$$k(z, w) = \frac{N(z - w)}{(Imz)(Imw)}$$

where $Nz = z\bar{z}$ and $\bar{z} = x - y\sqrt{d}$ and Re $z = x$ and Im$z = y$. We define a graph, $X_q(d, a)$, by letting the elements of H_q be the vertices of the graph and defining an edge between z and w where $k(z, w) = a$ for a fixed $a \in F_q - \{0\}$. We consider the origin to be the point $\sqrt{d}$. We call $H_q(d, a)$, the finite upper half-plane depending on a fixed a and d. We first concern ourselves with whether the eigenvalues, λ, of the adjacency matrices of the graphs satisfy the Ramanujan bound $|\lambda| \leq \sqrt{q}$. Since the graphs are of degree $q + 1$, the paper shows a method to use the representations for the additive and multiplicative groups of each F_q to find the smaller associated isospectral matrices. We then find the eigenvalues of the isospectral matrices. A computer program has verified the Ramanujan bound for most of the graphs up to the prime power 3^5. We next concern ourselves with the girth of the graphs. This paper shows that the girths are either 3 or 4 and shows that the girth is 3 if $a = 2d$ and $q \equiv 3(mod 4)$ or if a and $a - 3d$ are squares in F_q. The girth is 4 if $a = 2d$ and $q \equiv 1(mod 4)$.

Nicholas M Katz [7] has proven that the eigenvalues of the graphs do satisfy the Ramanujan bound in the paper "Estimates for Soto-Andrade Sums-1". Graphs whose eigenvalues satisfy the Ramanujan

bound are of interest in communications theory as are graphs with certain girths. See Lubotsky [9], Bien [2], Klawe [8] and Chung [5] for applications and more discussion. These graphs are discussed in Terras [12], Celniker et al [4], Poulos [11] and Angel [1].

1. Preliminary Results. Graphs of finite, upper half planes have been defined similarly in other papers. [4], [13]. The graphs in those papers were defined by vertices from the set

$$H_p = \{x + y\sqrt{d} | x, y \in F_p, y \neq 0\}$$

with an analogous definition for the distance between vertices. The initial results about the graphs described here are analogous to the previous results and are included for the reader's convenience.

LEMMA 1.1 (TERRAS [12]).

(1) *The points* $z = x + y\sqrt{d}$ *and* $\sqrt{d}$ *are adjacent in*

$$X_q(d, a) \Leftrightarrow x^2 = ay + d(y-1)^2.$$

(2) X_q *is a regular graph of degree* $q + 1$ *provided that* d *is a non-square in* F_q *and* $a \neq 0$ *or* $4d$.

Proof.

(1) Clear from the proof of (2).

(2) We can rewrite the equation in part 1 of the lemma as a norm equation in the finite field $F_q(\sqrt{d})$: $N(z + c) = n$, where $z = x + y\sqrt{d}$, $c = \sqrt{d}\ (\frac{a}{2d} - 1)$, and $n = \frac{a(4d-a)}{4d}$. But now the norm in $F_q(\sqrt{d})$ is given by $\mathrm{Nz} = z\bar{z} = zz^q = z^{q+1}$. Therefore we are solving the equation $w^{q+1} = \mathrm{n}$, for $\mathrm{w} = \mathrm{z}+\mathrm{c}$. Since we are in a finite field, there are exactly $q + 1$ solutions as long as $r \neq 0$, which is the case when $a \neq 4d$.

We notice we can find all the different $X_q(d, a)$ by fixing d and letting $a \in F_q - \{0\}$, $a \neq 4d$. □

From now on we will write $H_q(d, a)$ to denote the finite upper half-plane depending on a fixed d and a as defined earlier.

We recall the definition of the affine group,

$$\mathrm{Aff}(2,q) = \left\{ \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} | x, y \in F_q, y \neq 0 \right\}.$$

So we associate the vertices of $X_q(d,a)$ with the elements of Aff(2,q). We will denote elements of Aff(2,q) by $(y\ x)$. We now define

$$S_q(d,a) = \left\{ x + y\sqrt{d} \in \mathrm{Aff}(2,q) : x^2 = ay = d(y-1)^2 \right\}.$$

The affine group acts on $z \in H_q$ by the linear transformation

$$gz = az + b \in H_q, g \in \mathrm{Aff}(2,q).$$

We notice that $k(z,w) = k(gz,gw)$ since

$$N(gz - gw) = N(a(z-w)) = N(a)N(z-w) = a^2 N(z-w)$$

$$\text{and } Im(gz) = aIm(z).$$

THEOREM 1.2 (ANGEL [1] AND POULOS [11]). *For all odd primes p, $S_q(d,a)$ generates* Aff$(2,q)$.

Proof. From part (2) of Lemma 1.1, we know there are $q+1$ elements of the set S_q defined by the equation in part 1. Since $y \neq 0$,there must be at least one $(y\ x) \in S_q$ with $x \neq 0$. Since S_q is symmetric, for $(y\ x) \in S_q$, (y -x), (y^{-1} y^{-1}x) must also lie in S_q. Thus $(y\ x)\ (y^{-1}\ y^{-1}x) = (1\ 2x) \in G$. Then $(1\ 2x)^n = (1\ 2nx) \in G$ for all integers n.

The element $(1\ b)$, $b \neq 0$, has order p, since by induction it can be shown that the nth power of $(1\ b)$ is $(1\ nb)$. Next, the order of the element $(a\ b)$ where $a \neq 1$ is the same as the order of a. If $b = 0$, then it is obvious this is true. If $b \neq 0$, then conjugate $(a\ b)$ by the element $(b^{-1}(1-a^{-1})\ a^{-1})$ and the resulting element is $(a\ 0)$. Since conjugate elements have the same order, the order of $(a\ b)$ is the same as the order of a.

Next, we see that Aff$(2,q)$ can be generated by any element of order p and any element of order $q-1$.

Now any element of order p must be of the form $(1\ b)$. Let $(a\ b)$ be an element of order p. If $a \neq 1$, then the order of $(a\ b)$ is

the same as the order of a in the field of q elements. This order must divide $q-1$, and so can't be p, as p doesn't divide $q-1$. So a must be 1, and any element of order p has the form $(1\ b)$, where $b \neq 0$. And any element of order $q-1$ has the form $(a\ c)$ where the order of a is $q-1$. Let H be the subgroup generated by these two elements. Notice that $(a\ c)(1\ b)(a\ c)^{-1} = (1\ ab)$, so repetition of this conjugation will give us elements of the form $(1\ (a^n)b)$ for all powers of n. Each one of these elements is of order p, and we have $q-1$ of them since the order of a is $q-1$. Now, since the order of Aff$(2,q)$ is $q(q-1)$, Sylow theory tells us that Aff(2,q) has one p-Sylow subgroup of order q, containing every element of order p. Since H contains every element of order p (there are at most $q-1$ of them, and H contains $q-1$ of them), H contains the p-Sylow subgroup. So, H contains a subgroup of order q, and as H contains an element of order $q-1$, H contains a subgroup of order $q-1$. Since q and $q-1$ are relatively prime, the product of these two subgroups will have order $q(q-1)$, and so we must have H=Aff(2,q). Now, to show that the graphs are connected, we need to show that the set $S_q(d,a)$ generates Aff(2,q). From the above, it is sufficient to show that S=$S_q(d,a)$ can generate an element of order p and of order $q-1$. Let g be a generator of F_q. Let $T = \{y | (y\ x) \in S\}$. Then $\forall y \in T$, $y = g^{a_i}$ for some i. Let c be the gcd of all the a_i. Since for each distinct $y \in T$, there are at most two x s.t. $(y\ x) \in S$, then T contains at most $\frac{2(q-1)}{c}$ elements, as there are at most $\frac{(q-1)}{c}$ elements of the form (g^a) where c divides a, and a is between 0 and $q-2$. Since the cardinality of T is $q+1$ including repetitions, we must have $c=1$. Hence the subgroup generated by S contains an element of order $q-1$.

Since S has cardinality $q+1$ and the multiplicative group of F_q has order $q-1$, there is some element in $T, y, s.t. (y\ x_1), (y\ x_2) \in S$, with $x_1 \neq x_2$. Take any other $(c\ d) \in S$. Consider the element

$$(c\ d)(y\ x_1)(c\ d)^{-1}(y\ x_1)^{-1} = (1\ x_1(c-1) + d(1-y)).$$

If $x_1(c-1)+d(1-y) \neq 0$ (which can only happen if $x_1 \neq (y-1)d*(c-1)^{-1}$), we are done as this element has order p. If this is zero, then x_2 is not x_1, so doing the same with $(y\ x_2)$ instead of $(y\ x_1)$ will give us an element of order p. So, the subgroup generated by S

has an element of order p and an element of order $q-1$, and thus S generates Aff(2,q). □

THEOREM 1.3. *The graphs $X_q(d,a)$ are Cayley graphs.*

Proof. We think of the elements of $\mathrm{Aff}(2,q)$ as being the vertices and $S_q(d,a)$ as being the symmetric set or rather that

$$\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} \in S_q(d,a) \Leftrightarrow \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}^{-1} \in S_q(d,a).$$

This is because

$$\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1/y & -x/y \\ 0 & 1 \end{pmatrix}$$

and $x^2 = \mathrm{ay} + \mathrm{d}y - 1^2$ is equivalent to $(-x/y)^2 = a(1/y) + d(1/y-1)^2$. Consider $w, z \in \mathrm{Aff}(2,q)$. We need to show

$$(w,z) \in E\Gamma \Rightarrow w = zs \text{ where } s \in S_q(d,a).$$

$(\sqrt{d}r, \sqrt{d}) = (r, \sqrt{d}) \in E\Gamma$. We prove the statement by recalling that $k(z,w) = k(gz,gw)$ and letting $g = z^{-1}$. Then $(gz,gw) \in E\Gamma$ and $z^{-1}w \in S_q(d,a)$. □

2. Are these graphs good expanders? We now try to determine if the graphs are good expander graphs as graphs of this type are of interest in communications theory. See Lubotsky [**9**], Bien [**2**], Klawe [**8**] and Chung [**5**] for applications and more discussion. Lubotsky, Phillips and Sarnak [**9**] show that a regular graph of degree k is a good expander if it satisfies the Ramanujan bound, meaning that the second largest eigenvalue of the adjacency matrix, $\lambda \leq \sqrt{k-1}$. So we need to find the eigenvalues of the adjacency matrix. Unfortunately the adjacency matrices are of degree q^2-1, which makes it difficult to find the eigenvalues even on a computer. So we will use representation theory and take a Fourier transform to find eigenvalues of isospectral matrices of smaller dimension that the adjacency matrices.

3. Representation Theory for the Prime Power Case. We wish to mimic what Terras [**12**] did in the prime case. However we are not dealing with a cyclic additive group so the representation theory in this case involves taking traces. Also as all the elements of F_q are not integers, we cannot talk about taking powers of matrices for arbitrary elements. Thus most of the material in this section is unique to the prime power case. However the definitions in this section allow us to use the same proof in Section 4 that Terras [**12**] uses in the prime case. Some elementary proofs about traces will be given to help the reader unfamiliar with this material. For information on representation theory, we refer the reader to Diaconis [**6**], Mackey [**10**], and Terras [**13**].

Since F_q - $\{0\}$ is a cyclic multiplicative group with primitive element g, we can find the one-dimensional eigenvalues in a similar way to the prime case. Let

$$\chi_j(y) = exp\left(\frac{(2\pi ijk)}{q-1}\right), \quad \text{if} \quad y = g^k$$

where 0 $\leq$ j $\leq$ q - 1.

This leads to a representation we will also call χ_j:

$$\chi_j\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} = \chi_j(y).$$

For the q-1 dimensional eigenvalues, we would like to define the representation as we did earlier but we notice that F_q is not a cyclic additive group. We think of it as the cross product $F_q = F_p \times F_p \times \ldots \times F_p$ r times. So we need to consider the Galois group of order r.

Let $\sigma(x) = x^p$. Then Tr(x) = $\sum_{i=0}^{n-1} \sigma^i(x)$.

LEMMA 3.1. $\mathrm{Tr}(x+y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$.

LEMMA 3.2. *For p odd,* $\mathrm{Tr}(g(-x)) = -\mathrm{Tr}(gx)$.

Then as in the prime case, we can define the additive character of F_p,

$$\Psi(x) = exp\left(\frac{(2\pi ix)}{p}\right), \quad \text{for x} \quad \in F_p,$$

and define

$$\tilde{\Psi}(x) = \Psi(Tr(x)).$$

LEMMA 3.3.

$$\tilde{\Psi}(u+v) = \tilde{\Psi}(u)\tilde{\Psi}(v).$$

We need a representation for the additive group of F_q. We will use the abbreviation (y x) = $\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}$. Then we define the induced representation, $\rho = Ind_N^G \tilde{\Psi}$,

$$\text{where N} = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in F_q \right\}$$

$$\text{and G} = \text{Affine group} = \left\{ \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} : y \neq 0, x, y \in F_q \right\}.$$

Ψ gives a 1-dimensional representation of N via

$$\tilde{\Psi} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \tilde{\Psi}(b).$$

The matrix ρ(t), t $\in$ G, is obtained from right translation of functions in the space

$$V_{\tilde{\Psi}} = \left\{ f : G \to \mathcal{C} | f(nx) = \tilde{\Psi}(n) f(x) \text{ for all } n \in \mathcal{N} \text{ and all } x \in G \right\}$$

$$\text{Define } (\rho(g)f)(x) = f(xg) \forall x, g \in G.$$

This is a group representation since

$$\begin{aligned} (\rho(g_1 g_2)f)(x) &= f(x g_1 g_2) \\ (\rho(g_1)\rho(g_2)f)(x) &= (\rho(g_2)f)(x g_1) \\ &= f(x g_1 g_2). \end{aligned}$$

Choose the basis of $V_{\tilde{\Psi}}$ given by

$$f_j(\text{y x}) = \tilde{\Psi}(x)\delta(\text{i j}) \quad \text{if} \quad y = g^i, 0 \leq q-2.$$

And define $\delta(i,j) = 1$ if i=j and 0 otherwise.

We now notice that (a b) = (1 b)(a 0). Since representations are homomorphisms, if we wish to see what happens to an element

$(a\ b) \in \mathrm{Aff}(2,q)$ we can consider what happens to (a 0) under the induced representation and what happens to (1 b) under the induced representation. So $\rho(a\ b) = \rho(1\ b)\rho(a\ 0)$. Then $(\rho(1\ b)f_j)(y\ x) = f_j((y\ x)(1\ b))$. And $(\rho(a\ 0)f_j)(y\ x) = f_j((y\ x)(a\ 0))$.

LEMMA 3.4.

$$(\rho(1\ b)f_j)(y\ x) = \tilde{\psi}\left(g^j b\right) f_j(y\ x).$$

Proof. We use Lemma 3.2, the fact that $y = g^i$ for g a primitive root and the fact that $\delta(i,j) = 0$ for $i \neq j$.

$$\begin{aligned}(\rho(1\ b)f_j)(y\ x) &= f_j\left((y\ x)(1\ b)\right) &&= f_j(y\ yb + x)\\ &= f_j\left(g^i\ g^i b + x\right) &&= \tilde{\psi}\left(g^i b + x\right)\delta(i,j)\\ &= \tilde{\psi}\left(g^i b\right)\tilde{\psi}(x)\delta(i,j) &&= \tilde{\psi}\left(g^j b\right)\tilde{\psi}(x)\delta(i,j)\\ &= \tilde{\psi}\left(g^j b\right) f_j(y\ x).\end{aligned}$$

□

LEMMA 3.5.

$$(\rho(a\ 0)f_j)(y\ x) = \tilde{\psi}(x)\delta(t+i,j).$$

Proof. We use that $a = g^t$, $y = g^i$.

$$\begin{aligned}(\rho(a\ 0)f_j)(y\ x) &= f_j\left((y\ x)(a\ 0)\right) = f_j(ya\ x)\\ &= f_j(g^t g^i\ x) = f_j(g^{t+i}\ x) = \tilde{\psi}(x)\delta(t+i,j).\end{aligned}$$

□

LEMMA 3.6. *For* $g = (a\ b) \in Aff(2,q)$, $\rho(g) = DW^{\log a}$

$$\text{where } D = \begin{pmatrix} \tilde{\Psi}(g^0 b) & 0 & 0\ldots & 0\\ 0 & \tilde{\Psi}(g^1 b) & 0\ldots & 0\\ \vdots & 0 & 0\ddots & 0\\ 0 & 0 & 0\ldots & \tilde{\Psi}(g^{q-2} b)\end{pmatrix}$$

$$\textit{and where } W = \begin{pmatrix} 0\,1\,0\ldots 0 \\ 0\,0\,1\ldots 0 \\ \vdots\,0\,0\,\ddots\,0 \\ 0\,0\,0\ldots 1 \\ 1\,0\,0\ldots 0 \end{pmatrix}.$$

Proof. We have already determined that $\rho(a\ b) = \rho(1\ b)\rho(a\ 0)$. So we see the representation is a product of two matrices which we can call D and U. By Lemma 3.4 we get that

$$D_{i,j} = \begin{cases} \tilde{\psi}(g^j b) & \text{if i=j} \\ 0 & \text{otherwise.} \end{cases}$$

We see that D is a diagonal matrix with jth entry $\tilde{\psi}(g^j b)$. By Lemma 3.5 we get that

$$U_{i,j} = \begin{cases} 1 & \text{if } \log a + i = j \\ 0 & \text{otherwise.} \end{cases}$$

We see that U is an $\log a$-shift from the identity matrix and thus $U = W^{\log a}$. □

4. Fourier Transform. To mimic the prime case as much as we can, we apply the Fourier transform to the adjacency operator which we define to be

$$\mathcal{A}f(x) = \sum_{\text{y adjacent to x}} f(y).$$

We then see that

$$\mathcal{A}f(x) = \sum_{s \in S} f(sx)$$

because y = sx is true for $s \in S$ as shown earlier. We recall the definition of the Fourier transform $\mathcal{F} : L^2(G) \mapsto L^2(\hat{G})$ by

$$\mathcal{F}f(\rho) = \hat{f}(\rho) = \sum_{g \in G} f(g)\rho(g).$$

We define convolution between f and g to be

$$f * g(x) = \sum_{y \in G} f(y)g(y^{-1}x).$$

It is known that

$$\mathcal{F}(f * g)(x) = \mathcal{F}(f(x))\mathcal{F}(g(x)).$$

THEOREM 4.1. *Let A be the adjacency matrix of H_q. Now, as in the prime case if we take the Fourier Transform to diagonalize the adjacency matrix, we get*

$$\mathcal{F}A\mathcal{F}^{-1} = \begin{pmatrix} R & 0 \\ 0 & \tilde{M} \end{pmatrix}$$

where R is a $q \times q$ diagonal matrix with diagonal entries R_j coming from the one-dimensional representations of the Affine Group. (Thus the eigenvalue $q+1$ would occur here as it occurs only once.) Then

$$R_j = \sum_{(x,y) \in S_q(d,a)} \chi_j(y)$$

for $\chi_j(y)$ defined earlier and $O \leq j \leq q-2$. Then $\tilde{M}$ is a block diagonal matrix with $(q-1)$ identical blocks down the diagonal where each block is

$$M = \sum \rho(s) = \sum_{(x,y) \in S_q(d,a)} DW^{\log y}$$

where ρ is the $q-1$ dimensional representation of $\mathrm{Aff}(2,q)$ *over F_q and D and W are as defined in Lemma 3.6.*

Proof. We will mimic Terras's [**12**] proof of the prime case.
We define for $x \in G$

$$1_S(x) = \begin{cases} 1 & \text{if } x \in S \\ 0 & \text{otherwise.} \end{cases}$$

Then we notice that

$$\begin{aligned} \mathcal{A}f(x) &= \sum_{s \in S} f(sx) = \sum_{y \in G} 1_S(y) f(y^{-1}x) \\ &= 1_S * f(x). \end{aligned}$$

Then

$$\mathcal{F}A\mathcal{F}^{-1}k\rho = \mathcal{F}(A\mathcal{F}^{-1}k)\rho = \mathcal{F}(1_S * \mathcal{F}^{-1}k)\rho$$
$$= (\mathcal{F}1_S\rho)(\mathcal{F}\mathcal{F}^{-1}k\rho) = \Big(\sum_{g\in \mathrm{Aff}(2,q)} 1_S(g)\rho(g)\Big)k\rho.$$

If we choose first for k to be those elements of the basis of $L^2(\hat{G})$ which correspond to the one-dimensional representations of Aff(2,q), then we see we get a diagonal matrix with jth entry of $\chi_j(y)$.

If we choose next for k those elements of the basis of $L^2(\hat{G})$ which correspond to the q-1 dimensional representation of Aff(q). We then notice that the basis elements look like

$$(x, 0, ..., 0), (0, x, ..., 0), ..., (0, ..., 0, x).$$

Then we see that $MX = (Mx, Mx, Mx, ..., Mx)$ if we look at it in columns. Thus this corresponds to q-1 copies of the M matrix running diagonally down. □

5. Graphs with similar spectra in the prime power case. We will now talk about different graphs which have similar spectra. We will denote the two graphs $X_q(d, a_1)$ and $X_q(d, a_2)$ since the graphs will be over the same field, use the same non-square and will differ only in the "a-distance" between vertices. Then the corresponding M submatrices described in Theorem 4.1 will be called M_1 and M_2. And the matrix W is as defined in Lemma 3.6.

PROPOSITION 5.1. *If* $a_1 + a_2 \equiv 4d(mod\ q)$ *then* $M_2 = M_1 W^{\frac{q-1}{2}}$.

Proof.

$$a_1 + a_2 \equiv 4d(modq) \Leftrightarrow$$
$$y_1(a_1 + a_2) \equiv 4y_1 d(modq) \Leftrightarrow$$
$$a_1y_1 + d{y_1}^2 - 2dy_1 + d \equiv -a_2y_1 + d{y_1}^2 + 2dy_1 + d(modq) \Leftrightarrow$$
$$a_1y_1 + d(y_1 - 1)^2 \equiv -a_2y_1 + d(-y_1 - 1)^2(modq) \Leftrightarrow$$
$${x_1}^2 \equiv {x_2}^2 \text{ and } y_1 \equiv -y_2 \Leftrightarrow$$
$$(x_1, y_1) \in S_q(a_1, d) \Leftrightarrow$$
$$(x_1, -y_1) \in S_q(a_2, d).$$

$$\text{Then } M_1 = \sum_{(x,y)} D^x W^{\log y},$$

$$M_2 = \sum_{(x,-y)} D^x W^{\log(-y)} = \sum_{(x,y)} D^x W^{\log y + \frac{q-1}{2}}$$
$$= \sum_{(x,y)} D^x W^{\log y} W^{\frac{q-1}{2}} = M_1 W^{\frac{q-1}{2}}.$$

Since W is a 1-shift from the identity matrix, we see that

$$W^{\frac{q-1}{2}} = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}.$$

□

PROPOSITION 5.2. *The M's are block symmetric matrices.*

Proof. Recall

$$M = \sum \rho(s) = \sum_{(x,y)\in S_{q,a}} DW^{\log y}$$

and

$$D = \begin{pmatrix} \tilde{\Psi}(g^0 x) & 0 & 0 \ldots & 0 \\ 0 & \tilde{\Psi}(g^1 x) & 0 \ldots & 0 \\ \vdots & 0 & 0 \ddots & 0 \\ 0 & 0 & 0 \ldots & \tilde{\Psi}(g^{q-2} x) \end{pmatrix}$$

where

$$\tilde{\Psi}(x) = exp\left(\frac{(2\pi i Tr(x))}{p}\right), \text{ for x} \in F_p.$$

Since the D's are diagonal and for every y term we get both an x and an -x term the diagonal terms in the sum will be

$$\exp\left(\frac{2\pi i Tr(g^j x)}{p}\right) + \exp\left(\frac{2\pi i Tr(g^j(-x))}{p}\right)$$
$$= \exp\left(\frac{2\pi i Tr(g^j x)}{p}\right) + \exp\left(\frac{2\pi i - Tr(g^j x)}{p}\right)$$
$$= 2\cos\left(\frac{2\pi Tr(g^j x)}{p}\right).$$

Since g is a primitive root of q

$$Tr(g^{j+\frac{q-1}{2}}x) = Tr(g^j g^{\frac{q-1}{2}}x)$$
$$= Tr((-1)g^j x) = -Tr(g^j x)$$

and thus

$$cos\left(\frac{2\pi}{p}Tr(g^{j+\frac{p-1}{2}}x)\right) = cos\left(-\frac{2\pi}{p}Tr(g^j x)\right) = cos\left(\frac{2\pi}{p}Tr(g^j x)\right)$$

so we see the sum of the D's for opposite values of x leads to a block symmetric matrix.

Now we notice that W is block symmetric. In the $(p-1)/2 \times (p-1)/2$ submatrix (call it 1) of W we have a single right shift of I followed by a row of the zero matrix. Then the lower $(p-1)/2 \times (p-1)/2$ submatrix of W (call it 4) is identical as it does not include the row with the 1 entry in the $\frac{p-1}{2}+1$ place but includes all after it. Then the submatrix to the right of 1 contains all zeros except for a 1 in the first column of the (last) $\frac{p-1}{2}$ row. Then the submatrix to the left of 4 contains all zeros except for a 1 in the first column of the last row. So W is block symmetric.

We also see that each $W^{\log y}$ is of block symmetric matrix form as. we can see by induction.

$$\text{Let W} = \begin{pmatrix} U & V \\ V & U \end{pmatrix}.$$

$$\text{Then } W^2 = \begin{pmatrix} U^2+V^2 & UV+VU \\ VU+UV & U^2+V^2 \end{pmatrix}.$$

$$\text{Now assume } W^j = \begin{pmatrix} A & B \\ B & A \end{pmatrix}.$$

$$\text{Then } W^{j+1} = W^j W = \begin{pmatrix} UA+VB & UB+VA \\ VA+UB & UA+VB \end{pmatrix}.$$

The previous proof also shows us that $(D^x + D^{-x})\, W^{\log y}$ is block symmetric. An extremely simple induction shows us that

$$\text{M} = \sum_{(x,y)} D^x W^{\log y}$$

is also block symmetric. □

PROPOSITION 5.3. *If $a_1 + a_2 \equiv 4d(mod\ q)$, then the eigenvalues of the M's are the same up to a factor of -1.*

Proof. Using Propositions 5.1 and 5.2 we see that

$$M_1 = \begin{pmatrix} A & B \\ B & A \end{pmatrix} \Rightarrow M_2 = \begin{pmatrix} B & A \\ A & B \end{pmatrix}.$$

Then we take the Fourier transform to block diagonalize the matrices.

$$\text{Let} \quad \mathcal{F} = \begin{pmatrix} I & I \\ -I & I \end{pmatrix}.$$

$$\text{Then} \quad \mathcal{F}^{-1} = \begin{pmatrix} I & -I \\ I & I \end{pmatrix}.$$

$$\text{So} \quad FM_1F^{-1} = \begin{pmatrix} 2(A+B) & 0 \\ 0 & 2(A-B) \end{pmatrix}.$$

$$\text{But then} \quad FM_2F^{-1} = \begin{pmatrix} 2(B+A) & 0 \\ 0 & 2(B-A) \end{pmatrix}.$$

□

COROLLARY 5.4. *If $a = 2d$, the graph has at least $\frac{q-1}{2}$ zero eigenvalues.*

6. Computer Implementation. The two major differences in computing this case versus the prime case is that first of all F_q unlike F_p is not a cyclic additive group. Thus the software for computing the elements in S_q(d,a) versus S_p(d,a) and the representations for Aff(2,q) versus Aff(2,p) is quite different.

Since the elements of F_q are the elements of the splitting field $x^q - x = 0$, one element is 0 and the others are the p^{r-1} roots of unity. We can think of these elements as powers of the primitive root (a multiplicative group) or as linear combinations of the primitive root over the field F_p.

In some cases using the additive properties is better and in other using the multiplicative properties is better so in the computer implementation this time, the program computes a logarithm table for the powers of the primitive root. Then in calculating the solutions to

$$x^2 = ay + d(y-1)^2$$

the program switches back and forth in the log table depending on the if the operation is better suited to the additive or multiplicative properties. If $x = 0$ is a solution this is a special case as it is not a power of the primitive root and does not belong in the log table. This special case occurs if and only if $(a-4d)a$ is a square as will be seen in the Lemma 8.3 so the program accounts for this situation.

The program then finds the one-dimensional and (q-1)-dimensional eigenvalues as shown in Lemma 5.9 and compare them with the Ramanujan bound. The program uses the multiplicative properties to find the trace and representation as it is easy to take exponents. The program uses the result of Proposition 5.2 to cut the M matrix from being $q-2 \times q-2$ dimensional to $\frac{q-2}{2} \times \frac{q-2}{2}$ dimensional.

7. Computer Results. The program was run on a Solbourne 5/804. This machine is a four CPU system with 64 MB of memory. Each processor is rated at about 13.5 SPEC marks. for a total processing capacity equal to 68 DEC VAX11/780s. The processors implement SUN's SPARC architecture. The operating system software is OS/MP, which is derived from SunOS which is an implementation of UNIX. Computer results show that for q up to 11^2, the Ramanujan bound does hold for all values of a. For values of a up to 42, the bound holds for $q = 13^2$. For values of a up to 19, the bound hold for $q = 3^5$. The computer account ran out of processor time before more values of a could be checked.

Interestingly, for even powers of the primes 3,5,7,11 and 13, some of the eigenvalues are equal to the Ramanujan bound in the one-dimensional and sometimes q-dimensional eigenvalues as we see in Table 3. We recall that the one-dimensional eigenvalues from Theorem 4.1 to look like

$$\sum_{(x,y)\in S_q(d,a)} \cos\frac{2\pi j \log y}{q-1}$$

because the sin terms will cancel out since sin is an odd function and by an explanation given in Theorem 1.3, both $(y\ x)$ and $(y^{-1}\ -xy^{-1}) \in S_q(d,a)$. We now notice that these one-dimensional eigenvalues will be integers for appropriate values of y and j as will each term in the summation. Also for even powers of primes, the Ramanujan bounds will be integers. The Ramanujan bounds are not integers for odd powers of primes.

The table shows the prime power, the a values where the boundary eigenvalues occur, the eigenvalue and the j values as described above and in Theorem 4.1. The a values are given as powers of the primitive root of F_q which was used also as d.

8. Girths of the X_q. We now turn to the second purpose of this paper which is to explore the girths of these graphs. We define the girth to be the length of the shortest circuit in a graph. Except for the proof of Theorem 8.4 which shows the girth to be 4 if it is not 3, the proofs only prove the graphs to have girth 3.

LEMMA 8.1. *The girth of a graph of H_q is either 3 or 4.*

Proof. We use a result of Tutte's [**3**] that the number of vertices in a graph of valency k and odd girth is at least

$$1 + k + k(k-1) + \ldots + k(k-1)^{\frac{1}{2}(g-3)}.$$

So we assume the girth is 5. Then the number of vertices is at least

$$n = 1 + (q+1) + (q+1)q.$$

This is a contradiction since the number of vertices is q(q-1) and $n > q(q-1)$. □

LEMMA 8.2. *If the number of origin neighbors who are neighbors is at least one, the girth is 3. Otherwise the girth is 4.*

Proof. If $(o, s_1), (o, s_j), (s_1, s_j) \in E\Gamma$, clearly the girth is 3.

TABLE 3. Values of q, a and j For Boundary Eigenvalues

q	$\log_d a$	Eigenvalue	j
3^2	5	-6	4
5^2	1	-10	12
5^2	7	-10	6,8,16,18
5^2	9	-10	12
7^2	1	-14	24
7^2	6	14	16,32
7^2	9	-14	24
7^2	17	-14	8,12,24,36,40
7^2	36	14	16,32
3^4	41	18	10,16,30,32,40,48,50,64,70
11^2	13	22	60
11^2	25	22	40,80
11^2	37	22	12,20,36,40,60,80,84,100,108
11^2	53	22	60
11^2	61	22	40,80
11^2	85	-22	30,90
11^2	93	22	60
11^2	97	-22	30,90
11^2	109	22	60
13^2	15	26	14,24,42,48,70,96,98,120,126,144,154
13^2	24	26	84
13^2	33	26	84

Now assume Γ has girth 3. Then for some $w_1, w_2, w_3 \in V\Gamma$

$$(w_1, w_2), (w_2, w_3), (w_3, w_1) \in E\Gamma.$$

Since $k(w_1, w_2) = k(gw_1, gw_2)$,

$$(gw_1, gw_2) \in E\Gamma, (gw_2, gw_3) \in E\Gamma, (gw_3, gw_1) \in E\Gamma.$$

Now letting $g = w_1^{-1}$,

$$(gw_1, gw_2) = (o, gw_2) \Rightarrow gw_2 \in S$$

$$(gw_3, gw_1) = (gw_3, o) \Rightarrow gw_3 \in S.$$

So there is at least one pair of origin neighbors who are neighbors. □

LEMMA 8.3.

$$(y\ 0) \in S \Leftrightarrow a(a - 4d) \text{ is a square in } F_q.$$

Proof.

$$0 = ay + d(y-1)^2 \Leftrightarrow$$
$$0 = dy^2 + (a-2d)y + d \Leftrightarrow$$
$$y = \frac{2d - a \pm \sqrt{(a-2d)^2 - 4d^2)}}{2d} \Leftrightarrow .$$

There is a solution for $y \in F_q \Leftrightarrow a(a-4d)$ is a square. □

THEOREM 8.4. *Let $X_q(d, 2d) = \Gamma$. If $q \equiv 1(mod\ 4)$ the girth of of the graph is 4. If $q \equiv 3(mod\ 4)$, the girth of the graph is 3.*

Proof. Assume Γ has girth 3. Then by Lemma 8.2 for any $s_1 \in S$, there exists $s_2 \in S$, where $(s_1, s_2) \in E\Gamma$.

$$x_1^2 = ay_1 + d(y_1 - 1)^2 = dy_1^2 + d$$
$$x_2^2 = ay_2 + d(y_2 - 1)^2 = dy_2^2 + d$$

$$\frac{(x_2 - x_1)^2 - d(y_2 - y_1)^2}{y_1 y_2} = a \Leftrightarrow$$
$$x_2^2 - 2x_1x_2 + x_1^2 - dy_2^2 + 2dy_1y_2 - dy_1^2 = ay_1y_2 \Leftrightarrow$$
$$dy_2^2 + d - 2x_1x_2 + dy_1^2 + d - dy_2^2 + 2dy_1y_2 - dy_1^2 = ay_1y_2 \Leftrightarrow$$
$$2d - 2x_1x_2 = ay_1y_2 - 2dy_1y_2 \Leftrightarrow$$
$$2(d - x_1x_2) = (a-2d)y_1y_2 \Leftrightarrow$$
$$-2x_1x_2 = -2d + (a-2d)y_1y_2 \Leftrightarrow x_1x_2 = d.$$

First we consider the case $q \equiv 1(\text{mod } 4)$. We notice that -1 is a square. By the above equations, we have

$$y_1^2 + 1 = x_1^2/d = d/x_2^2$$

and

$$y_2^2 + 1 = x_2^2/d = d/x_1^2.$$

We notice that for $i \in 1, 2y_i^2 \neq -1$ since then $x_i^2 = 0$ and $x_1x_2 = 0$. Therefore

$$(y_1^2 + 1)(y_2^2 + 1) = y_1^2y_2^2 + y_1^2 + y_2^2 + 1 = y_1^2(y_2^2 + 1) + y_2^2 + 1 \equiv 1.$$

But this implies that

$$y_2^2 + 1 \equiv \frac{-y_2^2}{y_1^2}.$$

But the right hand is a square, while the left hand is not (since it's equal in F_q to x_2^2/d, and d is not a square), so we have a contradiction, and the girth must be 4.

Now we wish to show that for $q \equiv 3(\text{mod } 4)$, the girth is 3. We will show that

$$\forall(y_1\ x_1) \in S \exists (y_2\ x_2) \in S \qquad \text{so} \qquad x_1 x_2 = d.$$

Given $(y_1\ x_1) \in S$. Then

$$x_1^2 = dy_1^2 + d \Leftrightarrow y_1^2 = \frac{x_1^2 - d}{d} \Leftrightarrow \frac{x_1^2 - d}{d} \qquad \text{is a square.}$$

Recall that $d = g$, the first primitive root in F_q. We notice that for $q \equiv 3(\text{mod } 4)$, if g is the first primitive root in F_q, $g^{\frac{q-3}{2}}$ is a square.

$$g^{\frac{q-3}{2}} = g^{\frac{q-1}{2}-1} = \frac{g^{\frac{q-1}{2}}}{g} = \frac{-1}{d}.$$

Thus $\dfrac{-1}{d}$ is a square. Then, $-\dfrac{x_1^2}{d}$ is a square, and since we already determined that $\dfrac{x_1^2 - d}{d}$ is a square,

$$\frac{x_1^2 - d}{d} = (\frac{d}{x_1^2} - 1)(-\frac{x_1^2}{d}) \Rightarrow$$

$$\frac{d}{x_1^2} - 1 \text{ is a square } \Rightarrow \exists y_2 \text{ where } y_2^2 = \frac{d}{x_1^2} - 1.$$

$$\text{Thus } y_2^2 + 1 = \frac{d}{x_1^2} \Rightarrow dy_2^2 + d = \frac{d^2}{x_1^2} \Rightarrow$$

$$\left(y_2\ \frac{d}{x_1}\right) = (y_2\ x_2) \in S.$$

□

LEMMA 8.5. $(1\ \sqrt{a}) \in S \Leftrightarrow a$ *is a square in* F_q.

Proof. Since $x^2 = ay + d(y-1)^2, y = 1, y = \dfrac{d-a}{d} \Leftrightarrow x^2 = a$. □

THEOREM 8.6. *In* $X_q(d,a)$, *if* a *is a square in* F_q *and* $a - 3d$ *is a square in* F_q *then the girth is 3.*

Proof. By Lemma 8.5, if a is a square in F_q, $(1\ \sqrt{a}) \in S$. We see that the neighbors of $s_i \in S$ are of the form $s_i s_j$ for $1 \leq j \leq q+1$ since s_i is a neighbor of the origin and we do a left multiplication of the origin neighbors by s_i to get the neighbors of s_i.

$$(1\ \sqrt{a})(y_l\ x_l) = (y_l\ x_l + \sqrt{a}).$$

By Lemma 8.2 $X_q(d,a)$ has girth 3 whenever

$$\exists (y_l\ x_l) \in S \qquad \text{such that} \qquad (y_l\ x_l + \sqrt{a}) \in S.$$

Since $(y\ x) \in S \Leftrightarrow x^2 = ay + d(y-1)^2$, and we notice that the right hand side of the equation only depends on y, so both $(y_l\ x_l), (y_l\ x_l + \sqrt{a}) \in S$, if

$$x_l^2 = (x_l + \sqrt{a})^2 \Leftrightarrow x_l = -\frac{\sqrt{a}}{2}.$$

$$\text{Then} \qquad (1\ \sqrt{a})(y_l\ -\frac{\sqrt{a}}{2}) = (y_l\ \frac{\sqrt{a}}{2}).$$

$$\text{Now} \qquad (y_l\ \frac{\sqrt{a}}{2}) \in S \Leftrightarrow$$

$$\frac{a}{4} = ay_l + d(y_l - 1)^2 \Leftrightarrow$$

$$0 = dy_l^2 + (a-2d)y_l + (d - \frac{a}{4}) \Leftrightarrow$$

$$y_l = \frac{(2d-a) \pm \sqrt{a^2 - 3ad}}{2d}.$$

And there is a solution for $y_l \Leftrightarrow a^2 - 3ad$ is a square. □

REFERENCES

[1] J. Angel, Ph.D. Thesis, (U.C.S.D. 1993).

[2] F. Bien, *Construction of Telephone Networks by Group Representations*, Notices of the A.M.S., **36** (1989), 5-22.

[3] N. Biggs, *Algebraic Graph Theory*, Cambridge University Press, London 1974.

[4] N. Celniker, S. Poulos, A. Terras, C. Trimble and E. Velasquez, *Is There Life on Finite, Upper Half Planes?*, to appear in Contemporary Math., Amer. Math. Soc.,1990.

[5] F. R. K. Chung, *Diameters and Eigenvalues*, J. of the Amer. Math Soc. , **2** (1980), 187-196.

[6] P. Diaconis, *Group Representations in Probability and Statistics*, Inst. of Math. Stat., Lect. Note-Monograph Series, Haywood, **11** (1988).

[7] N. Katz, *Estimates for Soto-Andrade Sums - 1*, pre-print.

[8] M. Klawe, *Limitations on explicit constructions of expanding graphs*, S.I.A.M. J. Comput. **13** (1984), 156-166.

[9] A. Lubotsky, R. Phillips, and P. Sarnak, *Ramanujan Graphs*, Combinatorica, **8** (1988), 261-277.

[10] G. Mackey, *Unitary Group Representations in Physics, Probability and Number Theory*, Benjamin/Cummings, Reading, Mass, 1978.

[11] S. Poulos, Ph.D. Thesis, U.C.S.D. 1991.

[12] A. Terras, *Eigenvalue Problems Related to Finite Analogues of Upper Half-Planes*, to appear in H. Weyl memorial Volume, Texas A&M University, 1991.

[13] A. Terras, *Harmonic Analysis on Symmetric Spaces and Applications*, **I,II** 1985,1988, Springer-Verlag, New York.

Received June 20, 1991, revised September 11, 1993 and accepted for publication April 11, 1994.

WHITTIER COLLEGE
WHITTIER, CA 90608

PACIFIC JOURNAL OF MATHEMATICS

Volume 166 No. 1 November 1994