Serdica
Mathematical Journal
Сердика
Математическо списание

Serdica Math. J. **42** (2016), 235–250

Serdica
Mathematical Journal

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

THE ISOPERIMETRIC NUMBER OF A GENERALIZED PALEY GRAPH*

Spencer Johnson, Anthony Shaheen, Gustavo Subuyuj

Communicated by M. Domokos

Abstract. Let p be an odd prime, $m \geq 2$ be an integer, and $d = \gcd(m, p-1)$. Suppose that d divides $(p-1)/2$. We define the generalized Paley graph on p and m to be the Cayley graph whose vertex set is $\mathbb{Z}_p$ and whose generating set is the set of non-zero m-th powers modulo p. We derive basic properties of these graphs. We give bounds on the isoperimetric number of a generalized Paley graph.

1. Introduction.

Throughout this paper, let $\mathbb{Z}_p$ denote the integers modulo a prime p and $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$.

We begin by recalling the definition of an undirected Cayley graph. Let G be a group. Let Γ be a symmetric subset of G, that is, $\gamma \in \Gamma$ if and only if $\gamma^{-1} \in \Gamma$. The *Cayley graph* of G and Γ, denoted by $\mathrm{Cay}(G, \Gamma)$, is defined to be the graph whose vertex set is G and where two vertices x and y are adjacent iff $y^{-1}x \in \Gamma$.

2010 *Mathematics Subject Classification:* Primary 05C99; Secondary 11A07.
Key words: isoperimetric number, expansion number, Paley graph, Generalized Paley graph.
*This research was partially supported by NSF grant DMS-1247679.

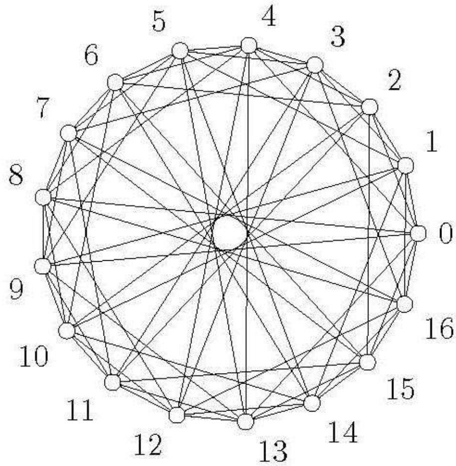

Fig. 1. The graph X_{17}^6

We now define generalized Paley graphs. We generalize the definition from [1] which only considers odd m. Let p be an odd prime, $m \geq 2$ be an integer, and $d = \gcd(p-1, m)$. Suppose that d divides $(p-1)/2$. Consider the set

$$\Gamma_p^m = \{a^m \mid a \in \mathbb{Z}_p^\times\}$$

of m-th powers of non-zero integers modulo p. We define the *generalized Paley graph* X_p^m to be the Cayley graph $\mathrm{Cay}(\mathbb{Z}_p, \Gamma_p^m)$.

We will see in Proposition 3 that the condition that d divides $(p-1)/2$ ensures that the generating set for the generalized Paley graph is symmetric which gives us an undirected graph. One may also consider directed graphs by relaxing this restriction, but we do not do that in this paper.

For example, let $p = 17$ and $m = 6$. Then $d = 2$ which divides $(p-1)/2 = 8$. We have that $\Gamma_{17}^6 = \{1, 2, 4, 8, 9, 13, 15, 16\}$. See Figure 1 for a picture of X_{17}^6.

When $m = 2$ and $p \equiv 1 (\mathrm{mod}\ 4)$ we get the standard definition of a Paley graph.

Let X be a graph with vertex set V. Given a subset of vertices F, the *boundary* of F, denoted by ∂F, is defined to be the set of edges of X with one endpoint in F and one endpoint in $V \setminus F$. The *isoperimetric number*, or *Cheeger constant*, of X is defined to be

$$h(X) = \min\left\{ \frac{|\partial F|}{|F|} \,\middle|\, F \subseteq V \text{ and } 0 < |F| \leq |V|/2 \right\}.$$

In general it is a difficult combinatorial problem to get an exact value for the isoperimetric number of a graph. Instead one gives approximations, which is what we do in this paper. In particular, we generalize the following result from [4]. Let $p \equiv 1 (\mathrm{mod}\ 4)$ and $m = 2$. Then as mentioned above we get that X_p^2 is a standard Paley graph. It was shown in [4] that

$$(1) \qquad \frac{p - \sqrt{p}}{4} \leq h(X_p^2) \leq \frac{p-1}{4}.$$

This implies that $\lim\limits_{p \to \infty} h(X_p^2)/p = 1/4$, where the limit is over primes congruent to 1 modulo 4.

In this paper, we generalize equation (1) to $m \geq 2$. In particular, we derive the following proposition.

Proposition 1. *Let p be an odd prime, $m \geq 2$ be an integer, and $d = \gcd(p-1, m)$. Assume that d divides $(p-1)/2$ and that $d > 1$. Then*

$$\frac{p + (1-d)\sqrt{p}}{2d} \leq h(X_p^m) \leq \frac{(d-1)p + M_m\sqrt{p} + (2d-1)}{d^2}.$$

Here M_m is the number of triples of rational numbers $(\alpha_0, \alpha_1, \alpha_2)$ satistfying $m\alpha_0, m\alpha_1, m\alpha_2 \in \mathbb{Z}$, $\alpha_0 + \alpha_1 + \alpha_2 \in \mathbb{Z}$, and $0 < \alpha_0, \alpha_1, \alpha_2 < 1$.

Note that when $d = 1$ we have that X_p^m is a complete graph (see Proposition 5) whose isoperimetric number is well-known.

See Sections 3 and 4 for a proof of Proposition 1. The lower bound of Proposition 1 is derived using an estimate on the eigenvalues of X_p^m (which are essentially Gauss sums). The upper bound is derived by estimating the number of solutions to the equation $x^m + y^m + z^m = 0$ modulo p.

When $m = 2$ we get that Proposition 1 gives essentially the same result as equation (1). Suppose that $p \equiv 1 (\mathrm{mod}\ 4)$ and $m = 2$. Then $d = \gcd(p-1, 2) = 2$. The integer M_2 is the number of triplets of rational numbers $(\alpha_0, \alpha_1, \alpha_2)$ satistfying the following conditions: $2\alpha_0, 2\alpha_1, 2\alpha_2 \in \mathbb{Z}$, $\alpha_0 + \alpha_1 + \alpha_2 \in \mathbb{Z}$ and $0 < \alpha_0, \alpha_1, \alpha_2 < 1$. This implies that $M_2 = 0$. In this case, Proposition 1 becomes

$$(2) \qquad \frac{p - \sqrt{p}}{4} \leq h(X_p^2) \leq \frac{p+3}{4},$$

which is asymptotically equivalent to equation (1).

We now consider the case when $m = 3$. Suppose that p is an odd prime. If $p \equiv 0 (\mathrm{mod}\ 3)$ or $p \equiv 2 (\mathrm{mod}\ 3)$, then $d = \gcd(p-1, 3) = 1$. This does not

Table 1. Approximate values where $m = 3$ and $p \equiv 1 (\mathrm{mod}\ 3)$

p	lower bound from Prop (1)	$h(X_p^3)$	γ-bound from Prop (2)	upper bound from Prop (1)
7	0.28475	0.6667	0.66667	2.69906
13	0.964816	1.6667	2	4.24568
19	1.7137	?	3.55556	5.74642
104, 743	17, 349.3	?	17, 465.8	23, 348.7
104, 827	17, 363.2	?	17, 529.3	23, 367.4
1, 299, 709	216, 238	?	216, 659	289, 078
2, 750, 161	457, 807	?	458, 707	611, 516

satisfy Proposition 1. Indeed, we will see in Proposition 5 that when $d = 1$ we get a complete graph, whose isoperimetric number is known. Now consider the infinite family of generalized Paley graphs X_p^3 where $p \equiv 1 (\mathrm{mod}\ 3)$. In this case $d = \gcd(p-1, 3) = 3$ which divides $(p-1)/2$. The integer M_3 is the number of triplets of rational numbers $(\alpha_0, \alpha_1, \alpha_2)$ satistfying the following conditions: $3\alpha_0, 3\alpha_1, 3\alpha_2 \in \mathbb{Z}$, $\alpha_0 + \alpha_1 + \alpha_2 \in \mathbb{Z}$ and $0 < \alpha_0, \alpha_1, \alpha_2 < 1$. This implies that $M_3 = 2$. Proposition 1 gives that

$$\frac{p - 2\sqrt{p}}{6} \leq h(X_p^3) \leq \frac{2p + 2\sqrt{p} + 5}{9} \tag{3}$$

See Table 1 for some example calculations of equation (3).

One can try other values of m. For example, any odd power m and $p \equiv 1 (\mathrm{mod}\ m)$ give $d = m$ in equation (1).

We derive a second upper bound for $h(X_p^m)$, which we call the γ-bound. This result is a generalization of the α-bound given in [4] for regular Paley graphs ($m = 2$). The γ-bound appears to give a better upper bound than Proposition 1 does. However, it is harder to deal with and is not in closed form.

In Proposition 3 it is shown that Γ_p^m is a symmetric subset of $\mathbb{Z}_p$ iff $d|(p-1)/2$, and therefore we can write it as

$$\Gamma_p^m = \{\gamma_1, \gamma_2, \cdots, \gamma_k, -\gamma_k, \cdots, -\gamma_2, -\gamma_1\}$$

where $k = \dfrac{p-1}{2d}$ and $0 \leq \gamma_i \leq (p-1)/2$. The proof of the following Proposition is given in Section 5.

Proposition 2 (The γ-bound). *The isoperimetric number of a generalized Paley graph satisfies the bound*

$$h(X_p^m) \leq \frac{4}{p-1} \sum_{i=1}^{k} \gamma_i$$

where $\Gamma_p^m = \{\gamma_1, \gamma_2, \ldots, \gamma_k, -\gamma_k, \ldots, -\gamma_2, -\gamma_1\}$ *and* $k = \dfrac{p-1}{2d}$ *are as above.*

Note that when calculating the sum in Proposition 2 we think of the γ_i as integers, not integers modulo p. For example, we have that $\Gamma_{17}^6 = \{1, 2, 4, 8, 9, 13, 15, 16\}$ where $\gamma_1 = 1$, $\gamma_2 = 2$, $\gamma_3 = 4$, $\gamma_4 = 8$. Thus,

$$h(X_{17}^6) \leq \frac{4}{17-1}(1+2+4+8) = 3.75.$$

See Table 1 for some sample calculations of the γ-bound.

At the very end of the paper we give an upper bound on $h(X_p^m)$ using Proposition 2 and a worse case distribution argument for the sizes of the elements in the first half of Γ_p^m. The argument leads to the following upper bound:

$$h(X_p^m) \leq \frac{(2d-1)p + (4d - 4d^2 + 1)}{2d^2}. \tag{4}$$

If $m = 2$ and $p \equiv 1 (\mathrm{mod}\ 4)$, then equation (4) becomes $h(X_p^2) \leq \frac{3p}{8} - \frac{7}{8}$. If $m = 3$ and $p \equiv 1 (\mathrm{mod}\ 3)$, then equation (4) becomes $h(X_p^3) \leq \frac{5p}{18} - \frac{23}{18}$. Comparing these results to (2) and (3) which were derived from Proposition 1, we see that Proposition 1 gives a better upper bound for the isoperimetric number. However, looking at Table 1 we see that the γ-bound seems to give a much better upper bound than Proposition 1. Perhaps if one got a better approximation on the worst case for the sizes of the elements in the first half of Γ_p^m, then one could get a much better explicit upper bound for $h(X_p^m)$ using the γ-bound. Perhaps this method could lead to an asymptotic formula for $\lim\limits_{p\to\infty} h(X_p^m)/p$ as p goes to infinity for $m > 2$.

2. Basic properties of generalized Paley graphs. In this section we collect together various facts about generalized Paley graphs.

Proposition 3. *Let p be an odd prime, let $m \geq 2$ be an integer, let $d = \gcd(m, p-1)$. Let $m = 2^n a$ for some odd integer a and $n \geq 0$. The following are equivalent.*

(1) Γ_p^m *is symmetric.*

(2) $-1 \in \Gamma_p^m$.

(3) $d \mid \dfrac{p-1}{2}$.

(4) $p \equiv 1 (\text{mod } 2^{n+1})$.

Proof. (1) $\iff$ (2): Suppose Γ_p^m is symmetric. Note that $1 = 1^m \in \Gamma_p^m$. So, $-1 \in \Gamma_p^m$. Conversely, suppose $-1 \in \Gamma_p^m$. Then $-1 = a^m$ for some $a \in \mathbb{Z}_p^\times$. If $x \in \Gamma_p^m$ with $x = b^m$ and $b \in \mathbb{Z}_p^\times$, then $-x = (ab)^m \in \Gamma_p^m$.

(2) $\iff$ (3): Since $\mathbb{Z}_p^\times$ is a cyclic group under multiplication there exists $g \in \mathbb{Z}_p^\times$ where $\mathbb{Z}_p^\times = \langle g \rangle = \{1, g, g^2, g^3, \ldots, g^{p-2}\}$. Since $\mathbb{Z}_p$ is a field there are only two solutions to the equation $x^2 - 1 = (x-1)(x+1) = 0$. These are $1 = g^0$ and $-1 = g^{(p-1)/2}$. Note that $-1 \in \Gamma_p^m$ if and only if $(g^i)^m = g^{(p-1)/2}$ for some integer i if and only if $im \equiv \dfrac{p-1}{2} (\text{mod } p-1)$. From [15, pg. 62], $ax \equiv b (\text{mod } m)$ has solutions for x if and only if $\gcd(a, m) \mid b$. Thus, $im \equiv \dfrac{p-1}{2} (\text{mod } p-1)$ if and only if $d \mid \dfrac{p-1}{2}$.

(3) $\implies$ (4): Suppose that $d \mid \dfrac{p-1}{2}$. Recall that $m = 2^n a$ where a is odd. Let $p-1 = 2^k b$ for some $k, b \in \mathbb{Z}$ where b is odd. Suppose that $n \geq k$. Then $d = \gcd(m, p-1) = \gcd(2^n a, 2^k b) = 2^k c$ for some integer c. But then d would not divide $\dfrac{p-1}{2} = 2^{k-1} b$. Thus $n < k$. Therefore, $p \equiv 1 (\text{mod } 2^{n+1})$.

(4) $\implies$ (2): Recall that $m = 2^n a$ where a is odd. Suppose $p \equiv 1 (\text{mod } 2^{n+1})$. Then $p - 1 = 2^{n+1} k$ for some integer k. Since $\mathbb{Z}_p^\times$ is cyclic there exists $g \in \mathbb{Z}_p^\times$ where $\mathbb{Z}_p^\times = \langle g \rangle = \{1, g, g^2, g^3, \ldots, g^{p-2}\}$. If we let $y = g^{\frac{p-1}{2}}$, then $y \neq 1$. Also $y^2 = g^{p-1} = 1$. Since $\mathbb{Z}_p$ is a field the only solutions to $z^2 - 1 = (z+1)(z-1) = 0$ are $z = 1$ and $z = -1$. Thus, $y = g^{\frac{p-1}{2}} = -1$. If we let $w = g^{\frac{p-1}{2^{n+1}}}$, then $w^m = g^{\frac{p-1}{2^{n+1}} 2^n a} = g^{\frac{p-1}{2} a} = (-1)^a = -1$. So $-1 \in \Gamma_p^m$. $\square$

The proof of the following lemma is left to the reader.

Lemma 4. *Let m be a positive integer, p be an odd prime, and $d = \gcd(m, p-1)$. Define the function $\phi : \mathbf{Z}_p^\times \to \mathbf{Z}_p^\times$ by $\phi(x) = x^m$. Then ϕ is d-to-one.*

The facts in the following proposition are proved in [1] for odd m, but in a different way than we present here. [1] also discusses the case where p is not prime, in which case the generalized Paley graph can sometimes be disconnected.

Proposition 5. *Let m be a positive integer, p be an odd prime, and $d = \gcd(m, p-1)$ where $d \mid \dfrac{p-1}{2}$. Then*

(1) $|\Gamma_p^m| = \dfrac{p-1}{d}$.

(2) X_p^m *is* $\dfrac{p-1}{d}$*-regular.*

(3) X_p^m *is connected.*

(4) X_p^m *is the complete graph iff* $d = 1$.

(5) X_p^m *is the cycle graph iff* $d = \dfrac{p-1}{2}$.

Proof. Let ϕ be the group homomorphism of $\mathbb{Z}_p^\times$ from Lemma 4. By Lemma 4 we have that $|\Gamma_p^m| = |\mathbb{Z}_p^\times|/|\ker(\phi)| = \dfrac{p-1}{d}$.

X_p^m is $\dfrac{p-1}{d}$-regular since X_p^m is a Cayley graph. This implies that X_p^m is complete iff $d = 1$. Similarly this shows that X_p^m is the cycle graph iff $d = \dfrac{p-1}{2}$.

It is easy to see that X_p^m is connected: since $1 \in \Gamma_p^m$ we have that the cycle with vertices $0, 1, 2, 3, \ldots, p-2, p-1, 0$ is contained in the graph. $\square$

We now mention a special case of a well-studied problem for Cayley graphs. Two Cayley graphs on the same group $\mathrm{Cay}(G, S)$ and $\mathrm{Cay}(G, T)$ are isomorphic if there exists a group isomorphism σ of G such that $S^\sigma = T$. A group G is called a CI-group if the converse is also true. See the survey [13] for more information. It was shown in [5] that $\mathbb{Z}_p$ is a CI-group. The following two propositions are special cases of these results and the proofs are left to the reader.

Proposition 6. *Let p be a prime and $m_1 > 1$ and $m_2 > 1$ be integers. Suppose that $d_1 = \gcd(m_1, p-1)$ and $d_2 = \gcd(m_2, p-1)$ and both d_1 and d_2 divide $\dfrac{p-1}{2}$. Then $X_p^{m_1}$ and $X_p^{m_2}$ are isomorphic as graphs if and only if $d_1 = d_2$. In particular, note that $X_p^{d_1}$ is isomorphic to $X_p^{m_1}$.*

Proposition 7. *Let p be a fixed odd prime. A complete list of non-isomorphic generalized Paley graphs of size p is given by the graphs X_p^m where m is a divisor of $(p-1)/2$.*

3. An eigenvalue lower bound.

In this section we give a proof of the lower bound given in Proposition 1. Throughout this section, let p be an odd prime, $m > 1$ be an integer, and $d = \gcd(p-1, m)$. Assume that d divides $(p-1)/2$.

Since X_p^m is a connected regular graph, by [11, pg. 12] we know that the eigenvalues of X_p^m are real. The next Proposition shows that the eigenvalues of X_p^m are essentially Gauss sums and we give an upper bound for them.

Proposition 8. *Let $e_p(x) = e^{\frac{2\pi i x}{p}}$. The eigenvalues of X_p^m are given by*

$$\lambda_a = \frac{1}{d}\left(\sum_{n=0}^{p-1} e_p(an^m) - 1\right), \text{ where } a = 0, 1, \ldots, p-1.$$

One has $\lambda_0 = \dfrac{p-1}{d}$. In addition for each $a = 1, 2, \ldots, p-1$ we have that

$$\lambda_a \leq \frac{(m-1)\sqrt{p} - 1}{d}.$$

Proof. Let λ be an eigenvalue of X_p^m. There exists $0 \leq a \leq p-1$ where $\lambda = \sum_{\gamma \in \Gamma_p^m} e_p(a\gamma)$. (See [3, pg. 183] or [11, pg. 195]).) If $a = 0$, the formula follows. Suppose that $0 < a$. By Lemma 4, for each $\gamma \in \Gamma_p^m$, $|\phi^{-1}(\gamma)| = d$, and so there are d elements $x_1, x_2, \ldots, x_d$ in $\mathbf{Z}_p^\times$ for which $\phi(x_i) = \gamma$. So,

$$\lambda = \sum_{\gamma \in \Gamma_p^m} e_p(a\gamma) = \frac{1}{d}\sum_{n=1}^{p-1} e_p(an^m).$$

Note that

$$\frac{1}{d}\sum_{n=1}^{p-1} e_p(an^m) = \frac{1}{d}\left(\sum_{n=0}^{p-1} e_p(an^m) - 1\right).$$

The Gauss sum $\sum_{n=0}^{p-1} e_p(an^m)$ can be bounded above (see [9, pg. 1]) by $\sum_{n=0}^{p-1} e_p(an^m) \leq (m-1)\sqrt{p}$. Therefore,

$$\lambda = \frac{1}{d}\left(\sum_{n=0}^{p-1} e_p(an^m) - 1\right) \leq \frac{(m-1)\sqrt{p} - 1}{d}. \qquad \square$$

We now give a proof of the lower bound given in Proposition 1. A known inequality (see [2] and [6], or [11, pg. 31]) tells us that if X is a k-regular graph, then

$$\frac{k - \lambda_1(X)}{2} \leq h(X), \tag{5}$$

where $\lambda_1(X)$ is the second largest eigenvalue of X. Since $d = \gcd(m, p-1) = \gcd(d, p-1)$, X_p^m and X_p^d must be isomorphic graphs by Proposition 6, and so by Proposition 8 we have that

$$\lambda_1(X_p^m) = \lambda_1(X_p^d) \le \frac{(d-1)\sqrt{p}-1}{d}. \tag{6}$$

We know X_p^m is $\frac{p-1}{d}$-regular by Proposition 5, so combining equations (5) and (6) gives us that

$$h(X_p^m) \ge \frac{\frac{p-1}{d} - \frac{(d-1)\sqrt{p}-1}{d}}{2} = \frac{p+(1-d)\sqrt{p}}{2d}.$$

4. An upper bound by estimating solutions to $\boldsymbol{x^m + y^m + z^m = 0}$ modulo $\boldsymbol{p}$. In this section we give a proof of the upper bound given in Proposition 1. Throughout this section, let p be an odd prime, $m > 1$ be an integer, and $d = \gcd(p-1, m)$. Assume that d divides $(p-1)/2$. Let $\Gamma = \Gamma_p^m$. Let $\overline{\Gamma} = \mathbb{Z}_p^\times \setminus \Gamma$.

Note that if F is a subset of $\mathbb{Z}_p$ with $|F| \le p/2$ then $h(X_p^m) \le |\partial F|/|F|$. Therefore, $h(X_p^m) \le |\partial\Gamma|/|\Gamma|$. We now estimate this ratio to get an upper bound on $h(X_p^m)$. We assume that $d > 1$ so that $|\Gamma| < p/2$. (Note that if $d = 1$, then X_p^m is the complete graph whose isoperimetric number is known.)

We first take a look at the structure of X_p^m. Please refer to Figure 2 during this discussion. Note that by the definition of a generalized Paley graph, a vertex x is adjacent to 0 if and only if $x \in \Gamma$. Recall that every element of Γ has degree $(p-1)/d$. Therefore, we have the following equation

$$|\Gamma| \cdot \frac{p-1}{d} = |\partial\Gamma| + 2(\text{number of edges internal to } \Gamma), \tag{7}$$

where the term on the left side of the equation counts one for each endpoint of an edge that lands in Γ. There is a 2 on the right side of the equation is because each edge that is internal to Γ is counted twice on the left side of the equation.

Let

$$S = \{(x,y,z) | x,y,z \in \mathbb{Z}_p^\times \text{ and } x^m + y^m + z^m = 0\}$$

and N denote the size of S. Using the facts that every element of Γ is an m-th power, $-1 \in \Gamma$, and every element of Γ can be represented by exactly d different elements of the form a^m where $a \in \mathbb{Z}_p^\times$, one can derive that

$$2(\text{number of edges internal to } \Gamma) = \frac{|S|}{d^3} = \frac{N}{d^3}.$$

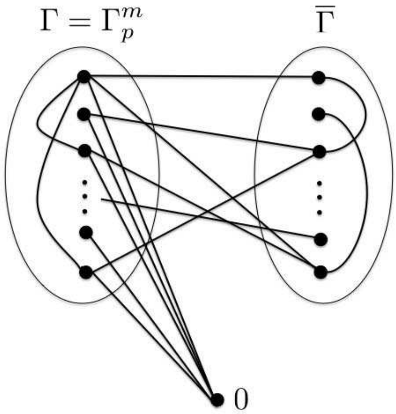

Fig. 2

Since $|\Gamma| = (p-1)/d$, we have that equation (7) becomes

$$|\partial\Gamma| = \left(\frac{p-1}{d}\right)^2 - \frac{N}{d^3}. \tag{8}$$

We now go about estimating the value of N.

Let

$$\hat{S} = \{(x, y, z) | x, y, z \in \mathbb{Z}_p \text{ and } x^m + y^m + z^m = 0\}$$

and $\hat{N}$ denote the size of $\hat{S}$. Then $\hat{N} = N + 1 + 3|T|$ where $T = \{(a, b) \mid a, b \in \mathbb{Z}_p^\times \text{ and } a^m + b^m = 0\}$. Suppose that $a, b \in \mathbb{Z}_p^\times$ with $a^m + b^m = 0$ and $-1 = u^m$ where $u \in \mathbb{Z}_p^\times$. Then $a^m = (ub)^m$. Conversely if $b \in \mathbb{Z}_p^\times$ then by Lemma 4 there are exactly d elements $a \in \mathbb{Z}_p^\times$ with $a^m = (ub)^m$. Thus, $|T| = d(p-1)$. Therefore,

$$N = \hat{N} - 1 - 3d(p-1).$$

Weil [18] showed that there exists a positive integer M_m, depending only on m, with $|\hat{N} - p^2| \leq M_m(p-1)p^{1/2}$. Moreover, he showed that M_m is the number of triples of rational numbers $(\alpha_0, \alpha_1, \alpha_2)$ satistfying the three conditions

$$m\alpha_0, m\alpha_1, m\alpha_2 \in \mathbb{Z}, \;\; \alpha_0 + \alpha_1 + \alpha_2 \in \mathbb{Z}, \text{ and } 0 < \alpha_0, \alpha_1, \alpha_2 < 1.$$

(Another derivation of the above is given as Theorem 5 in [10, pgs. 102–103], however they give a different way to calculate M_m.) This gives that

$$N \geq p^2 - M_m p^{3/2} + M_m p^{1/2} - 1 - 3d(p-1).$$

Plugging this into equation (8) yields

$$h(X_p^m) \leq \frac{|\partial\Gamma|}{|\Gamma|} \leq \left(\frac{p-1}{d}\right)^2 - \frac{p^2 - M_m p^{3/2} + M_m p^{1/2} - 1 - 3d(p-1)}{d^3}.$$

Simplifying the above equation yields the upper bound given in Proposition 1.

5. The γ-bound. In this section we give a proof of Proposition 2 and a derivation of equation (4). Throughout this section, let p be an odd prime, $m > 1$ be an integer, and $d = \gcd(p-1, m)$. Assume that d divides $(p-1)/2$.

We generalize the α-bound from [4] (where $m = 2$) to generalized Paley graphs ($m \geq 2$). The proof is almost exactly the same, however we have considerably rewritten the details of the proof to make it easier to understand and to simpify it. We have changed the name to the γ-bound as we use γ instead of α in this version of the proof.

Note that for each $\gamma \in \mathbb{Z}_p$ we have that $-\gamma$ = p - γ. Recall that $|\Gamma_p^m| = \dfrac{p-1}{d}$. Since Γ_p^m is symmetric we may arrange its elements in increasing order. For the remainder of this section we will use the following notation

$$\Gamma_p^m = \{\gamma_1, \gamma_2, \ldots, \gamma_k, -\gamma_k, \ldots, -\gamma_2, -\gamma_1\}$$

where $k = \dfrac{p-1}{2d}$ and $1 \leq \gamma_i \leq \dfrac{p-1}{2}$. Note that $\gamma_1 = 1$ and $-\gamma_1 = p-1$.

The following is what we call the adjacency table for X_p^m. The top row lists the vertices of X_p^m and below each vertex v is a column that contains the vertices that v it is adjacent to.

0	1	2	$\cdots$	$p-1$
1	2	3	$\cdots$	0
γ_2	γ_2+1	γ_2+2	$\cdots$	γ_2-1
γ_3	γ_3+1	γ_3+2	$\cdots$	γ_3-1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
γ_k	γ_k+1	γ_k+2	$\cdots$	γ_k-1
$-\gamma_k$	$-\gamma_k+1$	$-\gamma_k+2$	$\cdots$	$-\gamma_k-1$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$-\gamma_3$	$-\gamma_3+1$	$-\gamma_3+2$	$\cdots$	$-\gamma_3-1$
$-\gamma_2$	$-\gamma_2+1$	$-\gamma_2+2$	$\cdots$	$-\gamma_2-1$
$p-1$	0	1	$\cdots$	$p-2$

We will now use the adjacency table for X_p^m to get a bound on $h(X_p^m)$. We will do this by considering a special set. This set is $F = \{0, 1, 2, \ldots, \frac{p-3}{2}\}$. We will use the table to get formula for the size of ∂F. Once we have done this we will be able to bound $h(X_p^m)$ by using the formula $h(X_p^m) \leq |\partial F|/|F|$.

Proposition 9. *Let* $F = \left\{0, 1, 2, \ldots, \frac{p-3}{2}\right\}$ *be as above. Consider the row of the adjacency table for* X_p^m *that begins with* γ_i *where* $1 \leq i \leq k$. *The row corresponding to* γ_i *of the adjacency table for* X_p^m *contributes exactly* γ_i *edges to the boundary set* ∂F.

Proof. When looking at the row correspoding to γ_i we need to scan the entries from the column with header 0 to the column with header $\frac{p-3}{2}$ and count how many entries are greater than $\frac{p-3}{2}$. Each entry that we find that is greater than $\frac{p-3}{2}$ will contribute an edge to ∂F. Notice that as we move from left to right in the table each entry increases by one each time we move right.

Suppose we are in the row corresponding to γ_i. We break the proof into two cases: $\gamma_i \neq \frac{p-1}{2}$ and $\gamma_i = \frac{p-1}{2}$.

We begin with the first case. Assume that $\gamma_i \neq \frac{p-1}{2}$. Then $\gamma_i \leq \frac{p-3}{2}$. Suppose we start at the column with header 0 and scan one by one to the right until we arrive at the entry $\frac{p-3}{2}$ in some column β. So far we have not found any entries that contribute an edge to ∂F. Since $\frac{p-3}{2}$ is in row γ_i and column β we have that $\frac{p-3}{2} = \gamma_i + \beta$. So, $\beta = \frac{p-3}{2} - \gamma_i$. Scanning from column 0 to column β we have encountered $\beta + 1$ entries. Note that $|F| = \frac{p-1}{2}$. So we have exactly

$$\frac{p-1}{2} - (\beta + 1) = \frac{p-1}{2} - \left(\frac{p-3}{2} - \gamma_i + 1\right) = \gamma_i$$

entries left to consider in our scan of columns headed by elements of F. The remaining entries in the table consist of the elements $\frac{p-3}{2} + 1$ to $\frac{p-3}{2} + \gamma_i$. By definition we know that $\gamma_i \leq \frac{p-1}{2}$. Therefore $\frac{p-3}{2} + \gamma_i \leq p - 2 < p$. Hence as we scan the remaining entries we never pass $p - 1$ and cycle back to 0. Therefore, each of the remaining γ_i entries contributes an edge to ∂F, which is what we wanted to prove.

Suppose that we are in the second case, that is $\gamma_i = \dfrac{p-1}{2}$. Then every element in row γ_i starting from column 0 to column $\dfrac{p-3}{2}$ corresponds to an element that is not in F and hence contributes an edge to ∂F. This gives us $\gamma_i = \dfrac{p-1}{2}$ entries that contribute and edge to ∂F. $\square$

We now prove that the adjacency table has a symmetric property.

Proposition 10. $F = \left\{0, 1, 2, \ldots, \dfrac{p-3}{2}\right\}$ *be as above. The row beginning with entry* $-\gamma_i$ *of the adjacency table for* X_p^m *contributes the same number of edges to* ∂F *as does the row beginning with entry* γ_i*.*

Proof. Consider the row corresponding to $-\gamma_i$. As in Proposition 9, we only need to inspect the entries from column 0 to column $\dfrac{p-3}{2}$. As we do this we count the number of entries that are greater than $\dfrac{p-3}{2}$.

Suppose first that $\gamma_i = \dfrac{p-1}{2}$. Then in this case, $-\gamma_i = \dfrac{p+1}{2}$. Thus, every element from column 0 to column $\dfrac{p-3}{2}$ corresponds to an element that is not in F. Hence, we count $|F| = \dfrac{p+1}{2} = \gamma_i$ entries that correspond to edges in ∂F.

Now suppose that $1 \leq \gamma_i \leq \dfrac{p-3}{2}$ and again consider the row corresponding to $-\gamma_i$. We start in the column with 0 and scan until we reach $p-1$ in some column headed with say β. Doing this we have counted $\beta + 1$ entries. Since $p-1$ is in row $-\gamma_i$ and column β we have that $p - 1 = -\gamma_i + \beta$. This gives us that $\beta + 1 = \gamma_i$. So we have scanned exactly γ_i entries so far. Since $\beta = \gamma_i - 1$ and $1 \leq \gamma_i \leq \dfrac{p-3}{2}$ we know that $0 \leq \beta \leq \dfrac{p-5}{2}$. That is, β is an element of F and we still have at least one more entry in our row to scan to the right of column β. Since we have scanned exactly γ_i entries so far, the remaining entries to scan correspond to entry 0 in column $\beta + 1$ to entry $(p-1) + \left(\dfrac{p-1}{2} - \gamma_i\right) = \dfrac{p-3}{2} - \gamma_i \leq \dfrac{p-5}{2}$ in column $\dfrac{p-3}{2}$. Thus the remaining entries are all in F and hence do not contribute any edges to ∂F. Therefore, in this case we get exactly γ_i entries in row $-\gamma_i$ that correspond to an edge in ∂F. $\square$

Proposition 11. *Let* $F = \left\{0, 1, 2, \ldots, \dfrac{p-3}{2}\right\}$ *and*

$$\Gamma_p^m = \{\gamma_1, \gamma_2, \ldots, \gamma_k, -\gamma_k, \ldots, -\gamma_2, -\gamma_1\}$$

where $k = \dfrac{p-1}{2d}$ *as above. Then*

$$|\partial F| = 2\sum_{i=1}^{k} \gamma_i,$$

Proof. This follows from Proposition 9 and Proposition 10. □

We can now derive the γ-bound given in Proposition 2. Let $F = \left\{0, 1, 2, \ldots, \dfrac{p-3}{2}\right\}$. By Proposition 11 and the fact that $|F| = \dfrac{p-1}{2}$ we see that

$$h(X_p^m) \leq \frac{|\partial F|}{|F|} = \frac{2\sum\limits_{i=1}^{k} \gamma_i}{\frac{p-1}{2}} = \frac{4}{p-1}\sum_{i=1}^{k} \gamma_i.$$

We now derive equation (4) from the introduction. Recall that $1 \leq \gamma_k \leq \dfrac{p-1}{2}$, that is, the γ_k are all trapped in the first half of $\mathbb{Z}_p^\times$. Therefore, the worst that the γ-bound can be is if all the γ_k are grouped together as close as possible to $(p-1)/2$. Since $\gamma_1 = 1$, if all the remaining γ_k are grouped up next to $\dfrac{p-1}{2}$ then we would have that $\sum\limits_{i=1}^{k} \gamma_k$ is less than or equal to

$$1 + \left(\frac{p-1}{2} - (k-2)\right) + \left(\frac{p-1}{2} - (k-3)\right) + \cdots + \left(\frac{p-1}{2} - 1\right) + \frac{p-1}{2}.$$

Using the formula

$$a + (a+1) + (a+2) + \cdots + (a+n) = a(n+1) + \frac{n(n+1)}{2}$$

with $a = \dfrac{p-1}{2} - (k-2)$ and $n = k-2$ we get that

$$h(X_p^m) \leq \frac{4}{p-1}\left(1 + \left[\frac{p-1}{2} - (k-2)\right][k-1] + \frac{(k-2)(k-1)}{2}\right)$$

$$= \frac{2d(2+p) - p - 4d^2 + 1}{2d^2}$$
$$= \frac{(2d-1)p + (4d - 4d^2 + 1)}{2d^2}.$$

Acknowledgements. We would like to thank the referee for many useful comments and suggested changes, and for a thorough reading of our manuscript.

REFERENCES

[1] A. N. Elsawy. Paley graphs and their generalizations. Master's Thesis at Heinrich Heine University, Düsseldorf, German, 2009.

[2] N. Alon. Eigenvalues and expanders. *Combinatrica* **6**, *2* (1986), 83–96.

[3] L. Babai. Spectra of Cayley graphs. *J. Comb. Theory, Ser. B* **27**, *2* (1979), 180–189.

[4] K. Cramer, M. Krebs, N. Shabazi, A. Shaheen, E. Voskanian. *The Isoperimetric Constant and Kazhdan Constant of a Paley Graph*, Involve journal, in production.

[5] D. Ž. Djokovic. Isomorphism problem for a special class of graphs. *Acta Math. Acad. Sci. Hungar.* **21** (1970), 267–270.

[6] J. Dodziuk. Difference equations, isoperimetric inequality and transience of certain random walks. *Trans. Amer. Math. Soc.* **284**, *2* (1984), 787–794.

[7] C. Godsil, G. Royle. Algebraic graph theory. Graduate Texts in Mathematics, vol. **207**. New York, Springer-Verlag, 2001.

[8] J. Gross, J. Yellen, P. Zhang (eds) Handbook of Graph Theory, Second edition. Boca Raton–London–New York, CRC Press, 2014.

[9] D. R Heath-Brown, S. Konyagin. New bounds for Gauss sums derived from k-th powers, and for Heilbronn's exponential sum. *Q. J. Math.* **51**, *2* (2000), 221–235.

[10] K. Ireland, M. Rosen. A Classical Introduction to Modern Number Theory, Second edition. Graduate Texts in Mathematics, vol. **84**. New York, Springer-Verlag, 1990.

[11] M. Krebs, A. Shaheen. Expander families and Cayley graphs: a beginner's guide. Oxford, Oxford University Press, 2011.

[12] D. Lanphier, J. Rosenhouse. Cheeger constants of Platonic graphs. *Discrete Math.* **277**, *1–3* (2004), 101–113.

[13] C. H. Li. On isomorphisms of finite Cayley graphs – a survey. *Discrete Math.* **256**, *1–2* (2002), 301–334.

[14] B. Mohar. Isoperimetric numbers of graphs. *J. Combin. Theory Ser. B* **47**, *3* (1989), 274–291.

[15] I. Niven, H. S. Zuckerman, H. L. Montgomery. An introduction to the theory of numbers, Fifth edition. New York, John Wiley & Sons, Inc., 1991.

[16] J. Rosenhouse. Isoperimetric numbers of Cayley graphs arising from generalized dihedral groups. *J. Combin. Math. Combin. Comput.* **42** (2002), 127–138.

[17] R. Stanley. Topics in algebraic combinatorics, Version 1 of February 2013, `http://www-math.mit.edu/~rstan/algcomb/algcomb.pdf`.

[18] A. Weil. Number of solutions of equations in finite fields. *Bull. Amer. Math. Soc.* **55**, *5* (1949), 497–508.

Department of Mathematics
California State University
5151 State University Drive
CA 90032 Los Angeles, USA
e-mail: `ashahee@calstatela.edu` *(Anthony Shaheen)*
e-mail: `gsubuyu@calstatela.edu` *(Gustavo Subuyuj)*

Received September 28, 2015
Revised September 26, 2016