involve
a journal of mathematics

The isoperimetric and Kazhdan constants associated to a Paley graph

Kevin Cramer, Mike Krebs, Nicole Shabazi,
Anthony Shaheen and Edward Voskanian

msp

2016 vol. 9, no. 2

INVOLVE 9:2 (2016)
dx.doi.org/10.2140/involve.2016.9.293

The isoperimetric and Kazhdan constants associated to a Paley graph

Kevin Cramer, Mike Krebs, Nicole Shabazi,
Anthony Shaheen and Edward Voskanian

(Communicated by Kenneth S. Berenhaut)

In this paper, we investigate the isoperimetric constant (or expansion constant) of a Paley graph, and the Kazhdan constant of the group and generating set associated with a Paley graph.

We give two new upper bounds for the isoperimetric constant $h(X_p)$ for the Paley graph X_p. These bounds improve previously known eigenvalue bounds on $h(X_p)$. Along with a known eigenvalue lower bound for $h(X_p)$, they provide a narrow strip in which $h(X_p)$ must live. More precisely, we show that $(p-\sqrt{p})/4 \le h(X_p) \le (p-1)/4$, which implies that $\lim_{p\to\infty} h(X_p)/p = 1/4$.

In addition, we show that the Kazhdan constant associated with the integers modulo p and the generating set for the Paley graph X_p approaches 2 as p tends to infinity, which is the best possible limit that the Kazhdan constant can be.

1. Introduction

Paley graphs are interesting because they allow one to use graph-theoretic tools to study the theory of quadratic residues. They also have interesting properties that make them useful in graph theory. For example, they are strongly regular, self-complementary, and their eigenvalues are essentially Gauss sums.

Let p be an odd prime with $p \equiv 1 \pmod 4$. The Paley graph X_p is constructed as follows. The vertices of X_p consist of the integers modulo p, which we denote by $\mathbb{Z}_p$. Two vertices x and y from $\mathbb{Z}_p$ are adjacent if and only if $x-y$ is an element of $\Gamma_p = \{\gamma^2 \mid \gamma \in \mathbb{Z}_p \text{ and } \gamma \neq 0\}$. It is well known that -1 is in Γ_p since $p \equiv 1 \pmod 4$. Hence the above definition is well-defined; that is, $x-y$ is in Γ_p if and only if $y-x$ is in Γ_p.

For example, if $p=13$, then $\Gamma_{13} = \{1, 3, 4, 9, 10, 12\}$. Then 1 and 10 are adjacent since $10-1=9$, which is in Γ_{13}. A picture of X_{13} is given in Figure 1.

MSC2010: 05C99.
Keywords: isoperimetric constant, expansion constant, Paley graph, Kazhdan constant.
This research was partially supported by NSF grant DMS-1247679.

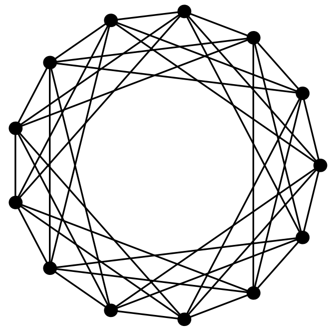

Figure 1. The Paley graph on $\mathbb{Z}_{13}$.

A great reference for Paley graphs is [Elsawy 2009]. Note that one can define a Paley graph on a finite field of size p^n. However, we are sticking with $n = 1$ in this paper.

We want to get approximations on two constants associated with the Paley graph: the isoperimetric constant and the Kazhdan constant. We first introduce the isoperimetric constant.

Let X be a graph with vertex set V. Let F be a subset of V. The boundary of F, denoted by ∂F, consists of the edges of X with one end in F and the other end in $V \setminus F$. The isoperimetric constant of X is defined to be

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

In layman's terms, the isoperimetric constant of a graph X gives a rough estimate for how "good" a graph is as a communications network. It has been heavily studied by both computer scientists and mathematicians. One main topic of investigation in this area is that of expander families. A family of finite regular graphs, each with the same degree, whose order is unbounded, is said to be an expander family if there is a uniform positive lower bound for $h(X)$ for all X in the family. Recently it has been shown that every family of finite nonabelian simple groups yields an expander family via the Cayley graph construction. This was proven for all families except Suzuki groups by Kassabov, Lubotzky, and Nikolov [Kassabov et al. 2006], with the final case of Suzuki groups proven by Breuillard, Green, and Tao [Breuillard et al. 2011].

In general it is a difficult combinatorial problem to get an exact value for the isoperimetric constant of a graph. Some examples where the isoperimetric constant of a graph family is known are as follows. The isoperimetric constant for cycle graphs of order n is equal to $4/n$ when n is even and $4/(n-1)$ when n is odd. The isoperimetric constant of a complete graph of order n is equal to $n/2$ when n is even and $(n+1)/2$ when n is odd. See [Krebs and Shaheen 2011] for proofs. Rosenhouse

[2002] shows that $h(X_n) = 4/n$, where X_n is the Cayley graph constructed using the dihedral group D_{2n} with generators r, r^{-1}, and s. Lanphier and Rosenhouse [2004] derive approximations on the isoperimetric constants of Platonic graphs.

Instead of calculating $h(X)$ exactly, one must usually be satisfied with approximations. One way to approximate $h(X)$ is to use the eigenvalues of X. The eigenvalues of X are especially useful in finding a lower bound on $h(X)$.

Let $\lambda_1(X)$ be the second largest eigenvalue of a d-regular graph. A well-known inequality is

$$\frac{d-\lambda_1(X)}{2} \le h(X) \le \sqrt{2d(d-\lambda_1(X))} \tag{1}$$

(see [Krebs and Shaheen 2011, p. 31]). One also has a tighter upper bound on $h(X)$ given by Mohar [1989]. It is

$$h(X) \le \sqrt{(d+\lambda_1(X))(d-\lambda_1(X))}. \tag{2}$$

Let us see what (1) and (2) tell us about Paley graphs. Since Paley graphs are strongly regular graphs, one can find a quadratic polynomial that the adjacency matrix satisfies. This leads one to the eigenvalues of a Paley graph. (For the details, see [Gross et al. 2014, pp. 684–685]). The eigenvalues of X_p are $(p-1)/2$ with multiplicity 1, $\sqrt{p}/2 - 1/2$ with multiplicity $(p-1)/2$ and $-\sqrt{p}/2 - 1/2$ with multiplicity $(p-1)/2$. Thus $\lambda_1(X_p) = \sqrt{p}/2 - 1/2$. Plugging this into (1) and using the fact that X_p is $(p-1)/2$ regular, we get that

$$\frac{p-\sqrt{p}}{4} \le h(X_p) \le \sqrt{\frac{p^2 - p\sqrt{p} - p + \sqrt{p}}{2}}. \tag{3}$$

Using the Mohar bound, given in (2), one gets

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

which reduces the upper bound in (3) by a factor of $\sqrt{2}$ as p tends to infinity.

The lower bound in (3) seems optimal for Paley graphs. However, the two upper bounds given above are far from optimal. In this paper, we will give two new upper bounds. One we call the α-bound, which is the average of the first half of the elements of Γ_p, and the other is the simpler bound of $(p-1)/4$. Both of these bounds give much better upper bounds than the eigenvalue bounds given above in (3) and (4). Consider Table 1. Note how close the eigenvalue lower bound is to both the α-bound and $(p-1)/4$, and how much better the two new upper bounds are. While $h(X_p)$ is still not known exactly, we have found a very narrow band in which it must exist. For example, we have $2{,}168{,}090 \le h(X_p) \le 2{,}168{,}277$ when $p = 8{,}675{,}309$.

prime p	13	577	40,961	8,675,309
eigenvalue lower bound from (3)	2.35	138.24	10,189	2,168,090
α-bound (new upper bound)	2.67	139.29	10,201	2,168,277
$(p-1)/4$ (new upper bound)	3	144	10,240	2,168,827
eigenvalue upper bound from (4)	5.86	287.77	20,479	4,337,654
eigenvalue upper bound from (3)	7.51	399.07	28,891	6,133,328

Table 1. Lower and upper bounds for $h(X_p)$.

Summarizing the above, we have our main result for the isoperimetric constant of a Paley graph.

Theorem 1. *Let p be an odd prime with $p \equiv 1 \pmod 4$. Then*

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

Note that inequalities (3) and (4) show that

$$\frac{1}{4} \leq \liminf_{p\to\infty} \frac{h(X_p)}{p} \leq \limsup_{p\to\infty} \frac{h(X_p)}{p} \leq \frac{1}{2}.$$

Theorem 1, however, shows more precisely that

$$\lim_{p\to\infty} \frac{h(X_p)}{p} = \frac{1}{4}.$$

Before moving on, we would like to note that we do not know if the α-bound is always smaller than $(p-1)/4$, but from calculations it appears to be so.

The second result of this paper concerns the Kazhdan constant of the pair $(\mathbb{Z}_p, \Gamma_p)$ associated with the Paley graph X_p. We begin by giving the general definition of a Kazhdan constant for any finite group. The definition greatly simplifies when the group is the integers modulo p. The reader who has never encountered representation theory may skim the next paragraph to get the idea with no loss of understanding.

Let G be a finite group, and let Γ be a nonempty subset of G. Let ρ be a unitary representation of G acting on some vector space V_ρ. We define

$$\kappa(G, \Gamma, \rho) = \min_{\substack{\|v\|=1 \\ v\in V_\rho}} \max_{\gamma\in\Gamma} \|\rho(\gamma)v - v\|.$$

The Kazhdan constant of the pair (G, Γ) is defined to be

$$\kappa(G, \Gamma) = \min_{\rho}\{\kappa(G, \Gamma, \rho)\},$$

where the minimum is over all irreducible, nontrivial, unitary representations ρ of G. Question: why is one interested in computing such a constant? One answer is because, when Γ is a symmetric subset of G, we know that $\kappa(G, \Gamma)$ is related to the isoperimetric constant of the Caley graph built from G and Γ. More specifically, suppose that Γ is a symmetric subset of the group G. That is, $\gamma \in \Gamma$ if and only if $\gamma^{-1} \in \Gamma$. Then one can build the Caley graph $X = \mathrm{Cay}(G, \Gamma)$, where the vertices of X are the elements of G and $x, y \in G$ are adjacent if and only if $y^{-1}x \in \Gamma$. (Note that if $G = \mathbb{Z}_p$, then $\Gamma = \Gamma_p$ gives the Paley graph.) Here X is a regular graph of degree $d = |\Gamma|$. In this case, we have the relationship $h(X) \geq \kappa(G, \Gamma)^2/4d$. Hence, by finding lower bounds on $\kappa(G, \Gamma)$, one can find lower bounds on $h(X)$. For more information on the above discussion, see [Krebs and Shaheen 2011, Chapter 8].

We would like to note that it is difficult to calculate $\kappa(G, \Gamma)$ in general. There are very few results in this area. As an example, Bacher and de la Harpe [1994] calculate $\kappa(\mathbb{Z}_n, \Gamma)$ for several very specific sets Γ, such as $\kappa(D_{2n}, \{r, s\})$, where D_{2n} is the dihedral group and r and s are its generators, and $\kappa(S_n, \Gamma_n)$, where $\Gamma_n = \{(1, 2), \ldots, (n-1, n)\}$.

We are interested in approximating the Kazhdan constant of the pair $(\mathbb{Z}_p, \Gamma_p)$. When $G = \mathbb{Z}_p$, the Kazhdan constant simplifies considerably. To simplify our notation, we set $\xi_p = e^{2\pi i/p}$. The irreducible, nontrivial, unitary representations of $\mathbb{Z}_p$ are given by the maps $\rho_a(\gamma) : \mathbb{C} \to \mathbb{C}$, where $\rho_a(\gamma)z = \xi_p^{a\gamma} z$, $V_a = \mathbb{C}$, and $a = 1, 2, \ldots, p-1$. Hence,

$$\begin{aligned}\kappa(\mathbb{Z}_p, \Gamma_p) &= \min_{1 \leq a \leq p-1} \min_{\substack{\|v\|=1 \\ v \in \mathbb{C}}} \max_{\gamma \in \Gamma} \|\xi_p^{a\gamma} v - v\| \\ &= \min_{1 \leq a \leq p-1} \max_{\gamma \in \Gamma} \|\xi_p^{a\gamma} - 1\|.\end{aligned}$$

In words, $\kappa(\mathbb{Z}_p, \Gamma_p)$ is calculated by considering each a and finding the γ for which $\xi_p^{a\gamma}$ is the maximal distance away from 1, and then one finds the minimum of these maximums. Or another way of saying it is that for any $1 \leq a \leq p-1$, there exists a $\gamma \in \Gamma$ such that $\|\xi_p^{a\gamma} - 1\| \geq \kappa(\mathbb{Z}_p, \Gamma_p)$.

Let $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ and $\overline{\Gamma}_p = \mathbb{Z}_p \setminus (\Gamma_p \cup \{0\})$. If $a \in \mathbb{Z}_p^\times$ then it is easy to show that $a\Gamma_p = \Gamma_p$ if $a \in \Gamma_p$; otherwise, $a\Gamma_p = \overline{\Gamma}_p$ if $a \in \overline{\Gamma}_p$. (To see this note that Γ_p is a subgroup of $\mathbb{Z}_p^\times$ under multiplication and there are only two cosets: Γ_p and $\overline{\Gamma}_p$.) Hence

$$\begin{aligned}\kappa(\mathbb{Z}_p, \Gamma_p) &= \min_{1 \leq a \leq p-1} \max_{\gamma \in \Gamma_p} \|\xi_p^{a\gamma} - 1\| \\ &= \min\Big\{\max_{\gamma \in \Gamma_p} \|\xi_p^{\gamma} - 1\|, \max_{\gamma \in \overline{\Gamma}_p} \|\xi_p^{\gamma} - 1\|\Big\}.\end{aligned}$$

Thus to calculate $\kappa(\mathbb{Z}_p, \Gamma_p)$, one must find the square $\gamma_1 \in \mathbb{Z}_p$, where $\xi_p^{\gamma_1}$ is as far away from 1 as possible, and the nonsquare $\gamma_2 \in \mathbb{Z}_p$, where $\xi_p^{\gamma_2}$ is as far away from 1 as possible. Then one calculates the minimum of those two distances. For example, when $p = 17$, we have that $\Gamma_{17} = \{1, 2, 4, 8, 9, 13, 15, 16\}$ and $\overline{\Gamma}_{17} = \{3, 5, 6, 7, 10, 11, 12, 14\}$; see Figure 2. We have labeled the elements ξ^γ by squares when γ is in Γ_{17} and by circles when γ is in $\overline{\Gamma}_{17}$. The element ξ^γ where

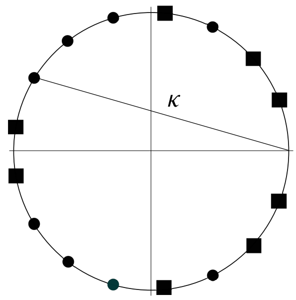

Figure 2. The Kazhdan constant $\kappa = \kappa(\mathbb{Z}_{17}, \Gamma_{17})$.

γ is a square that is furthest from 1 is ξ^8. The element ξ^γ where γ is a nonsquare that is furthest from 1 is ξ^7. Therefore, $\kappa(\mathbb{Z}_{17}, \Gamma_{17}) = \|\xi_{17}^7 - 1\|$.

For specific congruency classes of primes, one can use arguments involving the Legendre symbol to explicitly calculate $\kappa(\mathbb{Z}_p, \Gamma_p)$. For example, arguments from [Voskanian 2013] show that if p is a prime with $p \equiv 17 \pmod{24}$, then

$$\kappa(\mathbb{Z}_p, \Gamma_p) = \|e^{\pi i(1-3/p)} - 1\|.$$

And when $p \equiv 97 \pmod{120}$,

$$\kappa(\mathbb{Z}_p, \Gamma_p) = \|e^{\pi i(1-5/p)} - 1\|.$$

However, it seems that one cannot generalize these arguments to give a formula for $\kappa(\mathbb{Z}_p, \Gamma_p)$ for all $p \equiv 1 \pmod 4$.

Notice that $0 < \kappa(\mathbb{Z}_p, \Gamma_p) < 2$. We will not be able to explicitly calculate $\kappa(\mathbb{Z}_p, \Gamma_p)$; however, we will show the following theorem, which is our main result on the Kazhdan constant of a Paley graph.

Theorem 2. *We have that*

$$\lim_{p\to\infty} \kappa(\mathbb{Z}_p, \Gamma_p) = 2$$

as p goes over the primes which are congruent to 1 *modulo* 4.

2. The isoperimetric constant of a Paley graph

We now give the proofs of the new upper bounds for the isoperimetric constant of X_p that were discussed in the introduction to this paper. We begin with the α-bound and then proceed to the $(p-1)/4$ bound. Note that if $F \subseteq \mathbb{Z}_p$ with $0 < |F| \leq \mathbb{Z}_p/2$ then $h(X_p) \leq |\partial F|/|F|$. This is the technique that we will use in both proofs. That is, we will pick a specific F that will give an upper bound for $h(X_p)$.

2.1. ***The α-bound.*** The proof of the α-bound relies on a table that we call the adjacency table for X_p. The adjacency table for X_p is obtained by constructing the group addition table for $\mathbb{Z}_p$ (under the usual addition modulo p) with all the rows corresponding to any $\delta \notin \Gamma_p$ omitted.

For each $\alpha \in \Gamma_p$, we write the additive inverse of α as α^{-1}. Note that $\alpha^{-1} = p - \alpha$, and $|\Gamma_p| = (p-1)/2$; hence we can arrange the elements of Γ_p in increasing order and we will write

$$\Gamma_p = \{\alpha_1, \alpha_2, \ldots, \alpha_k, \alpha_k^{-1}, \ldots, \alpha_2^{-1}, \alpha_1^{-1}\},$$

where $k = (p-1)/4$. Since 1 is the smallest element of Γ_p, we will always have $\alpha_1 = 1$ and $\alpha_1^{-1} = p - 1$. Incorporating these considerations into our construction, we arrive at the following adjacency table:

0	1	2	$\cdots$	$p-1$
1	2	3	$\cdots$	0
α_2	α_2+1	α_2+2	$\cdots$	α_2-1
α_3	α_3+1	α_3+2	$\cdots$	α_3-1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
α_k	α_k+1	α_k+2	$\cdots$	α_k-1
α_k^{-1}	$\alpha_k^{-1}+1$	$\alpha_k^{-1}+2$	$\cdots$	$\alpha_k^{-1}-1$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
α_3^{-1}	$\alpha_3^{-1}+1$	$\alpha_3^{-1}+2$	$\cdots$	$\alpha_3^{-1}-1$
α_2^{-1}	$\alpha_2^{-1}+1$	$\alpha_2^{-1}+2$	$\cdots$	$\alpha_2^{-1}-1$
$p-1$	0	1	$\cdots$	$p-2$

For example, when $p = 13$ we have that $\Gamma_{13} = \{1, 3, 4, 9, 10, 12\}$, which gives the following table:

0	1	2	3	4	5	6	7	8	9	10	11	12
1	2	3	4	5	6	7	8	9	10	11	12	0
3	4	5	6	7	8	9	10	11	12	0	1	2
4	5	6	7	8	9	10	11	12	0	1	2	3
9	10	11	12	0	1	2	3	4	5	6	7	8
10	11	12	0	1	2	3	4	5	6	7	8	9
12	0	1	2	3	4	5	6	7	8	9	10	11

To get the α-bound, we will be considering the set $F = \{0, 1, 2, \ldots, (p-3)/2\}$. The following lemma and propositions will be useful when we tally the edges in ∂F row-wise.

Lemma 3. *Let* $\Gamma_p = \{\alpha_1, \alpha_2, \ldots, \alpha_k, \alpha_k^{-1}, \ldots, \alpha_2^{-1}, \alpha_1^{-1}\}$. *Then* $1 \le \alpha_i \le (p-1)/2$ *for all* $i = 1, \ldots, k$.

Proof. We know $\alpha_1 = 1$ is the smallest element in Γ_p, so we have $1 \le \alpha_i$. Now suppose that, for some i, we have $\alpha_i > (p-1)/2$. Since α_i is an integer and p

is odd, the smallest α_i can be is $(p+1)/2$. Thus, we see that $\alpha_i \geq (p+1)/2$. Therefore, it follows that

$$\alpha_i^{-1} = p - \alpha_i \leq p - \frac{p+1}{2} = \frac{p-1}{2}.$$

In this case, we have $\alpha_i \geq (p+1)/2$ and $\alpha_i^{-1} \leq (p-1)/2$. In particular, $\alpha_i^{-1} < \alpha_i$. Since this contradicts the ordering of Γ_p, we see that $\alpha_i \leq (p-1)/2$ for all $i = 1, 2, \ldots, k$. □

Proposition 4. *Let $F = \{0, 1, 2, \ldots, (p-3)/2\}$ be a subset of vertices in X_p. Then row α_i of the adjacency table for X_p contributes exactly α_i edges to the boundary set ∂F.*

Proof. By our choice of F, we only need to scan the entries in row α_i from column 0 to column $(p-3)/2$, and any entry we encounter contributes an edge to ∂F if and only if it is greater than $(p-3)/2$. Since $|F| = (p-1)/2$, there are a total of $(p-1)/2$ columns headed by elements of F, and thus $(p-1)/2$ entries to consider. Also, we recall that for any entry γ in the table, the entry in the same row, one column to the right, is $\gamma + 1$.

Let us tally the contributions made to ∂F by row α_i of the adjacency table. Starting at column 0, we scan row α_i until we arrive at the entry $(p-3)/2$ in some column β. In this case, all the entries encountered so far are less than or equal to $(p-3)/2$, and thus contribute no edges to ∂F. Since $(p-3)/2$ is the entry in row α_i, column β, we have $(p-3)/2 = \alpha_i + \beta$. Thus, $\beta = (p-3)/2 - \alpha_i$. Scanning from column 0 to column β, we have encountered $\beta + 1$ entries. This means there are

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

entries remaining to consider in the columns headed by the entries from F. These entries increase in unit increments from $(p-3)/2+1$ to $(p-3)/2+\alpha_i$. By Lemma 3, we have that $1 \leq \alpha_i \leq (p-1)/2$. This implies that $(p-3)/2 + \alpha_i \leq p-2$. This means the sequence of remaining entries never reaches p to revert to 0 modulo p. That is, each of the remaining α_i entries is strictly larger than $(p-3)/2$, and thus contributes an edge to ∂F. So row α_i contributes exactly α_i edges to ∂F. □

Proposition 5. *Let $F = \{0, 1, 2, \ldots, (p-3)/2\}$ be a subset of vertices in X_p. Then rows α_i and α_i^{-1} of the adjacency table each contribute the same number of edges to ∂F.*

Proof. By our choice of F, we only need to scan the entries in row α_i^{-1} from column 0 to column $(p-3)/2$, and any entry we encounter contributes an edge to ∂F if and only if it is greater than $(p-3)/2$. This gives a total of $(p-1)/2$ columns to scan through and, thus, $(p-1)/2$ entries to consider.

Noting that the entries increase in unit increments as we scan from left to right, we begin with the entry α_i^{-1} in column 0 and scan to the right until we reach the entry $p-1$ in column β. By Lemma 3, we have $1 \le \alpha_i \le (p-1)/2$, so it follows that $(p+1)/2 \le \alpha_i^{-1} \le p-1$. Thus, we see that every entry encountered so far, of which there are $\beta+1$, is greater than $(p-3)/2$ and contributes an edge to ∂F. Since $p-1$ resides in row α_i^{-1}, column β, we have $p-1 = \alpha_i^{-1} + \beta$, from which it follows that $\beta + 1 = p - \alpha_i^{-1} = \alpha_i$. That is, thus far we have encountered α_i entries in row α_i^{-1} contributing edges to ∂F.

Now, if $\alpha_i = (p-1)/2$, then we must have already scanned through all the necessary columns. This means there are no more entries to consider, and row α_i^{-1} contributes exactly α_i edges to ∂F.

If $1 \le \alpha_i \le (p-3)/2$, then there are $(p-1)/2 - \alpha_i$ entries, ranging from $(p-1)+1 = 0$ in column $\beta+1$ to

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

in column $(p-3)/2$, remaining to consider. However, since α_i is at least 1, $(p-3)/2-\alpha_i$ is no greater than $(p-5)/2$. So we see that the remaining entries range from 0 to at most $(p-5)/2$, which means that none of them contribute edges to ∂F.

We have shown that, for all possible values of α_i, row α_i^{-1} contributes exactly α_i edges to ∂F. But that is how many edges row α_i contributes. Thus, we see rows α_i and α_i^{-1} each contribute the same number of edges to ∂F. □

Proposition 6. *Let* $F = \{0, 1, 2, \ldots, (p-3)/2\}$ *be a subset of vertices in* X_p *and* Γ_p *be arranged in increasing order. Then*

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

where α_i *is the* i*-th element of* Γ_p *and* $k = (p-1)/4$.

Proof. Recall that when arranged in increasing order, we have labeled

$$\Gamma_p = \{\alpha_1, \alpha_2, \ldots, \alpha_k, \alpha_k^{-1}, \ldots, \alpha_2^{-1}, \alpha_1^{-1}\}$$

and that column 0 of the adjacency table is populated in increasing order from top to bottom by the elements of Γ_p. Since there are $2k$ elements in Γ_p and $|\Gamma_p| = (p-1)/2$, it follows that $k = (p-1)/4$.

Since $F = \{0, 1, 2, \ldots, (p-3)/2\}$, if we use the adjacency table to tally the edges in ∂F row-wise, by Proposition 5, rows α_i and α_i^{-1} each contribute exactly α_i edges to ∂F. Thus, we see rows α_1 through α_k contribute a total of $\sum_{i=1}^{k} \alpha_i$ edges to ∂F; as do rows α_k^{-1} through α_1^{-1}.

Since there are no other rows to consider, we see there are exactly $2\sum_{i=1}^{k} \alpha_i$ edges in ∂F, as required. □

Proposition 7. *The isoperimetric constant of a Paley graph satisfies the bound*

$$h(X_p) \le \frac{1}{k}\sum_{i=1}^{k}\alpha_i,$$

where $\Gamma_p = \{\alpha_1, \alpha_2, \ldots, \alpha_k, \alpha_k^{-1}, \ldots, \alpha_2^{-1}, \alpha_1^{-1}\}$ *and* $k = (p-1)/4$ *as above.*

Proof. Let $F = \{0, 1, 2, \ldots, (p-3)/2\}$. By Proposition 6, this choice gives $|\partial F| = 2\sum_{i=1}^{k}\alpha_i$. Noting that $|F| = (p-1)/2$, we see that

$$\frac{|\partial F|}{|F|} = \frac{2\sum_{i=1}^{k}\alpha_i}{\frac{p-1}{2}} = \frac{1}{\frac{p-1}{4}}\sum_{i=1}^{k}\alpha_i = \frac{1}{k}\sum_{i=1}^{k}\alpha_i. \qquad \square$$

2.2. *The* $((p-1)/4)$***-bound.*** We have the suspicion that the α-bound is smaller than $(p-1)/4$ for all primes p congruent to 1 modulo 4, though this has yet to be proven. In fact, early into our work, sample values for the α-bound supported this, and thus contributed to the plausibility for $(p-1)/4$ as an upper bound for $h(X_p)$. Whether or not the α-bound is smaller in general than the $((p-1)/4)$-bound, they appear to be very close.

We begin the proof for the $((p-1)/4)$-bound by introducing a key subset of vertices from the graph X_p. As above, let $\overline{\Gamma}_p = \mathbb{Z}_p \setminus (\Gamma_p \cup \{0\})$. That is, $\overline{\Gamma}_p$ consists of the nonsquares in $\mathbb{Z}_p$. We will prove that $h(X_p) \le (p-1)/4$ by showing that

$$\frac{|\partial(\overline{\Gamma}_p)|}{|\overline{\Gamma}_p|} = \frac{p-1}{4}. \tag{5}$$

Noting that $\overline{\Gamma}_p$ is the set of all nonzero nonsquares in $\mathbb{Z}_p$, two results follow that will contribute towards our goal: no element of $\overline{\Gamma}_p$ is adjacent to 0, and $\{\Gamma_p, \{0\}, \overline{\Gamma}_p\}$ is a partition of the vertices of X_p. From these two results, we can distill that $\partial(\overline{\Gamma}_p)$ contains only edges going between $\overline{\Gamma}_p$ and Γ_p. Therefore, we will determine $|\partial(\overline{\Gamma}_p)|$ by figuring out how many of the edges incident to vertices in Γ_p remain once the edges going between either an element of Γ_p and 0 or two elements of Γ_p are accounted for. We have that

$$\begin{aligned}|\Gamma_p| \cdot \frac{p-1}{2} = {}&(\#\text{ of edges going between } \Gamma_p \text{ and } \overline{\Gamma}_p)\\ &+ (\#\text{ of edges going between } \Gamma_p \text{ and } 0)\\ &+ 2\cdot(\#\text{ of edges going between vertices in } \Gamma_p).\end{aligned}$$

The first term on the right side is $|\partial(\overline{\Gamma}_p)|$. Also, $|\Gamma_p| = (p-1)/2$, and every vertex in Γ_p is adjacent to 0, so the first factor on the left-hand side and the second term on the right-hand side are both $(p-1)/2$. Substituting these values and solving for $|\partial(\overline{\Gamma}_p)|$, we get

$$|\partial(\overline{\Gamma}_p)| = \frac{p-1}{2}\cdot\frac{p-1}{2} - \frac{p-1}{2} - 2\cdot(\#\text{ of edges between vertices in }\Gamma_p). \tag{6}$$

We now set our sights on determining the number of adjacencies between vertices in Γ_p. The way to do this is to count walks of length 3 that start and end at 0 within X_p. We use the following theorem to do this.

Theorem 8 [Stanley 2013]. *Let G be a graph, $\lambda_1, \lambda_2, \dots, \lambda_n$ be the eigenvalues of G, and N_k be the number of closed walks in G of length k. Then*

$$N_k = \sum_{i=1}^{n} \lambda_i^k.$$

We noted in the introduction that the eigenvalues of the Paley graph X_p are $(p-1)/2$, with multiplicity 1; $(\sqrt{p}-1)/2$, with multiplicity $(p-1)/2$; and $(-\sqrt{p}-1)/2$, with multiplicity $(p-1)/2$. So the number of closed walks of length 3 in X_p is given by

$$\left(\frac{p-1}{2}\right)^3 + \left(\frac{p-1}{2}\right)\left(\frac{\sqrt{p}-1}{2}\right)^3 + \left(\frac{p-1}{2}\right)\left(\frac{-\sqrt{p}-1}{2}\right)^3 = \frac{p}{8}(p-5)(p-1).$$

Paley graphs are Caley graphs, which have a nice property: vertex transitivity. More specifically, if x_1 and x_2 are both vertices of X_p, then the number of closed walks of length k beginning at x_1 is equal to the number of closed walks of length k beginning at x_2. (One can see this by shifting the walks from x_1 to x_2 by adding $-x_1+x_2$ to all the vertices of the closed walk starting at x_1, and vice versa.). Since there are p vertices in X_p, we see that the number of closed walks of length 3 beginning at any one vertex of X_p is $\frac{1}{8}(p-5)(p-1)$. In particular, this is how many such walks begin at 0.

Again, noting that 0 is adjacent to each element of Γ_p (and only to elements of Γ_p), it follows that if δ and β are nonzero elements of $\mathbb{Z}_p$, then $(0, \delta^2, \beta^2, 0)$ is a closed walk of length 3 beginning at zero if and only if $(0, \beta^2, \delta^2, 0)$ is a closed walk of length 3 beginning at zero if and only if δ^2 and β^2 are adjacent vertices of Γ_p. When viewed in this fashion, we see the number of closed walks of length 3 beginning at 0 double counts adjacencies between vertices in Γ_p. That is,

$$\tfrac{1}{8}(p-5)(p-1) = 2\cdot(\#\text{ of edges between vertices in }\Gamma_p).$$

It follows immediately from (6) that

$$\begin{aligned}|\partial(\overline{\Gamma}_p)| &= \frac{p-1}{2}\cdot\frac{p-1}{2} - \frac{p-1}{2} - \tfrac{1}{8}(p-5)(p-1)\\ &= \frac{p-1}{2}\cdot\frac{p-1}{4}.\end{aligned}$$

Dividing the above result by $|\overline{\Gamma}_p| = (p-1)/2$ gives us (5). Hence, $h(X_p) \le (p-1)/4$.

3. The Kazhdan constant of the pair associated with a Paley graph

In this section, we prove Theorem 2. Recall that $\overline{\Gamma}_p = \mathbb{Z}_p \setminus (\Gamma_p \cup \{0\})$, $\xi_p = e^{2\pi i/p}$ and

$$\kappa(\mathbb{Z}_p, \Gamma_p) = \min\Big\{\max_{\gamma\in\Gamma_p} \|\xi^\gamma - 1\|, \max_{\gamma\in\overline{\Gamma}_p} \|\xi^\gamma - 1\|\Big\}.$$

To attack the problem of approximating the Kazhdan constant of a Paley graph, we need to use facts about squares and nonsquares in $\mathbb{Z}_p$. For this we need the Legendre symbol. Recall that the Legendre symbol is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \text{ divides } a, \\ 1 & \text{if } a \text{ is a square modulo } p, \\ -1 & \text{if } a \text{ is a nonsquare modulo } p. \end{cases}$$

One can show that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. Also, if $x \equiv y \pmod p$, then $\left(\frac{x}{p}\right) = \left(\frac{y}{p}\right)$. It can also be shown that $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 4$. Likewise $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod 8$.These results can be found in any standard book on number theory. For example, see [Niven et al. 1991].

We now show that $\lim_{p\to\infty} \kappa(\mathbb{Z}_p, \Gamma_p) = 2$, where the limit is over all primes with $p \equiv 1 \pmod 4$. We break this into two cases: when $p \equiv 1 \pmod 8$ and when $p \equiv 5 \pmod 8$.

Let $\epsilon > 0$ be an arbitrary small number.

Suppose that $p \equiv 5 \pmod 8$. In this case we have that

$$1 = \left(\frac{-1}{p}\right) = \left(\frac{(p-1)/2}{p}\right)\left(\frac{2}{p}\right) = -\left(\frac{(p-1)/2}{p}\right).$$

Hence $(p-1)\cdot 2^{-1}$ is in $\overline{\Gamma}_p$. Let N_1 be an integer such that if $p > N_1$ and $p \equiv 5 \pmod 8$, then

$$\|\xi_p^{(p-1)/2} - 1\| > 2 - \epsilon.$$

This gives us a nonsquare $(p-1)\cdot 2^{-1}$ of $\mathbb{Z}_p$, where $\xi_p^{(p-1)/2}$ is close to -1 in the complex plane. Now let α be a real number such that $1/2 < \alpha < 1$ and $\|e^{i\alpha\pi} - 1\| > 2 - \epsilon$. Consider the interval $\big[\sqrt{\alpha p/2}, \sqrt{p/2}\big]$. Note that $\lim_{p\to\infty}\big(\sqrt{p/2} - \sqrt{\alpha p/2}\big) = \infty$. Hence, there is a positive integer N_2 such that if $p > N_2$, then there exists an integer x such that $\sqrt{\alpha p/2} < x < \sqrt{p/2}$, which is equivalent to $\alpha\pi < (2\pi x^2)/p < \pi$. Hence if $p > N_2$ then there exists a square $\gamma \in \Gamma_p$ such that

$$\|\xi_p^\gamma - 1\| > \|e^{\alpha\pi i} - 1\| > 2 - \epsilon.$$

Combining the above, we have that if p is a prime with $p \equiv 5 \pmod 8$ and $p > \max\{N_1, N_2\}$ then $\kappa(\mathbb{Z}_p, \Gamma_p) > 2 - \epsilon$.

Now suppose that $p \equiv 1 \pmod 8$. In this case we have that

$$1 = \left(\frac{-1}{p}\right) = \left(\frac{(p-1)/2}{p}\right)\left(\frac{2}{p}\right) = \left(\frac{(p-1)/2}{p}\right).$$

Therefore $(p-1)\cdot 2^{-1}$ is in Γ_p. Let N_3 be an integer such that if $p > N_3$ and $p \equiv 1 \pmod 8$, then $\|\xi_p^{(p-1)/2} - 1\| > 2 - \epsilon$. Let $0 < j_p < p$ be the smallest nonsquare in $\overline{\Gamma}_p$. Note that j_p must be odd since if it was even, then

$$\left(\frac{j_p/2}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{j_p/2}{p}\right) = \left(\frac{j_p}{p}\right) = -1.$$

This would imply that $j_p \cdot 2^{-1}$ is a smaller nonsquare than j_p in $\overline{\Gamma}_p$, which is not true. We also have that

$$\left(\frac{(p-j_p)/2}{p}\right) = \left(\frac{(p-j_p)/2}{p}\right)\left(\frac{2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{j_p}{p}\right) = \left(\frac{j_p}{p}\right) = -1.$$

Thus, $(p-j_p)\cdot 2^{-1}$ is a nonsquare. We now introduce a lemma which is taken from [Pollack and Treviño 2014]. This lemma will give us a nice bound on j_p.

Lemma 9. $$0 < j_p < \tfrac{1}{2} + \sqrt{p}.$$

Proof. Note that $p < j_p\lceil p/j_p\rceil < p + j_p$. Hence the least nonnegative residue of $j_p\lceil p/j_p\rceil$ modulo p lies in the interval $(0, j_p)$. Therefore, $j_p\lceil p/j_p\rceil$ is a square modulo p. Since j_p is a nonsquare modulo p, we must have that $(j_p\lceil p/j_p\rceil)/j_p = \lceil p/j_p\rceil$ is a nonsquare. By the minimality of j_p, we have that $j_p \le \lceil p/j_p\rceil \le 1 + p/j_p$. Therefore, $j_p^2 - j_p < p$ and hence $j_p^2 - j_p + 1 \le p$. This implies that $(j_p - 1/2)^2 < j_p^2 - j_p + 1 \le p$. So, $j_p < 1/2 + \sqrt{p}$. □

By Lemma 9, we have that

$$\frac{p}{2} > \frac{p-j_p}{2} > \frac{p}{2} - \frac{\sqrt{p}}{2} - \frac{1}{4}.$$

Hence

$$\|\xi_p^{(p-j_p)/2} - 1\| > \|\xi_p^{p/2-\sqrt{p}/2-1/4} - 1\| = \|e^{\pi i - \pi i/\sqrt{p} - \pi i/2p} - 1\|.$$

Let N_4 be a positive integer such that if $p > N_4$ and $p \equiv 1 \pmod 8$, then

$$\|\xi^{(p-j_p)/2} - 1\| > 2 - \epsilon.$$

Thus, if p is a prime with $p \equiv 1 \pmod 8$ and $p > \max\{N_3, N_4\}$, then $\kappa(\mathbb{Z}_p, \Gamma_p) > 2 - \epsilon$.

Combining all of the above results, we have that Theorem 2 has been proved.

References

[Bacher and de la Harpe 1994] R. Bacher and P. de la Harpe, "Exact values of Kazhdan constants for some finite groups", *J. Algebra* **163**:2 (1994), 495–515. MR 95b:20018 Zbl 0842.20013

[Breuillard et al. 2011] E. Breuillard, B. Green, and T. Tao, "Suzuki groups as expanders", *Groups Geom. Dyn.* **5**:2 (2011), 281–299. MR 2012c:20066 Zbl 1247.20017

[Elsawy 2009] A. N. Elsawy, *Paley graphs and their generalizations*, Master's thesis, Heinrich Heine University, Düsseldorf, 2009. arXiv 1203.1818

[Gross et al. 2014] J. L. Gross, J. Yellen, and P. Zhang (editors), *Handbook of graph theory*, 2nd ed., CRC Press, Boca Raton, FL, 2014. MR 3185588 Zbl 1278.05001

[Kassabov et al. 2006] M. Kassabov, A. Lubotzky, and N. Nikolov, "Finite simple groups as expanders", *Proc. Natl. Acad. Sci. USA* **103**:16 (2006), 6116–6119. MR 2007d:20025 Zbl 1161.20010

[Krebs and Shaheen 2011] M. Krebs and A. Shaheen, *Expander families and Cayley graphs: a beginner's guide*, Oxford University Press, 2011. MR 3137611 Zbl 1238.05221

[Lanphier and Rosenhouse 2004] D. Lanphier and J. Rosenhouse, "Cheeger constants of Platonic graphs", *Discrete Math.* **277**:1-3 (2004), 101–113. MR 2005c:05102 Zbl 1033.05055

[Mohar 1989] B. Mohar, "Isoperimetric numbers of graphs", *J. Combin. Theory* (*B*) **47**:3 (1989), 274–291. MR 90m:05087 Zbl 0719.05042

[Niven et al. 1991] I. Niven, H. L. Montgomery, and H. S. Zuckerman, *An introduction to the theory of numbers*, 5th ed., Wiley, New York, 1991. MR 91i:11001 Zbl 0742.11001

[Pollack and Treviño 2014] P. Pollack and E. Treviño, "The primes that Euclid forgot", *Amer. Math. Monthly* **121**:5 (2014), 433–437. MR 3193727 Zbl 06367526

[Rosenhouse 2002] J. Rosenhouse, "Isoperimetric numbers of Cayley graphs arising from generalized dihedral groups", *J. Combin. Math. Combin. Comput.* **42** (2002), 127–138. MR 2004d:05092 Zbl 1019.05030

[Stanley 2013] R. P. Stanley, *Algebraic combinatorics: walks, trees, tableaux, and more*, Springer, New York, 2013. MR 3097651 Zbl 1278.05002

[Voskanian 2013] E. Voskanian, *Obtaining lower bounds for the Kazhdan constant*, Master's thesis, California State University, Los Angeles, 2013.

Received: 2014-10-28 Revised: 2015-01-25 Accepted: 2015-02-02

kevinhcramer@gmail.com *Department of Mathematics, California State University, Los Angeles, Los Angeles, CA 90032, United States*

mkrebs@calstatela.edu *Department of Mathematics, California State University, Los Angeles, Los Angeles, CA 90032, United States*

linus108nicole@yahoo.com *Department of Mathematics, California State University, Los Angeles, Los Angeles, CA 90032, United States*

ashahee@calstatela.edu *Department of Mathematics, California State University, Los Angeles, Los Angeles, 90032, United States*

voskanian@math.ucr.edu *Department of Mathematics, University of California, Riverside, Riverside, CA 92521, United States*

involve

msp.org/involve

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2016 is US $160/year for the electronic version, and $215/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFlow® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve

2016 vol. 9 no. 2

1944-4176(2016)9:2;1-3