ON THE PALEY GRAPH OF A QUADRATIC CHARACTER

JÁN MINÁČ, LYLE MULLER, TUNG T. NGUYEN, NGUYỄN DUY TÂN

Dedicated to Professor Moshe Rosenfeld on the occasion of his 85th birthday

ABSTRACT. Paley graphs represent a useful class of graphs with interesting properties. Classically, for each prime number p we can construct the corresponding Paley graph using quadratic and non-quadratic residues modulo p. In this article, we introduce the generalized Paley graphs. These are graphs that are associated with a general quadratic character. We will then provide some of their basic properties. In particular, we describe their spectrum explicitly. We then use those generalized Paley graphs to construct some new families of Ramanujan graphs. Finally, using special values of L-functions, we provide an effective upper bound for their Cheeger number.

1. INTRODUCTION

Let $q = p^n$ be a prime power. The Paley graph P_q is the graph with the following data

(1) The vertex set of P_q is $\mathbb{F}_q$.
(2) Two vertices u, v are connected iff $u - v$ a nonzero square in $\mathbb{F}_q$; i.e $u - v$ is an element of the set

$$S = \{x^2 | x \in \mathbb{F}_q, x \neq 0\}.$$

In other words, we can view P_q as the Cayley graph $\Gamma(\mathbb{F}_q, S)$ (see [6, 17]). We remark that $-1 \in S$ iff $q \equiv 1 \pmod 4$. Therefore, P_q is an undirected graph for $q \equiv 1 \pmod 4$.

The origin of Paley graphs can be traced back to Paley's 1933 paper [25] in which he implicitly used them to construct Hadamard matrices. These graphs were later rediscovered by Carlitz in [5], though this time in a different context. Gareth A. Jones had the following remark in [15] about Paley graphs

Date: October 8, 2022.

2020 *Mathematics Subject Classification.* Primary 05C25, 05C50, 11M06.

Key words and phrases. Paley graphs, Ramanujan graphs, Cheeger number, Gauss sums, Special values of L-functions.

Jan Minac is partially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) grant R0370A01. Jan Minac also gratefully acknowledges Faculty of Sciences Distinguished Research Professorship award for 2020/21. Jan Minac, Lyle Muller and Tung T Nguyen acknowledge the support of the Western Academy for Advanced Research. Nguyễn Duy Tân is funded by Vingroup Joint Stock Company and supported by Vingroup Innovation Foundation (VinIF) under the project code VINIF.2021.DA00030.

> Anyone who seriously studies algebraic graph theory or finite permutation groups will, sooner or later, come across the Paley graphs and their automorphism groups.

Due to its arithmetic and representation theoretic nature, we have various tools to study Paley graphs. Consequently, they have interesting properties that make them useful for graph theory and related fields. For example, Paley graphs have found applications in coding and cryptography theory (see [12, 13]).

In this article, we define and study generalized Paley graphs which are associated with general quadratic characters (we refer the reader to Section 2 for the precise definition of these graphs). Using the theory of Gauss sums and circulant matrices, we describe explicitly the spectrum of these generalized Paley graphs. We then answer the following question: which generalized Paley graphs are Ramanujan? In the final section, we provide an effective upper bound for the Cheeger number of these generalized Paley graphs using special values of L-functions.

In closing the introduction, we remark that our interest in this topic arises naturally from our recent works on generalized Fekete polynomials (see [20, 21]), on the join of circulant matrices (see [7, 10]), and on some new constructions of Ramanujan graphs (see [11]).

2. Quadratic characters and the associated Paley graphs

2.1. **Quadratic characters.** Let m be a squarefree integer. Let Δ be the discriminant of the quadratic extension $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$, which is given by

$$\Delta = \begin{cases} m & \text{if } m \equiv 1 \pmod 4 \\ 4m & \text{if } m \equiv 2, 3 \pmod 4. \end{cases}$$

From this definition, we can see that Δ necessarily determines the quadratic extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$. We have the following theorem.

Theorem 2.1. *(*[22, Theorem 9.13]*) Let $\chi_\Delta : \mathbb{Z} \to \mathbb{C}^\times$ be the function given by*

$$\chi_\Delta(a) = \left(\frac{\Delta}{a}\right),$$

where $\left(\frac{\Delta}{a}\right)$ is the Kronecker symbol introduced in the previous section. Then χ_Δ is a primitive quadratic character of conductor $D = |\Delta|$. Furthermore, every primitive quadratic character is given uniquely this way.

2.2. **Generalized Paley graphs and their spectra.** Let $\chi = \chi_\Delta$ be the primitive quadratic character of conductor $D = |\Delta|$ as explained in the previous section. We introduce the following definition (see also [4] for a similar approach).

Definition 2.2. The Paley graph P_Δ is the graph with the following data

(1) The vertices of P_Δ are $\{0, 1, \ldots, D-1\}$.
(2) Two vertices (u, v) are connected iff $\chi_\Delta(v-u) = 1$.

Example 2.3. We refer to Figure 1 and and Figure 2 for two concrete examples of generalized Paley graphs.

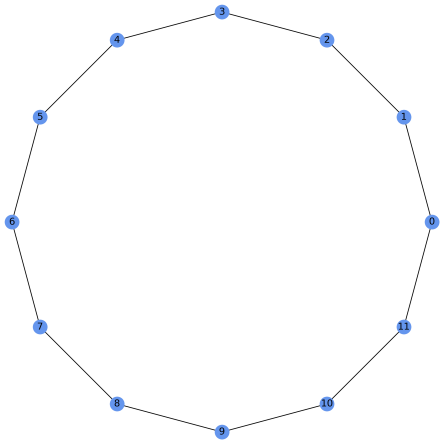

FIGURE 1. The Paley graph P_{12}

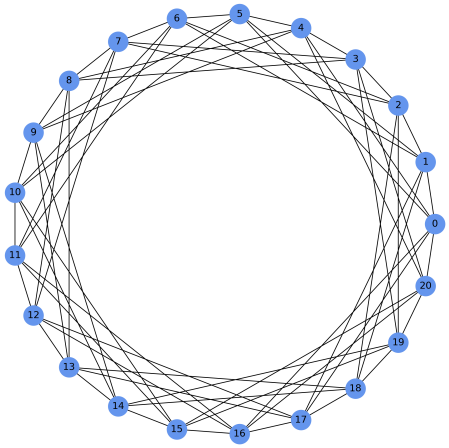

FIGURE 2. The Paley graph P_{21}.

We remark that if $\Delta < 0$, then $\chi_\Delta(-1) = -1$. In this case, P_Δ is a directed graph. Otherwise, if $\Delta > 0$ then $\chi_\Delta(-1) = 1$ and therefore, P_Δ is an undirected graph.

Since the connection in P_Δ is determined by $(v-u) \mod D$, we conclude that P_Δ is a circulant graph with respect to the cyclic group $\mathbb{Z}/D$ (see [7, 9]). In fact, its adjacency matrix is generated by the following vector

$$v = \left[\frac{1}{2}\chi(a)(\chi(a)+1)\right]_{0\le a\le D-1}.$$

This follows from the fact that

$$\frac{1}{2}\chi(a)(1+\chi(a)) = \begin{cases} 1 & \text{if } \chi(a) = 1 \\ 0 & \text{else.} \end{cases}$$

We first observe the following.

Proposition 2.4. *P_Δ is a regular graph of degree $\frac{1}{2}\varphi(D)$.*

Proof. We have

$$\begin{aligned} 2\deg(P_\Delta) &= \sum_{a=0}^{D-1} \chi(a)[1+\chi(a)] = \sum_{a=0}^{D-1} \chi(a) + \sum_{a=0}^{D-1} \chi^2(a) \\ &= 0 + \sum_{0\leq a\leq D-1, \gcd(a,D)=1} 1 = \varphi(D). \end{aligned}$$

Here we use the fact that

$$\sum_{a=0}^{D-1} \chi(a) = 0.$$

We conclude that $\deg(P_\Delta) = \frac{1}{2}\varphi(D)$. □

Corollary 2.5. *Suppose that $\Delta > 0$. Then P_Δ is a cycle graph if and only if $\Delta = 5$ or $\Delta = 8$ or $\Delta = 12$.*

Proof. Suppose that P_Δ is a cycle graph. Then the degree of P_Δ is 2. By Proposition 2.4, we must have $\varphi(D) = 4$. Therefore $\Delta = D \in \{5, 8, 12\}$. Conversely, if $\Delta \in \{5, 8, 12\}$, then $\chi(a) = 1$ if and if $a = \pm 1$. Consequently, an edge in P_Δ must have the form $(u, u+1)$ or $(u, u-1)$ for $u \in \mathbb{Z}/D$. In other words, P_Δ is a cycle graph. □

3. The spectrum of P_Δ

In this section, we compute the spectrum of P_Δ. By the Circulant Diagonalization Theorem (see [9]), the spectrum of P_Δ is given by

$$\left\{ \lambda(\omega) := \frac{1}{2} \sum_{a=0}^{D-1} \chi(a)(1+\chi(a))\omega^a \right\},$$

where ω runs over the set of all D-roots of unity. Note that for each ω, there exists a unique positive integer $d|D$ such that ω is a primitive d-root of unity. We first recall the definition of the Mobius function

Definition 3.1. The Mobius function $\mu(n)$ is defined as follow

$$\mu(n) = \begin{cases} 0 \text{ if } n \text{ has one or more repeated prime factors} \\ 1 \text{ if } n = 1 \\ (-1)^k \text{ if } n \text{ is a product of } k \text{ distinct primes.} \end{cases}.$$

Lemma 3.2. *(See* [24, Section 4.3, Exercise 28]*). Let d be a positive integer. Let ω be a primitive d-root of unity. Then*

$$\sum_{1\leq i\leq d, \gcd(i,d)=1} \omega^i = \mu(d).$$

In other words, the sum of all primitive d-roots of unity is equal to $\mu(d)$.

We recall the theory of Gauss sum. Let $\zeta_D = \exp\left(\frac{2\pi i}{D}\right)$ be a primitive D-root of unity.

Definition 3.3. ([1, Chapter V]) The Gauss sum $G(b,\chi)$ is defined as follow

$$G(b,\chi)=\sum_{a=1}^{D-1}\chi(a)\zeta_D^{ab}.$$

We recall the following fundamental property [1, Theorem 4.12, page 312]

$$G(b,\chi)=\chi(b)G(1,\chi).$$

Furthermore, by [1, Theorem 4.17], we have $G(1,\chi)=\sqrt{\Delta}$. Consequently $G(b,\chi)=\chi(b)\sqrt{\Delta}$. In particular, if ω is not a primitive D-root of unity then

$$\sum_{a=1}^{D-1}\chi(a)\omega^a=0.$$

On the other hand, if ω is a primitive D-root of unity, namely $\omega=\zeta_D^b$ with $\gcd(b,D)=1$ then

$$\sum_{a=0}^{D-1}\chi(a)\omega^a=\chi(b)\sqrt{\Delta}.$$

In summary, we have the following lemma.

Lemma 3.4. *Let ω be an D-root of unity.*

(1) If ω is not a primitive D-root of unity then

$$\sum_{a=1}^{D-1}\chi_\Delta(a)\omega^a=0.$$

(2) If $\omega=\zeta_D^b$ with $\gcd(b,D)=1$ then

$$\sum_{a=1}^{D-1}\chi_\Delta(a)\omega^a=\chi(b)\sqrt{\Delta}.$$

We can now simplify $\lambda(\omega)$. In fact

$$\begin{aligned}2\lambda(\omega)&=\sum_{a=0}^{D-1}\chi(a)\omega^a+\sum_{a=0}^{D-1}\chi^2(a)\omega^a\\&=\sum_{a=0}^{D-1}\chi(a)\omega^a+\sum_{0\le a\le D-1,\gcd(a,D)=1}\omega^a.\end{aligned}$$

We consider two cases.

Case 1. ω is a primitive d-root of unity with $d<D$. In this case

$$\sum_{a=0}^{D-1}\chi(a)\omega^a=0,$$

and

$$\sum_{0\le a\le D-1,\gcd(a,D)=1} \omega^a = \frac{\varphi(D)}{\varphi(d)}\mu(d).$$

Therefore

$$\lambda(\omega) = \frac{1}{2}\frac{\varphi(D)}{\varphi(d)}\mu(d).$$

Case 2. $\omega = \zeta_D^b$ is a primitve D-root of unity; namely $\omega = \zeta_D^b$ with $\gcd(b, D) = 1$. In this case we have

$$\sum_{a=0}^{D-1} \chi(a)\omega^a = \chi(b)\sqrt{D},$$

and

$$\sum_{0\le a\le D-1,\gcd(a,D)=1} \omega^a = \mu(D).$$

Consequently

$$\lambda(\omega) = \frac{1}{2}\left[\chi(b)\sqrt{\Delta} + \mu(D)\right].$$

Let us write $[a]_b$ for the multiset $\{\underbrace{a, \ldots, a}_{b \text{ times}}\}$. By the above calculations, we have the following conclusion.

Theorem 3.5. *The spectrum of the Paley graph P_Δ is the union of the following multisets*

$$\left[\frac{1}{2}\frac{\varphi(D)}{\varphi(d)}\mu(d)\right]_{\varphi(d)} \quad \text{for } d|D \quad \text{and } d < D,$$

and

$$\left[\frac{1}{2}(\sqrt{\Delta} + \mu(D))\right]_{\frac{\varphi(D)}{2}},$$

and

$$\left[\frac{1}{2}(-\sqrt{\Delta} + \mu(D))\right]_{\frac{\varphi(D)}{2}}.$$

We discuss a corollary of this theorem. First, we recall that an undirected graph $G = (V, E)$ is called a bipartite graph if $V(G)$ can be decomposed into two disjoint sets such that no two vertices within the same set are adjacent. As explained in [23], if G is regular of degree r then G is a bipartite graph if and only if $-r$ is an eigenvalue of G.

Corollary 3.6. *Suppose that $\Delta > 0$. Then, the Paley graph P_Δ is a bipartite graph if and only if Δ is even.*

Proof. If Δ is even then we can decompose $V(P_\Delta)$ into the following two sets

$$V_{\text{odd}} = \{a \in V(G) | a \equiv 1 \pmod 2\},$$

and

$$V_{\text{even}} = \{a \in V(G) | a \equiv 0 \pmod 2\}.$$

If u, v both belong to either V_{odd} or V_{even} then $u - v$ is even. Therefore, $\chi(u - v) = 0$. By definition, u and v are not adjacent. We conclude that P_Δ is a bipartite graph.

Conversely, let us assume that P_Δ is a bipartite graph. By the above remark and the fact that P_Δ is regular of degree $\frac{1}{2}\varphi(D)$, we conclude that one of its eigenvalues must be $-\frac{1}{2}\varphi(D)$. Clearly this eigenvalue cannot be either $\frac{1}{2}(\sqrt{\Delta} + \mu(D))$ or $\frac{1}{2}(-\sqrt{\Delta} + \mu(D))$ because these values are not integers. Consequently, by Theorem 4.3, there must exists $d|D$ and $d < D$ such that

$$\frac{1}{2}\frac{\varphi(D)}{\varphi(d)}\mu(d) = -\frac{1}{2}\varphi(D).$$

Equivalently, we must have $\varphi(d) = -\mu(d) \in \{-1, 1\}$. We conclude that $d = 2$ and hence D is even. □

4. Ramanujan Paley graphs

In this section, we investigate the following question: which P_Δ is a Ramanujan graph? For this question to make sense, we need to assume that P_Δ is a undirected graph. This requires χ_Δ is an even character; or equivalently $\Delta > 0$. We first recall the definition of a Ramanujan graph (see [19, 23]).

Definition 4.1. Let G be a connected r-regular graph with N vertices, and let $r = \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_N$ be the eigenvalues of the adjacency matrix of G. Since G is connected and r-regular, its eigenvalues satisfy $|\lambda_i| \leq r, 1 \leq i \leq N$. Let

$$\lambda(G) = \max_{|\lambda_i| < r} |\lambda_i|.$$

The graph G is a *Ramanujan graph* if

$$\lambda(G) \leq 2\sqrt{r-1}.$$

Lemma 4.2. *Suppose D is not a prime number. The graph P_Δ is a Ramanujan graph if and only if*

$$\frac{\varphi(D)}{(p-1)^2} + \frac{16}{\varphi(D)} \leq 8,$$

where p is the smallest odd prime divisor of D, and

$$\begin{cases} \dfrac{\varphi(D)}{D} \geq \dfrac{1}{8} + \dfrac{1}{4\sqrt{D}} + \dfrac{17}{8D} & \text{if } D \text{ is odd} \\ \dfrac{\varphi(D)}{D} \geq \dfrac{1}{8} + \dfrac{2}{D} & \text{if } D \text{ is even} \end{cases}.$$

Proof. Let d be an arbitrary divisor of D such that $1 < d < D$ and $d \neq 2$ if $4 \mid D$. One has

$$\frac{\varphi(D)}{2\varphi(d)} \leq 2\sqrt{\frac{\varphi(D)}{2} - 1} \Leftrightarrow \frac{\varphi(D)^2}{\varphi(d)^2} \leq 8\varphi(D) - 16 \Leftrightarrow \frac{\varphi(D)}{\varphi(d)^2} + \frac{16}{\varphi(D)} \leq 8.$$

Clearly if d has an odd prime divisor then $\frac{\varphi(D)}{\varphi(d)^2} + \frac{16}{\varphi(D)} \leq \frac{\varphi(D)}{(p-1)^2} + \frac{16}{\varphi(D)}$, where p is the smallest odd prime divisor of D.

One also has

$$\frac{\sqrt{D}+1}{2} \leq 2\sqrt{\frac{\varphi(D)}{2} - 1} \Leftrightarrow (1+\sqrt{D})^2 \leq 8\varphi(D) - 16 \Leftrightarrow \frac{\varphi(D)}{D} \geq \frac{1}{8} + \frac{1}{4\sqrt{D}} + \frac{17}{8D},$$

and

$$\frac{\sqrt{D}}{2} \leq 2\sqrt{\frac{\varphi(D)}{2} - 1} \Leftrightarrow D \leq 8\varphi(D) - 16 \Leftrightarrow \frac{\varphi(D)}{D} \geq \frac{1}{8} + \frac{2}{D}.$$

The lemma now follows from Theorem 3.5. □

Theorem 4.3. *The graph P_Δ is a Ramanujan graph if and only if*

(1) either $D = 8$,

(2) or $D = 4p$, where p is a prime number, $p \equiv 3 \pmod 4$,

(3) or $D = 8p$, where p is an odd prime number,

(4) or $D = 4p_1p_2$ where p_1 and p_2 are distinct primes, $p_1p_2 \equiv 3 \pmod 4$, $p_1 < p_2$, and

$$\frac{p_2-1}{p_1-1} + \frac{4}{(p_1-1)(p_2-1)} \leq 4.$$

(5) or $D = 8p_1p_2$ where p_1 and p_2 are distinct primes, $2 < p_1 < p_2$, and

$$\frac{p_2-1}{p_1-1} + \frac{1}{(p_1-1)(p_2-1)} \leq 2.$$

(6) or D is a prime number p with $p \equiv 1 \pmod 4$,

(7) or $D = p_1p_2$ where p_1 and p_2 are distinct primes, $p_1p_2 \equiv 1 \pmod 4$, $p_1 < p_2$, and

$$\frac{p_2-1}{p_1-1} + \frac{16}{(p_1-1)(p_2-1)} \leq 8.$$

Proof. a) We first consider the case that D is even. It is easy to check that for P_8 is a Ramanujan graph. So we suppose that $D \neq 8$ and P_Δ is a Ramanujan graph. Let $D = 2^a p_1^{a_1} \cdots p_k^{a_k}$ be the prime factorization of D with $2 < p_1 < \cdots < p_k$. One has $a \in \{2,3\}$, $k \geq 1$, and $a_2 = \cdots = a_k = 1$. By Lemma 4.2,

$$8 \geq \frac{\varphi(D)}{(p_1-1)^2} + \frac{16}{\varphi(D)} > \frac{\varphi(D)}{(p_1-1)^2} = 2^{a-1}\frac{p_2-1}{p_1-1}\cdots(p_k-1).$$

This inequality forces $k \leq 2$. In fact, if $k \geq 3$ then

$$2^{a-1}\frac{p_2-1}{p_1-1}\cdots(p_k-1) > 2(p_3-1) \geq 2(7-1) = 12 > 8.$$

Case 1: $k = 2$**.** In this case $D = 2^a p_1 p_2$, $a \in \{2,3\}$. One has

$$\frac{\varphi(D)}{D} \geq \frac{1}{8} + \frac{2}{D} \Leftrightarrow \frac{3}{4} \geq \frac{1}{p_1} + \frac{1}{p_2} + \frac{2^{2-a}-1}{p_1 p_2}.$$

The last inequality is true because

$$\frac{1}{p_1} + \frac{1}{p_2} + \frac{2^{2-a}-1}{p_1 p_2} \leq \frac{1}{3} + \frac{1}{5} < \frac{3}{4}.$$

Case 1: $k = 1$**.** In this case $D = 2^a p_1$, $a \in \{2,3\}$. One has

$$\frac{\varphi(D)}{D} \geq \frac{1}{8} + \frac{2}{D} \Leftrightarrow \frac{3}{4} \geq \frac{1+2^{2-a}}{p_1}.$$

The last inequality is true because

$$\frac{1+2^{2-a}}{p_1} \leq \frac{2}{3} < \frac{3}{4}.$$

Note also that

$$\frac{\varphi(D)}{(p_1-1)^2} + \frac{16}{\varphi(D)} = \frac{2^{a-1}+2^{5-a}}{p_1-1} \leq \frac{10}{3-2} = 5 < 8.$$

b) Now we consider the case D is odd. It is well-known that if Δ is a prime number then P_Δ is a Ramanujan graph.

Suppose that D is not a a prime number and that P_Δ is a Ramanujan graph. Let $D = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ be the prime factorization of D with $2 < p_1 < p_2 < \cdots < p_k$. Since d is square-free, $a_1 = \cdots = a_k = 1$, and $k \geq 2$. By Lemma 4.2,

$$8 \geq \frac{\varphi(D)}{(p_1-1)^2} + \frac{16}{\varphi(D)} > \frac{p_2-1}{p_1-1} \cdots (p_k-1).$$

This inequality forces $k \leq 3$. In fact, if $k \geq 4$ then

$$\frac{p_2-1}{p_1-1} \cdots (p_k-1) > (p_3-1)(p_4-1) \geq (5-1)(7-1) = 24 > 8.$$

Case 1: $k = 3$**.** Since $8 > \dfrac{p_2-1}{p_1-1}(p_3-1)$, we conclude that $p_3 = 7$. Hence $(p_1,p_2) = (3,5)$. However in this case, one has $\dfrac{p_2-1}{p_1-1}(p_3-1) > 8$, a contradiction.

Case 2: $k = 2$**.** In this case $D = p_1 p_2$. One has

$$\frac{\varphi(D)}{D} \geq \frac{1}{8} + \frac{1}{4\sqrt{D}} + \frac{17}{8D} \Leftrightarrow \frac{7}{8} \geq \frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{4\sqrt{p_1 p_2}} + \frac{4}{p_1 p_2}.$$

The last inequality is true because

$$\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{4\sqrt{p_1 p_2}} + \frac{4}{p_1 p_2} \leq \frac{1}{3} + \frac{1}{5} + \frac{1}{4\sqrt{15}} + \frac{4}{15} < \frac{7}{8}.$$

□

Remarks 4.4. (a) The condition $\dfrac{p_2-1}{p_1-1}+\dfrac{4}{(p_1-1)(p_2-1)}\leq 4$ in part (4) of Theorem 4.3 is equivalent to

$$4(p_1-1)-(p_2-1)\geq \frac{4}{p_2-1}.$$

In the case that $p_2\geq 7$, the latter condition is equivalent to

$$4(p_1-1)-(p_2-1)\geq 1,$$

which is equivalent to

$$p_2\leq 4p_1-5.$$

(b) The condition $\dfrac{p_2-1}{p_1-1}+\dfrac{1}{(p_1-1)(p_2-1)}\leq 2$ in part (5) of Theorem 4.3 is equivalent to

$$2(p_1-1)-(p_2-1)\geq \frac{1}{p_2-1}.$$

The latter condition is equivalent to

$$2(p_1-1)-(p_2-1)\geq 1,$$

which is equivalent to

$$p_2\leq 2p_1-3.$$

(c) The condition $\dfrac{p_2-1}{p_1-1}+\dfrac{16}{(p_1-1)(p_2-1)}\leq 8$ in part (7) of Theorem 4.3 is equivalent to

$$8(p_1-1)-(p_2-1)\geq \frac{16}{p_2-1}.$$

In the case that $p_2\geq 19$, the latter condition is equivalent to

$$8(p_1-1)-(p_2-1)\geq 1,$$

which is equivalent to

$$p_2\leq 8p_1-9.$$

(d) There are infinitely pairs of primes (p_1,p_2) satisfying the conditions in part (4) of Theorem 4.3. In fact, let us first recall the prime number theorem for arithmetic progressions. Let a, d be two positive integers with $\gcd(a,d)=1$. Let

$$\pi(x;a,d)=|\{p \text{ prime } \mid p\leq x, p\equiv a \pmod d\}|.$$

Then $\pi(x;a,d)\sim \dfrac{1}{\varphi(d)}\dfrac{x}{\ln x}$ as $x\to\infty$. (See for example [18, page 257].) Hence for any fixed number $k>1$,

$$\pi(kx;a,d)-\pi(x;a,d)=|\{p \text{ prime } \mid x<p\leq kx,\ p\equiv a \pmod d\}|\sim \frac{k-1}{\varphi(d)}\frac{x}{\ln x} \text{ as } x\to\infty.$$

In particular for x big enough, there exists a prime p such that

$$x<p\leq kx, \quad p\equiv a \pmod d.$$

Now let $p_1 > 5$ be a prime number congruent to 1 modulo 4 which is big enough so that there exists a prime p_2 such that

$$p_1 < p_2 \leq 3p_1, \quad p \equiv 3 \pmod 4.$$

Then $p_1 p_2 \equiv 3 \pmod 4$ and $p_2 < 4p_1 - 5$. Hence the pair (p_1, p_2) satifies the conditions in part (4) of Theorem 4.3.

Similarly, there are infinitely pairs of primes (p_1, p_2) satisfying the conditions in part (5), or in part (7), of Theorem 4.3.

5. Cheeger number of Paley graphs

Let $\chi = \chi_\Delta$ be an even quadratic character (in other words, $\Delta > 0$) and P_Δ the corresponding generalized Paley graph. In this section, we provide an upper bound for the Cheeger number of P_Δ (also known by other names such as isoperimetric number or edge expansion ratio). Our estimation gives a natural generalization of the results in [8]. We also answer the authors' suspicion about the relationship between the upper bounds that they used in this paper, namely the α-bound and the $\frac{p-1}{4}$-bound (see [8, Section 2.2].) While our result is more general and explicit, we remark that our approach is inspired by the method in [8].

First, let us recall the definition of Cheeger number. Let $G = (E, V)$ be an undirected graph. Let F be a subset of V. For a subset $F \subseteq V$, the boundary of F, denoted by ∂F, is the set of all edges going from a vertex in F to a vertex outside of F. The Cheeger number of G is defined as

$$h(G) := \min \left\{ \frac{|\partial F|}{|F|} \middle| \, F \subseteq V(G), 0 < |F| \leq \tfrac{1}{2}|V(G)| \right\}.$$

Cheeger number is of great important in various scientific fields. For example, it has found applications in graph clustering, analysis of Markov chain, and image segmentation (see [14, 16, 27, 28].)

Let $\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ be the set of all elements on the interval $[1, \ldots, \lfloor \frac{D}{2}]]$ such that $\chi(\alpha_i) = 1$. Note that since χ is even, $\chi(D - a) = \chi(a)$. Therefore, we can conclude that

$$\{\alpha_1, D - \alpha_1, \alpha_2, D - \alpha_2, \ldots, \alpha_k, D - \alpha_k\},$$

is the set of $a \in [0, D]$ such that $\chi(a) = 1$. In particular, we see that $k = \dfrac{\varphi(D)}{4}$.

The following proposition is a direct analog of [8, Proposition 6].

Proposition 5.1. *Let $F = \{0, 1, \ldots, \lfloor \frac{D}{2} \rfloor - 1\} \subset V(P_\Delta)$. Then $|F| = \lfloor \frac{D}{2} \rfloor$ and*

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

Proof. By definition, an element of ∂F will have the form $(i, i+a)$ where $i \in F$, $i+a \notin F$, and $\chi(a) = 1$. In particular, we know that

$$a \in \{\alpha_1, D-\alpha_1, \alpha_2, D-\alpha_2, \ldots, \alpha_k, D-\alpha_k\}.$$

Let us fix an index i where $1 \leq i \leq \dfrac{\varphi(D)}{4}$. The number of edges of the form $(j, j+\alpha_i)$ is equal to the number of $j \in F$ such that

$$(j+\alpha_i) \pmod{D} \geq \lfloor \frac{D}{2} \rfloor. \tag{1}$$

Because $\alpha \leq \lfloor \frac{D}{2} \rfloor$, we conclude that the number of $j \in F$ satisfying the inequality 1 is exactly α_i. Similarly, the number of edges of the form $(j, j+D-\alpha_i)$ is equal to the number of $j \in F$ such that

$$(j+D-\alpha_i) \pmod{D} = (j-\alpha_i) \pmod{D} \geq \lfloor \frac{D}{2} \rfloor \tag{2}$$

Again, the number of j satisfying the inequality 2 is exactly α_i. Summing up over all i, we have

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

□

By definition, we conclude that

$$h(P_\Delta) \leq \frac{2}{\lfloor D/2 \rfloor} \sum_{i=1}^{k} \alpha_i.$$

We can further simplify the right hand side of the above estimate using zeta values. In order to do so, we first recall the definition of the L-function $L(\chi, s)$ attached to χ

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

This L-function is convergent for $s \in \mathbb{C}$ such that $\Re(s) > 0$ and it is absolutely convergent if $\Re(s) > 1$. Furthermore, there is an Euler product formula

$$L(\chi, s) = \prod_p \frac{1}{1-\chi(p)p^{-s}},$$

where p runs over the set of all prime numbers. This Euler product formula shows that $L(\chi, s) > 0$ if $s \in \mathbb{R}$ and $s > 1$. We are now ready to state the following theorem.

Theorem 5.2.

$$h(P_\Delta) \leq \alpha := \frac{1}{8\lfloor D/2 \rfloor} \left(D\varphi(D) - \mu(D)\varphi(D) - \frac{8D\sqrt{D}}{\pi^2} \left(1 - \frac{\chi(2)}{4}\right) L(2, \chi) \right).$$

Proof. One has

$$2\sum_{i=1}^{k}\alpha_i = \sum_{a=1,\gcd(a,D)=1}^{\lfloor D/2\rfloor}(1+\chi(a))a = +\sum_{i=1}^{\lfloor D/2\rfloor}\chi(a)a = \sum_{a=1,\gcd(a,D)=1}^{\lfloor D/2\rfloor} a + \sum_{a=1}^{\lfloor D/2\rfloor}\chi(a)a.$$

By [3, Theorem 13.1],

$$\sum_{a=1}^{\lfloor D/2\rfloor}\chi(a)a = -\frac{D\sqrt{D}}{\pi^2}\left(1-\frac{\chi(2)}{4}\right)L(2,\chi).$$

By [2, Theorem],

$$\sum_{a=1,\gcd(a,D)=1}^{\lfloor D/2\rfloor} a = \frac{1}{8}(D\varphi(D)-\epsilon\psi(D)),$$

where $\epsilon = 1$ if D is odd and $\epsilon = 0$ if D is even; and $\psi(D) = \prod_{p|D}(1-p)$. Note that in the case that D is odd, D is then square-free, hence $\psi(D) = \mu(D)\varphi(D)$. Also if D is even then D is divisible by 4, hence $\mu(D) = 0$. Thus

$$\sum_{a=1,\gcd(a,D)=1}^{\lfloor D/2\rfloor} a = \frac{1}{8}(D\varphi(D)-\mu(D)\varphi(D)).$$

Therefore

$$\alpha := \frac{2\sum_{i=1}^{k}\alpha_i}{\lfloor D/2\rfloor} = \frac{1}{8\lfloor D/2\rfloor}\left(D\varphi(D)-\mu(D)\varphi(D)-\frac{8D\sqrt{D}}{\pi^2}\left(1-\frac{\chi(2)}{4}\right)L(2,\chi)\right).$$

□

Remark 5.3. Let the notation be as above. If D is even, then

$$\alpha = \frac{\varphi(D)}{4} - \frac{2\sqrt{D}}{\pi^2}\left(1-\frac{\chi(2)}{4}\right)L(2,\chi).$$

If D is odd, then

$$\begin{aligned}\alpha &= \frac{1}{4(D-1)}\left(D\varphi(D)-\mu(D)\varphi(D)-\frac{8D\sqrt{D}}{\pi^2}\left(1-\frac{\chi(2)}{4}\right)L(2,\chi)\right)\\ &= \frac{\varphi(D)}{4} - \frac{1}{4(D-1)}\left(\frac{8D\sqrt{D}}{\pi^2}(1-\frac{\chi(2)}{4})L(2,\chi)-(1-\mu(D))\varphi(D)\right).\end{aligned}$$

Corollary 5.4. *Let the notation be as above. Then* $\alpha < \frac{\varphi(D)}{4}$.

Proof. If D is even then statement follows from the previous corollary and the fact that $L(2,\chi) > 0$. So we suppose that D is odd. One can check that for $D = 5$ or $D = 13$ then the statement is true. So we suppose further that $D \geq 17$.

Case 1: $\chi(2) = 1$. In this case,

$$L(2,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^2} \geq 1 + \frac{1}{2^2} - \sum_{n=3}^{\infty} \frac{1}{n^2} = \frac{5}{2} - \frac{\pi^2}{6} > \frac{5}{6}.$$

Hence

$$\frac{8D\sqrt{D}}{\pi^2}(1 - \frac{\chi(2)}{4})L(2,\chi) - (1-\mu(D))\varphi(D) > \frac{8D\sqrt{D}}{\pi^2} \cdot \frac{3}{4} \cdot \frac{5}{6} - 2D > 0.$$

Thus $\alpha < \dfrac{\varphi(D)}{4}$.

Case 2: $\chi(2) = 1$. In this case,

$$L(2,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^2} \geq 1 - \sum_{n=2}^{\infty} \frac{1}{n^2} = 2 - \frac{\pi^2}{6} > \frac{1}{3}.$$

Hence

$$\frac{8D\sqrt{D}}{\pi^2}(1 - \frac{\chi(2)}{4})L(2,\chi) - (1-\mu(D))\varphi(D) > \frac{8D\sqrt{D}}{\pi^2} \cdot \frac{5}{4} \cdot \frac{1}{3} - 2D > 0.$$

Thus $\alpha < \dfrac{\varphi(D)}{4}$. □

In the particular case when D is a prime of the form $4k+1$, Corollary 5.4 shows that the α-bound discussed in [8] is better than the $\dfrac{p-1}{4}$-bound.

Remark 5.5. It is interesting to see whether the α-bound provides the optimal value for $h(P_\Delta)$; namely $h(P_\Delta) = \alpha$. This is true in the case P_Δ is a cycle graph (by Corollary 2.5, this happens if $\Delta \in \{5, 8, 12\}$). The reason is that in this case $\alpha = \dfrac{4}{D}$ if $D \in \{8, 12\}$ and $\alpha = \dfrac{4}{D-1}$ if $D = 5$ which is precisely the Cheeger number of P_Δ (by the result in [17], it is known that for a cycle graph of order n its Cheeger number is $\dfrac{4}{n}$ if n is even and $\dfrac{4}{n-1}$ if n is odd.)

ACKNOWLEDGEMENTS

The third named author is very grateful to Professor Moshe Rosenfeld who kindled his interest in using number theory to attack problems in graph theory and combinatorics. In particular, he learned several critical techniques in this article from Professor Rosenfeld during the Research Experience for Undergraduates Program at Vietnam National University in 2012 (see [26]).

REFERENCES

[1] R. Ayoub. *An introduction to the analytic theory of numbers*. Mathematical Surveys. American Mathematical Society, Providence, R.I., 1963.

[2] J. Baum. A number-theoretic sum. *Mathematics Magazine*, 55(2):111–113, 1982.

[3] B. C. Berndt. Classical theorems on quadratic residues. *Enseign. Math.(2)*, 22(3–4):261–304, 1976.

[4] M. Budden, N. Calkins, W. Hack, J. Lambert, and K. Thompson. Dirichlet character difference graphs. *Acta Mathematica Universitatis Comenianae*, 82(1):21–28, 2017.

[5] L. Carlitz. A theorem on permutations in a finite field. *Proceedings of the American Mathematical Society*, 11(3):456–459, 1960.

[6] P. Cayley. Desiderata and suggestions: No. 2. the theory of groups: graphical representation. *American Journal of Mathematics*, 1(2):174–176, 1878.

[7] S. K. Chebolu, J. L. Merzel, J. Mináč, L. Muller, T. T. Nguyen, F. W. Pasini, and N. D. Tân. On the joins of group rings. *arXiv preprint arXiv:2208.07413*, 2022.

[8] K. Cramer, M. Krebs, N. Shabazi, A. Shaheen, and E. Voskanian. The isoperimetric and kazhdan constants associated to a paley graph. *Involve, a Journal of Mathematics*, 9(2):293–306, 2016.

[9] P. J. Davis. *Circulant matrices*. American Mathematical Soc., 2013.

[10] J. Doan, J. Minac, L. Muller, T. T. Nguyen, and F. W. Pasini. Joins of circulant matrices. *arXiv preprint arXiv:2111.10059*, 2021.

[11] J. Doan, J. Mináč, L. Muller, T. T. Nguyen, and F. W. Pasini. On the spectrum of the joins of normal matrices and applications. *arXiv preprint arXiv:2207.04181*, 2022.

[12] D. Ghinelli and J. D. Key. Codes from incidence matrices and line graphs of paley graphs. *Advances in Mathematics of Communications*, 5(1):93, 2011.

[13] J. Javelle. *Cryptographie Quantique: Protocoles et Graphes*. PhD thesis, Université de Grenoble, 2014.

[14] M. Jerrum, A. Sinclair, and E. Vigoda. A polynomial-time approximation algorithm for the permanent of a matrix with nonnegative entries. *Journal of the ACM (JACM)*, 51(4):671–697, 2004.

[15] G. A. Jones, I. Ponomarenko, and J. Širáň. *Isomorphisms, Symmetry and Computations in Algebraic Graph Theory: Pilsen, Czech Republic, October 3–7, 2016*, volume 305. Springer Nature, 2020.

[16] R. Kannan, S. Vempala, and A. Vetta. On clusterings: Good, bad and spectral. *Journal of the ACM (JACM)*, 51(3):497–515, 2004.

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

[18] W. J. LeVeque. *Topics in number theory. Vol. I, II.* Dover Publications, Inc., Mineola, NY, 2002.

[19] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.

[20] J. Mináč, T. T. Nguyen, and N. D. Tân. Fekete polynomials, quadratic residues, and arithmetic. *Journal of Number Theory*, 2022.

[21] J. Mináč, T. T. Nguyen, and N. D. Tân. On the arithmetic of generalized fekete polynomials. *arXiv preprint arXiv:2206.11778*, 2022.

[22] H. L. Montgomery and R. C. Vaughan. *Multiplicative number theory I: Classical theory*. Cambridge Studies in Advanced Mathematics, 97. Cambridge University Press, Cambridge, 2007.

[23] M. R. Murty. Ramanujan graphs. *Journal of the Ramanujan Math. Society*, 18(1):1–20, 2003.

[24] I. Niven, H. S. Zuckerman, and H. L. Montgomery. *An introduction to the theory of numbers*. John Wiley & Sons, 1991.

[25] R. E. Paley. On orthogonal matrices. *Journal of Mathematics and Physics*, 12(1-4):311–320, 1933.

[26] M. Rosenfeld, N. Le, N. T. Tran, D. Tran, X. Vu, H. Do, T. Hoang, and T. Nguyen. Research Experiences for Undergraduates, Vietnam National University. `https://doi.org/10.13140/RG.2.2.29575.88480`, 2012.

[27] A. Sinclair and M. Jerrum. Approximate counting, uniform generation and rapidly mixing markov chains. *Information and Computation*, 82(1):93–133, 1989.

[28] D. A. Spielman and S.-H. Teng. Spectral partitioning works: Planar graphs and finite element meshes. In *Proceedings of 37th conference on foundations of computer science*, pages 96–105. IEEE, 1996.

DEPARTMENT OF MATHEMATICS, WESTERN UNIVERSITY, LONDON, ONTARIO, CANADA N6A 5B7
Email address: minac@uwo.ca

DEPARTMENT OF MATHEMATICS, WESTERN UNIVERSITY, LONDON, ONTARIO, CANADA N6A 5B7
Email address: lmuller2@uwo.ca

DEPARTMENT OF MATHEMATICS, WESTERN UNIVERSITY, LONDON, ONTARIO, CANADA N6A 5B7
Email address: tungnt@uchicago.edu

SCHOOL OF APPLIED MATHEMATICS AND INFORMATICS, HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY, 1 DAI CO VIET ROAD, HANOI, VIETNAM
Email address: tan.nguyenduy@hust.edu.vn