On the Paley graph of a quadratic character

Tung T. Nguyen

Western University

Korea-Taiwan-Vietnam joint seminar in Combinatorics and Analysis, 11/2022.

Plans of the talk.

- Classical Paley graphs.
- Quadratic characters and their Paley graphs.
- Spectra of generalized Paley graphs.
- Cheeger number of Paley graphs.

This talk is a report on joint work with Lyle Muller, Jan Mináč, and Nguyen Duy Tan. This is a natural continuation of our previous work on Fekete polynomials.

A motivational quote

The mathematician Gareth A. Jones once said the following.

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

Classical Paley graphs

Let p be a prime number. The Paley graph G_p associated with p is constructed as follow.

- The vertex set of G_p is $\mathbb{F}_p$.
- There is an edge from u to v iff

$$(u - v) \in (\mathbb{F}_p^\times)^2.$$

  Note that $(\mathbb{F}_p^\times)^2$ is the set of all quadratic residues in $\mathbb{F}_p$.
- By definition G_p is an undirected graph iff $p \equiv 1 \pmod 4$.
- We can see that P_p is exactly the Cayley graph $\Gamma(\mathbb{F}_q, S)$ where $S = (\mathbb{F}_p^\times)^2$.

Paley graph for $p = 13$

Let us consider $p = 13$. We have

$$(\mathbb{F}_{13}^{\times})^2 = \{1^2, 2^2, 3^2, 4^2, \ldots, 12^2\} = \{1, 3, 4, 9, 10, 12\}.$$

The vertices of P_{13} are $V(P_{13}) = \{0, 1, 2, \ldots, 12\}$. We observe that

- $(0, 1) \in E(P_{13})$ because

  $$1 - 0 = 1^2 \in (\mathbb{F}_{13})^{\times},$$

  and

  $$0 - 1 = 8^2 \in (\mathbb{F}_{13})^{\times}.$$

- $(0, 2) \notin E(P_5)$ because $2 - 0 = 2 \notin (\mathbb{F}_{13}^{\times})^2$.

Paley graph for $p = 13$

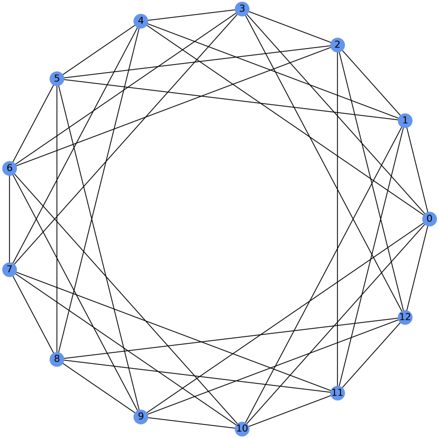

Figure: The Paley graph P_{13}

Paley graphs revisited

Let a be an integer and p a prime number. The Legendre symbol $\left(\frac{a}{p}\right)$ is defined as follows.

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

Let $\chi_p := \left(\frac{\cdot}{p}\right)$ denote the Legendre symbol. Then χ_p is a Dirichlet character of conductor p. Namely, $\chi_p : \mathbb{Z}/p \to \mathbb{C}$ such that

$$\chi_p(ab) = \chi_p(a)\chi_p(b).$$

With this convention, we see that $(u, v) \in E(G_p)$ iff $\chi_p(u - v) = 1$.

Dirichlet characters

Definition 1

A Dirichlet character of modulus n is a function $\chi : \mathbb{Z} \to \mathbb{C}$ such that for all integers $a, b \in \mathbb{Z}$

1. $\chi(ab) = \chi(a)\chi(b)$.
2. $$\chi(a) = \begin{cases} = 0 & \text{if} \quad \gcd(a, n) > 1 \\ \neq 0 & \text{if} \quad \gcd(a, n) = 1. \end{cases}$$
3. $\chi(a + n) = \chi(a)$.

We way that χ is even (respectively odd) if $\chi(-1) = 1$ (respectively $\chi(-1) = -1$).

Alternatively, we can view χ as a multiplicative function $\chi : (\mathbb{Z}/n)^{\times} \to \mathbb{C}^{\times}$. We say that χ is primitive if it does not factor through $(\mathbb{Z}/m)^{\times}$ for some $m|n$. In this case, we say that the conductor of χ is n.

Dirichlet characters

Example

- $\chi = \chi_p$ as explained in the previous part. It is a primitive character with conductor p.
- χ_n is the trivial character. Namely

$$\chi_n(a) = \begin{cases} 0 & \text{if} \quad \gcd(a, n) > 1 \\ 1 & \text{if} \quad \gcd(a, n) = 1. \end{cases}$$

This is not a primitive character.

The Paley graph of a Dirichlet character

Let $\chi : \mathbb{Z} \to \mathbb{C}$ be a Dirichlet character with modulus n.

Definition 2 (Budden et al.)

The Paley graph P_χ is the graph with the following data

1. The vertices of P_χ are $\{0, 1, \ldots, n-1\}$.
2. For two vertices u, v, $(u, v) \in E(P_\chi)$ iff $\chi(u - v) = 1$.

We remark that P_χ is an undirected graph iff $\chi(-1) = 1$ (in other words, χ is an even character.)

Works in the literature

1. When $\chi = \chi_p = \left(\frac{\cdot}{p}\right)$, $P_\chi = P_p$.
2. When $\chi = \chi_n$ the trivial character, the graph P_χ has the following simple description.
    - The vertices of P_χ are $\{0, 1, \ldots, n-1\}$.
    - Two vertices u, v are connected iff $\gcd(u - v, n) = 1$.

   In the literature, this is called a unitary Caley graph (see for example works of Walter, Torsten and others).
3. We will focus on the case of quadratic characters in this talk.

Kronecker symbol

The Kronecker symbol is a generalization of the Legendre symbol. Let a, n be integers. We define

- $\left(\frac{a}{-1}\right) = \begin{cases} 1 & \text{if } a \geq 0 \\ -1 & \text{if } a < 0, \end{cases}$
- $\left(\frac{a}{2}\right) = \begin{cases} 0 & \text{if } 2 | a \\ 1 & \text{if } a \equiv \pm 1 \pmod 8 \\ -1 & \text{if } a \equiv \pm 3 \pmod 8), \end{cases}$
- Suppose that n has the following factorization into product of distinct prime numbers
$$n = \operatorname{sgn}(n) p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}.$$
Here $\operatorname{sgn}(n)$ is the sign of n. Then we define
$$\left(\frac{a}{n}\right) = \left(\frac{a}{\operatorname{sgn(n)}}\right) \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \dots \left(\frac{a}{p_r}\right)^{e_r}.$$

Quadratic characters

- d a squarefree integer, Δ the discriminant of the quadratic extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, which is given by

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

- 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. Then χ_Δ is a primitive quadratic character of conductor $D = |\Delta|$.

- When $\Delta = p$ with $p \equiv 1 \pmod 4$, by the quadratic reciprocity law, we have

$$\left(\frac{\Delta}{a}\right) = \left(\frac{a}{p}\right) = \chi_p(a).$$

Paley graph of a quadratic character

Let $\chi = \chi_\Delta$ be the quadratic character of conductor $D = |\Delta|$ as explained in the previous section. Since χ is determined uniquely by Δ, we will write $P_\Delta := P_{\chi_\Delta}$.

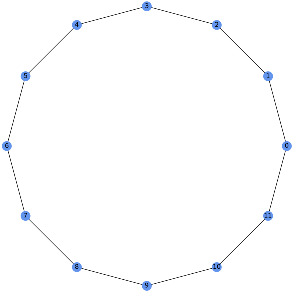

Figure: The Paley graph P_{12}

Graph spectra

Let G be a graph with vertex set $\{v_1, v_2, \dots, v_n\}$. The adjacency matrix A of G is defined as follow

$$A_{ij} = \begin{cases} 1 & \text{if } (v_i, v_j) \in E(G) \\ 0 & \text{else.} \end{cases}$$

Definition 3

The spectrum of G is the set of all eigenvalues of A. Equivalently, it is the set of all roots of the characteristic polynomial

$$p_A(t) = \det(tI - A).$$

Graph spectra

Definition 4

We say that a graph G is circulant if its adjacency matrix has the follow form

$$A = \begin{bmatrix} c_0 & c_1 & \cdots & c_{n-2} & c_{n-1} \\ c_{n-1} & c_0 & c_1 & & c_{n-2} \\ \vdots & c_{n-1} & c_0 & \ddots & \vdots \\ c_2 & & \ddots & \ddots & c_1 \\ c_1 & c_2 & \cdots & c_{n-1} & c_0 \end{bmatrix}.$$

In other words, the entry A_{ij} of A only depends on $(j-i)$ modulo n.

Note that A is determined by the first row vector

$$\vec{c} = [c_0, c_1, \ldots, c_{n-1}].$$

We will write

$$A = \mathrm{circ}(\vec{c}).$$

The Circulant Diagonalization Theorem

Let us take a concrete example of a circulant matrix of size 3×3.

$$A = \begin{pmatrix} c_0 & c_1 & c_2 \\ c_2 & c_0 & c_1 \\ c_1 & c_2 & c_0 \end{pmatrix}.$$

Let ω_3 be a 3rd root of unity (so $\omega_3 \in \{1, e^{\frac{2\pi i}{3}}, e^{\frac{4\pi i}{3}}\}$). Then we have

$$A \begin{pmatrix} 1 \\ \omega_3 \\ \omega_3^2 \end{pmatrix} = \begin{pmatrix} c_0 + c_1\omega_3 + c_2\omega_3^2 \\ c_2 + c_0\omega_3 + c_1\omega_3^2 \\ c_1 + c_2\omega_3 + c_0\omega_3^2 \end{pmatrix} = \begin{pmatrix} (c_0 + c_1\omega_3 + c_2\omega_3^2)1 \\ (c_0 + c_1\omega_3 + c_2\omega_3^2)\omega_3 \\ (c_0 + c_1\omega_3 + c_2\omega_3^2)\omega_3^2 \end{pmatrix}.$$

We see that $(1, \omega_3, \omega_3^2)^T$ is an eigenvector of A associated with the eigenvalue $c_0 + c_1\omega_3 + c_2\omega_3^2$.

Theorem [The Circulant Diagonalization Theorem]

Let

$$A = \begin{bmatrix} c_0 & c_1 & \cdots & c_{n-2} & c_{n-1} \\ c_{n-1} & c_0 & c_1 & & c_{n-2} \\ \vdots & c_{n-1} & c_0 & \ddots & \vdots \\ c_2 & & \ddots & \ddots & c_1 \\ c_1 & c_2 & \cdots & c_{n-1} & c_0 \end{bmatrix}.$$

be the circulant matrix formed by the vector $(c_0, c_1, \ldots, c_{n-1})$. Let $\omega_n = e^{\frac{2\pi i}{n}}$ and

$$v_{n,j} = \left(1, \omega_n^j, \omega_n^{2j}, \ldots, \omega_n^{(n-1)j}\right)^T, \quad j = 0, 1, \ldots, n-1.$$

Then $v_{n,j}$ is an eigenvector of A associated with the eigenvalue

$$\lambda_j^C = c_0 + c_1\omega_n^j + c_2\omega_n^{2j} + \cdots + c_{n-1}\omega_n^{(n-1)j}$$

Graph theoretic properties of generalized Paley graphs

Let $\chi = \chi_\Delta$ be a quadratic character of conductor $D = \Delta$. The Paley graph P_Δ has the following data

1. The vertices of P_χ are $\{0, 1, \ldots, D-1\}$.
2. For two vertices u, v, $(u, v) \in E(P_\chi)$ iff $\chi(u - v) = 1$.

Let A be the adjacency matrix of P_Δ.

Proposition

A is a circulant matrix. In fact $A = \text{circ}(\vec{c})$ where

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

This follows from the fact that

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

Graph theoretic properties of generalized Paley graphs

Proposition

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

We have

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

Corollary

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

Spectra of generalized Paley graphs

By the Circulant Diagonalization Theorem, 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-th roots of unity. To compute this number, we will calculate each of the following terms separately

$$\sum_{a=0}^{D-1} \chi(a)^2 \omega^a, \quad \sum_{a=0}^{D-1} \chi(a)\omega^a.$$

The first sum is easy to compute. Its determination follows from the following fact

Proposition

Let d be a positive integer. Let ω be a primitive d-th root of unity. Then

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

Quadratic Gauss sums

To compute the second sum, we recall the theory of Gauss sums.

Definition

The Gauss sum $G(b, \chi)$ is defined as follow

$$G(b, \chi) = \sum_{a=0}^{D-1} \chi(a)\zeta_D^{ab}.$$

Theorem [Gauss]

The Gauss sums have the following properties.

1. $G(b, \chi) = \chi(b)G(1, \chi)$.
2. $G(1, \chi) = \sqrt{\Delta}$.
3. $G(b, \chi) = \chi(b)\sqrt{\Delta}$.

Quadratic Gauss sums

Corollary

Let ω be a D-th root of unity.

- If ω is not a primitive D-th root of unity, then

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

- If ω is a primitive D-th root of unity, namely $\omega = \zeta_D^b$ with $\gcd(b, D) = 1$ then

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

Spectra of generalized Paley graphs

Theorem [Minac, Muller, Tân, Ng.]

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

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

Cheeger number of generalized Paley graphs

Definition

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 an important invariance of a graph. However, it is notoriously hard to compute. It is only known for a few classes of graphs.

Fact

The Cheeger number of the cycle graph C_n is $\dfrac{4}{n}$ if n is even and $\dfrac{4}{n-1}$ if n is odd.

Cheeger number of generalized Paley graphs

By definition for all $F \subset V$ such that $0 < |F| \leq \frac{1}{2}|V(G)|$

$$h(G) \leq \frac{|\partial F|}{|F|}.$$

To find an effective lower bound for $h(G)$, we need to find a “good” F.

Proposition [Cramer, Krebs, Shabazi, Shaheen, Voskanian]

Let $p \equiv 1 \pmod 4$ and P_p be the classical Paley graph. Let $F = \{0, 1, 2, \ldots, \frac{p-3}{2}\}$. Then

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

where $k = \frac{p-1}{4}$ and $\alpha_1, \alpha_2, \ldots, \alpha_k$ are the quadratic residues modulo p in the interval $[0, \frac{p-1}{2}]$. Consequently, $h(P_p)$ is bounded by

$$h(P_p) \leq \frac{1}{k} \sum_{i=1}^{k} \alpha_i.$$

This is called the α-bound.

Using a different set F (the set of the nonsquares in $\mathbb{F}_p$), Cramer, Krebs, Shabazi, Shaheen, Voskanian also show that

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

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

Figure: Comparison of the two bounds

Question

Is the α-bound sharper than the $\frac{p-1}{4}$-bound?

The answer is YES. In fact, we can generalize this bound to P_Δ (where χ_Δ is even). Let $k = \frac{\varphi(D)}{4}$ and $\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ the set of all elements on the interval $[1, \ldots, \lfloor \frac{D}{2} \rfloor]$ such that $\chi(\alpha_i) = 1$.

Proposition

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

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

Consequently

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

In order to estimate the α-bound, we use special values of the L-function associated with χ

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

This L-function has an Euler product formula

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

This Euler product formula shows that $L(\chi, s) > 0$ if $s \in \mathbb{R}$ and $s > 1$.

For simplicity, we will assume that D is even. We have

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

We also have

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

and

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

Consequently, the α-bound is given by

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

The case D is odd is similar. In all cases, we have

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

Question

Is it true that $h(P_\Delta) = \alpha$?

The answer is YES if P_Δ is a cycle graph (equivalently, $\Delta \in \{5, 8, 12\}$.)

Thank you and Happy Thanksgiving!

Figure: Photo credit: Unsplash