SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Spectral Graph Theory: Paley and Ramanujan Graphs

av

Emil Bertlin

2026 - No K31

Spectral Graph Theory: Paley and Ramanujan Graphs

Emil Bertlin

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Olof Sisask

2026

Abstract

A fundamental question in spectral graph theory asks how the eigenvalues of a graph reflect its combinatorial properties. Ramanujan graphs are regular graphs whose nontrivial eigenvalues are as small as possible, a spectral condition that makes them well connected but sparse. The Alon–Boppana bound shows that, asymptotically, this property is the best one can hope for among bounded-degree graphs.

This thesis approaches Ramanujan graphs from two complementary perspectives. The first studies Paley graphs, an explicit family whose construction draws on finite fields and number theory. Using Cayley graphs, character theory, and the quadratic Gauss sum, we establish their spectrum. Following this, a proof that the Paley graphs satisfy the Ramanujan bound is provided. The second perspective studies the existence of Ramanujan graphs through a nonconstructive proof by Marcus, Spielman, and Srivastava, which establishes the existence of an infinite family of d-regular bipartite Ramanujan graphs for every integer $d > 2$. Between these viewpoints, expander graphs are explored through Cheeger's inequality and the Alon–Boppana bound in order to place the Ramanujan property in its natural setting of expander families.

The exposition develops the necessary background alongside the main theorems and supplies proofs of many results that the original literature leaves to references.

Sammanfattning

En grundläggande fråga inom spektral grafteori är hur egenvärdena hos en graf återspeglar dess kombinatoriska egenskaper. Ramanujangrafer är reguljära grafer vars icke-triviala egenvärden är så små som möjligt, ett spektralt villkor som innebär att de har mycket goda konnektivitetsegenskaper trots att de är glesa. Alon–Boppanas sats visar att denna egenskap asymptotiskt är den bästa man kan hoppas uppnå bland grafer med begränsad maximal grad.

Denna uppsats behandlar Ramanujangrafer ur två kompletterande perspektiv. Det första studerar Paleygrafer, en explicit graffamilj vars konstruktion bygger på ändliga kroppar och talteori. Med hjälp av Cayleygrafer, karaktärteori och den kvadratiska Gaussumman hittar vi deras spektrum. Därefter visas att Paleygrafer är Ramanujangrafer. Det andra perspektivet behandlar existensen av Ramanujangrafer genom ett icke-konstruktivt bevis av Marcus, Spielman och Srivastava, som etablerar existensen av en oändlig familj av d-reguljära bipartita Ramanujangrafer för varje heltal $d > 2$. Mellan dessa två perspektiv studeras expandergrafer med hjälp av Cheegers olikhet och Alon–Boppanas sats för att placera Ramanujanegenskapen i sitt naturliga sammanhang, nämligen teorin om expanderfamiljer.

Framställningen utvecklar den nödvändiga bakgrunden parallellt med de centrala satserna och innehåller bevis för många resultat som i den ursprungliga litteraturen lämnas åt hänvisningar till andra källor.

Contents

1. Introduction

1.1 Motivation

Searching for sparse graphs with strong connectivity properties has driven much of the development of spectral graph theory, which this thesis tries to elucidate. Among bounded-degree regular graphs, the Alon–Boppana theorem shows that one cannot hope to make all nontrivial adjacency eigenvalues arbitrarily small. Ramanujan graphs asymptotically attain this bound, making them spectrally optimal among bounded-degree expander families.

This thesis studies Ramanujan graphs from two rather different directions. The first is through characterization of an explicit, Paley graphs, whose spectrum is determined exactly using methods from finite field theory and character theory. The second regards the problem of whether spectrally optimal bounded-degree expanders exist in every degree.

The thesis wraps up with a theorem by Marcus, Spielman, and Srivastava, a landmark result in the theory of Ramanujan graphs. Besides settling the existence problem for bipartite Ramanujan graphs in every degree (greater than 2), the proof shines light on an interesting interplay between graph theory, linear algebra, and the theory of real-rooted polynomials.

1.2 Preliminary Graph Theory

Basic concepts from graph theory are briefly introduced in order to establish a notational standard for the rest of the thesis.

A *graph* $G = (V, E)$ consists of a *vertex set* $V = V(G)$ and an *edge set* $E = E(G) \subseteq \{\{u, v\} \mid u, v \in V, u \neq v\}$. If $\{u, v\} \in E$ we call u and v *adjacent*, denoted $u \sim v$, and in this case we also say that v is a *neighbor* of u (and vice versa as being adjacent is a symmetric relation). The set of neighbors of a vertex $v \in V$ is denoted $N(v) = \{u \in V \mid \{u, v\} \in E\}$. The *degree* of $v \in V$ is its number of neighbors $\deg v = |N(v)|$. If the degree of each vertex in a graph G is equal to some fixed number d, we say that G is *d-regular*.

Two graphs G and G' are *isomorphic*, denoted $G \cong G'$, if there is a bijective map $\varphi : V(G) \to V(G')$ such that $u \sim v$ in G if and only if $\varphi(u) \sim \varphi(v)$ in G'.

A graph G is said to be *bipartite* if its vertex set can be partitioned by two nonempty disjoint sets $V_1, V_2 \subseteq V(G)$ such that no two vertices in the same set are adjacent. Equivalently, a bipartite graph is 2-colorable.

If $G = (V, E)$ and $G' = (V', E')$ are graphs where $V \cap V' = \emptyset$, then the *union graph* is $G \cup G' = (V \cup V', E \cup E')$.

Remark 1.2.1. Throughout this text, whenever the word "graph" is used, we implicitly assume it has finitely many vertices.

2. The Basics of Spectral Graph Theory

Spectral graph theory studies graphs through algebraic properties of associated matrices. Several matrices can be associated with a graph. The most fundamental is the adjacency matrix, which will take center stage in this thesis. While our focus will remain almost entirely mathematical, we note briefly that spectral graph theory is an important subject for applications as well; it has roots in quantum chemistry and its applications in computer science are numerous.

This section will be brief, as we introduce Paley graphs early and develop the pertinent theory around this motivating example. General references for this section are Godsil and Royle's *Algebraic Graph Theory* [GR01], and Fan Chung's *Spectral Graph Theory* [Chu97].

2.1 Spectra of Graphs

Definition 2.1.1 (Adjacency Matrix)**.** Let $G = (V, E)$ be a graph on n vertices. We define the *adjacency matrix* of G, denoted $A = A_G$, as the square matrix index by the vertex set V such that

$$A_{u,v} = \begin{cases} 1 & \text{if } u \sim v \\ 0 & \text{otherwise.} \end{cases}$$

On occasion we will assume an ordering of the vertex set for convenience. For instance if $|V| = n$, we might write $V = \{1, 2, \ldots, n\}$.

The adjacency matrix is a completely faithful representation of a graph, meaning that the adjacency matrix uniquely determines the graph. Likewise, two isomorphic graphs have the same adjacency matrix up to the ordering of their vertex sets.

Adjacency in a graph can equivalently be spoken about in a coordinate-free language using linear operators, which will be introduced in speaking about Cayley graphs in the next section.

Another common matrix associated with a graph G is the Laplacian matrix[1] L_G,

[1]N.B., some mathematicians, like Fan Chung in [Chu97], reserve the name "Laplacian matrix" to

most simply defined as $L_G = D - A_G$ where D is the diagonal degree matrix of G (that is, $D_{u,u} = \deg(u)$ and 0 elsewhere). For certain purposes, and in more general settings, there are "better" matrices to look at than the adjacency matrix, but we will primarily concern ourselves with regular graphs and the adjacency matrix is a natural choice in this case.

Recall the Real Spectral Theorem (see for instance Axler's *Linear Algebra Done Right* [Axl24], Section 7B, for a proof).

Theorem 2.1.2. *If M is a real symmetric $n \times n$ matrix, then M has n real eigenvalues, counted with multiplicities, and there is an orthonormal basis consisting of eigenvectors.*

Let G be an graph on n vertices. The $n \times n$ adjacency matrix A_G is real since it contains only zeroes and ones, and it is symmetric since G is undirected. Thus by the Real Spectral Theorem it has n real eigenvalues.

Definition 2.1.3. The multiset of eigenvalues of the adjacency matrix A_G of a graph G is called its *spectrum*.

Remark 2.1.4. Eigenvalues of a graph G is implicitly understood to mean eigenvalues of its adjacency matrix A_G. We will say either. Similarly, the spectrum of G means the spectrum of A_G.

It is common to index the n eigenvalues of a graph G according to their ordering on the real line,

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n.$$

Suppose G is d-regular and λ is one of its eigenvalues with corresponding eigenvector x, that is $A_G x = \lambda x$. Since the Laplacian matrix is $L_G = D - A_G$, it follows that

$$L_G x = (D - A_G)x = (dI - A_G)x = dx - \lambda x = (d - \lambda)x.$$

Hence, $d - \lambda$ is an eigenvalue of L_G with eigenvector x. In other words, there is a bijection from the spectrum of A_G to the spectrum of L_G given by $\lambda \mapsto d - \lambda$.

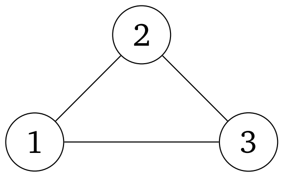
It is important to note that you lose information by looking at the spectrum of a graph. An interesting family of graphs are nonisomorphic *cospectral* graphs, that is graphs which have the same spectrum but are structurally different[2]. Hence, knowing the spectrum does not necessarily mean that you know everything about the graph. A large portion of spectral graph theory concerns the question: What can a graph's spectrum tell us about the combinatorial properties of the graph?

---

refer to a certain normalized version of this matrix.

[2]E.g., the complete bipartite graph $K_{1,4}$ and the disjoint union of the 1-vertex graph with the cycle graph on four vertices $K_1 \cup C_4$ are cospectral but $K_1 \cup C_4$ contains a 4-cycle while $K_{1,4}$ does not. Also note that $K_{1,4}$ is connected but $K_1 \cup C_4$ has two components.

Before we get ahead of ourselves, we will find the spectrum of a very simple graph in order to gain some intuition.



Consider the triangle graph C_3. This has adjacency matrix

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix},$$

which has characteristic polynomial

$$\begin{aligned} p_A(\lambda) = \det(A - \lambda I) = \begin{vmatrix} -\lambda & 1 & 1 \\ 1 & -\lambda & 1 \\ 1 & 1 & -\lambda \end{vmatrix} &= -\lambda \begin{vmatrix} -\lambda & 1 \\ 1 & -\lambda \end{vmatrix} - \begin{vmatrix} 1 & 1 \\ 1 & -\lambda \end{vmatrix} + \begin{vmatrix} 1 & -\lambda \\ 1 & 1 \end{vmatrix} \\ &= -\lambda(\lambda^2 - 1) - (-\lambda - 1) + (1 + \lambda) \\ &= -\lambda^3 + 3\lambda + 2 \\ &= -(\lambda - 2)(\lambda + 1)^2. \end{aligned}$$

Thus, $\lambda = 2$ and $\lambda = -1$ are its eigenvalues. Note that C_3 is 2-regular and $\lambda = 2$ is its largest eigenvalue. This is not a coincidence. We will later prove that the largest eigenvalue in the spectrum of d-regular graph is always d.

A simple but useful theorem has to do with the number of k-length walks between two vertices. A k-length *walk* is a sequence of vertices $v_0, v_1, \ldots v_k$ where v_i is adjacent to v_{i+1} for $0 \leq i \leq k - 1$. If $v_0 = v_k$, the walk is said to be *closed*.

Lemma 2.1.5. *If G is a graph with adjacency matrix A, then $(A^k)_{u,v}$ is the number of k-length walks from u to v.*

Proof. We induct on k. The case $k = 1$ follows immediately since there is a 1-length walk from u to v only if $u \sim v$.

Suppose the claim holds for $k - 1$. Then

$$(A^k)_{u,v} = (A^{k-1}A)_{u,v} = \sum_{w \in V} (A^{k-1})_{u,w} A_{w,v}.$$

For each fixed w, $(A^{k-1})_{u,w}$ is the number of $(k-1)$-length walks from u to w, by assumption, and $A_{w,v}$ is the number of edges (1-length walks) from w to v. Hence

$$(A^{k-1})_{u,w} A_{w,v}$$

counts the number of k-length walks from u to v whose final edge is $\{w, v\}$. Summing over all $w \in V$ counts every such k-length walk exactly once. $\square$

Recall that the *trace* of a square matrix is the sum of its diagonal elements. That is, if M is an $n \times n$ matrix, then its trace is $\mathrm{Tr}(M) = \sum_{j=1}^{n} M_{j,j}$.

Corollary 2.1.6. *Let $G = (V, E)$ be a graph with adjacency matrix A. Then*

$\mathrm{Tr}(A) = 0, \quad \mathrm{Tr}(A^2) = 2|E|, \quad$ *and* $\mathrm{Tr}(A^3) = 6t$ *where t is the number of triangles in G.*

Proof. The number of closed walks of length k is $\mathrm{Tr}(A^k)$ by Lemma 2.1.5. Thus, $\mathrm{Tr}(A) = 0$ is clear. For $\mathrm{Tr}(A^2) = 2|E|$, note every closed walk of length 2 traverses an edge back and forth. An edge $\{u, w\}$ forms two such walks (u, w, u and w, u, w), so $\mathrm{Tr}(A^2) = 2|E|$.

To see $\mathrm{Tr}(A^3) = 6t$, notice that a closed 3-length walk v, w, u, v corresponds to a triangle and each such triangle contributes exactly 6 such walks to the trace as there are

$$\binom{3}{1} \cdot \binom{2}{1} = 6$$

ways to first choose a starting vertex and then pick a direction to walk. $\square$

From linear algebra we know that if $\{\lambda_j\}_{j=1}^{n}$ is the spectrum of a graph G with adjacency matrix A, counted with multiplicity, then

$$\mathrm{Tr}(A^k) = \lambda_1^k + \lambda_2^k + \cdots + \lambda_n^k.$$

Thus, the spectrum uniquely determines the number of vertices, edges, and triangles in a graph.

Next we talk about how large the eigenvalues can be.

Proposition 2.1.7. *Suppose $G = (V, E)$ is a graph. Let $\Delta(G) = \max_{v \in V} \deg(v)$. If λ is an eigenvalue of G then $|\lambda| \leq \Delta(G)$.*

Proof. Without loss of generality, assume $V = \{1, \ldots, n\}$. Suppose A is the adjacency matrix of G with $Av = \lambda v$. Write $v = (x_1, \cdots, x_n)^T$ and let k be such that $|x_k| = \max_{1 \leq i \leq n} |x_i|$. Then, for this fixed k,

$$|\lambda||x_k| = \left| \sum_{j=1}^{n} A_{k,j} x_j \right| \leq |x_k| \sum_{j=1}^{n} A_{k,j} = |x_k| \deg v_k \leq |x_k| \Delta(G).$$

An eigenvector cannot be the zero vector so $|x_k| > 0$. Hence, we may divide by $|x_k|$, which yields the result $|\lambda| \leq \Delta(G)$. $\square$

Corollary 2.1.8. *If G is d-regular, then its eigenvalues λ satisfy $|\lambda| \leq d$.*

Proof. Follows directly from the above proposition. □

Corollary 2.1.9. *If G is a d-regular graph, then $\lambda_1 = d$ is its largest eigenvalue.*

Proof. As G is d-regular, each row of its adjacency matrix A sums to d. Let $\mathbf{1} = (1 \cdots 1)^T$. Then

$$d\mathbf{1} = A\mathbf{1}.$$

So d is an eigenvalue with eigenvector $\mathbf{1}$. By the preceding proposition, it must be the largest one. □

Since each d-regular graph has largest eigenvalue $\lambda_1 = d$, this is often called the *trivial eigenvalue*. You can prove something closely related when G is bipartite. In fact, a graph G is bipartite if and only if its spectrum is symmetric around 0. In particular, if G is d-regular and bipartite then both d and $-d$ are eigenvalues of G. The nontrivial part of the spectrum, then, are eigenvalues λ with $|\lambda| < d$. We will only prove one direction of this, the direction most important for our purposes.

Proposition 2.1.10. *If G is bipartite, then its spectrum is symmetric around 0.*

Proof. Since G is bipartite, the adjacency matrix A_G can be written as a block matrix,

$$A_G = \begin{pmatrix} 0 & B \\ B^T & 0 \end{pmatrix},$$

up to the ordering of its vertices. The above follows directly since G is bipartite, so B represents adjacency between the disjoint vertex sets. Note that B need not be a square matrix[3].

Consider any eigenvalue λ with eigenvector x, $A_G x = \lambda x$. Since

$$A_G x = \begin{pmatrix} 0 & B \\ B^T & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \text{ we write } x = \begin{pmatrix} z \\ y \end{pmatrix},$$

where z and y are column vectors. So $A_G x = \lambda x$ becomes $\lambda \begin{pmatrix} z \\ y \end{pmatrix} = \begin{pmatrix} 0 & B \\ B^T & 0 \end{pmatrix} \begin{pmatrix} z \\ y \end{pmatrix}$. Multiplying yields $By = \lambda z$ and $B^T z = \lambda y$.

[3]For instance, the complete bipartite graph $G = K_{1,3}$ has adjacency matrix $A_G = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$ so here $B = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$.

Now consider a vector $x' = \begin{pmatrix} z \\ -y \end{pmatrix}$. Left-multiplying by A_G yields

$$A_G x' = \begin{pmatrix} 0 & B \\ B^T & 0 \end{pmatrix} \begin{pmatrix} z \\ -y \end{pmatrix} = \begin{pmatrix} -By \\ B^T z \end{pmatrix} = \begin{pmatrix} -\lambda z \\ \lambda y \end{pmatrix} = -\lambda \begin{pmatrix} z \\ -y \end{pmatrix}.$$

This shows that if λ is an eigenvalue with eigenvector $x = \begin{pmatrix} z \\ y \end{pmatrix}$, then $-\lambda$ is also an eigenvalue with corresponding eigenvector $x' = \begin{pmatrix} z \\ -y \end{pmatrix}$. $\square$

This spectrum symmetry will prove to be important in Section 5.

3. Paley Graphs

Paley graphs are graphs on the finite field $\mathbb{F}_q$, where q is any prime power such that $q \equiv 1 \pmod 4$. In a Paley graph $P(q)$, two vertices are adjacent if their difference is a quadratic residue (nonzero square) in $\mathbb{F}_q$. As we will see, this relation is symmetric because -1 is a quadratic residue precisely when $q \equiv 1 \pmod 4$. So $P(q)$ is a well-defined undirected graph. To determine the spectrum of $P(q)$, we will see that they can be constructed as so-called Cayley graphs; this, along with the study of characters on the inner product space $L^2(G)$, will allow us to find the Paley graph's eigenvalues by relating them to the quadratic Gauss sum. The proofs in this section are largely self-contained and are based primarily on basic group theory with a natural introduction to the basics of character theory. We conclude by showing that Paley graphs are Ramanujan graphs.

For the sake of brevity, we will only consider the case when $q \equiv 1 \pmod 4$ is a prime number, but note that Paley graphs $P(q)$ are generally defined when $q = p^n \equiv 1 \pmod 4$ for some prime p and natural number n.

3.1 Properties of Paley Graphs

Recall that integers modulo p form a prime-order field, denoted $\mathbb{F}_p$, where addition and multiplication are both taken mod p. Consequently, $\mathbb{F}_p^*$ forms a group under multiplication where $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$.

Definition 3.1.1 (Quadratic residue)**.** Let

$$Q = \{x^2 \mid x \in \mathbb{F}_p, x \neq 0\} \subseteq \mathbb{F}_p.$$

The elements of Q are called *quadratic residues* of $\mathbb{F}_p$.

Remark 3.1.2. Throughout this section, the term "quadratic residue" will refer to a nonzero quadratic residue. Sometimes, so long as the context is clear, we will omit the word "quadratic". Likewise, the term "non-residue" will refer to a quadratic non-residue.

Definition 3.1.3 (Paley graph)**.** Let $p \equiv 1 \pmod 4$ be a prime. A *Paley graph* $P(p)$ has vertex set $\mathbb{F}_p$ and two vertices $a, b \in \mathbb{F}_p$ are adjacent if $a - b$ is a quadratic residue in $\mathbb{F}_p$.

We need to show that this defines an undirected graph, that is $a - b \in Q$ if and only if $b - a \in Q$, where Q is the set of residues in $\mathbb{F}_p$. Suppose $a - b = x^2 \in Q$ is a residue, then

$$-(a-b) = b - a = -x^2 = (-1)x^2$$

is a residue if and only if -1 is also a residue. That is, if we have $-1 = z^2 \in Q$, then

$$b - a = (-1)x^2 = (zx)^2 \in Q.$$

We show that this is indeed the case.

Proposition 3.1.4. *Let p be an odd prime. Then -1 is a quadratic residue in $\mathbb{F}_p$ if and only if $p \equiv 1 \pmod 4$.*

Remark 3.1.5. For the following proof, we note that the equation $x^2 - 1 = 0$ has at most two roots in any field, those being $x = -1$ or $x = 1$. It cannot have more than two roots (by, for instance, the Factor Theorem). It only has one root if the field has characteristic[1] 2, i.e. when $-1 = 1$. Importantly, $\mathbb{F}_p$ has characteristic greater than 2 whenever $p > 2$.

We will use Lagrange's theorem from group theory, so for completeness we will state it.

Theorem 3.1.6 (Lagrange's Theorem). *If H is a subgroup of a finite group G, then $|G| = [G : H]|H|$, where $[G : H]$ is the* index *of H in G, that is, the number of left cosets of H in G. Importantly, the order of H divides the order of G.*

Proof of Proposition 3.1.4. ($\Longrightarrow$) Assume -1 is a residue, that is, there is some $x \in \mathbb{F}_p^*$ with $x^2 = -1$. Squaring both sides gives $x^4 = 1$, which implies that the order of x is 4. By Lagrange's theorem, the order of an element divides the order of the group. Since $|\mathbb{F}_p^*| = p - 1$, this means 4 divides $(p - 1)$, which is equivalent to $p \equiv 1 \pmod 4$.

($\Longleftarrow$) It is a standard result that $\mathbb{F}_p^*$ is a cyclic group. Consider any generator $\langle a \rangle = \mathbb{F}_p^*$. As the order of a is $|\mathbb{F}_p^*| = p - 1$, we have that $(a^{\frac{p-1}{2}})^2 = a^{p-1} = 1$. Hence, either $a^{\frac{p-1}{2}} = 1$ or $a^{\frac{p-1}{2}} = -1$. Only the latter is possible since $\frac{p-1}{2} < p - 1 = \mathrm{order}(a)$.

By assumption, $p \equiv 1 \pmod 4$, thus for some $n \in \mathbb{Z}$, we have $p = 4n + 1$. Thus,

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

[1] The characteristic of a field F is the smallest positive integer n such that $n \cdot 1_F = 0$, where 1_F is the multiplicative identity in F. If no such n exists, we say that F has characteristic 0. The characteristic of $\mathbb{F}_p$ is p since $p \cdot 1 \equiv 0 \pmod p$.

Since $\mathbb{F}_p^*$ is a multiplicative group, multiplication of elements is closed, and a^n is some element of $\mathbb{F}_p^*$. Therefore, -1 is a quadratic residue in $\mathbb{F}_p$. $\square$

Consequently, the Paley graph $P(p)$ is a well-defined undirected graph whenever p is a prime with $p \equiv 1 \pmod 4$.

To get a clearer understanding of this graph, we want to know something about its number of edges. It is not hard to construct the Paley graph $P(5)$ and notice that it is isomorphic to the cycle graph on 5 vertices C_5. Note that C_5 is 2-regular, and so $P(5)$ is also 2-regular. We will show that all Paley graphs $P(p)$ are d-regular with $d = \frac{p-1}{2}$.

Theorem 3.1.7. *Let p be an odd prime. Then there are $\frac{p-1}{2}$ residues modulo p and as many quadratic non-residues.*

Proof. Let $S : \mathbb{F}_p^* \to \mathbb{F}_p^*$ be the squaring map $S(x) = x^2$. An element a is a quadratic residue if and only if it is in the image of S. For any $b^2 \in \operatorname{Image} S$, the equation $x^2 = b^2$ can be written as

$$(x-b)(x+b) = 0,$$

which has roots $\pm b$. Since p is an odd prime, the characteristic of $\mathbb{F}_p$ is greater than 2, so $b \neq -b$. Thus, every element in the image of S has exactly two preimages. Hence,

$$|\operatorname{Image} S| = \frac{|\mathbb{F}_p^*|}{2} = \frac{p-1}{2}.$$

To show that there are also $\frac{p-1}{2}$ quadratic non-residues, we note that every element in $\mathbb{F}_p^*$ is either a residue or a non-residue. So the set $\mathbb{F}_p^*$ is partitioned by the set of residues and the set of non-residues. Since $|\mathbb{F}_p^*| = p-1$, and there are $\frac{p-1}{2}$ residues, as we just showed, this means that there are

$$p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$$

quadratic non-residues. $\square$

Corollary 3.1.8. *Let $p \equiv 1 \pmod 4$. Then the Paley graph $P(p)$ is d-regular, with $d = \frac{p-1}{2}$.*

Proof. By definition, the neighbor set of x is

$$N(x) = \{y \in \mathbb{F}_p \mid y - x \in Q\},$$

where Q is the set of residues of $\mathbb{F}_p$. Since the map $y \mapsto y - x$ is a bijection[2] on $\mathbb{F}_p$

[2]To be pedantic, we should show that this translation is indeed a bijection. Suppose G is an abelian

onto itself, we have

$$\deg(x) = |N(x)| = |Q| = \frac{p-1}{2},$$

where the last equality follows from Theorem 3.1.7. As x is arbitrary, this shows that $P(p)$ is $\frac{p-1}{2}$-regular. $\square$

The so-called Handshaking Lemma states that if $G = (V, E)$ is a finite undirected graph then $\sum_{v \in V} \deg(v) = 2|E|$. This is intuitive, as every edge is incident to two vertices. By this we can see that the number of edges $|E(P(p))|$ of a Paley graph $P(p)$ is $|E(P(p))| = \frac{1}{2} \sum_{a \in \mathbb{F}_p} \deg(a) = \frac{p(p-1)}{4}$.

We will now show that Paley graphs are self-complementary, that is, they are isomorphic to their complement graph.

Informally, from a graph G we define its complement as a graph with the same vertex set but with its edges complemented.

Definition 3.1.9 (Complement Graph)**.** The *complement* $\overline{G}$ of a graph $G = (V, E)$ is a graph with vertex set V such that two vertices x and y are adjacent only if x and y are not adjacent in G. Put differently, the graph complement $\overline{G}$ of a graph G is defined as $\overline{G} = (V, \overline{E})$ where

$$\overline{E} = \{\{u, v\} \mid \{u, v\} \notin E \text{ where } u, v \in V \text{ and } u \neq v\}.$$

A graph which is isomorphic to its complement is called *self-complementary*.

For instance, the complement of the complete graph on n vertices K_n is the edgeless graph on n vertices.

Proving that Paley graphs are self-complementary will be easier by the introduction of a quadratic character, which will be important throughout this entire section.

Definition 3.1.10 (Quadratic Character)**.** Let $Q \subseteq \mathbb{F}_p^*$ be the set of quadratic residues modulo p. We define the *quadratic character* on elements of $\mathbb{F}_p$ as the map $\eta : \mathbb{F}_p \to \{-1, 0, 1\}$ given by

$$\eta(x) = \begin{cases} -1 & \text{if } x \in \mathbb{F}_p^* \setminus Q, \\ 0 & \text{if } x = 0, \\ 1 & \text{if } x \in Q. \end{cases}$$

Lemma 3.1.11. *The quadratic character on $\mathbb{F}_p$ is multiplicative.*

additive group, which $(\mathbb{F}_p, +)$ is, and define a map $t_g : G \to G$ via $t_g(x) = g + x$, where $g \in G$. Let $t_g^{-1} = t_{-g}$. Then $(t_g^{-1} \circ t_g)(x) = t_g^{-1}(g + x) = -g + g + x = x = g - g + x = (t_g \circ t_g^{-1})(x)$, and well-definedness is trivial. A map with a well-defined inverse is a bijection.

Proof. [3]We want to show $\eta(xy) = \eta(x)\eta(y)$ for all $x, y \in \mathbb{F}_p$. If $x = 0$ or $y = 0$, then $xy = 0$ and so $\eta(xy) = 0 = \eta(x)\eta(y)$. It remains to show that η restricted to $\mathbb{F}_p^*$ is a homomorphism. Let $Q \subseteq \mathbb{F}_p^*$ be the subgroup of quadratic residues[4]. Since $\mathbb{F}_p^*$ is abelian, every subgroup is normal, so the quotient group $\mathbb{F}_p^*/Q$ is well-defined. By Theorem 3.1.7, we have

$$|Q| = \frac{p-1}{2},$$

and so the index is

$$[\mathbb{F}_p^* : Q] = \frac{|\mathbb{F}_p^*|}{|Q|} = 2.$$

In other words, $\mathbb{F}_p^*/Q$ has order 2. As there is only one group of order 2 up to isomorphism, we have $\mathbb{F}_p^*/Q \cong (\{-1, 1\}, \cdot)$.

Therefore, η restricted to $\mathbb{F}_p^*$ is the composition

$$\mathbb{F}_p^* \xrightarrow{\pi} \mathbb{F}_p^*/Q \xrightarrow{\sim} \{-1, 1\},$$

where π is the canonical map $a \mapsto aQ$ and the second map is the isomorphism sending the identity coset Q to 1 and the other coset to -1. Since both maps are homomorphisms, their composition η is a homomorphism. Thus, $\eta(xy) = \eta(x)\eta(y)$ for all $x, y \in \mathbb{F}_p^*$. □

The important part of the above proof is that η restricted to $\mathbb{F}_p^*$ is a group homomorphism, which is used in the proof of the following.

Proposition 3.1.12. *The Paley graph $P(p)$ is self-complementary.*

Proof. Let Q be the set of quadratic residues of $\mathbb{F}_p$ and let N be the set of nonzero non-residues. There is an edge between two vertices $x, y \in \mathbb{F}_p$ in $P(p)$ if $x - y \in Q$, while its complement $\overline{P(p)}$ has an edge if $x - y \in N$.

We want to find a bijection $f : \mathbb{F}_p \to \mathbb{F}_p$ such that if $x \sim y$ in $P(p)$ (i.e. $x - y \in Q$), then $f(x) \sim f(y)$ in $\overline{P(p)}$ (i.e. $f(x) - f(y) \in N$).

[3]For completeness, some group theory definitions and properties are left in this footnote. The definitions of groups, binary operations, and subgroups are omitted. Let G and G' be groups. Recall that a *group homomorphism* is a map $\varphi : G \to G'$ such that $\varphi(gh) = \varphi(g)\varphi(h)$. All group homomorphisms satisfy $\varphi(e_G) = e_{G'}, \varphi(g^n) = \varphi(g)^n$, and $\varphi(g^{-1}) = \varphi(g)^{-1}$. A group is called *abelian* if its binary operation is commutative. If $H \subseteq G$ is a subgroup and $g \in G$, we call the following set the *left coset* of H with g, $gH = \{gh \mid h \in H\}$; the *right coset* Hg is defined mutatis mutandis. The *index* of a subgroup $H \subseteq G$ is the number of distinct left cosets. A subgroup $N \subseteq G$ is said to be *normal* if it is invariant under conjugation, i.e. for all $g \in G$, we have $gNg^{-1} = N$. If N is any normal subgroup of G we define the *quotient group* G/N as the group on the set of left cosets $\{gN \mid g \in G\}$ with the binary operation $gN \cdot hN = (gh)N$.

[4]This is clearly a subgroup because it is nonempty and closed: $x^2y^2 = (xy)^2 \in Q$. For a finite group, this suffices as a subgroup check.

Let $a \in N$ be a fixed non-residue and define the map $f : \mathbb{F}_p \to \mathbb{F}_p$ by $f(x) = ax$. Since $a \neq 0$, f is clearly a bijection.

We have that,

$$f(x) - f(y) \in N \iff a(x - y) \in N.$$

Let η be the quadratic character on $\mathbb{F}_p$. Since $\eta(a(x-y)) = \eta(a)\eta(x-y) = -1 \cdot 1 = -1$ by Lemma 3.1.11, the condition $x - y \in Q$ implies $a(x - y) \in N$. So f maps edges in $P(p)$ to edges in $\overline{P(p)}$. Since $|Q| = |N| = \frac{p-1}{2}$, by Theorem 3.1.7, f defines a graph isomorphism. $\square$

3.2 Paley Graphs Are Cayley Graphs

In order to find the spectrum of Paley graphs, we will first introduce a more general class of graphs called *Cayley graphs*. These are graphs constructed from groups where adjacency is determined by a specific subset of the group. It should be mentioned that Cayley graphs are a foundational and broadly studied class of objects in algebraic graph theory and make up for a lot more theory than what is presented here.

Definition 3.2.1 (Symmetric Subset)**.** Let G be a group. A subset $S \subseteq G$ is called *symmetric* if it is closed under taking inverses. That is, $s \in S$ implies $s^{-1} \in S$.

Definition 3.2.2 (Cayley Graph[5])**.** Let G be a finite group and let $S \subseteq G$ be a symmetric subset which generates G and which does not contain the identity element. The *Cayley graph* of G with respect to the *connection set* S, denoted $\Gamma(G, S)$, is the graph with vertex set G where two vertices $g, h \in G$ are adjacent if $g^{-1}h \in S$.

Paley graphs are Cayley graphs of the additive group $G = \mathbb{F}_p$ with S the quadratic residues modulo p, that is $S = Q = \{x^2 \mid x \in \mathbb{F}_p^*\}$. We want to show that this set of residues generates $\mathbb{F}_p$. We can prove something stronger.

Proposition 3.2.3. *Let p be a prime. Any nonzero element $a \in \mathbb{F}_p$ generates $\mathbb{F}_p$.*

Proof. Let $0 \neq a \in \mathbb{F}_p$ and consider the subgroup generated by a, $\langle a \rangle = \{ka : k \in \mathbb{Z}\}$. By Lagrange's theorem, the order $|\langle a \rangle|$ divides $|\mathbb{F}_p| = p$. Since p is prime, $|\langle a \rangle|$ can be either 1 or p, but the former is not possible since only the identity element has order 1. Hence, $|\langle a \rangle| = |\mathbb{F}_p|$ and so $\langle a \rangle = \mathbb{F}_p$. $\square$

[5]N.B., definitions of Cayley graphs vary a little. Some authors do not require that S generates G, cf. C. Godsil and G. Royle's *Algebraic Graph Theory* [GR01], Chapter 3. However, requiring that S generates G ensures that the graph is connected. By having $e_G \notin S$, we avoid loops.

We see that the Paley graph $P(p)$, where $p \equiv 1 \pmod 4$ is prime, is the Cayley graph of $G = \mathbb{F}_p$ with connection set $S = \{x^2 \mid x \in \mathbb{F}_p^*\}$. By Proposition 3.1.4, -1 is a quadratic residue, so $S = -S$. In other words, S is symmetric. Since S is a subset of $\mathbb{F}_p$, and $0 \notin S$, it contains only generators by Proposition 3.2.3. The edge condition $g^{-1}h \in S$ for $g, h \in G$ written in additive notation, in the setting of the (abelian) group $\mathbb{F}_p$, becomes $(-g)+h = h-g \in S$. This is the exact definition of a Paley graph.

3.3 Basic Character Theory on Abelian Groups: Finding the Spectrum of the Paley Graphs

Definition 3.3.1. Let G be a finite group of order n. The set of complex-valued functions on G, written $L^2(G) = \{f : G \to \mathbb{C}\}$, defines an n-dimensional vector space over $\mathbb{C}$. We define the inner product of $f, g \in L^2(G)$ as

$$\langle f, g\rangle = \sum_{x \in G} f(x)\overline{g(x)}.$$

The *norm* on $L^2(G)$ is $\|f\| = \sqrt{\langle f, f\rangle}$.

A standard calculation—which will be skipped—yields that this indeed defines an inner product space, that is, for each $f, g, h \in L^2(G)$

(i) $\langle f, f\rangle \geq 0$ with equality iff $f(x) = 0$ for every $x \in G$;

(ii) $\langle f, g\rangle = \overline{\langle g, f\rangle}$;

(iii) $\langle f+h, g\rangle = \langle f, g\rangle + \langle h, g\rangle$, and $a \in \mathbb{C}$ implies $\langle af, g\rangle = a\langle f, g\rangle$.

Definition 3.3.2 (Character)**.** Let G be an abelian group. A *character* of G is a group homomorphism $\chi : G \to \mathbb{C}^*$.

Note that $g \mapsto 1$ for every $g \in G$ is a homomorphism $G \to \mathbb{C}^*$. We call this the trivial character of G.

Consider a character χ of G. Because G is finite, any element a has finite order, call it n, so $a^n = e_G$ where e_G is the identity element in G. Applying χ to both sides yields $\chi(a^n) = \chi(a)^n = \chi(e_G) = 1$. Thus, $|\chi(a)|^n = 1$ and so the modulus of $\chi(a)$ satisfy $|\chi(a)| = 1$ for any character χ of G and any $a \in G$.

Proposition 3.3.3. *Let G be a finite abelian group. We have*

(i) if χ is nontrivial, then $\sum_{a \in G} \chi(a) = 0$;

(ii) if χ_1, χ_2 are two distinct characters of G, then $\langle \chi_1, \chi_2\rangle = 0$.

Proof. (i). There is some $g \in G$ such that $\chi(g) \neq 1$. Set $S = \sum_{a \in G} \chi(a)$. Multiplying by $\chi(g)$ yields,

$$\chi(g)S = \sum_{a \in G} \chi(ga).$$

Clearly $g \mapsto ga$ is a permutation of G, so

$$\chi(g)S = S \text{ which implies } (\chi(g) - 1)S = 0.$$

Since $\chi(g) \neq 1$, it follows that $S = 0$.

(ii). Let $\kappa(a) = \chi_1(a)\overline{\chi_2(a)}$. As $\chi_2(a)$ has modulus 1 for all a, we can write $\overline{\chi_2(a)} = \chi_2(a)^{-1} = \chi_2(a^{-1})$, so $\kappa(a) = \chi_1(a)\chi_2(a^{-1})$. We show that κ is itself a homomorphism $G \to \mathbb{C}^*$, i.e. a character,

$$\begin{aligned}
\kappa(ab) &= \chi_1(ab)\chi_2((ab)^{-1}) \\
&= \chi_1(a)\chi_1(b)\chi_2(b^{-1})\chi_2(a^{-1}) \\
&= \chi_1(a)\chi_2(a^{-1}) \cdot \chi_1(b)\chi_2(b^{-1}) \\
&= \kappa(a)\kappa(b).
\end{aligned}$$

Because χ_1 and χ_2 are distinct, κ is a nontrivial character[6] and therefore $\langle \chi_1, \chi_2 \rangle = \sum_a \kappa(a) = 0$ by (i).[7] □

We would like to show that if G is a finite abelian group, then $L^2(G)$ has an orthogonal basis of characters of G. This is true. However, we will not show this for an arbitrary finite abelian group G, only a special case.

If $|G| = n$,

$$\dim L^2(G) = n.$$

This is because a function on G is uniquely determined by its values on the n elements of G. We already showed that the all characters of G are orthogonal (Proposition 3.3.3); from linear algebra we know that a set of orthogonal vectors are linearly independent. This means that it remains to show that all characters of G span $L^2(G)$ or, viz., there are $|G| = n$ characters. In order to do this, we will introduce the dual group.

Definition 3.3.4 (Dual Group[8]). Let G be a finite abelian group. The set $\widehat{G}$ consisting

[6] Suppose for contradiction $\kappa(a) = \chi_1(a)\chi_2(a)^{-1} = 1$ for all a, then $\chi_1(a) = \chi_2(a)$, but χ_1 and χ_2 are assumed to be distinct.

[7] The latter part of this proof can be shortened by first proving that the set of characters forms a group, as shown in Proposition 3.3.5, because then $\chi_1\overline{\chi_2}$ is just another character in the group, and the claim follows immediately from part (i). However, the proof above feels more instructive.

[8] This is based on Steinberg's *Representation Theory on Finite Abelian Groups* [Ste12]. In the settings of representation theory we would say that the characters in this definition are *irreducible*. To clarify

of all characters $\chi : G \to \mathbb{C}^*$ is called the *dual group* of G.

Proposition 3.3.5. *Let G be a finite abelian group. The set $\widehat{G}$ of characters $\chi : G \to \mathbb{C}^*$, with the product*

$$(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g)$$

forms an abelian group.

Proof. Closure:

$$(\chi_1\chi_2)(gh) = \chi_1(gh)\chi_2(gh) = \chi_1(g)\chi_2(g)\chi_1(h)\chi_2(h) = (\chi_1\chi_2)(g)(\chi_1\chi_2)(h).$$

The product is trivially associative and commutative. The identity element is the trivial character $\chi_1(g) = 1$ for all $g \in G$. The inverse of an element is given by $\chi^{-1}(g) = \chi(g)^{-1} = \overline{\chi(g)}$. This inverse map is indeed a character since

$$\chi^{-1}(gh) = \chi(gh)^{-1} = \chi(g)^{-1}\chi(h)^{-1} = \chi^{-1}(g)\chi^{-1}(h).$$

□

It is true that if G is a finite abelian group, then $|G| = |\widehat{G}|$, and therefore there is an orthogonal basis of $L^2(G)$ consisting of the characters of G. However, we will only show this when $G = \mathbb{Z}/n\mathbb{Z}$, which is simpler and enough for our purposes. (For a more general treatment, refer to Steinberg's *Representation Theory of Finite Groups* [Ste12].)

Proposition 3.3.6. [9] *All characters of $\mathbb{Z}/n\mathbb{Z}$ are given by*

$$\chi_a(k) = \omega^{ak},$$

where $a \in \mathbb{Z}/n\mathbb{Z}$ and $\omega = e^{2\pi i/n}$ is an n-th root of unity.

what that means, we will introduce the most basic concepts from representation theory on groups, which is not a primary concern for this thesis, and why it is relegated to this footnote (this is more of an aside, it is not particularly relevant). A representation of a group G is a map from G to the group of invertible matrices over a vector space V, i.e. $\varphi : G \to GL(V)$. The degree of a representation is equal to $\dim(V)$. The action of φ_g on $v \in V$ is often denoted $\varphi_g(v)$. The notion of an *irreducible* representation is similar to that of a simple subgroup in group theory, but what, then, is the analogue of a subgroup? Well, if $\varphi : G \to GL(V)$ is a representation, a *G-invariant subspace* $W \subseteq V$ satisfies $\varphi_g(w) \in W$ for all $g \in G$, and $w \in W$. A representation $\varphi : G \to GL(V)$ where $\dim V > 0$ is called irreducible if the only G-invariant subspaces of V are $\{0\}$ and V. If $\varphi : G \to GL(V)$ is a representation, the *character* $\chi_\varphi : G \to \mathbb{C}$ of φ is defined by $\chi_\varphi(g) = \mathrm{Trace}(\varphi_g)$. If φ is irreducible, we say that the character χ_φ is an irreducible character. Any degree 1 representation $\varphi : G \to \mathbb{C}^*$ is irreducible since $\mathbb{C}$ has no proper nonzero subspaces as a vector space over itself, in fact any 1-dimensional vector space has no nonzero proper subspaces as the only possible dimensions of its subspaces are 0 or 1. Therefore, the characters (with our more limited definition of characters as homomorphisms $G \to \mathbb{C}^*$ where G is abelian) in this definition of dual groups are indeed irreducible.

[9] I found this statement in Marcin Kotowski and Michal Kotowski's *Lectures on Expanders* [KK].

Proof. Let $\chi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*$ be a character. Since 1 generates $\mathbb{Z}/n\mathbb{Z}$, every element can be written as $k \cdot 1$, and thus

$$\chi(k) = \chi(1 + 1 + \cdots + 1) = \chi(1)^k \quad \text{for all } k \in \mathbb{Z}/n\mathbb{Z}.$$

Set $z = \chi(1) \in \mathbb{C}^*$. Since $n \equiv 0 \pmod{n}$,

$$1 = \chi(0) = \chi(n) = z^n$$

so z is an n-th root of unity[10]. Thus every character χ is of the form $\chi(k) = z^k$ for some n-th root of unity z.

Every n-th root of unity can be uniquely written as ω^a where $\omega = e^{2\pi i/n}$ and $a \in \mathbb{Z}/n\mathbb{Z}$. Since the n-th roots of unity are precisely $\{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$, there exists a unique $a \in \mathbb{Z}/n\mathbb{Z}$ with $z = \omega^a$. Hence,

$$\chi(k) = z^k = (\omega^a)^k = \omega^{ak}$$

is a character. If $a \neq b$,

$$\chi_a(1) = \omega^a \neq \omega^b = \chi_b(1),$$

so these characters are distinct. Therefore there are exactly n characters

$$|\widehat{\mathbb{Z}/n\mathbb{Z}}| = n.$$

$\square$

Notice that with the above proof, along with our previous work showing orthogonality of characters, we have shown that $L^2(\mathbb{Z}/n\mathbb{Z})$ has an orthogonal basis of characters $\widehat{\mathbb{Z}/n\mathbb{Z}}$, because $\dim L^2(\mathbb{Z}/n\mathbb{Z}) = n$, and we established that there are exactly n distinct orthogonal characters, which must therefore span $L^2(\mathbb{Z}/n\mathbb{Z})$. Also, the isomorphism $\widehat{\mathbb{Z}/n\mathbb{Z}} \cong \mathbb{Z}/n\mathbb{Z}$ follows immediately.

We may generalize a little by noting that every cyclic group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

Before going onto find the eigenvalues and eigenvectors of Cayley graphs on finite abelian groups, we want to change our perspective on adjacency from a coordinate-based one to a coordinate-free one. That is, from the language of matrices to the language of operators. These are equivalent ways of speaking of the same thing, but when dealing with Cayley graphs and functions in $L^2(G)$, it is more natural to take the operator viewpoint.

[10]Recall that this is the definition of an n-th root of unity, i.e. some complex number z satisfying $z^n = 1$.

A general reference for this material is Terras' *Fourier Analysis on Finite Groups and Applications* [Ter99].

Definition 3.3.7 (Adjacency operator)**.** Given a graph $G = (V, E)$, the adjacency operator A acts on functions $f : V \to \mathbb{C}$ by

$$Af(x) = \sum_{y \in N(x)} f(y).$$

We may motivate this definition as follows. For $G = (V, E)$, a finite graph with adjacency matrix A, we have $A_{x,y} = 1$ whenever $x \sim y$, and $A_{x,y} = 0$ otherwise. Multiplying the adjacency matrix by any function $f : V \to \mathbb{C}$ yields

$$Af(x) = \sum_{y \in G} A_{x,y} f(y)$$

by the definition of matrix multiplication. However, $A_{x,y}$ only contributes to this sum whenever y is a neighbor of x, and then $A_{x,y} = 1$, so this becomes

$$Af(x) = \sum_{y \in N(x)} f(y).$$

Theorem 3.3.8. *Let $\Gamma(G, S)$ be a Cayley graph on a finite abelian group G. If χ is a character, the function $f : G \to \mathbb{C}$ given by $f(a) = \chi(a)$ is an eigenvector of the adjacency operator A_Γ with eigenvalue $\sum_{s \in S} \chi(s)$.*

Proof. By a slight rewording of the definition of Cayley graphs (Definition 3.2.2), $a, b \in G$ are adjacent in $\Gamma(G, S)$ only if there is some $s \in S$ such that $b = as$. The set of neighbors of a is therefore $N(a) = \{as \mid s \in S\}$. In other words, a is connected to each vertex as for every $s \in S$. Thus, using commutativity and the fact that χ is a homomorphism,

$$A_\Gamma f(a) = \sum_{s \in S} f(as) = \sum_{s \in S} \chi(as) = \sum_{s \in S} \chi(a)\chi(s) = \chi(a) \sum_{s \in S} \chi(s) = \left(\sum_{s \in S} \chi(s) \right) f(a).$$

Hence, $f = \chi$ is an eigenvector of A_Γ with eigenvalue $\sum_{s \in S} \chi(s)$. $\square$

By Proposition 3.3.6, any character of $\mathbb{Z}/n\mathbb{Z}$ can be written as $\chi_a(k) = \omega^{ak}$ where $\omega = e^{2\pi i/n}$. If A is the adjacency operator of the Paley graph, viewed as the Cayley graph $\Gamma(\mathbb{F}_p, Q)$, where Q are the residues $\{x^2 \mid x \in \mathbb{F}_p^*\}$, then for any character χ_a we get

$$A\chi_a(x) = \left(\sum_{q \in Q} \chi_a(q) \right) \chi_a(x).$$

It remains to evaluate the eigenvalue $\lambda_a = \sum_{q\in Q} \omega^{aq}$ for every $a \in \mathbb{F}_p$.

If $a = 0$, this is easy, as $\chi_0(q) = \omega^0 = 1$ for all q, so $\lambda_0 = \sum_{q\in Q} \omega^0 = |Q| = \frac{p-1}{2}$, using Theorem 3.1.7.

However, the case when $a \neq 0$ is not as easy.

Definition 3.3.9. Let S be a subset of some set X. We define the indicator function of S as

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

If η is the quadratic character on $\mathbb{F}_p$ (Definition 3.1.10) note that the indicator function of the set of residues $Q \subseteq \mathbb{F}_p$ can be written as

$$1_Q(x) = \frac{\eta(x) + 1}{2}$$

for any $x \neq 0$. Thus, if $a \neq 0$,

$$\begin{aligned} \lambda_a = \sum_{q\in Q} \chi_a(q) &= \sum_{x\in\mathbb{F}_p^*} 1_Q(x)\chi_a(x) \\ &= \frac{1}{2}\left(\sum_{x\in\mathbb{F}_p^*} \eta(x)\chi_a(x) + \sum_{x\in\mathbb{F}_p^*} \chi_a(x)\right). \end{aligned}$$

Earlier, in Proposition 3.3.3, we saw that if χ is a nontrivial character the sum over all elements is 0. The character χ_a is nontrivial since $a \neq 0$.

It follows that $\sum_{x\in\mathbb{F}_p^*} \chi_a(x) = \left(\sum_{x\in\mathbb{F}_p} \chi_a(x)\right) - 1 = -1$.

Thus, for $a \neq 0$,

$$\lambda_a = \frac{1}{2}\left(\sum_{x\in\mathbb{F}_p^*} \eta(x)\chi_a(x) - 1\right). \tag{Paley λ_a}$$

The problem reduces to evaluating

$$\sum_{x\in\mathbb{F}_p^*} \eta(x)\chi_a(x) = \sum_{x\in\mathbb{F}_p} \eta(x)\omega^{ax}.$$

This is called a quadratic Gauss sum (cf. Ireland–Rosen [IR90]).

Theorem 3.3.10. *Let $p \equiv 1 \pmod 4$ be a prime and $\omega = e^{2\pi i/p}$. For any $a \in \mathbb{F}_p^*$,*

$$g_a = \sum_{x\in\mathbb{F}_p} \eta(x)\omega^{ax}$$

is real and satisfies $g_a = \pm\sqrt{p}$.

Proof. We have previously shown that η is multiplicative (Lemma 3.1.11) and that $\eta(-1) = 1$ whenever $p \equiv 1 \pmod 4$ (Proposition 3.1.4), which will be used repeatedly in this proof. Begin by noticing that for $a \in \mathbb{F}_p^*$, substituting $x = a^{-1}k$ gives $g_a = \sum_{k \in \mathbb{F}_p} \eta(a^{-1}k)\omega^k$. Note that $\eta(a)^{-1} = \eta(a)$ for all $a \in \mathbb{F}_p^*$. Since $\eta(a^{-1}k) = \eta(a)^{-1}\eta(k) = \eta(a)\eta(k)$, we have

$$g_a = \sum_{k \in \mathbb{F}_p} \eta(a)\eta(k)\omega^k = \eta(a) \sum_{k \in \mathbb{F}_p} \eta(k)\omega^k = \eta(a)g_1.$$

It follows that $|g_a| = |g_1|$.

It suffices to show that $|g_1|^2 = g_1\overline{g_1} = p$ and that $|g_1|$ is real. Since $\eta(-x) = \eta(x)$ for all x,

$$\overline{g_1} = \sum_{x \in \mathbb{F}_p} \eta(x)\omega^{-x} = \sum_{y \in \mathbb{F}_p} \eta(-y)\omega^y = \sum_{y \in \mathbb{F}_p} \eta(y)\omega^y = g_1.$$

Thus, $g_1 \in \mathbb{R}$, and therefore, $|g_1|^2 = g_1^2$. We expand g_1^2 as a double sum

$$g_1^2 = \sum_{x \in \mathbb{F}_p} \sum_{y \in \mathbb{F}_p} \eta(x)\eta(y)\omega^{x+y} = \sum_{x \in \mathbb{F}_p^*} \sum_{y \in \mathbb{F}_p^*} \eta(x)\eta(y)\omega^{x+y},$$

where the last equality follows from $\eta(0) = 0$.

Write $x = ty$, then

$$g_1^2 = \sum_{t \in \mathbb{F}_p^*} \sum_{y \in \mathbb{F}_p^*} \eta(ty)\eta(y)\omega^{y(t+1)} = \sum_{t \in \mathbb{F}_p^*} \eta(t) \sum_{y \in \mathbb{F}_p^*} \omega^{y(t+1)}, \tag{$\star$}$$

because $\eta(m)^2 = 1$ for any $m \neq 0$.

If $t \equiv -1 \pmod p$, then the inner sum over y is $\sum_{y \in \mathbb{F}_p^*} \omega^0 = \sum_{y \in \mathbb{F}_p^*} 1 = p - 1$. For $t \not\equiv -1 \pmod p$, we get

$$\sum_{y \in \mathbb{F}_p^*} \omega^{y(t+1)} = -1 + \sum_{u \in \mathbb{F}_p} \omega^u = -1 + 0 = -1,$$

using Proposition 3.3.3. Rewriting the sum in ($\star$) with these cases yields

$$g_1^2 = \eta(-1)(p-1) + \sum_{t \in \mathbb{F}_p^* \setminus \{-1\}} \eta(t)(-1) = p - 1 - \sum_{t \in \mathbb{F}_p^* \setminus \{-1\}} \eta(t). \tag{$\star\star$}$$

Since η restricted to $\mathbb{F}_p^*$ is a nontrivial character, from Property 3.3.3 again, it follows that $\sum_{u \in \mathbb{F}_p^*} \eta(u) = 0$. Hence

$$\sum_{t \in \mathbb{F}_p^* \setminus \{-1\}} \eta(t) = 0 - \eta(-1) = -1.$$

Plugging this back into $(\star\star)$ gives

$$|g_a|^2 = g_1^2 = p - 1 - (-1) = p.$$

Thus, $g_a = \pm\sqrt{p}$ because g_a was already shown to be real. $\square$

Corollary 3.3.11. *Let $\Gamma(\mathbb{F}_p, Q)$ be the Paley graph for a prime $p \equiv 1 \pmod 4$. The eigenvalues of the adjacency operator of $\Gamma(\mathbb{F}_p, Q)$ are*

$$\frac{p-1}{2}, \frac{\sqrt{p}-1}{2}, \text{ and } \frac{-\sqrt{p}-1}{2}.$$

Proof. We previously found[11] that for $a \neq 0$,

$$\lambda_a = \frac{1}{2}\left(\sum_{x \in \mathbb{F}_p^*} \eta(x)\chi_a(x) - 1\right)$$

is an eigenvalue of $\Gamma(\mathbb{F}_p, Q)$.

The sum contained in λ_a is equal to the quadratic Gauss Sum g_a, that is,

$$\lambda_a = \frac{g_a - 1}{2}.$$

By the proof of the preceding Theorem, $g_a = \eta(a)g_1$. Since g_1 is real and $g_1^2 = p$, we have $g_1 \in \{\sqrt{p}, -\sqrt{p}\}$. So because $\eta(a) = \pm 1$, the set of nontrivial eigenvalues is exactly $\{\frac{\sqrt{p}-1}{2}, \frac{-\sqrt{p}-1}{2}\}$. (The multiplicity of both nontrivial eigenvalues is $(p-1)/2$ by Proposition 3.1.7.)

On the other hand, if $a = 0$, we already saw that,

$$\lambda_0 = \sum_{q \in Q} \chi_0(x) = \sum_{q \in Q} \omega^0 = |Q| = \frac{p-1}{2}.$$

In other words, λ_0 is the trivial eigenvalue. $\square$

We will show that Paley graphs $\Gamma(\mathbb{F}_p, Q)$ are *Ramanujan graphs,* which means that the magnitude of their nontrivial eigenvalues satisfy a very important bound. This has been the tacit goal of this entire section and we have enough to prove it at this point. Note, however, that we did not determine the sign when evaluating the quadratic Gauss Sum g_a, only that $|g_a| = \sqrt{p}$, and when $p \equiv 1 \pmod 4$, g_a is real. It can be shown that $g_1 = \sqrt{p}$ for $p \equiv 1 \pmod 4$, but this is a substantially harder problem. For determination of the sign, see for instance Waterhouse's one-page paper [Wat70] for a neat linear algebra approach, or Ireland–Rosen [IR90] for

[11] See the equation tagged (Paley λ_a).

a number-theoretic approach. For our purposes, $g_n = \pm\sqrt{p}$ suffices to establish the spectrum of the Paley graphs and, thus, also the Ramanujan property.

3.4 Paley Graphs Are Ramanujan Graphs

Ramanujan graphs are introduced here. At this point, it might seem like an arbitrary definition, but in the next section we will see that Ramanujan graphs, in certain contexts, are a very interesting class of graphs.

Recall that if G is d-regular, any eigenvalue λ of G is called nontrivial if $\lambda \neq d$ (or when G is also bipartite, then an eigenvalue λ is called nontrivial whenever $|\lambda| < d$, since $-d$ is inevitably an eigenvalue due to Proposition 2.1.10).

Definition 3.4.1 (Ramanujan graph[12]). A *Ramanujan graph* is a d-regular graph such that all nontrivial eigenvalues λ satisfy

$$|\lambda| \leq 2\sqrt{d-1}.$$

Proposition 3.4.2. *The Paley graph $\Gamma(\mathbb{F}_p, Q)$ is a Ramanujan graph for any prime $p \equiv 1 \pmod 4$.*

Proof. As $p \equiv 1 \pmod 4), p \geq 5$. Recall that Paley graphs are d-regular with $d = \frac{p-1}{2}$. The nontrivial eigenvalues of $\Gamma(\mathbb{F}_p, Q)$ are $\frac{\pm\sqrt{p}-1}{2}$. As $|\frac{-\sqrt{p}-1}{2}| > |\frac{\sqrt{p}-1}{2}|$, it suffices to show

$$\left|\frac{-\sqrt{p}-1}{2}\right| = \frac{\sqrt{p}+1}{2} \leq 2\sqrt{\frac{p-1}{2} - 1} = \sqrt{2p-6}.$$

This inequality holds for any $p \geq 5$ (this is just a routine check; for completeness, an analytical argument is left in this footnote[13]). Thus, $\Gamma(\mathbb{F}_p, Q)$ is a Ramanujan graph. $\square$

[12]The definition is the same for a d-regular multigraph.

[13]We define a function $f : [5, \infty) \to \mathbb{R}$ by $f(x) = \sqrt{2x-6} - \dfrac{\sqrt{x}+1}{2}$. We will show that f is increasing on $[5, \infty)$ and $f(5) > 0$, which yields the result. Differentiating gives

$$f'(x) = \frac{1}{\sqrt{2x-6}} - \frac{1}{4\sqrt{x}}.$$

It is clear that for any $x \geq 5$,

$$4\sqrt{x} > \sqrt{2x-6},$$

(since squaring gives $16x > 2x - 6$, i.e. $14x + 6 > 0$) so

$$\frac{1}{\sqrt{2x-6}} > \frac{1}{4\sqrt{x}}.$$

Hence, $f'(x) > 0$ for all $x \geq 5$, which means that f is increasing on $[5, \infty)$ and therefore $f(x) \geq f(5)$.

$$\text{for } p \geq 5.$$

Since $f(5) = 2 - \frac{\sqrt{5}+1}{2} = \frac{3-\sqrt{5}}{2} > 0$, it follows that $f(x) > 0$ for every $x \geq 5$. Therefore,

$$\frac{\sqrt{p}+1}{2} \leq \sqrt{2p-6} \quad \text{for } p \geq 5.$$

4. Expander Graphs and the Ramanujan Property

By the end of the last section, we said that d-regular graphs whose nontrivial eigenvalues λ satisfy $|\lambda| \leq 2\sqrt{d-1}$ are called Ramanujan graphs. We also showed that all Paley graphs are Ramanujan graphs. The present section serves to motivate this definition.

The Ramanujan property is an upper bound on the magnitude of nontrivial eigenvalues. As we will see, this is closely related to a lower bound on eigenvalues called the Alon–Boppana bound, which will be proven. This leads to the theory of expander graphs.

Informally, a graph is an *expander* if it has relatively few edges and a high level of connectivity. A graph with few edges relative to its number of vertices is called *sparse*. A graph which is not sparse is called *dense*. Paley graphs are an example of a dense family of graphs.

4.1 Expander Graphs and Cheeger's Inequality

To start, we consider the question, what does it mean for a graph to be well-connected?

A natural place to start is by considering the diameter of a graph.

Recall the definition of a path.

Definition 4.1.1 (Path)**.** A walk which repeats no vertices is called a path.

Definition 4.1.2 (Distance, Diameter)**.** Recall that if G is a graph and $x, y \in V(G)$, the *distance*, $\operatorname{dist} : V(G) \times V(G) \to \mathbb{Z}_{\geq 0} \cup \{+\infty\}$, between x and y is defined as the shortest path between x and y. If there is no path between x and y, we say $\operatorname{dist}(x, y) = +\infty$. If $\operatorname{dist}(x, y) < +\infty$ for every $x, y \in V(G)$, then G is said to be *connected*.

The *diameter* of a graph G is the largest distance between any two of its vertices. In symbols,

$$\operatorname{diam} G = \max_{x,y \in V(G)} \{\operatorname{dist}(x, y)\}.$$

The diameter of a graph G is a measure of the connectivity of G, that is, if the diameter is low, the graph has high connectivity, you can get from one point in the graph to another with a small number of steps. However, this is not all we care about in the setting of expanders. We exemplify a complication with an example.

We disregard the need for sparseness, for the moment, and consider the complete graph K_n. For any distinct $x, y \in V(K_n)$, we have $\operatorname{dist}(x, y) = 1$, by definition. Hence, the diameter of K_n is 1. Now consider another graph formed by taking two copies of K_n in space and joining the two K_n components by a single edge. Call this resulting connected $2n$-vertex graph G. By construction, $\operatorname{diam} G = 3$. However, note that this graph G is very easy to make disconnected: simply remove the one edge connecting the two K_n components. This is related to what is called the *robustness* of the graph.

Informally, robustness is a measure on a graph's resistance to damage. This ease of making a graph disconnected, for instance, can be bad in real-world systems modeled on graph theory, like computer networks. The entire system should ideally still function properly even if parts of the system have failed.

Let $G = (V, E)$ be a graph with subsets of vertices $V_1, V_2 \subseteq V$. We define

$$e_G(V_1, V_2)$$

as the number of edges between V_1 and V_2 in G. That is, the number of edges with one endpoint in V_1 and the other endpoint in V_2.

Definition 4.1.3 (The Cheeger Constant)**.** The *Cheeger constant* $h(G)$ of a graph $G = (V, E)$ is defined as

$$h(G) = \min_{S \subseteq V, 0 < |S| \leq \frac{|V|}{2}} \frac{e_G(S, V \setminus S)}{|S|}.$$

Remark 4.1.4. The Cheeger constant is also called the *edge-expansion ratio* or the *isoperimetric number* of G.

In other words, if $h(G) \geq h$, then for any nonempty subset $S \subseteq V$ with $|S| \leq |V|/2$, there are at least $h|S|$ edges leaving S.

Let $n \geq 2$. In the following theorem, we let $\gamma = \lambda_1 - \lambda_2 = d - \lambda_2$, where the eigenvalues of the d-regular graph G are ordered $\lambda_1 \geq \ldots \geq \lambda_n$. This constant γ is usually called the *spectral gap* of G.

Theorem 4.1.5 (Cheeger's Inequality)**.** *Let G be an n-vertex d-regular graph and let $\gamma = d - \lambda_2$. Then the Cheeger constant $h = h(G)$ satisfies*

$$\gamma/2 \leq h \leq \sqrt{2d\gamma}.$$

We will not prove this inequality here. See [Chu07].

Definition 4.1.6. Let $(G_n)_{n\in\mathbb{Z}_{\geq 1}}$ be a family of graphs $G_n = (V_n, E_n)$. Fix some $d \geq 2$. If each graph G_n is finite, connected, and d-regular, it is called an *expander family* if $|V_n| \to +\infty$ as n tends to infinity and if there also exists $\varepsilon > 0$ such that $h(G_n) \geq \varepsilon$ for every $n \geq 1$.

An equivalent condition of an expander family is that there exists $\delta > 0$ such that the spectral gap $\gamma_n \geq \delta$ for every $n \geq 1$. If $h(G_n) \geq \varepsilon$ for all $n \geq 1$, the Cheeger's Inequality (Theorem 4.1.5) implies that

$$\gamma_n \geq \frac{\varepsilon^2}{2d} > 0$$

for every $n \geq 1$.

Thus, good expanders have large spectral gap—as large as possible. However, this gap cannot be too large by the Alon–Boppana bound, which we will talk about next.

4.2 Lower Bounds On Eigenvalues and the Alon–Boppana Bound

Proposition 4.2.1 ([Chu91] Simple lower bound on eigenvalues). *Let $G = (V, E)$ be an n-vertex graph with eigenvalues $\lambda_1 \geq \ldots \geq \lambda_n$. Write $\lambda = \max\{|\lambda_2|, |\lambda_n|\}$. Then*

$$\lambda \geq \sqrt{\frac{-\lambda_1^2 + 2|E|}{n-1}}.$$

Proof. Let A_G be the adjacency matrix of G. Then

$$\lambda_1^2 + (n-1)\lambda^2 \geq \sum_{i=1}^{n} \lambda_i^2 = \operatorname{Tr} A_G^2 = 2|E|,$$

using Corollary 2.1.6. Solving for λ yields the result. □

With the same setup but with the added assumption that G is d-regular, $2|E| = \sum_{v\in V} \deg v = dn$ by the Handshaking Lemma, so we get

$$\lambda^2 \geq \frac{-\lambda_1^2 + 2|E|}{n-1} = \frac{-d^2 + dn}{n-1} = \frac{d(n-d)}{n-1}$$

or

$$\lambda = \sqrt{\frac{d(n-d)}{n-1}}.$$

We may consider the Paley graph on, say, $\mathbb{F}_{449}$, which is 224-regular and, by 3.3.11, $\lambda = \max\{|\lambda_2|, |\lambda_{449}|\} = \frac{\sqrt{449}+1}{2} \approx 11.0948$, while the above bound gives $\lambda \geq \sqrt{224 \cdot 225/448} \approx 10.6066$. Hence, the bound is nearly tight in this case.

Chung in [Chu91] states that, indeed, this simple bound works well when the regular constant d is quite large, for instance $d > \sqrt{n}$. We will not spend more time on this though. Instead, we will instead shift our attention to a more refined eigenvalue bound. The following theorem is in fact the most important theorem in this section, for our aims, as it motivates the Ramanujan graph definition better than any other.

Theorem 4.2.2 (The Alon–Boppana Bound). *Let $d \geq 3$ be a fixed integer, and let G be an n-vertex d-regular graph. If $\lambda_1 \geq \ldots \geq \lambda_n$ are the eigenvalues of G, then*

$$\lambda_2 \geq 2\sqrt{d-1} - o_n(1)$$

where $o_n(1) \to 0$ as $n \to \infty$.

In our proof of this, an explicit vector will be constructed, which is the approach taken in proof by Nilli [Nil91]. Our proof also draws on the one given by Zhao [Zha23], Section 3.6., which also based on Nilli's original proof.

Proposition 4.2.3. *Let $G = (V, E)$ be a d-regular graph with Laplacian matrix $L = dI - A_G$, where A_G is the adjacency matrix of G. Then $\langle x, Lx \rangle = \sum_{\{u,v\} \in E} (x_u - x_v)^2$.*

Proof. Since $L = dI - A_G$,

$$\langle x, Lx \rangle = x^T L x = d x^T x - x^T A_G x.$$

We compute each term separately. Since G is d-regular,

$$d x^T x = d \sum_{u \in V} x_u^2.$$

Also,

$$x^T A_G x = \sum_{u,v \in V} A_{u,v} x_u x_v.$$

Because $A_{u,v} = 1$ only when $u \sim v$, the sum $\sum_{u,v} A_{u,v} x_u x_v$ contains both the terms $x_u x_v$ and $x_v x_u$ for every edge $\{u, v\} \in E$, so

$$x^T A_G x = 2 \sum_{\{u,v\} \in E} x_u x_v.$$

We now expand the desired right-hand side (in the proposition statement),

$$\sum_{\{u,v\}\in E}(x_u - x_v)^2 = \sum_{\{u,v\}\in E}(x_u^2 + x_v^2 - 2x_u x_v). \tag{$*$}$$

Since each vertex has degree d, x_u^2 appears once for every edge incident to u, that is d times. Hence,

$$\sum_{\{u,v\}\in E}(x_u^2 + x_v^2) = \sum_{u\in V} dx_u^2 = d\sum_{u\in V} x_u^2.$$

Plugging this into $(*)$, gives

$$\sum_{\{u,v\}\in E}(x_u - x_v)^2 = d\sum_{u\in V} x_u^2 - 2\sum_{\{u,v\}\in E} x_u x_v,$$

which is exactly the expression obtained for $\langle x, Lx\rangle$. Thus,

$$\langle x, Lx\rangle = \sum_{\{u,v\}\in E}(x_u - x_v)^2.$$

$\square$

An important lemma is proven beforehand.

Recall the notion of vertex distance in a graph (Definition 4.1.2). We can similarly define the distance between edges. Let $G = (V, E)$. If $\{u, v\}, \{x, y\} \in E$, then the distance between edges $\{u, v\}$ and $\{x, y\}$ is defined as the minimum distance between any of their endpoints, which is $\min\{\mathrm{dist}(u, x), \mathrm{dist}(u, y), \mathrm{dist}(v, x), \mathrm{dist}(v, y)\}$. The distance between a vertex and an edge is defined analogously.

Lemma 4.2.4 (Test Vector). *Let $G = (V, E)$ be a d-regular graph, where $d \geq 2$, with adjacency matrix A. Let $\{s, t\} \in E$, let*

$$V_i = \{v \in V : \mathrm{dist}(v, \{s, t\}) = i\},$$

and let $r \geq 1$. Define $x = (x_v)_{v\in V} \in \mathbb{R}^V$ by

$$x_v = \begin{cases} (d-1)^{-i/2}, & \textit{if } v \in V_i,\ i \leq r, \\ 0, & \textit{otherwise, i.e. if } \mathrm{dist}(v, \{s, t\}) > r. \end{cases}$$

Then

$$\frac{\langle x, Ax\rangle}{\langle x, x\rangle} \geq 2\sqrt{d-1}\left(1 - \frac{1}{r+1}\right).$$

Proof. Let $L = dI - A$ denote the Laplacian of G. Since

$$\langle x, Ax \rangle = d\langle x, x \rangle - \langle x, Lx \rangle,$$

it suffices to estimate $\langle x, Lx \rangle$. We will use the identity $\langle x, Lx \rangle = \sum_{\{u,v\} \in E} (x_u - x_v)^2$ (Proposition 4.2.3).

Since x is constant on each layer V_i, edges contained entirely within one layer contribute nothing. Moreover, if $\{u, v\} \in E$, then

$$|\operatorname{dist}(u, \{s, t\}) - \operatorname{dist}(v, \{s, t\})| \leq 1,$$

so every contributing edge joins two consecutive layers. Hence

$$\langle x, Lx \rangle = \sum_{i=0}^{r-1} e(V_i, V_{i+1}) \left((d-1)^{-i/2} - (d-1)^{-(i+1)/2} \right)^2 + e(V_r, V_{r+1})(d-1)^{-r}.$$

Take any vertex $v \in V_i$ with $i \geq 1$. By definition of distance, there exists a shortest path from v to the edge $\{s, t\}$ of length i. Let u be the first vertex on such a shortest path after v. Then $\operatorname{dist}(u, \{s, t\}) = i - 1$, so $u \in V_{i-1}$. In particular, v has at least one neighbor in V_{i-1}. Since every neighbor of v must lie in $V_{i-1} \cup V_i \cup V_{i+1}$, and at least one neighbor lies in V_{i-1}, it follows that at most $d - 1$ neighbors of v can lie in V_{i+1}. For $i = 0$, the same conclusion holds trivially.

Therefore

$$e(V_i, V_{i+1}) \leq (d-1)|V_i|,$$

and so

$$\langle x, Lx \rangle \leq (d-1) \sum_{i=0}^{r-1} |V_i| \left((d-1)^{-i/2} - (d-1)^{-(i+1)/2} \right)^2 + |V_r|(d-1)^{1-r}.$$

Since

$$(d-1) \left((d-1)^{-i/2} - (d-1)^{-(i+1)/2} \right)^2 = (d - 2\sqrt{d-1})(d-1)^{-i},$$

it follows that

$$\begin{aligned}
\langle x, Lx \rangle &\leq (d - 2\sqrt{d-1}) \sum_{i=0}^{r-1} |V_i|(d-1)^{-i} + (d-1)|V_r|(d-1)^{-r} \\
&= (d - 2\sqrt{d-1}) \sum_{i=0}^{r} |V_i|(d-1)^{-i} + (2\sqrt{d-1} - 1)|V_r|(d-1)^{-r}.
\end{aligned}$$

Since every vertex in V_{i+1} has a neighbor in V_i, we have $e(V_i, V_{i+1}) \geq |V_{i+1}|$. Together with $e(V_i, V_{i+1}) \leq (d-1)|V_i|$, this gives $|V_{i+1}| \leq (d-1)|V_i|$, implying $|V_r|(d-1)^{-r} \leq |V_i|(d-1)^{-i}$ for every $0 \leq i \leq r$. Thus,

$$(r+1)|V_r|(d-1)^{-r} \leq \sum_{i=0}^{r} |V_i|(d-1)^{-i} = \langle x, x \rangle.$$

Therefore,

$$\langle x, Lx \rangle \leq \left(d - 2\sqrt{d-1} + \frac{2\sqrt{d-1}-1}{r+1} \right) \langle x, x \rangle.$$

Using $\langle x, Ax \rangle = d\langle x, x \rangle - \langle x, Lx \rangle$, we get

$$\frac{\langle x, Ax \rangle}{\langle x, x \rangle} \geq 2\sqrt{d-1} - \frac{2\sqrt{d-1}-1}{r+1} \geq 2\sqrt{d-1}\left(1 - \frac{1}{r+1}\right),$$

as required. □

We will use the following without proof. (Recall that $\mathbf{1} = (1, \cdots, 1)^T$ is the eigenvector corresponding to the trivial eigenvalue $\lambda_1 = d$.)

Lemma 4.2.5 (Rayleigh quotient characterization of λ_2)**.** *For a d-regular graph $G = (V, E)$,*

$$\lambda_2 = \max_{z \in \mathbb{R}^V, z \perp \mathbf{1}} \frac{\langle z, Az \rangle}{\langle z, z \rangle},$$

where $z \perp \mathbf{1}$ denotes orthogonality between z and $\mathbf{1}$.

We can now prove the important bound.

Proof of the Alon–Boppana Bound 4.2.2. Fix a positive integer r. By Lemma 4.2.5, it is enough to construct a nonzero vector $z \perp \mathbf{1}$ satisfying

$$\frac{\langle z, Az \rangle}{\langle z, z \rangle} \geq 2\sqrt{d-1}\left(1 - \frac{1}{r+1}\right).$$

We will choose $r = r(n)$ at the end of the proof.

As in Lemma 4.2.4, let $V_i = \{v \in V : \operatorname{dist}(v, \{s, t\}) = i\}$. Since $|V_{i+1}| \leq (d-1)|V_i|$ (motivated in the proof of Lemma 4.2.4) we have $|V_i| \leq 2(d-1)^i$ for every $i \geq 0$. Hence the number of vertices within distance $2r+1$ of any edge is at most

$$2\sum_{i=0}^{2r+1} (d-1)^i.$$

Thus if $n > 2(d+1)\sum_{i=0}^{2r+1}(d-1)^i$, then after choosing any edge $\{s,t\}$, some edge $\{s',t'\}$ has both endpoints outside this ball. Thus the distance between the two edges is at least $2r+2$.

Let x be the test vector from Lemma 4.2.4 associated with the edge $\{s,t\}$, and let y be the corresponding test vector associated with $\{s',t'\}$. Since each vector is supported[1] on the vertices within distance r of its defining edge, the supports of x and y are disjoint. In fact, they are at distance at least 2 from one another. Consequently, $\langle x,y\rangle = 0$, and, since there are no edges joining the two supports, $\langle x, Ay\rangle = 0$.

Choose $c \in \mathbb{R}$ so that $z = x - cy$ is orthogonal to $\mathbf{1}$. Such a choice is possible since every entry of y is nonnegative and at least one entry is positive. Then

$$\langle z,z\rangle = \langle x,x\rangle + c^2\langle y,y\rangle,$$

while

$$\langle z,Az\rangle = \langle x,Ax\rangle + c^2\langle y,Ay\rangle,$$

because the mixed terms vanish.

Applying Lemma 4.2.4 to both x and y gives

$$\begin{aligned}\langle z,Az\rangle &\geq 2\sqrt{d-1}\left(1-\frac{1}{r+1}\right)\langle x,x\rangle + 2\sqrt{d-1}\left(1-\frac{1}{r+1}\right)c^2\langle y,y\rangle\\ &= 2\sqrt{d-1}\left(1-\frac{1}{r+1}\right)\langle z,z\rangle.\end{aligned}$$

Hence

$$\frac{\langle z,Az\rangle}{\langle z,z\rangle} \geq 2\sqrt{d-1}\left(1-\frac{1}{r+1}\right).$$

Since $z \perp \mathbf{1}$, the Rayleigh quotient characterization (Lemma 4.2.5) of λ_2 yields

$$\lambda_2 \geq 2\sqrt{d-1}\left(1-\frac{1}{r+1}\right).$$

Finally, choose $r = r(n)$ so that $r(n) \to \infty$ and

$$2\sum_{i=0}^{2r(n)+1}(d-1)^i = o(n),$$

for example

$$r(n) = \left\lfloor \frac{1}{4}\log_{d-1} n \right\rfloor.$$

[1]Support of a vector $x = (x_v)_{v\in V}$ used here simply means the set of vertices where x is nonzero, i.e. $\{v \in V : x_v \neq 0\}$.

Then the above construction is valid for all sufficiently large n, while

$$1 - \frac{1}{r(n)+1} \longrightarrow 1.$$

Therefore

$$\lambda_2 \geq 2\sqrt{d-1} - o(1),$$

as claimed. □

Another proof of the Alon–Boppana bound shows that the spectral radius of the infinite d-regular tree is equal to $2\sqrt{d-1}$ and relates this to closed walks on the graph. This might seem a bit odd but, in fact, the infinite d-regular tree T_d is the so-called universal cover of d-regular graphs since it is a cover [2] of every such graph. To properly deal with this other proof, we must work with an infinite-dimensional inner product space, and it will therefore be left out (see [LPS88] or [Zha23]). A tangentially related proof to that of the derivation of the spectral radius of T_d will, however, be given in our exposition on the matching polynomial, that is, in the proof of Theorem 5.6.3.

Definition 4.2.6. An (n, d, λ)-graph is an n-vertex d-regular graph such that all non-trivial eigenvalues λ_i satisfy $|\lambda_i| \leq \lambda$.

For instance, Ramanujan graphs are $(n, d, 2\sqrt{d-1})$-graphs.

Corollary 4.2.7. *For every fixed $d \geq 3$ and $\lambda < 2\sqrt{d-1}$, there are only finitely many (n, d, λ)-graph up to isomorphism.*

Proof. Fix $d \geq 3$ and suppose there are infinitely many (n, d, λ)-graphs with $\lambda < 2\sqrt{d-1}$. Then we can take a sequence of such graphs with $n \to \infty$. But by the Alon–Boppana bound (Theorem 4.2.2), any d-regular graph satisfies

$$\lambda_2 \geq 2\sqrt{d-1} - o_n(1),$$

where $o_n(1) \to 0$ as $n \to \infty$.

Thus, for sufficiently large n, we must have$\lambda_2 > \lambda$, since $\lambda < 2\sqrt{d-1}$. This contradicts the assumption that all nontrivial eigenvalues satisfy $|\lambda_i| \leq \lambda$.

Therefore, only finitely many (n, d, λ)-graphs can exist (up to isomorphism). □

[2](We will not use this definition directly.) A graph C *covers* a graph G if there is a map $\varphi : V(C) \to V(G)$ such that (1) for every $\{u, v\} \in E(C), \{\varphi(u), \varphi(v)\} \in E(G)$ and (2) for every $v \in V(C)$, the restriction $\varphi : N_C(v) \to N_G(\varphi(v))$ is a bijection.

Let $d \geq 3$ be fixed. An expanding family $(G_n)_n$ of connected n-vertex d-regular Ramanujan graphs, where $|V_n| \to +\infty$ as $n \to +\infty$, are evidently a special object due to the Alon–Boppana bound, as these are bounded-degree expanding families with the largest possible spectral gap. In other words, Ramanujan graphs meet the Alon–Boppana bound.

5. Infinite Families of d-regular Bipartite Ramanujan Graphs

The previous chapter established the Alon–Boppana bound (Theorem 4.2.2), showing that every infinite family of d-regular graphs satisfies

$$\lambda_2 \geq 2\sqrt{d-1} - o(1).$$

As a consequence, an infinite family of d-regular Ramanujan graphs is optimal in the spectral sense among bounded-degree expander families. Altough the Paley graphs studied earlier are Ramanujan,they are dense, with degree growing proportionally to the number of vertices, and therefore do not answer the natural question of whether such optimal families exists for every fixed degree d.

This chapter presents a proof by Marcus, Spielman, and Srivastava which establishes the existence of an infinite family of d-regular bipartite Ramanujan graphs for every integer $d \geq 3$. The proof is nonconstructive, showing the existence of such a family through an indirect spectral argument and completes the narrative of the thesis by showing that optimal bounded-degree expanders exists in every degree.

5.1 2-Lifts and Signings

Definition 5.1.1 (Matching)**.** A *matching* of a graph G is a set of edges with no common vertices.

That is, no two edges in a matching set share a vertex. A vertex $v \in V(G)$ is said to be *covered* by a matching M if v is the endpoint of some edge in M. A *perfect matching* of G is a matching such that all vertices of G are covered[1]. (E.g., if $G = (V, E) = (\{v_1, v_2, v_3\}, \quad \{\{v_1, v_2\}, \{v_2, v_3\}, \{v_1, v_3\}\})$, then $M_1 = \{\{v_1, v_2\}\} \subseteq E$

[1]A matching may be viewed as a 1-regular subgraph of G. Indeed, if $M \subseteq E(G)$ is a matching, then the subgraph with edge set M (and vertex set consisting of the endpoints of the edges in M, i.e. all vertices covered by M) is 1-regular. Conversely, every 1-regular subgraph of G determines a matching of G.

is a matching which covers v_1 and v_2, but $M_2 = \{\{v_1, v_2\}, \{v_2, v_3\}\} \subseteq E$ is not a matching since v_2 is a common vertex. Note that this graph G does not have a perfect matching; it is not hard to realize that a graph with an odd number of vertices cannot have a perfect matching.)

Definition 5.1.2 (Graph lift)**.** Let $[m] = \{1, 2, \ldots, m\}$ and let $G = (V, E)$ be a graph. For a fixed $m \in \mathbb{N}$, an *m-lift* of G is a graph $\widetilde{G}$ obtained by replacing each vertex $v \in V$ by a *cloud* $\{(v, i)\}_{i \in [m]} = \{(v, i) : i \in [m]\}$, and for each edge $\{u, v\} \in E$, adding a set of m edges that forms a perfect matching between the clouds, that is, each vertex of the cloud of u is joined to exactly one vertex of the cloud of v, and vice versa.

Note that if G is d-regular, then every m-lift $\widetilde{G}$ is also d-regular and $|V(\widetilde{G})| = m|V(G)|$.

Example. Let G be a 2-vertex graph consisting of a single edge $\{u, v\}$ and let $m = 2$. The clouds are $\{(u, 1), (u, 2)\}$ and $\{(v, 1), (v, 2)\}$. There are exactly 2 possible perfect matchings between these clouds, namely

$$\{\{(u, 1), (v, 1)\}, \{(u, 2), (v, 2)\}\}$$

and

$$\{\{(u, 1), (v, 2)\}, \{(u, 2), (v, 1)\}\}.$$

Each choice gives a distinct 2-lift of G.

Definition 5.1.3. Let G be a graph. A *signing* is a map $\sigma : E(G) \to \{\pm 1\}$, for which we define the associated *signed adjacency matrix* A_σ of G by

$$(A_\sigma)_{u,v} = \begin{cases} \sigma(\{u, v\}) & \text{if } \{u, v\} \in E(G) \\ 0 & \text{otherwise.} \end{cases}$$

A signing σ determines a graph $G^{(\sigma)}$, which is a 2-lift of G. For each vertex $v \in V$, the corresponding cloud is $\{(v, 1), (v, 2)\}$. If an edge $\{u, v\} \in E(G)$ is positively signed (i.e. $\sigma(\{u, v\}) = 1$) then the corresponding perfect matching between the clouds of u and v is

$$\{(u, 1), (v, 1)\} \text{ and } \{(u, 2), (v, 2)\}.$$

If instead $\{u, v\} \in E(G)$ is negatively signed ($\sigma(\{u, v\} = -1$), then the corresponding perfect matching between the clouds of u and v is

$$\{(u, 1), (v, 2)\} \text{ and } \{(u, 2), (v, 1)\}.$$

To restate, a base edge $\{u, v\}$ gets "lifted" to either

parallel edges $\{\{(u,1),(v,1)\},\{(u,2),(v,2)\}\}$ if $\sigma(\{u,v\})=1$
or *cross edges* $\{\{(u,1),(v,2)\},\{(u,2),(v,1)\}\}$ if $\sigma(\{u,v\})=-1$.

Given a signing σ, if the resulting 2-lift $G^{(\sigma)}$ only has edges that are parallel, then $G^{(\sigma)}$ is just two disjoint copies of the original graph. On the other hand, if the edges of $G^{(\sigma)}$ are only cross edges, then $G^{(\sigma)}$ is the so-called *bipartite double cover* of G, which just means that every original adjacency is converted into a bipartite relation between the two copies, so the 2-lift is bipartite with parts V_0 and V_1.

Proposition 5.1.4 (Lemma 3.1 in [BL06]). *Let G be an n-vertex graph and σ a signing on $E(G)$. The spectrum of the 2-lift of G is the multiset union of the spectrum of G (the "old" eigenvalues) and the spectrum of A_σ (the "new" eigenvalues).*

Proof. The adjacency matrix $A_{\widetilde{G}}$ of the 2-lift $\widetilde{G}$ is a $2n \times 2n$ matrix and the vertices can be ordered so that

$$A_{\widetilde{G}} = \begin{pmatrix} A_1 & A_2 \\ A_2 & A_1 \end{pmatrix}$$

where A_1 and A_2 are the adjacency matrices of $(V,\sigma^{-1}(1))$ and $(V,\sigma^{-1}(-1))$, respectively. That is, the adjacency matrix of the original graph is $A_G = A_1 + A_2$ while the signed adjacency matrix is $A_\sigma = A_1 - A_2$.

Let λ be an eigenvalue of A_G with eigenvector v. Then if $\widetilde{v} = \begin{pmatrix} v \\ v \end{pmatrix}$, we have

$$A_{\widetilde{G}}\widetilde{v} = \begin{pmatrix} A_1 & A_2 \\ A_2 & A_1 \end{pmatrix}\begin{pmatrix} v \\ v \end{pmatrix} = \begin{pmatrix} (A_1+A_2)v \\ (A_2+A_1)v \end{pmatrix} = \begin{pmatrix} A_G v \\ A_G v \end{pmatrix} = \lambda\widetilde{v}.$$

Hence, if λ is an eigenvalue of A_G, then it is also an eigenvalue of $A_{\widetilde{G}}$.

A similar calculation shows that if α is an eigenvalue of the signed adjacency matrix A_σ with eigenvector u, then α is also an eigenvalue of $A_{\widetilde{G}}$ with eigenvector

$$\widetilde{u} = \begin{pmatrix} u \\ -u \end{pmatrix}.$$

Now let $\{v_1,\ldots,v_n\}$ be an eigenbasis for A_G and $\{u_1,\ldots,u_n\}$ be an eigenbasis for A_σ. Then

$$\begin{pmatrix} v_i \\ v_i \end{pmatrix}, \quad \begin{pmatrix} u_j \\ -u_j \end{pmatrix}$$

are all eigenvectors of $A_{\widetilde{G}}$. Moreover, every vector of the first form is orthogonal to every vector of the second form, so these $2n$ vectors form an eigenbasis of $\mathbb{R}^{2n}$. Therefore the spectrum of $\widetilde{G}$ is exactly the multiset union of the spectra of G and A_σ. □

5.2 Matching Polynomials

Definition 5.2.1 (Matching Polynomial). For an n-vertex graph G, let m_k be the number of matchings of G with k edges. Set $m_0 = 1$. The *matching polynomial* of G is

$$\mu_G(x) = \sum_{k \geq 0} (-1)^k m_k x^{n-2k}.$$

Since $m_0 = 1, \mu_G(x)$ is an n-degree polynomial.

Example. If G is the triangle K_3, then $m_0 = 1$ by definition, $m_1 = 3$ (pick any edge), and $m_2 = 0$ (any choice of two edges shares a vertex). Thus,

$$\mu_{K_3}(x) = x^3 - 3x.$$

We want to prove that for any d-regular graph G, its matching polynomial μ_G is real-rooted and all its roots lie in $[-2\sqrt{d-1}, 2\sqrt{d-1}]$. Our proof of this will be based on the work of Godsil [God81].

We state two important theorems, Theorem 5.2.2 and 5.2.3. The proof of these will be given in Subsection 5.6.

Theorem 5.2.2. *For any graph G, the matching polynomial μ_G has only real roots.*

Theorem 5.2.3. *For any d-regular graph G, all roots of μ_G lie in the interval $[-2\sqrt{d-1}, 2\sqrt{d-1}]$.*

Theorem 5.2.4. *Let G be a graph with m edges and n vertices. For a signing $\sigma \in \{\pm 1\}^m$, we let $f_\sigma(x) = \det(xI - A_\sigma)$ be the characteristic polynomial of the signed adjacency matrix A_σ. Then*

$$\frac{1}{2^m} \sum_{\sigma \in \{\pm 1\}^m} f_\sigma(x) = \mu_G(x).$$

Equivalently, if a signing σ is chosen uniformly at random from $\{\pm 1\}^m$ then the expected characteristic polynomial is equal to the matching polynomial, that is

$$\mathbb{E}[f_\sigma(x)] = \mu_G(x).$$

Indeed,

$$\mathbb{E}[f_\sigma(x)] = \frac{1}{2^m} \sum_{\sigma \in \{\pm 1\}^m} f_\sigma(x).$$

Proof of Theorem 5.2.4. Let S_n be the symmetric group on n letters and let $\operatorname{sgn} : S_n \to \{\pm 1\}$ map even permutations to 1 and odd permutations to -1. (Recall that the parity of a permutation is odd if and only if the number of transpositions is odd, and the it has even parity if and only if the number of transpositions is even. A cycle can always be written as a product of transpositions. Note that the identity transposition is even because, for instance, in cycle notation $(1\,2)(2\,1) = (1)(2)(3)\ldots(n) = \mathrm{id}$. An important fact to recall is that any permutation can be written as a product of disjoint cycles.)

Expanding the determinant over permutations yields

$$\begin{aligned} 2^{-m} \sum_{\sigma \in \{\pm 1\}^m} f_\sigma(x) &= 2^{-m} \sum_{\sigma \in \{\pm 1\}^m} \sum_{\pi \in S_n} \operatorname{sgn} \pi \prod_{i=1}^{n} (xI - A_\sigma)_{i,\pi(i)}, \\ &= \sum_{\pi \in S_n} \operatorname{sgn} \pi \left(2^{-m} \sum_{\sigma \in \{\pm 1\}^m} \prod (xI - A_\sigma)_{i,\pi(i)} \right). \end{aligned}$$

The exchange of sums is valid since the sums are finite.

Fix a permutation π. If $\pi(i) = i$, then $(xI - A_\sigma)_{i,\pi(i)} = x$.

If $\pi(i) \neq i$, the $(xI - A_\sigma)_{i,\pi(i)} = (-A_\sigma)_{i,\pi(i)}$. Thus the term vanishes except when $\{i, \pi(i)\}$ is an edge of G, and so the whole product vanishes unless π is a permutation for which every i, either $\pi(i) = i$ or $\{i, \pi(i)\}$ is an edge. Assuming $\{i, \pi(i)\} \in E(G)$ whenever $\pi(i) \neq i$, we get

$$\prod_{i=1}^{n} (xI - A_\sigma)_{i,\pi(i)} = x^{\operatorname{fix} \pi} (-1)^{n - \operatorname{fix} \pi} \prod_{i : \pi(i) \neq i} \sigma(\{i, \pi(i)\}),$$

where $\operatorname{fix} \pi$ gives the number of fixed points of π. That is, $\operatorname{fix} \pi = |\{i \mid \pi(i) = i\}|$.

We write π as a product of disjoint cycles. Suppose π contains a cycle $(i_1\, i_2\, \cdots\, i_r)$ of length $r \geq 3$. Then the factor

$$\prod_{i : \pi(i) \neq i} \sigma(\{i, \pi(i)\})$$

contains the term $\sigma(\{i_1, i_2\})\sigma(\{i_2, i_3\}) \cdots \sigma(\{i_r, i_1\})$.

Since $(i_1 \ldots i_r)$ is a cycle in the disjoint cycle decomposition of π, none of the edges $\{i_1, i_2\}, \{i_2, i_3\}, \ldots, \{i_r, i_1\}$ can arise from any other cycle of π. Hence, each of the corresponding sign variables occurs exactly once in $\prod_{i:\pi(i)\neq i} \sigma(\{i, \pi(i)\})$. Thus the product contains a factor $\sigma(\{i_j, i_{j+1})$ that occurs exactly once. Averaging over all signings, the contributions from the two choices $\sigma(\{i_j, i_{j+1}\}) = \pm 1$ cancels, so the inner sum is 0. Therefore whenever π contains a cycle of length ≥ 3 the inner sum $2^{-m} \sum_\sigma \prod_{i=1}^{n} (xI - A_\sigma)_{i,\pi(i)}$ is equal to 0.

Therefore the only permutations which contribute are those whose cycle decomposition contains no cycle of length greater than 2. Equivalently, the cycle decomposition contains only fixed points and transpositions making up edges. Such permutations are in bijection with matchings in G as each transposition $(u\,v)$ corresponds to the edge $\{u, v\}$ and disjointness of the transpositions is exactly the matching condition.

Let π correspond to a matching of size k. Then π consists of k disjoint transpositions and $n-2k$ fixed points. For each transposition $(u\,v)$ we obtain the factor

$$(-A_\sigma)_{u,v}(-A_\sigma)_{v,u} = (-\sigma(\{u,v\}))^2 = 1.$$

Thus

$$2^{-m} \sum_{\sigma\in\{\pm 1\}^m} \prod_{i=1}^{n} (xI - A_\sigma)_{i,\pi(i)} = x^{n-2k}.$$

Since π is the product of k transpositions, $\operatorname{sgn}\pi = (-1)^k$. Therefore every matching of size k contributes $(-1)^k x^{n-2k}$.

There are $m_k(G)$ matchings of size k, so summing over all contributing permutations yields

$$2^{-m} \sum_{\sigma\in\{\pm 1\}^m} f_\sigma(x) = \sum_{k\geq 0} (-1)^k m_k(G) x^{n-2k} = \mu_G(x).$$

□

5.3 Interlacing Families

The key method pioneered in the original paper is called the Method of Interlacing Polynomials. The key application of this, for our aims, is to show that the characteristic polynomials $\{f_\sigma\}_{\sigma\in(\pm 1)^m}$ forms a so-called interlacing family, which means it has nice properties. In particular, the fact that $\{f_\sigma\}_\sigma$ is an interlacing family allows us to relate it to the expected characteristic polynomial, which as we have seen is equal to the matching polynomial μ_G, whose roots are real (Theorem 5.2.2) and are bounded in absolute value by $2\sqrt{d-1}$. (Theorem 5.2.3).

The treatment presented here is less general than what is presented in Marcus, Spielman, and Srivastava's paper [MSS14] as the authors there focus on arbitrary finite sets but we focus on products of $\{\pm 1\}$. It is important to point out that the Method of Interlacing Polynomials is useful in broader contexts and so the general method is worth seeking out.

Definition 5.3.1 (Interlacing polynomial)**.** A monic polynomial $g(x) = \prod_{i=1}^{n-1}(x-\alpha_i)$ *interlaces* a polynomial $f(x) = \prod_{i=1}^{n}(x-\beta_i)$ if

$$\beta_1 \leq \alpha_1 \leq \beta_2 \leq \alpha_2 \leq \cdots \leq \alpha_{n-1} \leq \beta_n.$$

We restrict attention to monic polynomials for convenience. Since multiplying a polynomial by a nonzero constant does not change its roots, any polynomial with nonzero leading coefficient may be normalized to be monic without affecting the notion of interlacing.

Definition 5.3.2 (Common interlacing)**.** We say polynomials $f_1, \dots, f_k$ have a *common interlacing* if there exists a polynomial g which interlaces every polynomial $f_1, \dots, f_k$.

We give two examples of interlacings.

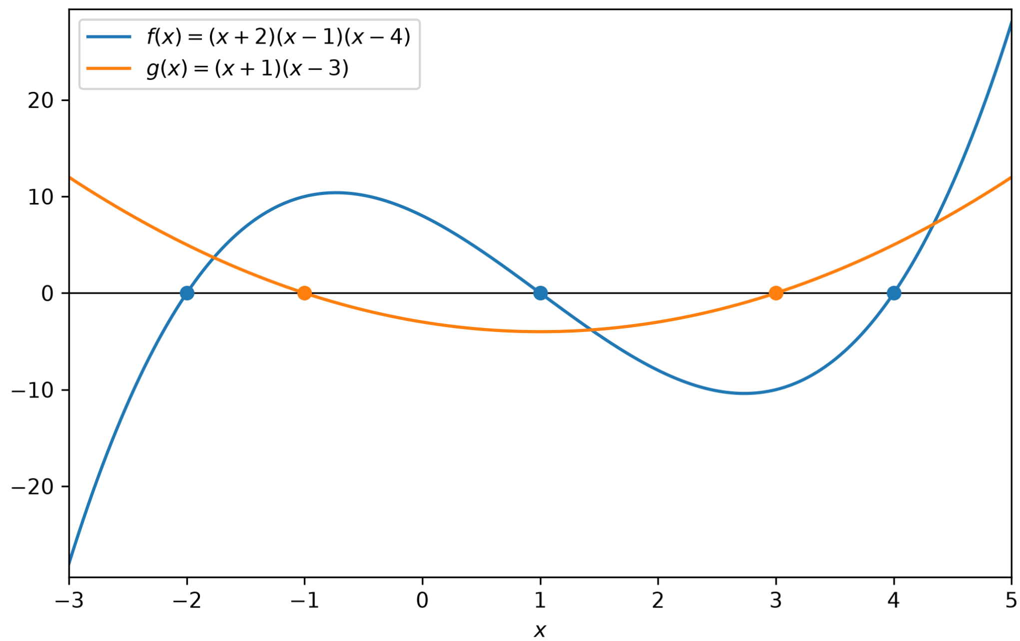


Figure 5.1: First Example of a Polynomial Interlacing Another

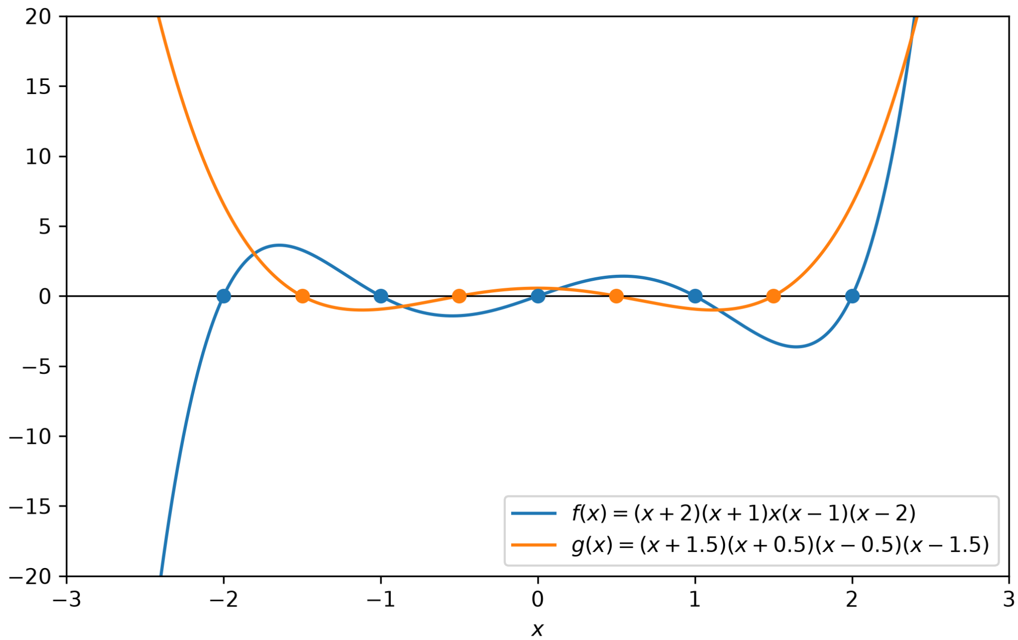


Figure 5.2: Second Example of a Polynomial Interlacing Another

Theorem 5.3.3. *Let f and g be real-rooted monic polynomials both of degree n such that $tf + (1-t)g$ is real-rooted for every $t \in [0,1]$, then f and g have a common interlacing.*

The proof of this will be omitted. The idea behind the result is that the roots of the continuously varying family $f_t = (1-t)f + tg$ can be followed continuously as t varies from 0 to 1. Since all intermediate polynomials are real-rooted, these root trajectories remain on the real line and force the roots of f and g to share a common interlacing. The formal justification of this relies on a somewhat substantial fact (the roots of a polynomial depend continuously on its coefficients) which would be a digression in our main exposition. We refer the reader to Theorem 4 in [Sri14].

Lemma 5.3.4. *Let $f_1, \ldots, f_k$ be real-rooted n-degree polynomials and a common interlacing. Then there exists an index j such that the largest root of f_j is at most the largest root of*

$$F_\emptyset = f_1 + \cdots + f_k.$$

Proof. For a real-rooted polynomial p, denote the max root of p by $\rho(p) = \max\{x \in \mathbb{R} : p(x) = 0\}$. [2]

Let g be a polynomial interlacing $f_1, \ldots, f_k$, and let $\alpha_{n-1} = \rho(g)$. Since g interlaces each f_i, every polynomial f_i has exactly one root in the interval $[\alpha_{n-1}, +\infty)$. As the

[2] Two numbers will be defined using ρ, those being α_{n-1}, the largest root of g, and β_n, the largest root of $F_\emptyset$. This notation is chosen to match Definition 5.3.1.

leading coefficients are positive $\lim_{x\to+\infty} f_i(x) = +\infty$ and

$$f_i(\alpha_{n-1}) \leq 0 \tag{-:-}$$

for every i. Hence $F_\emptyset(\alpha_{n-1}) = \sum_{i=1}^k f_i(\alpha_{n-1}) \leq 0$. On the other hand, $\lim_{x\to+\infty} F_\emptyset(x) = +\infty$, since the leading coefficient of $F_\emptyset$ is also positive. By continuity, $F_\emptyset$ has a root in $[\alpha_{n-1}, +\infty)$. In particular, $\rho(F_\emptyset) \geq \alpha_{n-1}$.

Let $\beta_n = \rho(F_\emptyset)$. This β_n is a root, so $F_\emptyset(\beta_n) = 0$. If $f_i(\beta_n) < 0$ for every i, then necessarily $F_\emptyset(\beta_n) = \sum_{i=1}^k f_i(\beta_n) < 0$, contradicting $F_\emptyset(\beta_n) = 0$. Therefore there exists some index j such that $f_j(\beta_n) \geq 0$. For this particular fixed j, we have $f_j(\alpha_{n-1}) \leq 0$ by line (-:-) and $f_j(\beta_n) \geq 0$, so the Intermediate Value Theorem implies f_j has a root in $[\alpha_{n-1}, \beta_n]$. As established, f_j has exactly one root in $[\alpha_{n-1}, \infty)$, its largest root. Hence $\rho(f_j) \in [\alpha_{n-1}, \beta_n]$.

Thus, $\rho(f_j) \leq \beta_n = \rho(F_\emptyset)$, which proves the claim. $\square$

We now specialize to the family of characteristic polynomials obtained from signings.

Definition 5.3.5. Let G be a graph with edge set $E(G) = \{e_1, \dots, e_m\}$, where the edges are distinct. For each signing $\sigma : E(G) \to \{\pm 1\}$, let $f_\sigma(x) = \det(xI - A_\sigma)$ be the characteristic polynomial of the corresponding signed adjacency matrix.

For a partial signing $\tau = (\tau_1, \dots, \tau_k) \in \{\pm 1\}^k$, where $k < m$, define

$$F_\tau(x) = \sum_{\sigma_{k+1},\dots,\sigma_m \in \{\pm 1\}} f_{\tau_1,\dots,\tau_k,\sigma_{k+1},\dots,\sigma_m}(x).$$

Thus F_τ is obtained by summing the characteristic polynomials corresponding to all complete signings[3] extending τ. If τ is an empty partial signing, we write the above sum of polynomials as $F_\emptyset(x)$.

A simple example will be given. Suppose $m = 3$. If the partial signing is $\tau = (+1)$, then

$$F_\tau(x) = F_{(+1)} = f_{(+1,+1,+1)} + f_{(+1,+1,-1)} + f_{(+1,-1,+1)} + f_{(+1,-1,-1)}.$$

Since k edges are determined by the partial signing τ, there are $m - k$ undetermined edges. Hence F_τ is a sum with 2^{m-k} terms. In this example, $m = 3$ and $k = 1$ so here $2^{m-k} = 4$.

The importance of F_τ stems from the identity

$$F_\tau = F_{\tau,+1} + F_{\tau,-1},$$

[3] To be clear, a complete signing just means a signing where all m edges are determined.

which follows since every signing extending τ must assign either $+1$ or -1 to the next edge. Consequently, the set of all extensions of τ partitions into two classes, those extending $(\tau, +1)$ and those extending $(\tau, -1)$. Summing over all these extensions therefore yields the above identity.

It can be more intuitive to take a geometric view of these partial signings. One may view the collection of partial signings as a binary tree. The root corresponds to the empty partial signing ($k = 0$) and each vertex τ has two children $(\tau, +1)$ and $(\tau, -1)$. The polynomial F_τ is therefore the sum of polynomials associated with all leaves below τ, and the identity $F_\tau = F_{\tau,+1} + F_{\tau,-1}$ simply means that these leaves are partitioned according to the sign assigned to the next edge. Hence, a complete signing corresponds to some leaf in this binary tree, and all leaves have depth m, the number of edges in the original graph. The family $\{f_\sigma\}_{\sigma\in\{\pm1\}^m}$ can be seen as the collection of leaves of this tree.

Definition 5.3.6 (Interlacing Family)**.** We say that the family $\{f_\sigma\}_{\sigma\in\{\pm1\}^m}$ is an interlacing family if for every partial signing $\tau = (\tau_1, \dots, \tau_k) \in \{\pm1\}^k$ where $k = 0, 1 \dots, m-1$, the two polynomials $F_{\tau,+1}$ and $F_{\tau,-1}$ have a common interlacing.

Theorem 5.3.7 (Theorem 4.4. in [MSS14])**.** *If the polynomials $\{f_\sigma\}_{\sigma\in\{\pm1\}^m}$ form an interlacing family, then there exists some complete signing $\sigma = (\sigma_1, \dots, \sigma_m) \in \{\pm1\}^m$ so that the largest root of f_σ is at most the largest root of $F_\emptyset$.*

Remark 5.3.8. Note that we do not yet know whether the antecedent of this implication is true.

Proof. We induct on the depth $k \in \{0, 1, \dots, m\}$ of the binary tree associated with the partial signings to prove that at depth k, there exists a partial signing $\tau = (\tau_1, \dots, \tau_k)$ satisfying $\rho(F_\tau) \leq \rho(F_\emptyset)$. At the root, we have $F_\emptyset = F_{+1} + F_{-1}$. Since F_{+1} and F_{-1} have a common interlacing, Lemma 5.3.4 implies that at least one of them, say F_{τ_1}, satisfies

$$\rho(F_{\tau_1}) \leq \rho(F_\emptyset),$$

where $\rho(\cdot)$ gives the max root of a real-rooted polynomial.

Suppose inductively that we have chosen a partial signing $\tau = (\tau_1, \dots, \tau_k)$ with $\rho(F_\tau) \leq \rho(F_\emptyset)$. Since the family is an interlacing family, $F_{\tau,+1}$ and $F_{\tau,-1}$ have a common interlacing. Again we apply Lemma 5.3.4 to $F_\tau = F_{\tau,+1} + F_{\tau,-1}$, there exists a $\tau_{k+1} \in \{\pm1\}$ such that $\rho(F_{\tau,\tau_{k+1}}) \leq \rho(F_\tau)$, together with the induction hypothesis, gives

$$\rho(F_{\tau,\tau_{k+1}}) \leq \rho(F_\tau) \leq \rho(F_\emptyset).$$

Continuing this way, inductively, we eventually extend all the way to a complete signing $\sigma = (\sigma_1, \dots, \sigma_m)$. At this point, there are no remaining extensions (it is a leaf), so $F_\sigma = f_\sigma$. Thus,

$$\rho(f_\sigma) = \rho(F_\sigma) \leq \rho(F_\emptyset),$$

which proves the theorem. $\square$

Visually, the proof can be thought of using the binary tree of partial signings. Starting at the root $F_\emptyset$, Lemma 5.3.4 guarantees that at least one of the two children has largest root no larger than its parent. Repeating this argument at every depth allows us to move down the tree while never increasing the largest root. Since every root-to-leaf path gives a complete signing, there must be a leaf vertex f_σ whose largest root is no greater than that of the root polynomial $F_\emptyset$.

5.4 The Main MSS Theorem

In order to show that $\{f_\sigma\}$ is an interlacing family, we will state a theorem that essentially means that if we pick each sign in $\sigma = (\sigma_1, \dots, \sigma_m)$ independently with any probabilities, then the resulting polynomial is still real-rooted. However, the following theorem will not be proven. We refer to the reader to Section 6 of [MSS14] on real stable polynomials for a proof. Section 6 is a little more than three pages of very terse exposition of this fact and related theory, relying on cited results (primarily results by P. Brändén and J. Borcea).

Theorem 5.4.1 (Theorem 5.1. in [MSS14])**.** *Let $p_1, \dots, p_m$ be numbers in the interval $[0, 1]$. Then the following polynomial is real-rooted*

$$\sum_{\sigma \in \{\pm 1\}^m} \left(\prod_{i:\sigma_i = 1} p_i \right) \left(\prod_{i:\sigma_i = -1} (1 - p_i) \right) f_\sigma(x).$$

Corollary 5.4.2. *The polynomials $\{f_\sigma\}_{\sigma \in \{\pm 1\}^m}$ is an interlacing family.*

Proof. For $0 \leq k \leq m - 1$, let $\tau = (\tau_1, \dots, \tau_k) \in \{\pm 1\}^k$ be a partial assignment. For every $t \in [0, 1]$, we want to show that the polynomial

$$tF_{\tau,1} + (1 - t)F_{\tau,-1}$$

is real-rooted. The statement then follows by Theorem 5.3.3. To show real-rootedness of this polynomial, we apply Theorem 5.4.1 with $p_{k+1} = t, \quad p_{k+2}, \dots, p_m = \frac{1}{2}$, and $p_i = \frac{1+\tau_i}{2}$ for $1 \leq i \leq k$, since for this choice of p_i, the coefficient

$$\left(\prod_{i:\sigma_i = 1} p_i \right) \left(\prod_{i:\sigma_i = -1} (1 - p_i) \right)$$

evaluates to $(1/2)^{m-(k+1)}t$ if σ extends $(\tau, 1)$, evaluates to $(1/2)^{m-(k+1)}(1-t)$ if σ extends $(\tau, -1)$, and equals 0 otherwise. Factoring out the positive constant $(1/2)^{m-(k+1)}$ yields $tF_{\tau,1} + (1-t)F_{\tau,-1}$, whose real-rootedness follows from Theorem 5.4.1. $\square$

Lemma 5.4.3. *For every $d \geq 2$, the complete bipartite graph $K_{d,d}$ is a d-regular Ramanujan graph.*

Proof. It is clear that $K_{d,d}$ is d-regular. The spectrum of every bipartite graph is symmetric around zero (by Proposition 2.1.10), and because d is the trivial eigenvalue, $-d$ must also be an eigenvalue. The adjacency matrix of $K_{d,d}$ has rank 2, so all other eigenvalues must be 0 because if we let J_d denote the $d \times d$ matrix where every entry is 1, then the adjacency matrix $A_{K_{d,d}}$ of $K_{d,d}$ is a $2d \times 2d$ matrix which can, by the definition of bipartite graphs, be written as the block matrix

$$A_{K_{d,d}} = \begin{pmatrix} 0 & J_d \\ J_d & 0 \end{pmatrix}$$

up to the order of its vertices. Hence, the dimension of the row space of $A_{K_{d,d}}$ is 2.

Thus, the only non-trivial eigenvalue is 0 and, of course, $0 \leq 2\sqrt{d-1}$. $\square$

We have all the pieces of the main result now, so let us prove it.

Theorem 5.4.4. *For every $d \geq 3$, there is an infinite family of d-regular bipartite Ramanujan graphs.*

Proof. Since $G = K_{d,d}$ is a d-regular Ramanujan graph (Lemma 5.4.3), given a signing, the spectrum of the 2-lift of G is the multiset union of the eigenvalues of G and the eigenvalues of the signed adjacency matrix by Proposition 5.1.4. Hence, to ensure the 2-lift is Ramanujan, it suffices to bound the eigenvalues of A_σ; equivalently, to bound the roots of its characteristic polynomial f_σ. We know that the characteristic polynomials $\{f_\sigma\}_{\sigma \in \{\pm 1\}^m}$ form an interlacing family (Corollary 5.4.2), hence, due to Theorem 5.3.7, there is a complete signing $\sigma \in \{\pm 1\}^m$ such that the largest root of f_σ is at most the largest root of $F_\emptyset$. By Definition 5.3.5 $F_\emptyset(x) = \sum_{\sigma \in \{\pm 1\}^m} f_\sigma(x)$, and by Theorem 5.2.4, $2^{-m}F_\emptyset(x) = \mu_G(x)$, where μ_G is the matching polynomial of G. The roots of $2^{-m}F_\emptyset(x)$ and $F_\emptyset(x)$ are of course the same. The roots of the matching polynomial all lie in the interval $[-2\sqrt{d-1}, 2\sqrt{d-1}]$ by Theorem 5.2.3. Our graph $G = K_{d,d}$ is bipartite, so its spectrum is symmetric around 0. Therefore, all eigenvalues of A_σ (the "new eigenvalues" in the 2-lift) also satisfy the Ramanujan inequality. Viz., the 2-lift of $G = K_{d,d}$ given this good signing σ (from Theorem 5.3.7) yields another d-regular bipartite Ramanujan graph with $2 \cdot (2d)$ vertices ($|V(K_{d,d})| = 2d$). Repeating this process infinitely, iterating 2-lifts one after the other, gives the infinite family of d-regular bipartite Ramanujan graphs. $\square$

5.5 Discussion

We want to relate the MSS result to expander families directly. In order to do this, we state a proposition about connectivity.

Proposition 5.5.1. *Let G be a d-regular graph. The multiplicity of its trivial eigenvalue d is 1 if and only if G is connect.*

Proof. ($\Longrightarrow$) Let A be the adjacency matrix of G. Then $A\mathbf{1} = d\mathbf{1}$, so d is an eigenvalue (Corollary 2.1.9).

If G is disconnected with $k \geq 2$ components, then (after reordering vertices) A is diagonal block matrix

$$A = \begin{pmatrix} A_1 & 0 & 0 \\ & \ddots & \\ 0 & 0 & A_k \end{pmatrix}.$$

Each component is d-regular, so for each i, the vector $\mathbf{1}_i$ (defined as 1's on component i, 0 elsewhere) satisfies

$$A\mathbf{1}_i = d\mathbf{1}_i.$$

These k vectors are linearly independent, so d has multiplicity at least $k \geq 2$.

Thus, if d has multiplicity 1, G must be connected.

($\Longleftarrow$) Now let G be a connected d-regular graph. Recall that its Laplacian matrix is defined as $L = dI - A$.

If $Ax = dx$, then $Lx = 0$. By Proposition 4.2.3,

$$x^\top Lx = \sum_{\{i,j\} \in E} (x_i - x_j)^2.$$

Thus $Lx = 0$ implies $x^\top Lx = 0$, so each term $(x_i - x_j)^2 = 0$, hence $x_i = x_j$ for every edge $\{i, j\}$.

Since G is connected, all coordinates of x are equal, so x is a scalar multiple of $\mathbf{1}$. Therefore the eigenspace for eigenvalue d is one-dimensional, and d has multiplicity 1. □

By Proposition 5.5.1, a d-regular graph is connected if and only if the eigenvalue d has multiplicity 1. In the MSS construction, we start from the connected graph $K_{d,d}$, for which d has multiplicity 1. At each 2-lift, the spectrum consists of the "old" eigenvalues together with the "new" eigenvalues coming from A_σ (consequence of Proposition 5.1.4). It is derived that, all new eigenvalues lie in the interval $[-2\sqrt{d-1}, 2\sqrt{d-1}]$, and hence have absolute value strictly less than d.

Therefore, the eigenvalue d continues to have multiplicity 1 throughout the iteration, so every graph in the family is connected. In particular, this infinite family forms a family of bounded-degree expanders.

The most lasting contribution of the Marcus–Spielman–Srivastava paper [MSS14] was the introduction of the method of interlacing families. The influence of this method, pioneered in the paper [MSS14], extends beyond the theory of Ramanujan graphs. Most notably, a follow-up paper by Marcus, Spielman, and Srivastava [MSS15] used the method for an affirmative solution to the Kadison–Singer problem, a long-standing problem in functional analysis posed in 1959.

5.6 Real-Rootedness of the Matching Polynomial and a Root-Bound

Recall, $\mu_G(x) = \sum_{k\geq 0}(-1)^k m_k(G)x^{n-2k}$, where G is an n-vertex graph and $m_k(G)$ is the number of k-edge matchings on G. We will prove that the matching polynomial μ_G of a graph G is real-rooted and, when G is d-regular, all roots of μ_G lie in $[-2\sqrt{d-1}, 2\sqrt{d-1}]$. Our proof will be based on the work of Godsil [God81]. Another reference is [Spi18]. Specifically, we will show that μ_G divides the matching polynomial of trees you can associate with paths on G.

Theorem 5.6.1. *If T is a tree with adjacency matrix A_T, its matching polynomial μ_T coincides with the characteristic polynomial of A_T.*

Proof. Let $|V(T)| = n$, and write $[n] = \{1, 2, \cdots, n\}$. We will show $\det(xI - A_T) = \mu_T(x)$. Like in the proof of Theorem 5.2.4, we begin by expanding the determinant by summing over permutations

$$\begin{aligned}\det(xI - A_T) &= \sum_{\pi\in S_n} \operatorname{sgn}\pi \prod_{a\in[n]} (xI - A_T)_{a,\pi(a)} \\ &= \sum_{\pi\in S_n} \operatorname{sgn}\pi x^{\operatorname{fix}\pi} \prod_{a:\pi(a)\neq a} (-A_T)_{a,\pi(a)}.\end{aligned}$$

We will not dwell on this last equality since it was explained (essentially in this form) in the proof of Theorem 5.2.4. We will show that the only permutations π which contribute to to this sum are involutions, that is, permutations satisfying $\pi\circ\pi = \mathrm{id}$.

If $\pi(\pi(a)) \neq a$ for some $a \in [n]$, then π must necessarily contain a cycle of length at least 3, so assuming π contains a cycle $(a_1\, a_2\, \ldots, a_k)$ with $k \geq 3$ and $\pi(a_i) = a_{i+1}$ for all $1 \leq i < k$ and $\pi(a_k) = a_1$. For this term to contribute to the sum it must be the case that $(A_T)_{a_i,a_{i+1}} = 1$ for $1 \leq i < k$ and $(A_T)_{a_1,a_k} = 1$. However, if $k \geq 3$, this results in a cycle in T, and trees have no cycles.

Hence the only permutations which contribute are involutions $\pi(\pi(a)) = a$, which correspond to permutations with only fixed points (1-cycles) and transpositions (2-cycles). These involutions can be decomposed as a product of disjoint cycles. Each 2-cycle that contributes a nonzero term correspond to an edge in the graph. Thus, the number of permutations with k 2-cycles is equal to the number of k-edge matchings (disjointness ensures it is a matching)[4]. As the sign of an involution with k 2-cycles is

[4]N.B., the identity permutation id is an involution containing only fixed points. So $\pi = \mathrm{id}$ implies $k = 0$.

$(-1)^k$, the coefficient of x^{n-2k} is $(-1)^k m_k(T)$, where $m_k(T)$ is the number of k-edge matchings on T.

Therefore,

$$\det(xI - A_T) = \sum_{k \geq 0} (-1)^k m_k(T) x^{n-2k} = \mu_T(x).$$

□

In light of this, we will bound the roots of $\det(xI - A_T)$. Of course, roots of $\det(xI - A_T)$ are the eigenvalues of A_T.

Lemma 5.6.2. *Let M be a nonnegative matrix and let s be the maximum row sum of M. Then for every eigenvalue λ of M, $|\lambda| \leq s$.*

Proof. If $Mv = \lambda v$, $v \neq 0$, and a is an index such that $|v_a| = \max_i |v_i|$ is the largest entry of v in absolute value, then

$$|\lambda||v_a| = |\lambda v_a| = |(Mv)_a| = \left| \sum_b M_{a,b} v_b \right| \leq \sum_b |M_{a,b} v_b| = \sum_b M_{a,b} |v_b| \leq s|v_a|,$$

where first inequality follows from the triangle inequality (and M is nonnegative, so $|M_{a,b}| = M_{a,b}$), and the last inequality follows from the definition of $|v_a|$ and s. Dividing the above by $|v_a| \neq 0$ yields the result. □

Note that Proposition 2.1.7 is implied by the above lemma.

Theorem 5.6.3. *Let T be a tree in which every vertex has degree at most $d \geq 2$. Then all eigenvalues of A_T lie in $[-2\sqrt{d-1}, 2\sqrt{d-1}]$.*

Proof. Choose any vertex $r \in V(T)$ to be the root of the tree T. Define the height map $h : V(T) \to \mathbb{Z}_{\geq 0}$ as $h(v) = \operatorname{dist}(r, v)$. In particular, $h(r) = 0$. Let D be the diagonal matrix such that

$$D_{a,a} = \left(\sqrt{d-1}\right)^{h(a)}.$$

Since $D_{a,a}$ is nonzero for every a, D is invertible, and $(D^{-1})_{a,a} = \frac{1}{D_{a,a}}$. Similar matrices have the same eigenvalues[5]. Therefore, A_T and DA_TD^{-1} have the same eigenvalues.

[5]This is an elementary fact from linear algebra. Its proof will be omitted. Intuitively, this should make sense since similar matrices should be thought of as the same linear map $T : V \to V$ on a vector space V, just in different bases. An eigenvalue, then, is a number λ such that for some nonzero (abstract) vector $v \in V$, we have $Tv = \lambda v$. This number λ is therefore independent of the choice of basis in representing the linear map as a matrix. However, the vector v may of course differ.

To finish the proof, we apply Lemma 5.6.2 to $M = DA_TD^{-1}$. Then

$$M_{u,v} = \begin{cases} (\sqrt{d-1})^{h(u)-h(v)} & \text{if } u \sim v \\ 0 & \text{otherwise.} \end{cases}$$

Because T is a tree, adjacent vertices differ in height by exactly 1. Every nonroot vertex u has one parent neighbor v (where $h(u) - h(v) = 1$ so then $M_{u,v} = \sqrt{d-1}$) and all other neighbors are children (where $h(u) - h(v) = -1$, so $M_{u,v} = \frac{1}{\sqrt{d-1}}$). We compute the row sums $R_u = \sum_{v \in N(u)} M_{u,v}$ for the three types of vertices in the tree.

The tree's root r has no parent and at most d children, so $R_r \leq \frac{d}{\sqrt{d-1}} \leq 2\sqrt{d-1}$. This inequality follows directly from the fact that $\frac{d}{\sqrt{d-1}} = \frac{d}{d-1}\sqrt{d-1}$ and $\frac{d}{d-1} \leq 2$ when $d \geq 2$.

Any leaf $u \neq r, \deg u = 1$ has no children and 1 parent so $R_u = \sqrt{d-1} \leq 2\sqrt{d-1}$.

Any intermediate vertex (not the root and not a leaf) $u \neq r, \deg u \geq 2$ has 1 parent and at most $d-1$ children, so $R_u \leq \sqrt{d-1} + \frac{d-1}{\sqrt{d-1}} = 2\sqrt{d-1}$. □

Lemma 5.6.4. *If G and H are graphs with disjoint vertex sets, then*

$$\mu_{G \cup H}(x) = \mu_G(x)\mu_H(x).$$

Proof. Every matching in $G \cup H$ is the union of a matching on G and a matching on H. Hence, $m_k(G \cup H) = \sum_{j=0}^{k} m_j(G) m_{k-j}(H)$. By a standard calculation, plugging this into $\mu_{G \cup H}(x)$, the lemma follows. □

In particular, if G is a disconnected graph with n components $G_1, \ldots, G_n$, then $\mu_G(x) = \prod_{i=1}^{n} \mu_{G_i}(x)$.

If $G = (V, E)$ is a graph and $a \in V$, then we will write $G - a$ to mean the graph $(V - \{a\}, E')$ where $E' = \{\{u, v\} \in E : u \neq a \text{ and } v \neq a\}$.

Lemma 5.6.5. *Let G be a graph and $a \in V(G)$. Then*

$$\mu_G(x) = x\mu_{G-a}(x) - \sum_{b \sim a} \mu_{G-a-b}(x).$$

Proof. All matchings on G can be split into two disjoint classes, those involving the vertex a and those that do not. Those k-edge matchings which include a connect a to some neighbor $b \in N(a)$. A k-edge matching including the edge $\{a, b\}$ can be written as the union of $\{a, b\}$ and a $(k-1)$-edge matching in the graph $G - a - b$. Hence, the number of matchings involving a is

$$\sum_{b \sim a} m_{k-1}(G - a - b).$$

Thus,

$$m_k(G) = m_k(G-a) + \sum_{b\sim a} m_{k-1}(G-a-b).$$

Multiplying both sides by $x^{n-2k}(-1)^k$ gives

$$x^{n-2k}(-1)^k m_k(G) = x \cdot x^{(n-1)-2k}(-1)^k m_k(G-a) - \sum_{b\sim a} x^{(n-2)-2(k-1)}(-1)^{k-1} m_{k-1}(G-a-b).$$

Summing yields the result. □

Path Trees

Let the *path tree* of a graph G starting at $a \in V(G)$, denoted $T_a(G)$, be the tree whose vertices correspond to paths in G starting at a which do not repeat any vertex. There is an edge between two paths if one path extends the other path by exactly 1 vertex.

Path trees are simple constructions. An examples makes this clear.

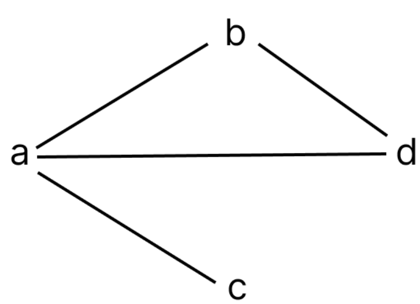


Figure 5.3: Example graph G.

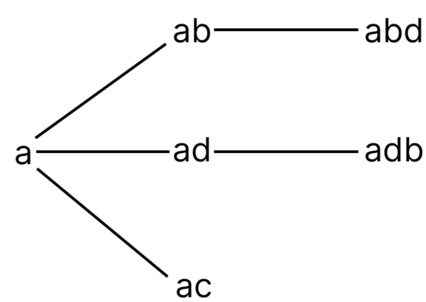


Figure 5.4: Path tree associated to vertex a, $T_a(G)$.

Proposition 5.6.6. *If T is a tree, then for any $a \in V(T)$ the path tree $T_a(T)$ is isomorphic to T.*

Proof. Since T is a tree, there is a unique path from u to v for any $u, v \in V(T)$. This makes the following map well-defined. Let $\psi : V(T) \to V(T_a(T))$ be a map sending a vertex $x \in V(T)$ to the a-to-x path in $T_a(T)$. Since paths in trees are necessarily unique, ψ is bijection.

If x is adjacent to y in T, then vertices $\psi(x)$ and $\psi(y)$ are adjacent in $T_a(T)$ when one of the corresponding paths is obtained from the other by appending one vertex. The a-to-x and a-to-y paths differ by exactly one, since $x \sim y$, so for any $a \in V(T)$,

$$\{x, y\} \in E(T) \iff \{\psi(x), \psi(y)\} \in E(T_a(T)).$$

□

The following is a somewhat strange equality that will be used to prove that the matching polynomial μ_G of a graph G divides $\mu_{T_a(G)}$ for any $a \in G$.

Theorem 5.6.7. *For any graph G and any vertex $a \in V(G)$,*

$$\frac{\mu_G}{\mu_{G-a}} = \frac{\mu_{T_a(G)}}{\mu_{T_a(G)-a}}.$$

Proof. First note that $\mu_{T_a(G)-a}$ is a forest obtained from removing the root of the path tree $T_a(G)$. Hence,

$$T_a(G) - a = \bigcup_{b \sim a} T_b(G - a). \tag{$\star$}$$

We induct on the number of vertices of G. All 1-vertex are trees. Note, if G is a tree, the left and right side of the equation in the theorem statement are identical by Proposition 5.6.6.

We induct on $n = |V(G)|$. Expanding the left-hand side by applying Lemma 5.6.5

$$\frac{\mu_G}{\mu_{G-a}} = \frac{x\mu_{G-a} - \sum_{b\sim a} \mu_{G-a-b}}{\mu_{G-a}} = x - \sum_{b \sim a} \frac{\mu_{G-a-b}}{\mu_{G-a}}.$$

The graph $G - a$ has $n - 1$ vertices, so by the induction hypothesis,

$$x - \sum_{b\sim a} \frac{\mu_{G-a-b}}{\mu_{G-a}} = x - \sum_{b\sim a} \frac{\mu_{T_b(G-a)-b}}{\mu_{T_b(G-a)}}.$$

Due to the line tagged ($\star$),

$$T_b(G - a) - b = \bigcup_{c\sim b, c\neq a} T_c(G - a - b), \tag{$\star\star$}$$

and

$$T_a(G) - a = \bigcup_{c\sim a} T_c(G - a).$$

It follows that

$$\mu_{T_a(G)-a} = \prod_{c\sim a} \mu_{T_c(G-a)}.$$

If $ab \in V(T_a(G))$ is the vertex for the path from a to b,

$$\begin{aligned} T_a(G) - a - ab &= \left(\bigcup_{c\sim a, c\neq b} T_c(G - a) \right) \cup \left(\bigcup_{c\sim b, c\neq a} T_c(G - a - b) \right) \\ &= \left(\bigcup_{c\sim a, c\neq b} T_c(G - a) \right) \cup (T_b(G - a) - b), \end{aligned}$$

by the line $(\star\star)$. This implies

$$\frac{\mu_{T_a(G)-a-ab}}{\mu_{T_a(G)-a}} = \frac{\left(\prod_{c\sim a, c\neq b} \mu_{T_c(G-a)}\right) \mu_{T_b(G-a)-b},}{\prod_{c\sim a} \mu_{T_c(G-a)}}$$
$$= \frac{\mu_{T_b(G-a)-b}}{\mu_{T_b(G-a)}}.$$

Putting this together, we obtain

$$\frac{\mu_G}{\mu_{G-a}} = x - \sum_{b\sim a} \frac{\mu_{T_a(G)-a-ab}}{\mu_{T_a(G)-a}}$$
$$= \frac{x\mu_{T_a(G)-a} - \sum_{b\sim a} \mu_{T_a(G)-a-ab}}{\mu_{T_a(G)-a}}$$
$$= \frac{\mu_{T_a(G)}}{\mu_{T_a(G)-a}}.$$

□

Theorem 5.6.8. *Let G be a connected graph. For every $a \in V(G)$, μ_G divides $\mu_{T_a(G)}$.*

Proof. Again we induct on the n number of vertices of G. If $n = 1$, G is a tree so for the vertex $a \in V(G)$, $G \cong T_a(G)$ by Proposition 5.6.6 (or trivially). This handles the base case.

Assume inductively that the claim holds for all connected graphs with fewer than n vertices. Since G is connected, every connected component C of $G - a$ contains at least one neighbor of a. For any neighbor $b \sim a$ belonging to a component C of $G-a$, the path tree $T_b(G-a)$ is simply $T_b(C)$. By the induction hypothesis, μ_C divides $\mu_{T_b(C)}$.

Since $T_a(G) - a = \bigcup_{b\sim a} T_b(G - a) = \bigcup_{b\sim a} T_b(C_b)$, its matching polynomial is $\mu_{T_a(G)-a} = \prod_{b\sim a} \mu_{T_b(C_b)}$. Because each component C of $G - a$ contains at least one $b \sim a$, $\mu_{G-a} = \prod_C \mu_C$ divides $\prod_{b\sim a} \mu_{T_b(C_b)} = \mu_{T_a(G)-a}$. Therefore,

$$\frac{\mu_{T_a(G)-a}}{\mu_{G-a}}$$

is a polynomial.

By Theorem 5.6.7,

$$\mu_{T_a(G)} = \frac{\mu_G}{\mu_{G-a}} \mu_{T_a(G)-a} = \mu_G \frac{\mu_{T_a(G)-a}}{\mu_{G-a}},$$

which finishes the proof. □

Corollary 5.6.9. *For any graph G, the matching polynomial μ_G is real-rooted. Furthermore, if G is d-regular and r a root of μ_G, then $|r| \leq 2\sqrt{d-1}$.*

Proof. Let $G_1, \ldots, G_k$ be the connected components of G. By Lemma 5.6.4, $\mu_G(x) = \prod_{i=1}^{k} \mu_{G_i}(x)$, so r is a root of μ_G if and only if r is a root of μ_{G_i} for some component G_i.

For each connected component G_i, pick a vertex $a_i \in V(G_i)$. By Theorem 5.6.8, there is a polynomial $q_i(x)$ such that

$$\mu_{T_{a_i}(G_i)}(x) = \mu_{G_i}(x) q_i(x).$$

Therefore, any root of μ_{G_i} is also a root of $\mu_{T_{a_i}(G_i)}$.

By Theorem 5.6.3, all roots of $\mu_{T_{a_i}(G_i)}$ are real and lie in the interval $[-2\sqrt{d_i - 1}, 2\sqrt{d_i - 1}]$, where d_i is the maximum degree of the vertices of $T_{a_i}(G_i)$ (which equals the maximum degree of G_i). Thus, every μ_{G_i} is real-rooted, making μ_G real-rooted.

If G is d-regular, every component G_i has maximum degree d, so the maximum degree of $T_{a_i}(G_i)$ is d. Hence, every root r of μ_G satisfies $|r| \leq 2\sqrt{d-1}$. $\square$

Bibliography

[Axl24] Sheldon Axler. *Linear Algebra Done Right*. Springer Cham, 2024. DOI: https://doi.org/10.1007/978-3-031-41026-0.

[BL06] Yonatan Bilu and Nathan Linial. “Lifts, discrepancy and nearly optimal spectral gap”. In: *Combinatorica* 26.5 (2006), pp. 495–519.

[Chu91] Fan R. K Chung. “Constructing random-like graphs”. In: *Proceedings of Symposia in Applied Mathematics* 44 (1991), pp. 21–55.

[Chu07] Fan R. K. Chung. *Four proofs for the Cheeger inequality and graph partition algorithms*. 2007. URL: https://api.semanticscholar.org/CorpusID:14788842.

[Chu97] Fan R. K. Chung. *Spectral Graph Theory*. American Mathematical Soc., 1997, 1997. ISBN: 9780821803158.

[God81] C. D. Godsil. “Matchings and walks in graphs”. In: *Journal of Graph Theory* 5.3 (1981), pp. 285–297. DOI: https://doi.org/10.1002/jgt.3190050310. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/jgt.3190050310. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/jgt.3190050310.

[GR01] Chris Godsil and Gordon Royle. *Algebraic Graph Theory*. Springer New York, NY, 2001. ISBN: 978-1-4613-0163-9. DOI: https://doi.org/10.1007/978-1-4613-0163-9.

[IR90] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. Springer New York, NY, 1990. DOI: https://doi.org/10.1007/978-1-4757-2103-4.

[KK] Marcin Kotowski and Michał Kotowski. *Lectures on expanders*. URL: https://marcin-kotowski.github.io/research/spectral.pdf.

[LPS88] Alexander Lubotzky, Ralph Phillips, and Peter Sarnak. “Ramanujan graphs”. In: *Combinatorica* 8.3 (1988), pp. 261–277.

[MSS14] Adam Marcus, Daniel A. Spielman, and Nikhil Srivastava. *Interlacing Families I: Bipartite Ramanujan Graphs of All Degrees*. 2014. arXiv: 1304.4132 [math.CO]. URL: https://arxiv.org/abs/1304.4132.

[MSS15] Adam W Marcus, Daniel A Spielman, and Nikhil Srivastava. "Interlacing families ii: Mixed characteristic polynomials and the kadison—singer problem". In: *Annals of Mathematics* (2015), pp. 327–350.

[Nil91] A. Nilli. "On the second eigenvalue of a graph". In: *Discrete Mathematics* 91.2 (1991), pp. 207–210. ISSN: 0012-365X. DOI: https://doi.org/10.1016/0012-365X(91)90112-F. URL: https://www.sciencedirect.com/science/article/pii/0012365X9190112F.

[Spi18] Daniel A. Spielman. *Matching Polynomials of Graphs*. 2018. URL: https://www.cs.yale.edu/homes/spielman/561/lect26-18.pdf.

[Sri14] Nikhil Srivastava. *Restricted Invertiblity by Interlacing Polynomial*. 2014. URL: https://windowsontheory.org/2014/04/15/restricted-invertiblity-by-interlacing-polynomials/.

[Ste12] Benjamin Steinberg. *Representation Theory of Finite Groups*. Springer New York, NY, 2012. ISBN: 978-1-4614-0776-8. DOI: https://doi.org/10.1007/978-1-4614-0776-8.

[Ter99] Audrey Terras. *Fourier Analysis on Finite Groups and Applications*. London Mathematical Society Student Texts. Cambridge University Press, 1999.

[Wat70] William C Waterhouse. "The sign of the Gaussian sum". In: *Journal of Number Theory* 2.3 (1970), p. 363. ISSN: 0022-314X. DOI: https://doi.org/10.1016/0022-314X(70)90065-X. URL: https://www.sciencedirect.com/science/article/pii/0022314X7090065X.

[Zha23] Yufei Zhao. *Graph Theory and Additive Combinatorics: Exploring Structure and Randomness*. Cambridge University Press, 2023. ISBN: 9781009310956. DOI: 10.1017/9781009310956.