AN EXPLICIT CONSTRUCTION OF AN EXPANDER FAMILY

IAN COLEY

Submitted 30 April 2013

Abstract. This paper proves that there exist infinite families of graphs which satisfy a uniform lower bound on their spectral gap. We first prove existence via a probabilistic method. The explicit construction involves various results from algebra and representation theory, which we explore at some length. It turns out that the expander family we construct achieves a maximal condition on expander families, though with our methods we cannot prove this fact.

Contents

1. Introduction

To begin with, we will present some basic definitions that will be necessary to discuss the central topic of this paper. In general, we will discuss finite, undirected, simple, and connected k-regular graphs. But we may start with some more general definitions and see how our specifications manifest themselves in their light.

Definition 1.1. Let $X = (V, E)$ be a finite, undirected graph, with vertex set $V = \{v_1, v_2, \ldots, v_n\}$. We define the *adjacency matrix* A of X to have entries $A_{ij} =$# of edges joining v_i to v_j.

If we assume that X is simple, then $A_{ii} = 0$ for all i and $A_{ij} \in \{0, 1\}$ for all $i \neq j$. Additionally, if A is k-regular then $\sum_{j \in V} A_{ij} = k$ for all i. A has a natural action on the function space $\ell^2(V)$, which we define as the set of functions $f : V \to \mathbb{C}$. We have an inner product on $\ell^2(V)$, where for $f, g \in \ell^2(V)$,

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

For $f \in \ell^2(V)$ and $v_i \in V$ as labeled above, we let

$$(Af)(v_i) = \sum_{j=1}^{n} A_{ij}\, f(v_j),$$

which is still certainly in $\ell^2(V)$. Thus A is a linear transformation on $\ell^2(V)$. Furthermore, every A is real and symmetric (because it is undirected), so by the spectral theorem has n real eigenvalues, which we may denote $\mu_0 \geq \mu_1 \geq \cdots \geq \mu_{n-1}$. With these eigenvalues are associated eigenfunctions in $\ell^2(V)$. Simple functions in this space will be enlightening when searching for particular bounds on the eigenvalues for a graph X, as in the following proposition.

Proposition 1.2. Let X be a finite, connected k-regular graph. Then $\mu_0 = k$ and corresponds to the constant eigenfunction $f = 1$. Further, $|\mu_j| \leq k$ for all j.

Proof. That k is the eigenvalue corresponding to $f = 1$ is trivial. However, we still need to prove that μ_0 is maximal among the eigenvalues of X. Therefore let g be a real-valued eigenfunction corresponding to some eigenvalue μ. Since X is finite, we can choose $x \in V$ such that

$$|g(x)| = \max_{y \in V} |g(y)|.$$

If $g(x) < 0$, then replace g by $-g$. Then

$$g(x)\,|\mu| = |g(x)\,\mu| = \left| \sum_{y \in V} A_{xy}\, g(y) \right| \leq \sum_{y \in V} A_{xy}\, |g(y)| \leq g(x) \sum_{y \in V} A_{xy} = g(x)\, k,$$

and cancelling $g(x)$ gives us $|\mu| \leq k$. Therefore $\mu_0 = k$ is the greatest eigenvalue. □

If X happens to be a bipartite graph, we can deduce more about its spectrum, following Proposition 1.1.4 of [2].

Proposition 1.3. Let X be a connected, k-regular graph on n vertices. Then the following are equivalent:

(i) X is bipartite.
(ii) The spectrum of X is symmetric about 0.
(iii) $\mu_{n-1} = -k$.

Proof. Recall that if X is bipartite, then we may let $V = V_+ \cup V_-$ with the following property: for all $x, y \in V$ such that $A_{xy} \neq 0$, if $x \in V_+$, then $y \in V_-$ (or vice versa). Let f be a real-valued eigenfunction corresponding to an eigenvalue μ. Then we define a function g such that

$$g(x) = \begin{cases} f(x) & \text{if } x \in V_+ \\ -f(x) & \text{if } x \in V_- \end{cases}.$$

First, assume $x \in V_+$. Then

$$(Ag)(x) = \sum_{y \in V} A_{xy}\, g(y) = -\sum_{y \in V_-} A_{xy}\, f(y) = f(x)(-\mu) = g(x)(-\mu).$$

If $x \in V_-$,

$$(Ag)(x) = \sum_{y \in V} A_{xy}\, g(y) = \sum_{y \in V_+} A_{xy}\, f(y) = f(x)\mu = g(x)(-\mu).$$

Thus g corresponds to the eigenvalue $-\mu$.

Now assume X has a symmetric spectrum. By Proposition 1.2, $\mu_0 = k$, so $\mu_{n-1} = -k$.

Finally, assume $\mu_{n-1} = -k$. Then let f be a real-valued eigenfunction corresponding to μ_{n-1}. As in the preceding proof, we may choose $x \in V$ such that $|f(x)| = \max_{y \in V} |f(y)|$ such that $f(x) > 0$. Then

$$f(x) = -\frac{1}{k}(Af)(x) = \sum_{y \in V} \frac{A_{xy}}{k}\, f(y) = \sum_{y \in V} \frac{A_{xy}}{k}(-f(y)).$$

Thus $f(x)$ is the sum of k terms each of which attain an absolute value less than $\frac{f(x)}{k}$. Thus $-f(y) = f(x)$ for all y satisfying $A_{xy} \neq 0$. Therefore replacing x with y in the above equation, we see any z satisfying $A_{yz} \neq 0$ must have $f(x) = -f(y) = f(z)$. Thus we may establish a bipartition given by $V_+ = \{x \in V : f(x) > 0\}$ and $V_- = \{x \in V : f(x) < 0\}$. This completes the proof. □

We call $\mu_0 - \mu_1 = k - \mu_1$ the *spectral gap* of a finite k-regular graph. To illustrate its importance, we examine the 'random walk' on the connected, k-regular graph X with n vertices. Start at an arbitrary vertex and at each step move to an adjacent vertex, each option with probability $\frac{1}{k}$. The probability of reaching a vertex v after N steps can be described as

$$\left(\frac{A}{k}\right)^N \delta_v(x),$$

where δ_v is the Dirac delta function for the vertex v. Because $\delta_v \in \ell^2(V)$, we may decompose it into a sum of eigenfunctions of A:

$$\delta_v = a_0 f_0 + \ldots + a_{n-1} f_{n-1}, \quad a_i = \langle f_i, \delta_v \rangle = \sum_{x \in V} f_i(x)\overline{\delta_v(x)} = f_i(v).$$

Substituting in this sum,

$$\left(\frac{A}{k}\right)^N \delta_v(x) = \frac{A^N}{k^N}\sum_{j=0}^{n-1} a_j f_j(x) = \sum_{j=0}^{n-1} \frac{a_j \mu_j^N}{k^N} f_j(x).$$

In particular, recall that $f_0(x) = \frac{1}{\sqrt{n}}$ is the constant (normed) eigenfunction on the graph. Then $a_0 = \frac{1}{\sqrt{n}}$ as well. By the above considerations, we know $|\mu_j| \leq k$ for all j. Assume that X is not bipartite, so that $\mu_{n-1} > -k$, and let $\eta = \max_{j\neq 0} \frac{|\mu_j|}{k} < 1$. Thus for all eigenvalues $\mu_j \neq k$,

$$\frac{\mu_j^N}{k^N} \leq \eta^N \to 0 \text{ as } N \to \infty.$$

As we take increasingly many steps, the probability of arriving at a vertex v is

$$\frac{a_0 \mu_0^N}{k^N} f_0(x) + \sum_{j=1}^{n-1} \frac{a_j \mu_j^N}{k^N} f_j(x) = \frac{1}{n} + O(\eta^N), \tag{1}$$

where $O(\eta^N)$ is the usual Big-O notation. So indeed, as $N \to \infty$, our walk becomes truly random. The rate at which the sum of Equation 1 decays is exponential, and this decay is quicker for smaller values of η. Thus a large spectral gap $k - \mu_1$ is important to quicker decay, as the more μ_{n-1} and μ_1 are bounded away from k, the more uniform the random walk after N steps.

As such, one of our primary concerns in this paper will be maximising this quantity. The process of calculating eigenvalues in the usual way is somewhat onerous, so we will look for another way to attack this problem through graph theoretical means.

To that end, we define the *boundary* of a subset $F \subset V$, denoted ∂F, to be the set of edges with one vertex in F and the other in $V \setminus F$. Note that $\partial F = \partial(V \setminus F)$.

Definition 1.4. We define the *expanding constant* of a (possibly infinite) graph X to be

$$h(X) = \inf\left\{\frac{|\partial F|}{\min\{|F|, |V \setminus F|\}} : F \subset V, 0 < |F| < +\infty\right\}.$$

If $|V| = n < +\infty$ (which it shall always be in this paper), it is equivalent to write

$$h(X) = \min\left\{\frac{|\partial F|}{|F|} : F \subset V, 0 < |F| \leq \frac{n}{2}\right\}.$$

Definition 1.5. Let $\{X_n\}_{n\in\mathbb{N}}$ be a family of finite, connected, k-regular graphs with $|V_n| \to +\infty$ as $n \to +\infty$. We say that $\{X_n\}$ is a *family of expanders* or *expander family* if there exists $\varepsilon > 0$ such that $h(X_n) \geq \varepsilon$ for all $n \in \mathbb{N}$.

As with the spectral gap, it is necessary to explore the importance of this quantity. The expanding constant of a graph quantitively describes its 'well-connectedness'. Though we assume throughout that our graphs are connected and k-regular, by no means do these two qualities imply a satisfactory degree of connectedness. Consider the cyclic graph C_n with $V = \{1, 2, \ldots, n\}$, and for convenience let n an even integer. C_n is connected and 2-regular, and it is easy to see the subgraph $F = \{1, 2, \ldots, \frac{n}{2}\}$ corresponds to the minimum boundary to subgraph ratio, namely $h(C_n) = \frac{4}{n}$. As $n \to \infty$, $h(C_n) \to 0$. Thus $\{C_n\}$ is not an expander family.

Consider now the complete graph K_n, again with n even for convenience, which is connected and $(n-1)$-regular. If $F \subset V$ with $|F| = \ell$, then $|\partial F| = \ell(n-\ell)$, corresponding to all possible pairings of $x \in F$ and $y \in V \setminus F$. Thus $h(K_n) = \frac{n}{2}$ by choosing any subgraph of order $\ell = \frac{n}{2}$. This establishes that $\{K_n\}$ acts like an expander family; $h(K_n) \to \infty$ as $n \to \infty$, but there is no bound on the degree of regularity. This still confirms our intuition that large $h(X)$ corresponds to well-connectedness.

What is most interesting is the interaction between the spectral gap and the expanding constant. Theorem 1.2.3 in [2] allows us to bound the expanding constant both above and below.

Theorem 1.6. Let $X = (V, E)$ be a finite, connected, k-regular graph without loops. Let μ_1 be as above. Then

$$\frac{k - \mu_1}{2} \leq h(X) \leq \sqrt{2k(k - \mu_1)}.$$

We omit the proof, despite its intrinsic interest. It follows from this theorem that we may rephrase our above definition of an expander family in terms of the spectral gap. This is stated explicitly as Corollary 1.2.4 in [2].

Corollary 1.7. $\{X_n\}$ is family of expanders if and only if there exists $\varepsilon > 0$ such that $k - \mu_1(X_n) \geq \varepsilon$ for all $n \in \mathbb{N}$.

Furthermore, the 'quality' of a family of expanders can be measured by maximising the spectral gap, since it bounds the expanding constant below. However, it is not obvious from the preceding discussion that expander families exist at all! It is a central focus of this paper not only to show that they exist, but also to construct explicitly an expander family.

Given that we would like to maximise the spectral gap, an important question is what the best possible maximum is. Theorem 1.3.1 in [2] gives us a strict upper bound for the spectral gap in expander families.

Theorem 1.8. Let $\{X_n\}_{n \in \mathbb{N}}$ be a family of finite, connected, k-regular graphs with $|V_n| \to +\infty$ as $n \to +\infty$. Then

$$\liminf_{n \to \infty} \mu_1(X_n) \geq 2\sqrt{k-1}.$$

This motivates the following definition.

Definition 1.9. A finite, connected, k-regular graph X is *Ramanujan* if $\mu_1 \leq 2\sqrt{k-1}$.

In words, a Ramanujan graph realises the maximum spectral gap for expander families. If we construct an expander family of Ramanujan graphs, then we know their expanding constants are bounded below by the largest value possible. In this sense, they are optimal with respect to their spectral properties. But we have not seen that a single Ramanujan graph exists, let alone an infinite family!

To illustrate their existence, we examine a particularly salient Ramanujan graph: the Petersen graph (Figure 1).

The Petersen graph is 3-regular, and we claim it satisfies $\mu_1 \leq 2\sqrt{2}$. Its eigenvalues may be calculated directly via its adjacency matrix, but we prefer the more clever method outlined in [3]. We see that $\mu_1 = 1$ and $|\mu_j| \leq 2\sqrt{2}$ for all $j \neq 0$. Thus the Petersen graph is Ramanujan and relatively well-connected for its low degree.

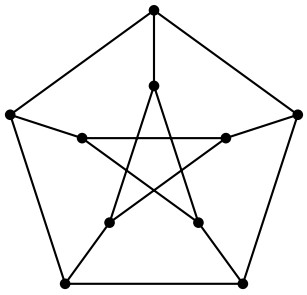

FIGURE 1. The Petersen graph.

Further, infinite families of Ramanujan graphs exist. The Ramanujan conjecture, cited at Remark 4.4.7 in [2], may be used to prove that the expander family constructed in this paper is indeed Ramanujan. Due to its complexity, we cannot include a full discussion, and leave exploration of this result to the reader.

Our first task will be to develop a firm vocabulary of graph theoretic concepts in order to address our main problem. With this basic understanding, we may prove the existence of expander families probabilistically. From there, we explore quaternion algebras and properties thereof, which are necessary for the backbone of the graphs of our explicit expander family. We construct the family in two isomorphic ways, each providing us with certain insights. Following a small result from representation theory, we complete the spectral analysis of our family of graphs and prove that it is an expander family.

By way of acknowledgements, first and foremost, this thesis would not exist without the advice and guidance of Simon Marshall. His outstanding knowledge of the topic and clear explanations allowed for a thorough examination of topics I had not seen before undertaking this work. Further thanks are due to Mike Stein for teaching me a solid mathematical foundation in algebra and Frank Calegari for being a second reader and graduate school advisor. Of my many peers who have been a part of this thesis, I would like to thank in particular Dan Kaplan for his companionship in our parallel undergraduate careers and Camille Beredjick for sharing her tea and her constant encouragement and life-friendship. Finally, outside of Northwestern, I would like to thank my grandmother, Clare Friedman, to whom I undoubtedly owe my interest in mathematics and ambition for graduate studies.

2. Preliminaries and the Probabilistic Method

2.1. **Motivation.**

Before moving into our construction, we will motivate the process by proving Theorem 1.8. Our goal is to define the trace formula of a graph and through it prove the asymptotic behaviour of the graph's eigenvalues.

Hereafter, let $X = (V, E)$ be an arbitrary finite k-regular simple graph with $|V| = n$ and adjacency matrix A. We say a path with origin x_0 and extremity x_r, which we denote $x_0, x_1, \ldots, x_r$ is *without backtracking* if $x_{i+1} \neq x_{i-1}$ for all $i \in \{1, \ldots, r-1\}$. We define a series of matrices A_r where

$$(A_r)_{xy} = \#\text{ of paths of length } r \text{ without backtracking with origin } x \text{ and extremity } y.$$

Given that $A_0 = \mathrm{Id}$ and $A_1 = A$, the following lemma allows us to recursively define A_r.

Lemma 2.1.

(i) $A_2 = A_1^2 - k \cdot \mathrm{Id}$.

(ii) For $r \geq 2$, $A_{r+1} = A_r A_1 - (k-1)\, A_{r-1}$.

Proof.

(i) Let $x, y \in V$. Then $(A_1^2)_{xy}$ is the number of all paths of length 2 between x and y. If $x \neq y$, we cannot have backtracking, thus $(A_1^2)_{xy} = (A_2)_{xy}$. If $x = y$, then the only way for a path of length 2 between x and itself is along of the exactly k edges connected to x, and is therefore found through backtracking. Thus we must subtract $k \cdot \mathrm{Id}$ to eliminate these choices, and thus $A_2 = A_1^2 - k \cdot \mathrm{Id}$ as required.

(ii) As above, let $x, y \in V$. Then $(A_r A_1)_{xy}$ is the number of paths of length $r+1$ between x and y without backtracking, except possibly at the last step. Let $x = x_0, \ldots, x_{r-1}, x_r, x_{r+1} = y$ be such a path. If $x_{r-1} \neq y$, then there cannot be backtracking and so $(A_{r+1})_{xy} = (A_r A_1)_{xy}$. However if $x_{r-1} = y$, then we have backtracking at the last step. There are $(k-1)(A_{r-1})_{xy}$ such paths and they must be deleted. This completes the proof.

□

We let

$$T_m = \sum_{0 \leq r \leq \frac{m}{2}} A_{m-2r}$$

for all $m \in \mathbb{N}$ and further define a series of polynomials which will expedite our proof.

Definition 2.2. The *Chebyshev polynomials of the second kind* are defined to be the degree m polynomials satisfying

$$U_m(\cos\theta) = \frac{\sin(m+1)\theta}{\sin\theta} \qquad (m \in \mathbb{N}).$$

We now prove Proposition 1.4.5 from [2] which relates U_m to T_m.

Proposition 2.3. For all $m \in \mathbb{N}$,

$$T_m = (k-1)^{\frac{m}{2}} U_m\left(\frac{A}{2\sqrt{k-1}}\right).$$

Proof. We use here the various lemmas from §1.4 of [2]. Based on the recursive definition of the matrices A_r, it can be easily checked by the above lemma that

$$\sum_{r=0}^{\infty} A_r t^r = \frac{1-t^2}{1 - At + (x-1)t^2}.$$

From this, we can calculate a similar equation for T_m.

$$\begin{aligned}
\sum_{m=0}^{\infty} T_m t^m &= \sum_{m=0}^{\infty} \sum_{0 \leq r \leq \frac{m}{2}} A_{m-2r} t^m = \sum_{r=0}^{\infty} \sum_{m \geq 2r} A_{m-2r} t^m = \sum_{r=0}^{\infty} t^{2r} \sum_{m \geq 2r} A_{m-2r} t^{m-2r} \\
&= \left(\sum_{r=0}^{\infty} t^{2r}\right)\left(\sum_{\ell=0}^{\infty} A_\ell t^\ell\right) = \frac{1}{1-t^2} \cdot \frac{1-t^2}{1 - At + (x-1)t^2} \\
&= \frac{1}{1 - At + (x-1)t^2}.
\end{aligned}$$

The Chebyshev polynomials also satisfy a recursive formula, namely $U_{m+1}(x) = 2x\,U_m(x) - U_{m-1}(x)$. Therefore, similar to the above, we may readily compute

$$\sum_{m=0}^{\infty} U_m(x)t^m = \frac{1}{1-2xt+t^2}.$$

Therefore we perform a change of variables to compare T_m and U_m. We send $x \mapsto \frac{x}{2\sqrt{k-1}}$ and $t \mapsto t\sqrt{k-1}$. Then

$$\sum_{m=0}^{\infty} U_m\left(\frac{x}{2\sqrt{k-1}}\right)\left(t\sqrt{k-1}\right)^m = \frac{1}{1-xt+(x-1)t^2}.$$

Replacing x by A shows that

$$\sum_{m=0}^{\infty}(k-1)^{\frac{m}{2}} U_m\left(\frac{A}{2\sqrt{k-1}}\right)t^m = \sum_{m=0}^{\infty} T_m t^m.$$

Therefore they must agree at every power of t, and the proof holds. □

As before, we let $\mu_0 = k \geq \mu_1 \geq \cdots \geq \mu_{n-1}$ be the eigenvalues of A. We are concerned with the trace of T_m, which we may write in two different ways. First, using a basis of eigenfunctions of A, we may write

$$\operatorname{Tr} T_m = (k-1)^{\frac{m}{2}} \sum_{j=0}^{n-1} U_m\left(\frac{\mu_j}{2\sqrt{k-1}}\right)$$

using the above equality. However, by the first definition of T_m,

$$\operatorname{Tr} T_m = \sum_{0\leq r\leq \frac{m}{2}} \operatorname{Tr} A_{m-2r} = \sum_{x\in V}\sum_{0\leq r\leq \frac{m}{2}} (A_{m-2r})_{xx}.$$

We let $f_{\ell,x}$ denote the number of paths of length ℓ in X which do not backtrack and both start and end at x. It is easy to verify $f_{\ell,x} = (A_\ell)_{xx}$. Then we may rewrite the above equation to obtain what Theorem 1.4.6 of [2] calls the *trace formula*:

Theorem 2.4. For all $m \in \mathbb{N}$,

$$\sum_{x\in V}\sum_{0\leq r\leq \frac{m}{2}} f_{m-2r} = (k-1)^{\frac{m}{2}} \sum_{j=0}^{n-1} U_m\left(\frac{\mu_j}{2\sqrt{k-1}}\right).$$

The right side of this equation is somewhat opaque, and that it is a nonnegative integer (because the left side must be) is by no means immediately clear. The exploration of this result is quite lengthy and occupies the next subsection of this paper.

2.2. **Analysis of the Trace Formula.**

We first establish the following property of the Chebyshev polynomials, following Proposition 1.4.8 of [2].

Proposition 2.5. Let $L \geq 2$ and $\varepsilon > 0$ be real numbers. There exists a constant $C = C(\varepsilon, L) > 0$ with the following property: for any probability measure ν on $[-L, L]$, such that

$$\int_{-L}^{L} U_m\left(\frac{x}{2}\right)\, d\nu(x) \geq 0$$

for every $m \in \mathbb{N}$, we have

$$\nu[2-\varepsilon, L] \geq C.$$

Proof. For the sake of notation, we let $X_m(x) = U_m\left(\frac{x}{2}\right)$ and note that these polynomials satisfy the recursive relation $X_{m+1}(x) = x\,X_m(x) - X_{m-1}(x)$ and that $X_m(2\cos\theta) = \frac{\sin(m+1)\theta}{\sin\theta}$. Thus the roots of X_m are $2\cos\frac{\ell\pi}{m+1}$ for $\ell \in \{1, \ldots, m\}$, and so the largest root of X_m is $\alpha_m = 2\cos\frac{\pi}{m+1}$.

We must first see how to multiply these polynomials.

Lemma 2.6. For $k \leq \ell$, $X_k X_\ell = \sum_{m=0}^{k} X_{k+\ell-2m}$.

We may prove this by induction on k. Because $X_0(x) = 1$ and $X_1(x) = x$, this lemma is trivial for the cases $k = 0, 1$. Then for $k \geq 2$,

$$\begin{aligned} X_k X_\ell &= (x\,X_{k-1} - X_{k-2})X_\ell \\ &= x\,(X_{k+\ell-1} + X_{k+\ell-3} + \cdots + X_{\ell-k+3} + X_{\ell-k+1}) \\ &\quad - (X_{k+\ell-2} + X_{k+\ell-4} + \cdots + X_{\ell-k+4} + X_{\ell-k+2}) \end{aligned}$$

Using the substitution $x\,X_m(x) = X_{m+1}(x) + X_{m-1}(x)$,

$$\begin{aligned} &= (X_{k+\ell} + X_{k+\ell-2}) + (X_{k+\ell-2} + X_{k+\ell-4}) \\ &\quad + \cdots + (X_{\ell-k+4} + X_{\ell-k+2}) + (X_{\ell-k+2} + X_{\ell-k}) \\ &\quad - (X_{k+\ell-2} + X_{k+\ell-4} + \cdots + X_{\ell-k+4} + X_{\ell-k+2}) \\ &= X_{k+\ell} + X_{k+\ell-2} + \cdots + X_{\ell-k+2} + X_{\ell-k} = \sum_{m=0}^{k} X_{k+\ell-2m}. \end{aligned}$$

We now examine the division of these polynomials.

Lemma 2.7.

$$\frac{X_m(x)}{x-\alpha_m} = \sum_{i=0}^{m-1} X_{m-1-i}(\alpha_m)\cdot X_i(x).$$

We prove this by multiplying through by the denominator. Recalling that $X_1(x) = x$,

$$\begin{aligned} &(x-\alpha_m)\left(\sum_{i=0}^{m-1} X_{m-1-i}(\alpha_m)\cdot X_i(x)\right) \\ &\quad = X_{m-1}(\alpha_m)X_1(x) + \sum_{i=1}^{m-1} X_{m-1-i}(\alpha_m)(X_{i+1}(x) + X_{i-1}(x)) \\ &\qquad - \sum_{i=0}^{m-1} X_{m-1-i}(\alpha_m)\alpha_m X_i(x) \\ &\quad = (X_{m-2}(\alpha_m) - X_{m-1}(\alpha_m)\alpha_m)X_0(x) \\ &\qquad + \sum_{i=1}^{m-2} \left(X_{m-i}(\alpha_m) + X_{m-i-2}(\alpha_m) - \alpha_m X_{m-1-i}(\alpha_m)\right) X_i(x) \\ &\qquad + \left(X_1(\alpha_m) - \alpha_m X_0(\alpha_m)\right) X_{m-1}(x) + X_0(\alpha_m)X_m(x). \end{aligned}$$

Because $X_0(\alpha_m) = 1$ and $X_1(\alpha_m) - \alpha_m X_0(\alpha_m) = 0$, the $X_{m-1}(x)$ term cancels in the last line. Additionally, by the recursion formula, all the coefficients in the sum in the penultimate line are 0. Finally, in the third to last line, we have $X_{m-2}(\alpha_m) - X_{m-1}(\alpha_m = -X_m(\alpha_m) = 0$, since α_m was the largest root of X_m. Thus our entire equality reduces to $X_0(\alpha_m)X_m(x) = X_m(x)$.

We now introduce another polynomial, Y_m, where we let

$$Y_m(x) = \frac{X_m(x)^2}{x - \alpha_m}.$$

Lemma 2.8. We claim that

$$Y_m = \sum_{i=0}^{2m-1} y_i \, X_i,$$

for some constants $y_i \geq 0$.

By Lemma 2.7, we have $Y_m = \sum_{i=0}^{m-1} X_{m-1-i}(\alpha_m) X_i \, X_m$. We now examine $\alpha_m = 2\cos\frac{\pi}{m+1}$. Note that as $m \to \infty$, α_m increases up to 2, which is positive. So for all $j < m$, because $\alpha_j < \alpha_m$ and α_j is the largest root of X_j, we must have $X_j(\alpha_m) > 0$. Hence all the coefficients $X_{m-1-i}(\alpha_m) > 0$. Furthermore, each $X_i \, X_m$ is a linear combination of $X_0, X_1, \ldots, X_{2m-1}$ by Lemma 2.6. Thus Y_m has the claimed presentation.

We may now complete the proof. Let ν be a probability measure on $[-L, L]$, $L \geq 2$, and assume by contradiction that $\nu[2 - \varepsilon, L] = 0$ for some $\varepsilon > 0$. This means that the support of ν is contained in $[-L, 2 - \varepsilon]$. Choose $m \in \mathbb{N}$ such that $\alpha_m > 2 - \varepsilon$. Since $Y_m(x) \leq 0$ for $x \leq \alpha_m$ (because its numerator is positive and denominator negative), we have $\int_{-L}^{L} Y_m(x) \, d\nu(x) \leq 0$. However, by Lemma 2.8 and the assumption on ν, $\int_{-L}^{L} Y_m(x) \, d\nu(x) \geq 0$. Therefore $\int_{-L}^{L} Y_m(x) \, d\nu(x) = 0$, which implies that ν is supported only in the set of zeroes of Y_m, namely the finite set $F_m = \left\{2\cos\frac{\ell\pi}{m+1} : \ell \in \{1, \ldots, m\}\right\}$. This clearly holds for all m satisfying $\alpha_m > 2 - \varepsilon$. Because $m+1$ and $m+2$ are relatively prime, we see that $\frac{\ell\pi}{m+1} \neq \frac{k\pi}{m+2}$ for any $\ell \in \{1, \ldots, m\}$ and $k \in \{1, \ldots, m+1\}$. Thus $F_m \cap F_{m+1} = \emptyset$, so the support of ν is empty. But this is impossible, and we reach a contradiction. This completes the proof. $\square$

If we are careful in choosing a measure ν, we may apply the preceding proposition to the case of finite, connected, k-regular graphs. This choice is made explicit in Theorem 1.4.9 of [2].

Theorem 2.9. For every $\varepsilon > 0$, there exists a constant $C = C(\varepsilon, k) > 0$ such that, for every connected, finite, k-regular graph X on n vertices, the number of eigenvalues of X in the interval $[(2 - \varepsilon)\sqrt{k-1}, k]$ is at least $C \cdot n$.

Proof. First, notice that we may let $L = \frac{k}{\sqrt{k-1}} \geq 2$. Choose

$$\nu = \frac{1}{n} \sum_{j=0}^{n-1} \delta_{\frac{\mu_j}{\sqrt{k-1}}},$$

where δ_α is the Dirac measure at $\alpha \in [-L, L]$ with the property that

$$\int_{-L}^{L} f(x) \, d\delta_\alpha(x) = f(\alpha)$$

for every continuous function f on $[-L, L]$. ν is clearly a probability measure on $[-L, L]$ and $\int_{-L}^{L} U_m(\frac{x}{2})\, d\nu(x) = \frac{1}{n}\sum_{j=0}^{n-1} U_m(\frac{\mu_j}{2\sqrt{k-1}})$ is nonnegative by the trace formula of Theorem 2.4. Therefore all the assumptions of the preceding proposition are met, so there exists $C > 0$ such that $\nu[2-\varepsilon, L] > C$. To interpret this result, this means we have

$$0 < C < \nu[2-\varepsilon, L] = \frac{1}{n} \cdot \left| \left\{ j : 2-\varepsilon \leq \frac{\mu_j}{\sqrt{k-1}} \leq L \right\} \right|$$

Multiplying through by n and reinterpreting the set of j, we have our conclusion:

$$C \cdot n < \#\text{ of eigenvalues of } X \text{ in the interval } \left[(2-\varepsilon)\sqrt{k-1}, k\right].$$

□

To finish our examination of the asymptotic behaviour of eigenvalues, we prove Theorem 1.4.10 of [2]. We give one definition first.

Definition 2.10. The *girth* of a graph, denoted $g(X)$, is defined to be the length of the shortest circuit in X, that is, the shortest path starting and ending at the same vertex.

While the statement of the theorem is somewhat technical, its meaning becomes apparent through the proof and subsequent corollary, 1.4.11 in [2].

Theorem 2.11. Let $(X_m)_{m\geq 1}$ be a sequence of connected, k-regular, finite graphs for which $g(X_m) \to \infty$ as $m \to \infty$. If $\nu_m = \nu(X_m)$ is the measure on $\left[-\frac{k}{\sqrt{k-1}}, \frac{k}{\sqrt{k-1}}\right]$ defined by

$$\nu_m = \frac{1}{|X_m|} \sum_{j=0}^{|X_m|-1} \delta_{\frac{\mu_j}{\sqrt{k-1}}}(X_m),$$

then, for every continuous function f on $\left[-\frac{k}{\sqrt{k-1}}, \frac{k}{\sqrt{k-1}}\right]$,

$$\lim_{m\to\infty} \int_{\frac{-k}{\sqrt{k-1}}}^{\frac{k}{\sqrt{k-1}}} f(x)\, d\nu_m(x) = \int_{-2}^{2} f(x)\sqrt{4-x^2}\, \frac{dx}{2\pi}.$$

In other words, the sequence of measures $(\nu_m)_{m\geq 1}$ on $\left[-\frac{k}{\sqrt{k-1}}, \frac{k}{\sqrt{k-1}}\right]$ weakly converges to the measure ν supported on $[-2, 2]$ given by $d\nu(x) = \frac{\sqrt{4-x^2}}{2\pi}\, dx$.

Proof. Let $L = \frac{k}{\sqrt{k-1}}$ and recall that $f_{\ell,x}$ was defined to be the number of non-backtracking paths starting and ending at $x \in V$. Fix some $n \geq 1$. If m is large enough such that $g(X_m) > n$, then

$$f_{n-2r,x} = 0$$

for all $x \in X_m$ and $0 \leq r \leq \frac{n}{2}$. Therefore for m large enough, the left-hand side of the trace formula is zero, and so the right hand side must be as well. Therefore

$$\int_{-L}^{L} U_n\left(\frac{x}{2}\right) d\nu_m(x) = \frac{1}{|X_m|} \sum_{j=0}^{|X_m|-1} U_n\left(\frac{\mu_j}{2\sqrt{k-1}}\right) = 0.$$

Because $U_0(x) = 1$, we also know

$$\int_{-L}^{L} U_0\left(\frac{x}{2}\right) d\nu_m(x) = \frac{1}{|X_m|} \sum_{j=0}^{|X_m|-1} U_0\left(\frac{\mu_j}{2\sqrt{k-1}}\right) = 1.$$

We may also compute $\int_{-L}^{L} U_n(x)\, d\nu$ using the change of variables $x \mapsto 2\cos\theta$.

$$\begin{aligned}\int_{-L}^{L} U_n\left(\frac{x}{2}\right) d\nu(x) &= \int_0^{\pi} U_n(\cos\theta) 2\sin^2\theta \,\frac{d\theta}{\pi} \\ &= \frac{1}{\pi}\int_0^{\pi} 2\sin((n+1)\theta)\sin\theta\, d\theta \\ &= \delta_0(n).\end{aligned}$$

Hence for any $n \geq 0$,

$$\lim_{m\to\infty} \int_{-L}^{L} U_n\left(\frac{x}{2}\right) d\nu_m(x) = \int_{-L}^{L} U_n\left(\frac{x}{2}\right) d\nu(x).$$

Based on the recursion formula of the Chebyshev polynomials in Proposition 2.3, we see that linear span of $U_0(\frac{x}{2}), U_1(\frac{x}{2}), \ldots, U_n(\frac{x}{2})$ is equal to the space of polynomials of degree n or less. Thus, by the linearity of the integral, for any $p(x)$ with $\deg p \leq n$,

$$\lim_{m\to\infty} \int_{-L}^{L} p(x)\, d\nu_m(x) = \int_{-L}^{L} p(x)\, d\nu(x).$$

Now fix $\varepsilon > 0$. Given that polynomials are dense in continuous functions, for any continuous $f(x)$, choose $p(x)$ such that $|f(x) - p(x)| < \varepsilon$ for all $x \in [-L, L]$. We proceed in the usual $\frac{\varepsilon}{3}$ fashion.

$$\begin{aligned}&\left|\int_{-L}^{L} f(x)\, d\nu_m(x) - \int_{-L}^{L} f(x)\, d\nu(x)\right| \\ &\qquad \leq \left|\int_{-L}^{L} (f(x) - p(x))\, d\nu_m(x)\right| + \left|\int_{-L}^{L} p(x)\, d\nu_m(x) - \int_{-L}^{L} p(x)\, d\nu(x)\right| \\ &\qquad\qquad + \left|\int_{-L}^{L} (f(x) - p(x))\, d\nu(x)\right|.\end{aligned}$$

The first and third quantities may be made as small as necessary because ν_m and ν are probability measures. By the limit above, the second quantity can also be made small for sufficiently large m. Choosing $M > 0$ large enough such that $\frac{\varepsilon}{3}$ for each, we see that

$$\left|\int_{-L}^{L} f(x)\, d\nu_M(x) - \int_{-L}^{L} f(x)\, d\nu(x)\right| < \varepsilon,$$

as required, and we are done. □

Corollary 2.12. Let $(X_m)_{m\geq 1}$ be a family of connected, k-regular, finite graphs, with $g(X_m) \to \infty$ as $m \to \infty$. For every $\varepsilon > 0$, there exists a constant $C \geq 0$ such that the number of eigenvalues of X_m in the interval $[-k, (-2+\varepsilon)\sqrt{k-1}]$ is at least $C|X_m|$.

Proof. We keep the notation of the above proof. Define the function

$$f(x) = \begin{cases} 1 & x \in \left[\frac{-k}{\sqrt{k-1}}, -2\right] \\ 0 & x \in \left[-2+\varepsilon, \frac{k}{\sqrt{k-1}}\right] \end{cases}$$

and f interpolates linearly between 1 and 0 on $[-2, -2+\varepsilon]$. For every $m \geq 1$,

$$\nu_m \left[-\frac{k}{\sqrt{k-1}}, -2+\varepsilon\right] \geq \int_{-\frac{k}{\sqrt{k-1}}}^{\frac{k}{\sqrt{k-1}}} f(x)\, d\nu_m(x).$$

By the previous result, letting $m \to \infty$, we have

$$\liminf_{m\to\infty} \nu_m \left[-\frac{k}{\sqrt{k-1}}, -2+\varepsilon\right] \geq \int_{-2}^{2} f(x)\, d\nu(x).$$

Putting this in words, we have

$$\liminf_{m\to\infty} \frac{1}{|X_m|} \cdot \left(\#\text{ of eigenvalues of } X_m \text{ in } [-k, (-2+\varepsilon)\sqrt{k-1}]\right) \quad \geq \quad \int_{-2}^{2} f(x)\, d\nu(x).$$

The proof follows. □

These results provide us a full picture of the asymptotic behaviour of eigenvalues of expander families with unbounded girth, which is not a particularly restrictive condition. As $m \to \infty$, a positive proportion of eigenvalues falls within any subinterval of the Ramanujan interval $[-2\sqrt{k-1}, 2\sqrt{k-1}]$, and the portion falling outside it goes to zero. Thus it is easy to characterise the 'location' of the eigenvalues of the graph in bulk by appealing to a measure argument, but difficult to find the location of any particular eigenvalue. Bearing this in mind, we are able to begin our first proof that expander families exist.

3. The Probabilistic Method

We will now take our first step to realising an actual expander family by constructing one through probabilistic means.

We follow the method prescribed in section 3.1.2 of [6]. Let I and O be two vertex sets of size n, where we will let $n \to \infty$. We will construct a k-regular bipartite graph $X = (V, E)$ such that $V = I \cup O$ and for every $e \in E$, e has one vertex in I and the other in O. We will assume $k \geq 5$ for the duration of this proof.

Label the vertices $V = \{1_i, 1_o, \ldots, n_i, n_o\}$, where $j_i \in I$ and $j_o \in O$. Let $\pi = \{\pi_1, \ldots, \pi_k\}$ be a set of permutations in $\mathcal{S}_n$, the symmetric group on n elements, and define the edges of X by joining j_i to $\pi_r(j)_o$ for each $j \in \{1, \ldots, n\}$ and $r \in \{1, \ldots, k\}$. This makes X a k-regular bipartite graph, and we claim that almost all choices of π will yield a graph X_π satisfying $h(X_\pi) \geq c$ for some fixed $2 \geq c > 1$. Note that while there are $(n!)^k$ choices for π, not every X_π will be distinct.

Let $\Pi = \{\pi = (\pi_1, \ldots, \pi_k) : \pi_r \in \mathcal{S}_n\}$, and let $\mathcal{B}$ be the set of 'bad' π, that is there exists some $A \subset I$ with $|A| \leq n/2$ and some $B \subset O$ with $|B| \leq c\,|A|$ such that $\pi_r(A) \subset B$ for $r = 1, \ldots, k$. We would like to bound $|\mathcal{B}|$ above. To that end, we will try to calculate

the number of $\pi \in \mathcal{B}$ which fail for a given $A \subset I$ and $B \subset O$. Let $|A| = t \leq n/2$ and $t \leq |B| = m \leq c\,t$. Then the number of $\pi \in \Pi$ which fail corresponding to these A and B is

$$\left(\frac{m!\,(n-t)!}{(m-t)!}\right)^k.$$

Therefore we can bound $|\mathcal{B}|$ above thus:

$$\begin{aligned}
|\mathcal{B}| &\leq \sum_{t\leq n/2} \sum_{t\leq m\leq c\,t} \binom{n}{t}\binom{n}{m}\left(\frac{m!\,(n-t)!}{(m-t)!}\right)^k \\
&= \sum_{t\leq n/2c} \sum_{t\leq m\leq c\,t} \binom{n}{t}\binom{n}{m}\left(\frac{m!\,(n-t)!}{(m-t)!}\right)^k \\
&\qquad + \sum_{n/2c\leq t\leq n/2} \sum_{t\leq m\leq c\,t} \binom{n}{t}\binom{n}{m}\left(\frac{m!\,(n-t)!}{(m-t)!}\right)^k \\
&= X + Y.
\end{aligned}$$

We write X, Y to further examine these two quantities (respectively) separately. Now,

$$X \leq (c-1)t \sum_{t\leq n/2c} \binom{n}{t}\binom{n}{c\,t}\left(\frac{(c\,t)!\,(n-t)!}{((c-1)t)!}\right)^k \leq \frac{n^2}{4c}\,X', \text{ where}$$

$$X' = \max_{t\leq n/2c}\left\{X_t = \binom{n}{t}\binom{n}{c\,t}\left(\frac{(c\,t)!\,(n-t)!}{((c-1)t)!}\right)^k\right\}.$$

For $k \geq 5$, X_t is maximal for $t = 1$, so we have

$$X \leq \frac{n^2}{4c}\cdot n \cdot \binom{n}{2}(2!(n-1)!)^k \leq n^4((n-1)!)^k.$$

As n gets large, we can examine the ratio of number of bad graphs of type X to the total Π to see

$$\lim_{n\to\infty}\frac{X}{|\Pi|} \leq \lim_{n\to\infty}\frac{n^4((n-1)!)^k}{(n!)^k} \leq \lim_{n\to\infty}\frac{1}{n^{k-4}} = 0,$$

where we bear in mind that we assumed $k \geq 5$.

To examine Y,

$$\begin{aligned}
Y &\leq (c-1)t \sum_{n/2c\leq t\leq n/2} \binom{n}{t}\binom{n}{c\,t}\left(\frac{(c\,t)!\,(n-t)!}{((c-1)t)!}\right)^k \\
&\leq 2^{2n}\,n \sum_{n/2c\leq t\leq n/2}\left(\frac{(c\,t)!\,(n-t)!}{((c-1)t)!}\right)^k \leq 2^{2n}\,n^2\,Y', \text{ where}
\end{aligned}$$

$$Y' = \max_{n/2c\leq t\leq n/2}\left\{Y_t = \left(\frac{(c\,t)!\,(n-t)!}{((c-1)t)!}\right)^k\right\}.$$

Y_t achieves a maximum at either $t = \frac{n}{2c}$ or $t = \frac{n}{2}$. Using Stirling's formula, we can verify that either choice still yields

$$\lim_{n\to\infty} \frac{Y}{|\Pi|} = 0.$$

Therefore we conclude that

$$\lim_{n\to\infty} \frac{|\mathcal{B}|}{|\Pi|} \leq \lim_{n\to\infty} \frac{X+Y}{|\Pi|} = 0.$$

So as n gets large, almost all choices for $\pi \in \Pi$ yield a graph X_π satisfying $h(X_\pi) \geq c$. This yields, without an explicit construction, families of expanders satisfying lower bounds on their expanding constants. We will now move to the explicit construction of an expander family of Ramanujan graphs. To do that, however, we will need first to explore the quaternion algebras over rings and fields.

4. Quaternion Algebras

4.1. **Examples and Categorisation.**

We now state the definition of a quaternion algebra over a general field F with characteristic $\neq 2$, as given in Definition 2.1.1 of [5].

Definition 4.1. A *quaternion algebra* A over F is a four-dimensional F-space with basis vectors 1, i, j, and k, where multiplication is defined on A by requiring that 1 is a multiplicative identity element, that

$$i^2 = a\,1, \quad j^2 = b\,1, \quad ij = -ji = k$$

for some a and b in $F^\times$ and by extending the multiplication linearly so that A is an associative algebra over F. It is denoted by the Hilbert symbol

$$\left(\frac{a,b}{F}\right).$$

Further note that $k^2 = (ij)^2 = -ab$, and that the elements i, j, and k anti-commute. A notable quaternion algebra is the usual Hamiltonian quaternions

$$\mathbb{H}(\mathbb{R}) = \{x_0 + x_1 i + x_2 j + x_3 k : i^2 = j^2 = ijk = -1, x_i \in \mathbb{R}\} = \left(\frac{-1,-1}{\mathbb{R}}\right).$$

Additionally, for any field F, we have the matrix algebra

$$M_2(F) \cong \left(\frac{1,1}{F}\right),$$

where we use

$$i = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad j = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad k = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

We state a few elementary facts following Lemma 2.1.2 of [5] but providing a different proof. The proof for (iii) is drawn from Theorem 1.5 of [1].

Lemma 4.2.

(i) $\left(\frac{a,b}{F}\right) \cong \left(\frac{ax^2,by^2}{F}\right)$ for any $a, b, x, y \in F^\times$.

(ii) The centre of $\left(\frac{a,b}{F}\right)$ is $F\,1 \cong F$.

(iii) $\left(\frac{a,b}{F}\right)$ is a simple algebra, that is, it has no proper two-sided ideals.

Proof.

(i) Let $A = \left(\frac{a,b}{F}\right)$ and $A' = \left(\frac{ax^2,by^2}{F}\right)$. Define a map $\varphi : A' \to A$ extending linearly from the basis elements of A', with $1 \mapsto 1$, $i \mapsto xi$, $j \mapsto yj$, and (as required by the previous two) $k \mapsto xyk$. We see that $(xi)^2 = ax^2$, $(yj)^2 = by^2$, and $(xi)(yj) = (xy)(ij) = -(yx)(ji) = -(yj)(xi)$. Thus φ must properly be a F-algebra isomorphism.

(ii) First, take any $x_0 \in F$, which we identify with $x = x_0\,1 \in F\,1$. Then for any element $y = y_0 + y_1 i + y_2 j + y_3 k$, we have

$$xy = x_0y_0 + x_0y_1i + x_0y_2j + x_0y_3k = y_0x_0 + y_1ix_0 + y_2jx_0 + y_3kx_0 = yx,$$

so $F\,1$ is contained in the centre of $\left(\frac{a,b}{F}\right)$. Now assume there exists $y_0+y_1i+y_2j+y_3k = y \in Z(A) \setminus F\,1$. Then $i \cdot y = y \cdot i$, so $-y_1 + y_0i - y_3j + y_2k = -y_1 + y_0i + y_3j - y_2k$, which implies $y_2 = y_3 = 0$. Similarly, $j \cdot y = y \cdot j$ shows that $y_1 = 0$. Thus no such y exists and $Z(A) = F\,1$.

(iii) If I is a nonzero ideal, then let $x = x_0 + x_1i + x_2j + x_3k \in I$. If $x = x_0$, then $x_0 \cdot x_0^{-1} = 1 \in I$, and we are done. Similarly if $x = x_1i$, then $i \cdot x \in I \cap F^\times$ and $I = A$ again. The same holds for $x = x_2j$ and $x = x_3k$.

Therefore assume without loss of generality that x has both $x_0 \neq 0$ and $x_1 \neq 0$. Then $x \cdot j - j \cdot x = 2x_1k - 2x_3i \in I$, and hence $\frac{1}{2}j(2x_1k - 2x_3i) = x_1i + x_3k \in I$. Therefore $x-(x_1i+x_3k) = x_0+x_2j \in I$ as well. By similar means $x_0+x_1i, x_0+x_3k \in I$. Finally,

$$x - (x_0 + x_1i) - (x_0 + x_2j) - (x_0 + x_3k) = -2x_0 \in I.$$

Because $x_0 \neq 0$, $-2x_0 \in F^\times$. Thus, as before, $1 \in I$ so $I = A$.

□

The extent of the utility of the following definition will become apparent in the subsequent discussion of quadratic forms, but it is somewhat helpful immediately.

Definition 4.3. We define the subspace of *pure quaternions* of A, denoted A_0, by the subspace spanned by the basis elements $\{i, j, k\}$.

Additionally, it can be shown that every $x \in A$ has a unique decomposition $x = a + \alpha$ where $a \in F$ and $\alpha \in A_0$. We have a conjugation operation on $x \in \left(\frac{a,b}{F}\right)$ given by

$$x_0 + x_1i + x_2j + x_3k \mapsto x_0 - x_1i - x_2j - x_3k.$$

Equivalently, if we let $x = a + \alpha$ as above, the conjugation operation is defined as $a + \alpha \mapsto a - \alpha$. It is easy to verify that $\overline{x + y} = \overline{x} + \overline{y}$ and $\overline{xy} = \overline{y}\,\overline{x}$. We define the *(reduced) norm* of x by $N(x) = x\overline{x}$, and it is straightforward to verify that $N(xy) = N(x)N(y)$. We make the further definition of the *(reduced) trace* of x by $\mathrm{tr}(x) = x + \overline{x}$. Both the norm and trace of x lie in the base field F. If we examine $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(F)$, the matrix algebra over F, we see the definition of the conjugation operator must be

$$\overline{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

This gives

$$N(\alpha) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} = (ad-bc) \cdot I,$$

where I is the identity matrix in $M_2(F)$. Similarly,

$$\mathrm{tr}(\alpha) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} a+d & 0 \\ 0 & a+d \end{pmatrix} = (a+d) \cdot I.$$

Thus norm and trace of a general element in a quaternion algebra are consistent with the determinant and trace of a matrix, respectively.

Henceforth let A be a quaternion algebra over F. Let $w \in A$ and examine the polynomial $f(X) = X^2 - \mathrm{tr}(w)X + N(w) \in F[X]$. By definition, we see that $f(w) = w^2 - [(w+\overline{w})w] + w\overline{w} = 0$. Let $F(w)$ be the smallest subalgebra of A containing $F\,1$ and w so that $F(w)$ is commutative. If we assume A is a division algebra, then f reduces over F if and only if $w \in F\,1$. Thus if we choose $w \notin F\,1$, then $F(w) = E$ is a quadratic field extension of F. Of course, A need not be a division algebra; we gave above that the matrix algebra $M_2(F)$ is always a quaternion algebra of F. Indeed, these are the only non-division quaternion algebras, and this is a consequence of Wedderburn's Structure Theorem, found at 2.9.6 in [5], which we state below.

Theorem 4.4. Let A be a simple algebra of finite dimension over the field F. Then A is isomorphic to the matrix algebra $M_n(D)$, where $D \cong \mathrm{End}_A(N)$ is a division algebra with N a minimal right ideal of A. The integer n and the division algebra D are uniquely determined by A.

The proof goes outside the scope of our discussion, but the theorem is necessary for the full categorisation of quaternion algebras. The dimension of $M_n(D)$ over F is mn^2, where $m = \dim_F(D)$. Because $\dim_F(A) = 4$, we only have the choices $m = 1, n = 2$ and $m = 4, n = 1$. The latter option corresponds to the case where A itself is a division algebra, and the former to the (unique) matrix algebra $M_2(F)$. This is summarised in Theorem 2.1.7 of [5].

Theorem 4.5. If A is a quaternion algebra over F, then A is a division algebra or $A \cong M_2(F)$.

We may go one step further in our characterisation, this time depending on the Skolem Noether Theorem, stated at 2.9.8 in [5].

Theorem 4.6. Let A be a finite-dimensional central simple algebra over F and let B be a finite-dimensional simple algebra over F. If $\varphi, \psi : B \to A$ are algebra homomorphisms, then there exists an invertible element $c \in A$ such that $\varphi(b) = c^{-1}\psi(b)c$ for all $b \in B$.

Again, we omit the proof. But now we may prove this useful result, stated in Theorem 2.1.8 of [5].

Theorem 4.7. Every four-dimensional central simple algebra over a field F of characteristic $\neq 2$ is a quaternion algebra.

Proof. Let A be a four-dimensional central simple algebra over F. If A is isomorphic to $M_2(F)$, then it is a quaternion algebra. Therefore assume A is a division algebra. Then

as discussed above, for $w \notin F$, $F(w) = E$ is a commutative subalgebra of A, and indeed $F(w) \subset A$ is still a division algebra. Therefore $F(w)$ is a field.

Choose $w' \in A \setminus F(w)$, which is nonempty. The centre of A is F and the centre of $F(w)$ is $F(w) \supset F$. It is clear that $\{1, w, w', ww'\}$ is an independent set over F, and thus these elements form a basis for A over F. Thus we may write

$$w^2 = x_0 + x_1 w + x_2 w' + x_3 ww',$$

where $x_i \in F$. But since $w' \notin F(w)$, we must have $x_2 = x_3 = 0$, so we write $w^2 = x_0 + x_1 w$. Thus w satisfies a quadratic polynomial in $F[X]$ and $F(w) = E$ is a quadratic extension of F. Thus we may choose an element $y \in E$ such that $y^2 = a \in F$ and $E = F(y)$.

Let φ be the automorphism on E sending y to $-y$ and let ψ be the identity automorphism. Then by the Skolem Noether theorem, there exists $z \in E$ such that $\varphi(y) = z^{-1}\psi(y)z$, that is $-y = z^{-1}yz$. Clearly this $z \notin E$ since it does not commute with $y \in E$ and thus $\{1, y, z, yz\}$ is independent over F. But $z^{-2}yz^2 = y$, and because y generates E, we have $z^2 \in F$, and we let $z^2 = b$. Therefore A has $\{1, y, z, yz\}$ as a basis with $y^2 = a, z^2 = b$, and so $A \cong \left(\frac{a,b}{F}\right)$. $\square$

We now extend our discussion to quadratic forms on quaternion algebras and how they allow fuller characterisation of a given quaternion algebra given its underlying field.

4.2. **Quadratic Forms.**
Let A again be a quaternion algebra over F. We now introduce the norm form of a quaternion algebra and show how it may be used to characterise a given quaternion algebra as a division algebra or the matrix algebra $M_2(F)$. Define the quadratic form $B : A \to F$, depending on the norm N, by

$$B(x, y) = \frac{1}{2}[N(x + y) - N(x) - N(y)] = \frac{1}{2}[x\overline{y} + y\overline{x}].$$

This form is symmetric and bilinear, and it is easy to see that the standard basis $\{1, i, j, k\}$ for A is orthogonal with respect to B. We say the pair (A, B) is a *quadratic space* with respect to this map. Further, we see that $B(x, x) = N(x)$, and we recall that the space A is called *isotropic* if there exists a nonzero $x \in A$ such that $N(x) = 0$. Otherwise we call A *anisotropic*. These definitions allow us to determine more easily if a given quaternion algebra is the matrix algebra. We follow Theorem 2.3.1 of [5].

Theorem 4.8. Let $A \cong \left(\frac{a,b}{F}\right)$. Then the following are equivalent:

(i) $A \cong M_2(F) \cong \left(\frac{1,1}{F}\right)$.
(ii) A is not a division algebra.
(iii) A is isotropic as a quadratic space with respect to N.
(iv) A_0 is isotropic as a quadratic space with respect to N.
(v) The quadratic form $ax^2 + by^2 = 1$ has a solution with $(x, y) \in F \times F$.

Proof. (i) $\iff$ (ii) was already shown in Theorem 4.5.

To see (ii) $\implies$ (iii), assume that A is not a division algebra. Then there exist nonzero $x, y \in A$ such that $xy = 0$. Then $N(xy) = N(x)N(y) = 0 \in F$, but because F is a field, this implies that one of $N(x)$ and $N(y)$ equals 0. Thus A is isotropic.

To see (iii) $\implies$ (iv), choose a nonzero element $x \in A$ with $N(x) = 0$. Write $x = x_0 + x_1 i + x_2 j + x_3 k$. If $x \in A_0$ we are done, so assume that $x_0 \neq 0$ and some $x_i \neq 0$ as well

for $i \in \{1,2,3\}$. Assume without loss of generality that $x_1 \neq 0$. Then since $0 = N(x) = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2$, we have the relation $x_0^2 - bx_2^2 = ax_1^2 + abx_3^2$. Then define $y \in A_0$ by

$$y = b(x_0x_3 + x_1x_2)i + a(x_1^2 - bx_3^2)j + (x_0x_1 + bx_2x_3)k.$$

Then by straightforward but lengthy calculation we see

$$N(y) = -a[b(x_0x_3 + x_1x_2)]^2 - b[a(x_1^2 - bx_3^2)]^2 + ab[x_0x_1 + bx_2x_3]^2 = 0.$$

Assume that A_0 is anisotropic. Then $y = 0$, so the coefficient of its j term $ax_1^2 - abx_3^2 = 0$. Let $z = x_1i + x_3k$. Then $N(z) = -ax_1^2 + abx_3^2 = -(ax_1^2 - abx_3^2) = 0$. But since we assumed A_0 is anisotropic, we must have $x_1 = x_3 = 0$, which is a contradiction. Thus A_0 is isotropic.

To see (iv) $\implies$ (v), if we assume A_0 is isotropic, then there exists $x = x_1i + x_2j + x_3k$ such that $N(x) = -ax_1^2 - bx_2^2 + abx_3^2 = 0$, i.e. $abx_3^2 = ax_1^2 + bx_2^2$. We may assume that at least two of $x_1, x_2, x_3 \neq 0$. First assume $x_3 \neq 0$. Then

$$a\left(\frac{x_2}{ax_3}\right)^2 + b\left(\frac{x_1}{bx_3}\right)^2 = \frac{ax_1^2 + bx_2^2}{abx_3^2} = 1,$$

so we have a solution to $ax^2 + by^2 = 1$. Now assume $x_3 = 0$. Then $ax_1^2 + bx_2^2 = 0$. Thus

$$\begin{aligned} a\left(\frac{1+a}{2a}\right)^2 + b\left(\frac{x_2(1-a)}{2ax_1}\right)^2 &= \frac{(ax_1^2 + bx_2^2)(a^2+1) + 2a(ax_1^2 - bx_2^2)}{4a^2x_1^2} \\ &= \frac{2a(2ax_1^2)}{4a^2x_1^2} = 1, \end{aligned}$$

so again we have a solution to $ax^2 + by^2 = 1$.

Finally, to see (v) $\implies$ (ii), let x, y be as above. Then let $\alpha \in A$ such that $\alpha = 1 + xi + yj$. Then

$$N(\alpha) = \alpha\overline{\alpha} = 1 - ax^2 - by^2 = 1 - (ax^2 + by^2) = 0.$$

Clearly $\alpha, \overline{\alpha} \neq 0$, but their product is 0, so A cannot be a division algebra. This completes the proof. □

An immediate corollary to this theorem, 2.3.3 in [5], is a broader characterisations of $M_2(F)$ in terms of a and b.

Corollary 4.9. The quaternion algebras $A' = \left(\frac{1,a}{F}\right)$ and $A'' = \left(\frac{a,-a}{F}\right)$ are isomorphic to $M_2(F)$.

Proof. For A', we notice that $(1,0) \in F \times F$ satisfies $x^2 + ay^2 = 1$ from Theorem 4.8(v). For A'', we notice that from Theorem 4.8(iv), on A_0'' we have $N(x_1i + x_2j + x_3k) = -ax_1^2 + ax_2^2 - a^2x_3^2$. It is clear that $N(ai + aj) = 0$, so A_0'' is isotropic. □

We now apply these results to classify quaternion algebras over various specified fields, namely algebraically closed fields, finite fields, and $\mathbb{R}$. Further, we will examine a quaternion algebra over the commutative ring $\mathbb{Z}$ that will be required for our forthcoming construction.

4.3. **Quaternion Algebras over Specific Fields and $\mathbb{H}(\mathbb{Z})$.**
We examine the simplest case first. If F is an algebraically closed field, then for any $a \in F^\times$, there exists $x \in F^\times$ such that x is a root of the polynomial $x^2 - \frac{1}{a} = 0$, i.e. $ax^2 = 1$. Let $x, y \in F^\times$ such that $ax^2 = by^2 = 1$. Thus by Theorem 4.8,

$$\left(\frac{a,b}{F}\right) \cong \left(\frac{ax^2, by^2}{F}\right) = \left(\frac{1,1}{F}\right) \cong M_2(F).$$

Therefore every quaternion algebra over an algebraically closed field is isomorphic to the matrix algebra.

Let $\mathbb{F}_q$ be a finite field of odd prime order. As in the case of algebraically closed fields, we have a complete characterisation of quaternion algebras over $\mathbb{F}_q$. We first state a result which relies on Wedderburn's little theorem, reproduced from Theorem 1.19 of [1].

Theorem 4.10. Let A be a finite division ring. Then A is a field.

Proof. Let $Z(A) = F$. Then as a commutative division ring, F is a field, and we let $|F| = q$. Further let $\dim_F(A) = n$. We shall show by contradiction that $n = 1$. Let $A^\times$ act on itself by conjugation. Then by the class equation,

$$\left|A^\times\right| = q^n - 1 = q - 1 + \sum_a \left[A^\times : C_A(a)^\times\right],$$

where $C_A(a)$ denotes the centraliser of a and a runs over a set of representatives for the non-singleton conjugacy classes of $A^\times$. For each a, write $r(a) = \dim_F(C_A(a))$. Then $1 \leq r(a) < n$ for all a, and $r(a) \mid n$ by the transitivity of dimensions. Thus we may rewrite the class equation

$$q^n - 1 = q - 1 + \sum_a \frac{q^n - 1}{q^{r(a)} - 1}.$$

Let r be one of the $r(a)$. Recall the definition of the nth cyclotomic polynomial:

$$x^n - 1 = \prod_{d|n} \Phi_d(x) = \Phi_n(x) \cdot \prod_{d<n:d|n} \Phi_d(x).$$

Since $r < n$ and $r \mid n$, we may write

$$q^n - 1 = \Phi_n(q) \cdot (q^r - 1) \cdot h(q),$$

where $h(x)$ is a product of cyclotomic polynomials and unimportant for our purposes. Thus $q^n - 1$ and every term of $\sum_a \frac{q^n-1}{q^{r(a)}-1}$ is divisible by $\Phi_n(q)$, so $q - 1$ must be divisible by it as well. Additionally,

$$q - 1 \geq |\Phi_n(q)| = \prod_\zeta |q - \zeta|,$$

where ζ runs over all the primitive nth roots of unity, of which there are $\varphi(n)$. By the reverse triangle inequality, we have

$$|q - \zeta| \geq \big||q| - |\zeta|\big| = q - 1,$$

and because $q \geq 2$ (as it is a prime power), we have a contradiction if $\varphi(n) \geq 2$. This is true for all $n > 2$. If $n = 2$, then we have the single choice $\zeta = -1$, which gives the contradiction $q - 1 \geq |q - (-1)| = q + 1$. Thus we must have $n = 1$ and so A is of dimension 1 over its centre. Therefore A is itself a commutative division ring, so A is a field as claimed. $\square$

We have an immediate corollary, 1.20 in [1], applying to the case of finite algebras.

Theorem 4.11. Every quaternion algebra over a finite field $\mathbb{F}_q$ is isomorphic to the matrix algebra $M_2(\mathbb{F}_q)$.

Proof. Assume to the contrary that there exists a quaternion division algebra D over $\mathbb{F}_q$. D is itself a division ring, thus by the preceding theorem D is a field, and in particular commutative. But this is absurd, since $ij = -ji$ necessarily. Thus by Theorem 4.5, any quaternion algebra over $\mathbb{F}_q$ must be isomorphic to $M_2(\mathbb{F}_q)$. □

We now examine quaternion algebras over $\mathbb{R}$. For every positive $a \in \mathbb{R}$, we have $x \in \mathbb{R}$ such that $ax^2 = 1$, same as above. Thus if we let $a, b \in \mathbb{R}$, we know

$$\left(\frac{a,b}{\mathbb{R}}\right) \cong \left(\frac{1,1}{\mathbb{R}}\right) \text{ or } \left(\frac{1,-1}{\mathbb{R}}\right) \text{ or } \left(\frac{-1,-1}{\mathbb{R}}\right),$$

though these are not necessarily distinct. The first is isomorphic to $M_2(\mathbb{R})$ by previous proofs and the last isomorphic to $\mathbb{H}(\mathbb{R})$, which is a division algebra. We can see it is a division algebra because it is anisotropic with respect to its norm, namely $N(x_0 + x_1 i + x_2 j + x_3 k) = x_0^2 + x_1^2 + x_2^2 + x_3^2$. We see the second is also isomorphic to $M_2(\mathbb{R})$ by Corollary 4.9. This is summarised in Theorem 2.5.1 of [5].

Theorem 4.12. A quaternion algebra $\left(\frac{a,b}{\mathbb{R}}\right)$ is isomorphic to exactly one of $\mathbb{H}(\mathbb{R})$ and $M_2(\mathbb{R})$ according to whether both a and b are negative or not.

The previous discussion has been limited to algebras over fields. However, the integral quaternions, $\mathbb{H}(\mathbb{Z})$, will be necessary to construct our expander family. These defined to be

$$\mathbb{H}(\mathbb{Z}) = \{a_0 + a_1 i + a_2 j + a_3 k : a_i \in \mathbb{Z}, i^2 = j^2 = k^2 = ijk = -1\}.$$

The same properties of conjugation and norm extend to $\mathbb{H}(\mathbb{Z})$ as in our previous discussion. The following definition will be necessary shortly.

Definition 4.13. Two quaternions $\alpha, \alpha' \in \mathbb{H}(\mathbb{Z})$ are *associate* if there exist units $\varepsilon, \varepsilon' \in \mathbb{H}(\mathbb{Z})^\times = \{\pm 1, \pm i, \pm j, \pm k\}$ such that $\alpha' = \varepsilon \alpha \varepsilon'$.

All units satisfy $N(\varepsilon) = 1$, so we see $N(\varepsilon\alpha\varepsilon') = N(\varepsilon)N(\alpha)N(\varepsilon) = N(\alpha)$. Thus associates have the same norm. We will soon reduce large sets of integral quaternions through association. At last, we may now begin to construct our expander family.

5. The Constructive Method

5.1. $\mathbb{H}(\mathbb{Z})$ and Cayley Graphs.

A famous theorem of Lagrange allows us to begin our main purpose.

Theorem 5.1. Every positive integer is the sum of four squares.

In particular, any prime p is the sum of four squares. Thus for every prime p, there exists $\alpha \in \mathbb{H}(\mathbb{Z})$ such that $N(\alpha) = p$. We are not only interested in representing p as the norm of a quaternion, but in how many unique ways this is possible. Theorem 386 of [4] provides the answer.

Theorem 5.2.

$$|\{\alpha \in \mathbb{H}(\mathbb{Z}) : N(\alpha) = n\}| = 8 \sum_{m|n, 4\nmid n} m.$$

Corollary 5.3. For any prime p,

$$|\{\alpha \in \mathbb{H}(\mathbb{Z}) : N(\alpha) = p\}| = 8(p+1).$$

However, we would like to find a subset of these quaternions which are further 'distinguished'. Recall that for all odd $n \in \mathbb{N}$, $n^2 \equiv 1 \pmod 4$, and for all even $n \in \mathbb{N}$, $n^2 \equiv 0 \pmod 4$. Now, let p be a prime such that $p \equiv 1 \pmod 4$. Then if $N(\alpha) = p$, we must have

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 \equiv 1 \pmod 4 \implies \text{some } a_i \text{ is odd, for unique } i \in \{0,1,2,3\}.$$

Similarly, if we have $p \equiv 3 \pmod 4$, then for $N(\alpha) = p$ there must be a unique a_i such that a_i is even. In any case, we let a_i° be the distinguished coefficient of the quaternion α.

If we have $a_i^\circ \neq 0$, then out of the 8 associates $\varepsilon\alpha$, $\varepsilon \in \mathbb{H}(\mathbb{Z})^\times$, there exists exactly one such that $a_0 = |a_i^\circ|$. If $a_i^\circ = 0$, possible if $p = 3 \pmod 4$, then two associates $\pm\varepsilon\alpha$ have $a_0 = 0$, one of which we call distinguished without loss of generality. Therefore by association we have reduced the set of all quaternions with norm p to a set of distinguished quaternions S_p with $|S_p| = p + 1$. We set this aside for the moment to introduce our methodology for constructing graphs.

Definition 5.4. Let G be a group, and let S be a nonempty, finite, symmetric subset of G, that is, if $x \in S$, then $x^{-1} \in S$. We define the *Cayley graph* $\mathcal{G}(G, S)$ to be the graph with $V = G$ and edge set

$$E = \{(x, y) : x, y \in G \text{ such that } y = xs \text{ for some } s \in S\}.$$

Cayley graphs allow us to create graphs from groups. These graphs are undirected because, by the symmetry of S, if $y = xs$, then $x = ys^{-1}$, and thus both $(x, y), (y, x) \in E$. Knowing some other properties of Cayley graphs will be necessary.

Proposition 5.5. Let $\mathcal{G}(G, S)$ be a Cayley graph with $|S| = k$.

(i) $\mathcal{G}(G, S)$ is a simple, k-regular, vertex-transitive graph.
(ii) $\mathcal{G}(G, S)$ has no loop if and only if $1 \notin S$.
(iii) $\mathcal{G}(G, S)$ is connected if and only if S generates G.

Proof.

(i) We can construct the adjacency matrix of $\mathcal{G}(G, S)$ as follows:

$$A_{xy} = \begin{cases} 1 & \text{there exists } s \in S \text{ such that } y = xs \\ 0 & \text{otherwise.} \end{cases}$$

It is clear that $\mathcal{G}(G, S)$ is simple and k-regular. Futhermore, the action of G on $V = G$ by left multiplication is clearly transitive.

(ii) If $(x, x) \in E$ for any $x \in G$, then we must $1 \in S$ so that $x = xs$ is possible. If $1 \in S$, then we have $(x, x) \in E$ for all $x \in G$. Hence $\mathcal{G}(G, S)$ has a loop if and only if $1 \in S$, and taking the contrapositive provides the result.

(iii) $\mathcal{G}(G, S)$ is connected if and only if every vertex $x \in G$ can be connected to $1 \in G$ by some path $1, x_1, \ldots, x_n = x$. Thus we must have

$$x_1 = 1s_1,\ x_2 = x_1 s_2, \ldots,\ x = x_{n-1}s_n \implies x = s_1 s_2 \cdots s_n$$

for all $x \in G$. This is possible if and only if S generates G.

□

Hence for a graph $\mathcal{G}(G, S)$ to be Ramanujan, it is necessary to have $1 \notin S$, and $\langle S \rangle = G$. We can now explore the utility of the set S_p in its capacity as a 'minimal' set of quaternions with norm p.

5.2. **Construction of $X^{p,q}$.**
Throughout, let p and q be distinct odd primes and let S_p be the distinguished set in $\mathbb{H}(\mathbb{Z})$ as above. Consider the reduction

$$\tau_q : \mathbb{H}(\mathbb{Z}) \to \mathbb{H}(\mathbb{F}_q),$$

where, similar to the integral quaternions,

$$\mathbb{H}(\mathbb{F}_q) = \{a_0 + a_1 i + a_2 j + a_3 k : a_i \in \mathbb{F}_q, i^2 = j^2 = k^2 = ijk = -1\}.$$

Using our notation from §4.1, $\mathbb{H}(\mathbb{F}_q) \cong \left(\frac{-1,-1}{\mathbb{F}_q}\right)$. Thus from Theorem 4.11, we have the following conclusions.

Corollary 5.6. Let q be an odd prime. Then $\mathbb{H}(\mathbb{F}_q) \cong M_2(\mathbb{F}_q)$. Further, let $\psi_q : \mathbb{H}(\mathbb{F}_q) \to M_2(\mathbb{F}_q)$ be an isomorphism. Then for $\alpha \in \mathbb{H}(\mathbb{F}_q)$, $N(\alpha) = \det \psi_q(\alpha)$. Finally, if $\alpha = \overline{\alpha}$, then $\psi_q(\alpha)$ is a scalar matrix.

Proof. $\mathbb{H}(\mathbb{F}_q) \cong M_2(\mathbb{F}_q)$ follows immediately. Second, the norm on a matrix algebra is precisely the determinant, and the isomorphism ψ_q preserves norm. Finally, if $\alpha = \overline{\alpha}$, then $\alpha \in Z(\mathbb{H}(\mathbb{F}_q))$. The centre of the matrix algebra is exactly the subalgebra of scalar matrices, and we must have $Z(\mathbb{H}(\mathbb{F}_q)) \cong Z(M_2(\mathbb{F}_q))$. □

We therefore may apply properties of matrices to $\mathbb{H}(\mathbb{F}_q)$. If $\alpha \in S_p$, then $N(\alpha) \not\equiv 0 \pmod{q}$, so $\psi_q(\tau_q(\alpha)) \in \mathrm{GL}_2(q)$, the set of invertible matrices over $\mathbb{F}_q$. We have a further canonical quotient map

$$\varphi : \mathrm{GL}_2(q) \to \mathrm{PGL}_2(q),$$

where

$$\mathrm{PGL}_2(q) = \mathrm{GL}_2(q) \Big/ \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}, \lambda \in \mathbb{F}_q^\times \right\}.$$

Finally we let $S_{p,q} = (\varphi \circ \psi_q \circ \tau_q)(S_p)$. It is easy to verify that $S_{p,q}$ is a symmetric subset of $\mathrm{PGL}_2(q)$. However, the map from S_p to $S_{p,q}$ is not always injective, but we may show it is for large enough q. We establish a lower bound on q by Lemma 4.2.1 in [2].

Lemma 5.7. If $q > 2\sqrt{p}$, then $|S_{p,q}| = p + 1$.

Proof. Let α and β be two distinct elements of $S_{p,q}$. We will show that for our choice of q, it is impossible for α and β to be identified by φ, ψ_q, or τ_q.

Let $\alpha = a_0 + a_1 i + a_2 j + a_3 k$ and $\beta = b_0 + b_1 i + b_2 j + b_3 k$. Then we must have $a_i \neq b_i$ for some $i \in \{0, 1, 2, 3\}$. Because $N(\alpha) = N(\beta) = p$, we must have $a_j, b_j \in (-\sqrt{p}, \sqrt{p})$ for each $j \in \{0, 1, 2, 3\}$. Because $q > 2\sqrt{q}$, we cannot have $a_i \equiv b_i \pmod{q}$, thus $\tau_q(\alpha) \neq \tau_q(\beta)$.

Let $A = \psi_q(\tau_q(\alpha))$ and $B = \psi_q(\tau_q(\beta))$. Because ψ_q is an isomorphism, $A \neq B$. Assume by contradiction that $\varphi_A = \varphi_B$. Then there exists $1\lambda \in \mathbb{F}_q^\times$ such that $A = \lambda B$. Therefore $p = \det A = \lambda^2 \det B = \lambda^2 p$. Therefore $\lambda = \pm 1$, but since $\lambda = 1$ implies $A = B$ (which we already showed was impossible), we must have $\lambda = -1$ and $A = -B$. Under ψ_q^{-1}, we have $\alpha \equiv -\beta \pmod{q}$, thus $a_j \equiv -b_j \pmod{q}$ for all $j \in \{0, 1, 2, 3\}$. Recall that in S_p, our distinguished coefficients were positive, that is $a_0, b_0 \geq 0$, so we must have $a_0 = b_0 = 0$.

Therefore $\alpha = \overline{\beta}$. However, this contradicts our assumption that, if $a_0 = 0$, then only one of α and $\overline{\alpha}$ is an element of S_p. Thus we cannot have $\varphi_A = \varphi_B$, and every α and β is preserved uniquely into $S_{p,q}$. □

It is convenient at this point to recall both the special linear and projective special linear groups of $M_2(\mathbb{F}_q)$.

Definition 5.8. For $M_2(\mathbb{F}_q)$, we define the *special linear group* by $\mathrm{SL}_2(q) = \{A \in \mathrm{GL}_2(q) : \det A = 1\}$. We further define the *projective special linear group* to be

$$\mathrm{PSL}_2(q) = \mathrm{SL}_2(q) \Big/ \left\{ \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon \end{pmatrix}, \varepsilon = \pm 1 \right\}.$$

Using our previously defined notation, for $A \in \mathrm{GL}_2(q)$, $\varphi_A \in \mathrm{PSL}_2(q)$ if and only if $\det A$ is a square in $\mathbb{F}_q^\times$. Because $\det A = p$ for all $A = \psi_q(\tau_q(\alpha)), \alpha \in S_p$, we have two distinct cases when p is a square in $\mathbb{F}_q^\times$ and when it is not. We will use the following notation.

Definition 5.9. We define the *Legendre symbol*, $\left(\frac{p}{q}\right)$, by

$$\left(\frac{p}{q}\right) = \begin{cases} 0 & \text{if } p \equiv 0 \pmod{q} \\ 1 & \text{if } p \text{ is a nonzero square modulo } q \\ -1 & \text{otherwise} \end{cases}$$

Therefore we define our graphs $X^{p,q}$ in two different ways. If p is a square in $\mathbb{F}_q^\times$, that is $\left(\frac{p}{q}\right)$, then we let $X^{p,q} = \mathcal{G}(\mathrm{PSL}_2(q), S_{p,q})$. If $\left(\frac{p}{q}\right) = -1$, we let $X^{p,q} = \mathcal{G}(\mathrm{PGL}_2(q), S_{p,q})$. These are the only two choices because $\left(\frac{p}{q}\right) \neq 0$ for two primes p and q. In either case, we have $1 \notin S_{p,q}$ and $|S_{p,q}| = p + 1$, so $X^{p,q}$ is simple, $(p+1)$-regular, and without loop. However to even begin to prove $X^{p,q}$ is Ramanujan, we must first show it is connected, that is $\langle S_{p,q} \rangle = \mathrm{PSL}_2(q)$ or $\mathrm{PGL}_2(q)$ (depending on the situation). We will only be able to prove this by constructing connected graphs which we will then prove are isomorphic to $X^{p,q}$.

5.3. Construction of $Y^{p,q}$.

We will need to construct a new series of graphs $Y^{p,q}$ which, for large values of q, we will show are identical to $X^{p,q}$. Recall that each $\alpha \in S_p$ has distinguished $a_0 \geq 0$, either the only odd or only even coefficient.

Our definition of distinguished means that $\alpha \in S_p$ satisfies either $\alpha \equiv 1 \pmod 2$ or $\alpha \equiv i + j + k \pmod 2$. Furthermore, if $a_0 > 0$, then both $\alpha, \overline{\alpha} \in S_p$ because they are not associate but have equal norm. However if $a_0 = 0$, then we have only one of $\alpha, \overline{\alpha} \in S_p$. Therefore we may write

$$S_p = \{\alpha_1, \overline{\alpha}_1, \ldots, \alpha_s, \overline{\alpha}_s, \beta_1, \ldots, \beta_t\},$$

where α_i has $a_0 > 0$, β_j has $a_0 = 0$, and $\alpha_i \overline{\alpha}_i = -\beta_j^2 = p$. By this notation, we have $2s + t = p + 1$.

We need the following definition to link the concepts of paths in graphs and products of group elements.

Definition 5.10. A *reduced word* over S_p is a word $w = \gamma_1 \gamma_2 \cdots \gamma_n$ such that $\gamma_i \in S_p$ and $\alpha_j \overline{\alpha}_j$, $\overline{\alpha}_j \alpha_j$, and $\beta_j \beta_j$ do not appear consecutively in w. The *length* of w is the number of symbols.

Theorem 2.6.13 in [2] provides us a unique factorisation as a reduced word for any $\alpha \in \mathbb{H}(\mathbb{Z})$ with $N(\alpha) = p^k$ using S_p.

Theorem 5.11. Let $\alpha \in \mathbb{H}(\mathbb{Z})$ such that $N(\alpha) = p^k$. Then α admits a unique factorisation $\alpha = \varepsilon\, p^r\, w_m$, where $\varepsilon \in \mathbb{H}(\mathbb{Z})^\times$, w_m is a reduced word of length m over S_p, and $k = 2r + m$.

We can find an even more specific factorisation for a subset of such α.

Corollary 5.12. Let $\Lambda' = \{\alpha \in \mathbb{H}(\mathbb{Z}) : \alpha \equiv 1 \pmod 2 \text{ or } \alpha \equiv i+j+k \pmod 2, N(\alpha) = p^k\}$. Every $\alpha \in \Lambda'$ with $N(\alpha) = p^k$ has a unique factorisation $\alpha = \pm p^r w_m$, where w_m is a word of length m over S_p and $k = 2r + m$.

The final thing we note is that Λ' is a semigroup under multiplication. Clearly $1 \in \Lambda'$ is the identity element, and by noting

$$(i+j+k)(i+j+k) = i^2 + j^2 + k^2 + (ij + ji) + (ik + ki) + (jk + kj) = -3 \equiv 1 \pmod 2,$$

we verify that Λ' is closed under multiplication. We may reduce Λ' to a group by the following equivalence relation. For $\alpha, \beta \in \Lambda'$, we say $\alpha \sim \beta$ if and only if there exist $m, n \in \mathbb{N}$ such that $p^m \alpha = \pm p^n \beta$. We define the reduction $Q : \Lambda' \to \Lambda'/\!\sim$, where $\alpha \mapsto [\alpha]$, and let $\Lambda = \Lambda'/\!\sim$. Proposition 4.3.1 of [2] allows us to bridge the gap between this construction and the last.

Proposition 5.13.

(i) Λ is a group.
(ii) $\mathcal{G}(\Lambda, Q(S_p))$ is the $(p+1)$-regular tree.

Proof.

(i) To see Λ is closed under multiplication, we note that if $\alpha_1 \sim \beta_1$ and $\alpha_2 \sim \beta_2$,

$$p^{m_1}\alpha_1 p^{m_2}\alpha_2 = \pm p^{n_1}\beta_1 p^{n_2}\beta_2 \implies p^{m_1+m_2}\alpha_1\alpha_2 = \pm p^{n_1+n_2}\beta_1\beta_2,$$

because integers commute with $\mathbb{H}(\mathbb{Z})$. Thus $\alpha_1\alpha_2 \sim \beta_1\beta_2$. Therefore multiplication is well-defined in Λ though multiplication in Λ', that is $[\alpha][\beta] = [\alpha\,\beta]$. Furthermore, $[1] \in \Lambda$ is its identity element. The remaining question concerns inverse elements. Let $\alpha \in \Lambda'$. Then $\alpha\overline{\alpha} = \overline{\alpha}\alpha = p^k \sim 1$. Thus $[\alpha]^{-1} = [\overline{\alpha}]$. Therefore Λ is a group.

(ii) It is clear that $|Q(S_p)| = p + 1$, because $\alpha \sim \beta$ implies $\alpha = \beta$ for $\alpha, \beta \in S_p$. By Corollary 5.12, any $\alpha \in \Lambda'$ can be written as a reduced word over S_p, hence Λ is generated by $Q(S_p)$. By Proposition 5.5, $\mathcal{G}(\Lambda, Q(S_{p,q}))$ is $(p+1)$-regular and connected. Therefore we only need show that it contains no circuits.

Assume that we have some circuit $x_0, x_1, \ldots, x_{g-1}, x_g = x_0$, where $g \geq 3$. Again by Proposition 5.5, $\mathcal{G}(\Lambda, Q(S_{p,q}))$ is vertex-transitive, so we may let $x_0 = [1]$. Using the definition of a Cayely graph, we have $x_1 = 1[\gamma_1], x_2 = [\gamma_1][\gamma_2] = [\gamma_1\gamma_2], \ldots, x_g = [\gamma_1\gamma_2\cdots\gamma_g]$ for some $\gamma_i \in S_p$. Since our circuit has no backtracking, that is $x_{k-1} \neq x_{k+1}$ for all $1 \leq k \leq n-1$, the word $\gamma_1\gamma_2\cdots\gamma_g$ is reduced. This gives us

$$[1] = [\gamma_1\gamma_2\cdots\gamma_g] \in \Lambda \implies p^m = \pm p^n \gamma_1\gamma_2\cdots\gamma_g \in \Lambda',$$

which is a contradiction since $\gamma_1\gamma_2\cdots\gamma_g$ is a nontrivial reduced word over S_p, and by Propsition 5.12, we cannot have two representations for the same element of Λ'. Thus $\mathcal{G}(\Lambda, Q(S_p))$ has no circuit, and the proof is complete.

□

The method used in the proof of (ii) will be used later in girth calculations. We will now, as before, work on reducing Λ and S_p by various homomorphisms. Using the same $\tau_q : \mathbb{H}(\mathbb{Z}) \to \mathbb{H}(\mathbb{F}_q)$, we see Λ' maps to $\mathbb{H}(\mathbb{F}_q)^\times$. By Corollary 5.6, the centre of $\mathbb{H}(\mathbb{F}_q)$, which we denote Z_q, is exactly $\mathbb{F}_q^\times$. We may equivalently write $Z_q = \{\alpha \in \mathbb{H}(\mathbb{F}_q) : \alpha = \overline{\alpha}\}$. Furthermore, for $\alpha, \beta \in \Lambda'$, we see that if $\alpha \sim \beta$, then $\tau_q(\alpha)^{-1}\tau_q(\beta) \in Z_q$. Therefore we may define

$$\Pi_q : \Lambda \to \mathbb{H}(\mathbb{F}_q)^\times / Z_q,$$

which is a well-defined group homomorphism which is derived from τ_q. We let $\ker \Pi_q = \Lambda(q)$ and the image of $\Pi_q \cong \Lambda/\Lambda(q)$. We finally let $T_{p,q} = (\Pi_q \circ Q)(S_p)$.

Lemma 5.7 applies here as well, so that if $q > 2\sqrt{p}$, then $|T_{p,q}| = p + 1$. Therefore we define the Cayley graph

$$Y^{p,q} = \mathcal{G}(\Lambda/\Lambda(q), T_{p,q})$$

which is clearly $(p+1)$-regular. However, because we know $Q(S_p)$ generates Λ and no elements are lost under Π_q, we know $\langle T_{p,q} \rangle = \Lambda/\Lambda(q)$. Thus we know $Y^{p,q}$ is connected. It is useful here to elucidate the structure of $\Lambda(q)$ so that we may better characterise this group.

Lemma 5.14.

$$\Lambda(q) = \{[\alpha] \in \Lambda : \alpha = a_0 + a_1 i + a_2 j + a_3 k, q \mid a_1, a_2, a_3\}.$$

Proof. Let $\alpha \in \mathbb{H}(\mathbb{Z})$. Ascending from Π_q to τ_q, we know that $[\alpha] \in \Lambda(q)$ if and only if $\tau_q(\alpha) \in Z_q$. This occurs if and only if $a_1, a_2, a_3 \equiv 0 \pmod{q}$, and $a_0 \not\equiv 0 \pmod{q}$. But since $N(\alpha) = a_0^2 + a_1^2 + a_2^2 + a_3^2 = p^k \not\equiv 0 \pmod{q}$, and the last three terms are zero modulo q, we are guaranteed $a_0^2 \not\equiv 0 \pmod{q} \iff a_0 \not\equiv 0 \pmod{q}$ since q is a prime. Hence the conditions given are both necessary and sufficient. □

Our final task is to prove that $Y^{p,q} = X^{p,q}$ for large q. However, we first need to identify $Y^{p,q}$ with its equivalent Cayley graph in $\mathrm{PGL}_2(q)$ for easier comparison.

We have already shown $\psi_q : \mathbb{H}(\mathbb{F}_q)^\times \to \mathrm{GL}_2(q)$ is an isomorphism. By Corollary 5.6, we see that $Z_q = \mathbb{F}_q^\times$ maps isomorphically under ψ_q to scalar matrices in $\mathrm{GL}_2(q)$. Therefore ψ_q descends to an isomorphism

$$\beta : \mathbb{H}(\mathbb{F}_q)^\times / Z_q \to \mathrm{PGL}_2(q).$$

This allows us to compare $X^{p,q}$ and $Y^{p,q}$ directly by means of a commutative diagram, taken from §4.3 of [2].

$$\begin{array}{ccccc} S_p \subset \Lambda' & \xrightarrow{\tau_q} & \mathbb{H}(\mathbb{F}_q)^\times & \xrightarrow{\psi_q} & \mathrm{GL}_2(q) \\ \downarrow Q & & \downarrow & & \downarrow \varphi \\ \Lambda & \xrightarrow[\Pi_q]{} & \mathbb{H}(\mathbb{F}_q)^\times / Z_q & \xrightarrow[\beta]{} & \mathrm{PGL}_2(q) \end{array}$$

Each row of the diagram affords us different information. $X^{p,q}$ is derived through $\varphi \circ \psi_q \circ \tau_q$, and we know its Cayley graph has either $\mathrm{PGL}_2(q)$ or $\mathrm{PSL}_2(q)$ as its group but is not necessarily connected. $Y^{p,q}$ comes from $\Pi_q \circ Q$ and is connected, but we know little about its group $\Lambda/\Lambda(q)$. However, it is important to note that $\beta(T_{p,q}) = S_{p,q}$, so we know that $Y^{p,q}$ is a connected component of $X^{p,q}$. We can use this fact to finally prove $X^{p,q}$ is connected, and subsequently that it is an expander family.

5.4. **Connectedness of $X^{p,q}$.**
Recall that the girth of a graph, denoted $g(X)$, is the length of the shortest circuit in X. We will need another simple definition to attack the main theorem of this section.

Definition 5.15. A group G is *metabelian* if there exists a normal subgroup $N \triangleleft G$ such that both N and G/N are abelian.

We can now prove Theorem 4.3.5 of [2].

Theorem 5.16. Assume $p \geq 5$. For $q > p^8$, $X^{p,q}$ is connected. As a result, $X^{p,q} \cong Y^{p,q}$.

Proof. Recall that we need to show that $\langle S_{p,q} \rangle = \mathrm{PSL}_2(q)$ if $\left(\frac{p}{q}\right) = 1$ and $\langle S_{p,q} \rangle = \mathrm{PGL}_2(q)$ if $\left(\frac{p}{q}\right) = -1$. We prove this through the isomorphism β, and restate our objective:

$$\beta(\Lambda/\Lambda(q)) = \begin{cases} \mathrm{PSL}_2(q) & \text{if } \left(\frac{p}{q}\right) = 1 \\ \mathrm{PGL}_2(q) & \text{if } \left(\frac{p}{q}\right) = -1. \end{cases}$$

In the latter case, we know $S_{p,q} \subset \mathrm{PGL}_2(q) \setminus \mathrm{PSL}_2(q)$. Let $H_{p,q} = \mathrm{PSL}_2(q) \cap \beta(\Lambda/\Lambda(q))$. We therefore need only prove, for both cases,

$$H_{p,q} = \mathrm{PSL}_2(q).$$

We will need the following facts, drawn from Theorem 3.3.4 and Remark 4.3.4.

(i) If H is a subgroup of $\mathrm{PSL}_2(q)$ such that $|H| > 60$ and H is not metabelian, then $H = \mathrm{PSL}_2(q)$.
(ii) For $p \geq 5$, $|Y^{p,q}| \geq q/p$.

To prove $|H_{p,q}| > 60$, because $q > p^8$ and $p \geq 5$, we have

$$|\Lambda/\Lambda(q)| \geq \frac{q}{p} > p^7 > 120,$$

and therefore $|H_{p,q}| > 60$.

To prove $H_{p,q}$ is not metabelian, it suffices to show that there exist $g_1, g_2, g_3, g_4 \in H_{p,q}$ such that

$$[[g_1, g_2], [g_3, g_4]] \neq 1,$$

where $[x, y] = x^{-1}y^{-1}xy$ is the commutator of x and y.

In the case that $\left(\frac{p}{q}\right) = 1$, we choose $g_1 \in S_{p,q}$ and $g_2 \neq g_1^{\pm 1}$. Let $g_3 = g_1$ and $g_4 \notin \{g_1^{\pm 1}, g_2^{\pm 1}\}$. Then $[[g_1, g_2], [g_3, g_4]] = w$ is a reduced word of length 16 over $S_{p,q}$. However, by the lower bound on our girth given by Proposition 4.3.3,

$$g(Y^{p,q}) \geq 2 \log_p q > 16.$$

Therefore we cannot have $w = 1$ otherwise, by vertex transitivity, we would have a circuit of length 16, which is a contradiction.

In the case that $\left(\frac{p}{q}\right) = -1$, we first take any $h_1 \in S_{p,q}$, $h_2 \neq h_1^{\pm 1}$, and $h_3 \notin \{h_1^{\pm 1}, h_2^{\pm 1}\}$. Now we let $g_1 = h_1h_3$, $g_2 = h_2h_3$, $g_3 = h_1h_2$, and $g_4 = h_3h_2$, which are elements in $H_{p,q}$. Then we have

$$[[g_1, g_2], [g_3, g_4]] = [h_1h_3h_2h_1^{-1}h_3^{-1}h_2^{-1}, h_1h_2h_3h_1^{-1}h_2^{-1}h_3^{-1}]$$

which, expanded further, is a reduced word of length 24 on $S_{p,q}$. Again by Proposition 4.3.3,

$$g(Y^{p,q}) \geq 4\log_p q - \log_p 4 > 24,$$

so this commutator cannot be equal to 1. Therefore in either case, $H_{p,q}$ is not metabelian, and thus $H_{p,q} = \mathrm{PSL}_2(q)$ and $X^{p,q} \cong Y^{p,q}$. □

Thus we have finally shown that $X^{p,q}$ are simple, connected $(p+1)$-regular graphs. Our last step would be to show that these graphs are Ramanujan. As we alluded to in the introduction, we will be unable within the scope of this paper to prove this outright, but will show that $X^{p,q}$ is an expander family. In order to complete this spectral analysis, we will need to take a brief excursion into representation theory.

6. Representations of $\mathrm{PSL}_2(q)$

A small result from representation theory will be necessary in examining the structure of $X^{p,q}$. In particular, we will examine representations of $\mathrm{PSL}_2(q)$, a group which has remained of great importance throughout this thesis. We will attempt to include a minimal amount of superfluous background material; a more thorough discussion may be found in §3 of [2].

Let $\mathbb{F}_q$ be a finite field with odd prime order and let B be the group of affine transformations of $\mathbb{F}_q$, namely maps of the form

$$z \mapsto az + b \qquad (a \in \mathbb{F}_q^\times, b \in \mathbb{F}_q).$$

It is trivial to verify that this is a group under composition. We may view $\mathbb{F}_q$ as a B-space, in that we have a natural homomorphism $B \to \mathrm{Sym}(\mathbb{F}_q)$ which defines a left multiplication by elements of B on $\mathbb{F}_q$. We let $\mathbb{C}\,\mathbb{F}_q$ be the set of complex-valued functions on $\mathbb{F}_q$. Then we define the *permutation representation* $\lambda_{\mathbb{F}_q}$ of B on $\mathbb{C}\,\mathbb{F}_q$ by

$$(\lambda_{\mathbb{F}_q}(g)\, f)(z) = f(g^{-1}z),$$

where $f \in \mathbb{C}\,\mathbb{F}_q$, $g \in B$, and $z \in \mathbb{F}_q$. This representation has an invariant subspace

$$W_0 = \left\{ f \in \mathbb{C}\,\mathbb{F}_q : \sum_{z \in \mathbb{F}_q} f(z) = 0 \right\}$$

with subrepresentation $\lambda^0_{\mathbb{F}_q}$.

Lemma 3.5.2 of [2] gives us our first insight.

Lemma 6.1. The representation $\lambda^0_{\mathbb{F}_q}$ is an irreducible representation of B of degree $q-1$.

Proof. By Proposition 3.4.26 of [2], it suffices to show that $\mathbb{F}_q$ is 2-*transitive* as a B-space, i.e. for every ordered pair $(w_1, z_1), (w_2, z_2) \in \mathbb{F}_q \times \mathbb{F}_q$, with $w_i \neq z_i$, there exists $b \in B$ such that $b \cdot w_1 = w_2$ and $b \cdot z_1 = z_2$. The proof of this proposition is omitted as it is out of scope.

Let $(w_1, z_1), (w_2, z_2) \in \mathbb{F}_q \times \mathbb{F}_q$ as above. Then the affine transformation

$$g(x) = \frac{z_2 - z_1}{w_2 - w_1}(x - w_1) + z_1$$

precisely satisfies what we require. □

Recall that in §5.2 we let $\varphi : \mathrm{SL}_2(q) \to \mathrm{PSL}_2(q)$ be the canonical projection, where $A \mapsto \varphi_A$. Then we define

$$B_0 = \varphi\left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} : a \in \mathbb{F}_q^\times, b \in \mathbb{F}_q \right\}.$$

We identity B_0 with a subgroup of B via, for $A = \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}, \varphi_A(z) = a^2 z + ab$. More specifically, if we let α be the surjection

$$\alpha : B \to \mathbb{F}_q^\times : (z \mapsto az + b) \mapsto a,$$

then B_0 is precisely the preimage of the subgroup of squares in $\mathbb{F}_q^\times$, which we denote $\mathbb{F}_q^{\times 2}$. We may now prove the proposition essential to the representation theory of B_0, 3.5.3 in [2].

Proposition 6.2. Let q be an odd prime. Then up to equivalence, there are $\frac{q+3}{2}$ irreducible representations of B_0, comprising

(i) $\frac{q-1}{2}$ group homomorphisms $B_0 \to \mathbb{C}^\times$, factoring through $\alpha|_{B_0}$, and
(ii) two inequivalent representations ρ_+, ρ_- of degree $\frac{q-1}{2}$.

Proof. This proof is lengthy in [2], so we will attempt to abridge it somewhat. The first category of representations are of little concern to us, and it suffices to say that these all have degree 1.

Consider the restriction of $\lambda^0_{\mathbb{F}_q}$ to B_0. We will prove that this decomposes into two distinct and irreducible representations. Let $\omega = e^{\frac{2\pi i}{q}}$ and for all $c \in \mathbb{F}_q$, define the homomorphism

$$e_c : \mathbb{F}_q \to \mathbb{C}^\times \text{ given by } e_c(z) = \omega^{cz}.$$

Then by Exercise 4 of §3.4, $\{e_c : c \in \mathbb{F}_q\}$ is a basis for $\mathbb{C}\mathbb{F}_q$. In particular, if we restrict to $\{e_c : c \in \mathbb{F}_q^\times\}$, then we have a basis for W_0 described above. For a general $g \in B$ with $g(z) = az + b$, we see

$$(\lambda^0_{\mathbb{F}_q}(g)e_c)(z) = e_c(g^{-1}z) = e_c\left(\frac{z-b}{a}\right) = \omega^{-\frac{cb}{a}} \cdot \omega^{\frac{cz}{a}} = \omega^{-\frac{cb}{a}} e_{c/a}(a),$$

and in general,

$$\lambda^0_{\mathbb{F}_q}(g)e_c = \omega^{-\frac{cb}{a}} e_{c/a}. \tag{2}$$

We may decompose W_0 into two subspaces, W_+ and W_-, generated by the e_c's as follows:

$$W_+ = \left\langle e_c : c \in \mathbb{F}_q^{\times 2} \right\rangle$$
$$W_- = \left\langle e_c : c \in \mathbb{F}_q^\times \setminus \mathbb{F}_q^{\times 2} \right\rangle.$$

These are invariant subspaces for the restriction of $\lambda^0_{\mathbb{F}_q}$ to B_0, so we let ρ_+ and ρ_- be the restrictions of $\lambda^0_{\mathbb{F}_q}|_{B_0}$ to W_+ and W_-, respectively. Because $|\mathbb{F}_q^\times \setminus \mathbb{F}_q^{\times 2}| = |\mathbb{F}_q^{\times 2}| = \frac{q-1}{2}$, we have

$$\dim_{\mathbb{C}} W_+ = \dim_{\mathbb{C}} W_- = \frac{q-1}{2},$$

and thus ρ_+ and ρ_- both have degree $\frac{q-1}{2}$. We must show that ρ_+ and ρ_- are not only irreducible, but also that they are distinct.

We examine the additive subgroup $N \subset B_0$, namely matrices of the form $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. It is evident that, as an additive group, $N \cong \mathbb{F}_q$. Thus, similar to the above, we may define the characters

$$\chi_c : N \to \mathbb{C}^\times$$

for each $c \in \mathbb{F}_q$. We now prove that ρ_+ is irreducible, the proof for ρ_- being identical. Let $v \in W_+$ be a nonzero vector, and write

$$v = \sum_{c \in \mathbb{F}_q^{\times 2}} x_c e_c,$$

where $x_c \in \mathbb{C}$. We choose a specific element in the group algebra $\mathbb{C}[N]$:

$$z = \frac{1}{q} \sum_{g \in N} g \, \overline{\chi_c}(g).$$

Then

$$\rho_+(z)v = \sum_{d \in \mathbb{F}_q^{\times 2}} x_d \rho_+(z) e_d.$$

For each d, we see

$$\begin{aligned} \rho_+(z)e_d &= \frac{1}{q} \sum_{g \in N} \rho_+(g) e_d \, \overline{\chi_c}(g) \\ &= \frac{1}{q} \sum_{g \in N} \chi_d(g) \, \overline{\chi_c}(g) e_d \\ &= \delta_c(d), \end{aligned}$$

where this last step is given by the orthogonality of characters. Thus $\rho_+(z)v = x_c e_c$. Because $v \neq 0$, there exists some c such that $x_c \neq 0$. Therefore we may choose z with respect to that c, so $0 \neq \rho_+(z)v = x_c e_c \in W_+$ because W_+ is invariant under ρ_+. We now examine the span of $x_c e_c$. By Equation 2, we may choose g such that $\lambda^0_{\mathbb{F}_q}(g)e_c = \omega^{-\frac{cb}{a}} e_{c/a}$ for any a. Thus because $\mathbb{F}_q^{\times 2}$ is a group under multiplication, we may generate all eigenvectors e_c with $c \in \mathbb{F}_q^{\times 2}$.

That ρ_+ and ρ_- are distinct follows from the fact that the restrictions of their characters to N differ. The final matter is whether the only representations of B_0 are of the types described. It can be shown that $|B_0| = \frac{q(q-1)}{2}$, and the sum of the squares of the degrees of these irreducible representations is

$$\frac{q-1}{2} \cdot 1^2 + 2 \cdot \left(\frac{q-1}{2} \right)^2 = \frac{q(q-1)}{2}.$$

This completes the proof. □

How we use this proposition in the context of our construction is of greater relevance. We may now prove Theorem 3.5.1 of [2] that will be of absolute importance in §7.2.

Theorem 6.3. Let $q \geq 5$ be a prime. Then the degree of any nontrivial representation of $\mathrm{PSL}_2(q)$ is at least $\frac{q-1}{2}$.

Proof. Let π be such a nontrivial representation and consider its restriction to B_0 as above. $\pi|_{B_0}$ may be decomposed into irreducible representations of the types described in Proposition 6.2. By Theorem 3.2.2 of [2], $\mathrm{PSL}_2(q)$ is a simple group, and we use the fact that every nontrivial representation on a finite, simple group is faithful, i.e. $\pi|_{B_0}(g) \neq I$ if $g \neq I$. Let $\chi : B_0 \to \mathbb{C}^\times$ be a representation of type (i) from Proposition 6.2. Then on any element of the commutator subgroup of B_0, which is nontrivial because B_0 is not abelian, we have

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

because of commutativity in $\mathbb{C}^\times$. Thus since $\pi|_{B_0}$ is nontrivial on every element of B_0, we must have either ρ_+ or ρ_- as an irreducible representation in the decomposition of $\pi|_{B_0}$. Therefore the degree of π must be at least the degree of ρ_+ or ρ_-, so $\deg \pi \geq \frac{q-1}{2}$. □

Having established this fact, we may now at long last analyse the spectrum of $X^{p,q}$.

7. Spectral estimates of $X^{p,q}$

7.1. **The Revised Trace Formula.**

Let $|X^{p,q}| = n$, and let

$$\mu_0 = p + 1 \geq \mu_1 \geq \ldots \geq \mu_{n-1}$$

be the eigenvalues of its adjacency matrix. We will need to recall much of the material and notation from §2.1 in proving the spectral properties of $X^{p,q}$.

Recall that we let $f_{\ell,x}$ denote the number of paths of length ℓ in X which do not backtrack and both start and end at x. If we assume that X is vertex-transitive, we have $f_{\ell,x} = f_{\ell,y}$ for all $x, y \in V$, and thus instead write f_ℓ. The results of Theorem 2.4 and Corollary 1.4.7 in [2] establish the following.

Corollary 7.1. Given that $X^{p,q}$ is vertex-transitive and $p+1$-regular from Proposition 5.5, we have the revised trace formula

$$\sum_{0 \leq r \leq \frac{m}{2}} f_{m-2r} = \frac{p^{\frac{m}{2}}}{n} \sum_{j=1}^{n-1} U_m\left(\frac{\mu_j}{2\sqrt{p}}\right), \tag{3}$$

where μ_j are the eigenvalues of its adjacency matrix.

This allows us to equate a quantity derived from a graph's geometry with one derived from its spectral properties. We will now analyse the right side of the equation within the context of $X^{p,q}$ specifically.

The following subset $\Theta_p \subset \mathbb{C}$,

$$\Theta_p = [i \log \sqrt{p}, 0] \cup [0, \pi] \cup [\pi, \pi + i \log \sqrt{p}],$$

will be necessary in analysing the Chebyshev polynomials. It is straightforward to verify that $z \mapsto 2\sqrt{p}\cos z$ maps Θ_p onto $[-(p+1), p+1]$, and in particular that $[0, \pi]$ maps to $[-2\sqrt{p}, 2\sqrt{p}]$. Because the spectrum of any $(p+1)$-regular graph is contained within $[-(p+1), p+1]$, for every eigenvalue μ_j, we may define $\theta_j \in \Theta_p$ such that $\mu_j = 2\sqrt{p}\cos\theta_j$ for all $j \in \{0, 1, \ldots, n-1\}$. In particular, $\theta_0 = i \log \sqrt{p}$ is imaginary.

One potential method to show $X^{p,q}$ is Ramanujan would be to prove that, excepting θ_0 and possibly θ_{n-1}, every θ_j is real and so maps into $[-2\sqrt{p}, 2\sqrt{p}]$. Unfortunately, we cannot accomplish this. Instead, we examine how eigenvalues outside the Ramanujan interval affect the size of the right hand side of Equation 3.

For every μ_j not in the Ramanujan interval, we may write

$$\begin{aligned} \theta_j &= i\psi_j \qquad \text{if } 2\sqrt{p} < \mu_j \leq p+1 \\ \theta_j &= \pi + i\psi_j \qquad \text{if } -(p+1) \leq \mu_j < -2\sqrt{p}, \end{aligned}$$

where $0 < \psi_j \leq \log\sqrt{p}$ in either case.

Recall the definition of the hyperbolic sine and cosine for a complex number $z \in \mathbb{C}$:

$$\sinh z = \frac{e^z - e^{-z}}{2} = i\sin(-iz), \quad \cosh z = \frac{e^z + e^{-z}}{2} = \cos(iz)$$

Hereafter we assume m is even. Then for every μ_j outside the Ramanujan interval $[-2\sqrt{p}, 2\sqrt{p}]$,

$$\frac{\sin(m+1)\theta_j}{\sin\theta_j} = \frac{\sin i(m+1)\psi_j}{\sin i\psi_j} = \frac{\sinh(m+1)\psi_j}{\sinh\psi_j} = \frac{e^{(m+1)\psi_j} - e^{-(m+1)\psi_j}}{e^{\psi_j} - e^{-\psi_j}}.$$

For larger values of p, $e^{-\psi_j}$ and $e^{-(m+1)\psi_j}$ become negligible, so we may approximate

$$\frac{\sin(m+1)\theta_j}{\sin\theta_j} \sim e^{m\psi_j}.$$

Thus the larger the 'imaginary portion' of an eigenvalue μ_j, which corresponds to its distance outside the Ramanujan interval, the larger the value of $U_m\left(\frac{\mu_j}{2\sqrt{p}}\right)$. It also follows that the more eigenvalues fall within the Ramanujan interval, the smaller the right hand side of Equation 3. Therefore we will attempt to bound above the left hand side of Equation 3, accomplished through Diophantine means.

We define the quadratic form Q in four variables by

$$Q(x_0, x_1, x_2, x_3) = x_0^2 + q^2(x_1^2 + x_2^2 + x_3^2),$$

and further define the quantity, for $m \in \mathbb{N}$,

$$\begin{aligned} s_Q(p^m) = |\{(x_0, x_1, x_2, x_3) \in \mathbb{Z}^4 : Q(x_0, x_1, x_2, x_3) = p^m \text{ such that} \\ x_0 \text{ is either the only odd or the only even element.}\}| \end{aligned}$$

Lemma 4.4.2 of [2] provides us the first insight into the utility of this quantity.

Lemma 7.2. For $m \in \mathbb{N}$,

$$s_Q(p^m) = 2\sum_{0 \leq r \leq \frac{m}{2}} f_{m-2r}.$$

Proof. Assume that we may identify $X^{p,q}$ and $Y^{p,q}$, and recall the maps and sets defined in the construction of $Y^{p,q}$ from §3.3. Let $1 = x_0, x_1, \ldots, x_\ell = 1$ be a path of length ℓ without backtracking, starting and ending at 1. We may find $t_1, \ldots, t_\ell \in T_{p,q}$ such that $x_i = t_1 t_2 \ldots t_i$ for every $i \in \{1, \ldots, \ell\}$. Additionally, we may write $t_i = \Pi_q([\alpha_i])$ for unique $\alpha_i \in S_p$ for each i. Hence in Λ, $[\alpha_1][\alpha_2]\ldots[\alpha_\ell]$ is a reduced word of length ℓ. Furthermore, $\Pi_q([\alpha_1][\alpha_2]\ldots[\alpha_\ell]) = x_\ell = 1$, thus $[\alpha_1][\alpha_2]\ldots[\alpha_\ell] \in \Lambda(q)$. Therefore f_ℓ is the number of reduced words of length ℓ in Λ which belong to $\Lambda(q)$.

From its definition, we know that if (x_0, x_1, x_2, x_3) contributes to $s_Q(p^m)$, then we may define a quaternion $\alpha = x_0 + qx_1 i + qx_2 j + qx_3 k$ such that $N(\alpha) = p^m$. We recall that

$$\Lambda' = \{\alpha \in \mathbb{H}(\mathbb{Z}) : \alpha \equiv 1 \pmod 2 \text{ or } \alpha \equiv i + j + k \pmod 2, N(\alpha) = p^k\}$$

so every such α is in Λ'. Furthermore, we recall that, from Lemma 5.14,

$$\Lambda(q) = \{[\alpha] \in \Lambda : \alpha = a_0 + a_1 i + a_2 j + a_3 k, q \mid a_1, a_2, a_3\}$$

so every such α additionally has its equivalence class in $\Lambda(q)$. Thus we know

$$s_Q(p^m) = |\{\alpha = a_0 + a_1 i + a_2 j + a_3 k \in \Lambda' : N(\alpha) = p^m, q \mid a_1, a_2, a_3\}|.$$

Suppose α contributes to $s_Q(p^m)$. By Corollary 5.12, α admits a unique factorisation $\alpha = \pm p^\ell w$, where w is a reduced word of length $m - 2\ell$ over S_p. Thus $[\alpha]$ is a reduced word of length $m - 2\ell$ in Λ that belongs to $\Lambda(q)$.

However, from a reduced word w in $\Lambda(q)$ of length $m - 2\ell$, we may derive two quaternions $\alpha = \pm p^\ell w$. From these facts, we may conclude

$$|\{\alpha \in \Lambda' : N(\alpha) = p^m, [\alpha] \in \Lambda(q)\}| = 2 \sum_{0 \le r \le \frac{m}{2}} f_{m-2r}$$

□

Bearing this in mind, we rewrite the trace formula:

$$s_Q(p^m) = \frac{2}{n}\, p^{\frac{m}{2}} \sum_{j=1}^{n-1} U_m\left(\frac{\mu_j}{2\sqrt{p}}\right). \tag{4}$$

By bounding $s_Q(p^m)$ above, we restrict the number of eigenvalues that fall outside of the Ramanujan interval. Making this claim more precise comprises the last section of this paper.

7.2. $X^{p,q}$ is an expander family.

Though we cannot prove $X^{p,q}$ is Ramanujan, we will be able to bound the imaginary part of θ_j above by a constant depending on p, which will sufficiently show that $X^{p,q}$ is a family of expanders. We follow Theorem 4.4.4 from [2].

Theorem 7.3. Fix a real number $0 < \varepsilon < \frac{1}{6}$. Then for q sufficiently, large, every nontrivial eigenvalue μ, that is $|\mu| \neq p + 1$, satisfies

$$|\mu| \le p^{\frac{5}{6}+\varepsilon} + p^{\frac{1}{6}}.$$

In particular, the graphs $X^{p,q}$ are a family of expanders.

Proof. Using the definition of the Chebyshev polynomial, we may now write

$$s_Q(p^m) = \frac{2}{n}\, p^{\frac{m}{2}} \sum_{j=1}^{n-1} \frac{\sin(m+1)\theta_j}{\sin\theta_j}$$

for every $m \in \mathbb{N}$.

Fix a specific nontrivial eigenvalue μ_k outside the Ramanujan interval. Denote the multiplicity of μ_k within the set of all eigenvalues by $M(\mu_k)$. Then given

$$s_Q(p^m) = \frac{2}{n}\, p^{\frac{m}{2}}\, M(\mu_k) \frac{\sinh(m+1)\psi_k}{\sinh\psi_k} + \frac{2}{n}\, p^{\frac{m}{2}} \sum_{j:\mu_j \neq \mu_k} \frac{\sin(m+1)\theta_j}{\sin\theta_j},$$

we may remove all eigenvalues outside of the Ramanujan interval. This gives the inequality

$$s_Q(p^m) \geq \frac{2}{n}\, p^{\frac{m}{2}} M(\mu_k) \frac{\sinh(m+1)\psi_k}{\sinh \psi_k} + \frac{2}{n}\, p^{\frac{m}{2}} \sum_{j:|\mu_j|\leq 2\sqrt{p}} \frac{\sin(m+1)\theta_j}{\sin \theta_j}.$$

Further recall that for real θ, $\left|\frac{\sin(m+1)\theta}{\sin\theta}\right| \leq m+1$. This yields

$$s_Q(p^m) \geq \frac{2}{n}\, p^{\frac{m}{2}} M(\mu_k) \frac{\sinh(m+1)\psi_k}{\sinh \psi_k} - 2p^{\frac{m}{2}}(m+1).$$

We now estimate $s_Q(p^m)$ by Diophantine methods.

Lemma 7.4.

$$s_Q(p^m) = O_\varepsilon\left(\frac{p^{m(1+\varepsilon)}}{q^3} + \frac{p^{\frac{m}{2}(1+2\varepsilon)}}{q}\right),$$

for all $\varepsilon > 0$, where $f(n) = O_\varepsilon(g(n,\varepsilon))$ means there exists a constant C depending on ε and $N \in \mathbb{N}$ such that $f(n) \leq C(\varepsilon) g(n,\varepsilon)$ for all $n > N$.

Proof. Because m is even, by Remark 4.4.1 of [2] we know that $p^m \pmod 4 = 1$. Thus the only type of solution to $Q(x_0,x_1,x_2,x_3) = p^m$ must have x_0 odd and x_1, x_2, x_3 even which means we may write

$$x_0^2 + q^2(x_1^2+x_2^2+x_3^2) = x_0 + 4q^2\left(\left(\frac{x_1}{2}\right)^2 + \left(\frac{x_2}{2}\right)^2 + \left(\frac{x_3}{2}\right)^2\right),$$

where $\frac{x_1}{2}, \frac{x_2}{2}, \frac{x_3}{2}$ are still integers. Thus $s_Q(p^m)$ is exactly equal to the number of integral solutions of $x_0^2 + 4q^2(x_1^2+x_2^2+x_3^2) = p^m$. Clearly $x_0^2 \leq p^m$ so $|x_0| \leq p^{\frac{m}{2}}$. Further, $x_0^2 \equiv p^m \pmod{q^2}$. It is simple to verify that we may combine these facts to conclude

$$x_0 \equiv \pm p^{\frac{m}{2}} \pmod{2q^2}.$$

Thus there are at most $2\left(\frac{p^{\frac{m}{2}}}{q^2}+1\right)$ choices for x_0. Now given a value for x_0, we must find how many integer tuples (x_1,x_2,x_3) satisfy the requirements for $s_Q(p^m)$.

Recall Theorem 5.2, which gives us the number of ways a number can be expressed as the sum of four integral squares. While we do not have such a precise result for the sum of three squares, Corollary 2.2.13 in [2] states that the number of ways a number can be the sum of three squares, denoted $r_3(n)$, is $O_\varepsilon(n^{\frac{1}{2}+\varepsilon})$ for every $\varepsilon > 0$ Therefore

$$r_3\left(\frac{p^m - x_0}{4q^2}\right) = O_\varepsilon\left(\left(\frac{p^m}{q^2}\right)^{\frac{1}{2}+\varepsilon}\right)$$

for every $\varepsilon > 0$. Thus allows us to bound $s_Q(p^m)$ as such:

$$\begin{aligned} s_Q(p^m) &= O_\varepsilon\left(\frac{p^{\frac{m}{2}+\varepsilon m}}{q^{1+2\varepsilon}}\left(\frac{p^{\frac{m}{2}}}{q^2}+1\right)\right) \\ &= O_\varepsilon\left(\frac{p^{m(1+\varepsilon)}}{q^{3+2\varepsilon}} + \frac{p^{\frac{m}{2}(1+2\varepsilon)}}{q^{1+2\varepsilon}}\right) \\ &= O_\varepsilon\left(\frac{p^{m(1+\varepsilon)}}{q^3} + \frac{p^{\frac{m}{2}(1+2\varepsilon)}}{q}\right). \end{aligned}$$

□

Thus for some $C_\varepsilon > 0$, and recalling Equation 4, we have

$$\frac{2}{n}\, p^{\frac{m}{2}} M(\mu_k) \frac{\sinh(m+1)\psi_k}{\sinh \psi_k} \leq C_\varepsilon \left(\frac{p^{m(1+\varepsilon)}}{q^3} + \frac{p^{\frac{m}{2}(1+2\varepsilon)}}{q} \right) + 2p^{\frac{m}{2}}(m+1).$$

Using the estimate $n \leq q^3$,

$$M(\mu_k) \frac{\sinh(m+1)\psi_k}{\sinh \psi_k} \leq C_\varepsilon \left(p^{m(\frac{1}{2}+\varepsilon)} + q^2 p^{m\varepsilon} \right) + q^3(m+1).$$

Further, if we assume that $p^{\frac{m}{2}} \leq q^3$,

$$M(\mu_k) \frac{\sinh(m+1)\psi_k}{\sinh \psi_k} \leq C_\varepsilon \left(q^{3+6\varepsilon} + q^{2+6\varepsilon} \right) + q^3(1 + 6\log_p q).$$

Recalling that $\psi_k \leq \log \sqrt{p}$, we also know $\sinh \psi_k \leq \sinh \log \sqrt{p}$, and so

$$M(\mu_k) \sinh(m+1)\psi_k = O_\varepsilon \left(q^{3+6\varepsilon} \right).$$

Now let m be the largest even integer which satisfies the assumption $p^{\frac{m}{2}} \leq q^3$. Thus for sufficiently large q,

$$\sinh(m+1)\psi_k \geq \frac{e^{(m+1)\psi_k}}{3} \geq \frac{e^{(-1+6\log_p q)\psi_k}}{3} \geq \frac{p^{-\frac{1}{2}}}{3} e^{6\log_p q \cdot \psi_k},$$

This allows us to conclude

$$M(\mu_k) = O_\varepsilon \left(q^{3+6\varepsilon - \frac{6\psi_k}{\log p}} \right).$$

This gives an upper bound for $M(\mu_k)$. We now prove Proposition 4.4.3 of [2] to establish a lower bound on $M(\mu_k)$.

Lemma 7.5. Let μ be a nontrivial eigenvalue of $X^{p,q}$. Then $M(\mu) \geq \frac{q-1}{2}$.

Proof. Let V_μ be the eigenspace corresponding to μ, which is a representation space of the group underlying $X^{p,q}$. Because $\mathrm{PSL}_2(q)$ is contained in this group in every case, we view V_μ as a representation of $\mathrm{PSL}_2(q)$. By Theorem 6.3, any nontrivial representation of $\mathrm{PSL}_2(q)$ has degree at least $\frac{q-1}{2}$. Hence we must prove if μ is a nontrivial eigenvalue, then the representation of $\mathrm{PSL}_2(q)$ on V_μ is likewise nontrivial. We proceed by proving the contrapositive.

Assume the representation of $\mathrm{PSL}_2(q)$ on V_μ is trivial. We have two cases. First, if $\left(\frac{p}{q}\right) = 1$, then every function in V_μ is constant. But as we showed in Proposition 1.2, constant functions correspond to the eigenvalue $\mu = p + 1$.

Second, if $\left(\frac{p}{q}\right) = -1$, then each $0 \neq f \in V_\mu$ must be constant on the the two cosets of $\mathrm{PSL}_2(q)$ in $\mathrm{PGL}_2(q)$. We define a_+ and a_- such that $f = a_+$ on $\mathrm{PSL}_2(q)$ and $f = a_-$ on $\mathrm{PGL}_2(q) \setminus \mathrm{PSL}_2(q)$. Since f is an eigenfunction of the adjacency matrix of $X^{p,q}$, we see

$$\mu\, a_- = (p+1)a_+$$
$$\mu\, a_+ = (p+1)a_-.$$

Because we assumed f is nonzero, the only solution to this system of equations is $\mu^2 = (p+1)^2$, which implies $|\mu| = p+1$ and so is a trivial eigenvalue. Thus every nontrivial eigenvalue yields a nontrivial representation, as required, and we establish our lower bound on the multiplicity of nontrivial μ. □

We may now finish our final proof. Our total bounds on $M(\mu_k)$ are

$$\frac{q-1}{2} \leq M(\mu_k) = O_\varepsilon\left(q^{3+6\varepsilon-\frac{6\psi_k}{\log p}}\right).$$

Taking the logarithm base q, and assuming q is large enough, we have

$$1 \leq 3 + 6\varepsilon - \frac{6\psi_k}{\log p} \implies \psi_k \leq \left(\frac{1}{3}+\varepsilon\right)\log p.$$

Recall that we defined $\theta_k = i\psi_k$ or $\theta_k = \pi + i\psi_k$, and $\mu_k = 2\sqrt{p}\cos\theta_k$, so

$$|\mu_k| = 2\sqrt{p}\,|\cos(i\psi_k)| = 2\sqrt{p}\cosh\psi_k \leq p^{\frac{5}{6}+\varepsilon} + p^{\frac{1}{6}-\varepsilon},$$

which completes the proof. □

This proves that $X^{p,q}$ is an expander family. Further, using the Ramanujan conjecture, $X^{p,q}$ is indeed a Ramanujan expander family. But even without this addendum, we have not only shown that expander families exist, but also constructed one explicitly.

References

[1] Wai Ku Chan. Arithmetic of quarternion algebras. `http://wkchan.web.wesleyan.edu/quaternion-2012.pdf`, 2012.

[2] Guiliana Davidoff, Peter Sarnak, and Alain Valette. *Elementary Number Theory, Group Theory, and Ramanujan Graphs*. Cambridge University Press, Cambridge, 2003.

[3] Jacob Fox. The Petersen graph and Moore graphs. `http://math.mit.edu/~fox/MAT307-lecture19.pdf`, 2009.

[4] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, Oxford, sixth edition, 2008.

[5] Colin Maclachlan and Alan W. Reid. *The Arithmetic of Hyperbolic 3-Manifolds*. Springer-Verlag, New York, 2003.

[6] Peter Sarnak. *Some applications of modular forms*. Cambridge University Press, Cambridge, 1990.