Special Families of Generalized Paley Graphs and the Riemann Hypothesis for Graphs

Lewis Glabush

APPLMATH 4999Z FW 2021-22

Summary

The Ihara zeta function presents an intersection between number theory and algebraic graph theory. The Riemann hypothesis for graphs is a property that certain graphs have with respect to the poles of their Ihara zeta function, named for its similarity to the classical Riemann hypothesis. There is an equivalence between graphs which satisfy the Riemann hypothesis and Ramanujan graphs. A certain infinite family of graphs, called Paley graphs, satisfy the Riemann hypothesis. Paley graphs have edges which are determined by the quadratic residues of a finite field. Generalized Paley graphs have edge sets determined by higher order residues. In this paper, I will explore certain properties of Paley graphs, and investigate whether these properties still hold for special families of generalized Paley graphs. In particular, I will show that properties of finite fields can be used to determine the degree of a generalized Paley graph. This, together with a statement about the spectrum of generalized Paley graphs, can determine whether certain infinite families of generalized Paley graphs are Ramanujan. I will also describe three infinite families of generalized Paley graphs that satisfy the Riemann hypothesis. Also discussed will be the significance of Ramanujan graphs, as an infinite family of expander graphs, and the applications of Ramanujan graphs to post-quantum cryptography.

Introduction

Graphs, Walks, and Cycles.—

A graph G is an ordered pair of sets, denoted by $G = (V, E)$, with V being the set of **vertices** and $E \subseteq V^2$ being the set of **edges**. Graphs have endless applications in any subject where one considers a set of objects, and some relationship between them, such as, social networks, highways, and neural networks. A graph is **directed** if the edges are oriented, meaning that $(v_1, v_2) \neq (v_2, v_1)$, when $v_1 \neq v_2$. Otherwise a graph is called **undirected**. One can also say that a graph is undirected if $(u, v) \in E$ if and only if $(v, u) \in E$ for arbitrary $u, v \in V$.[1]

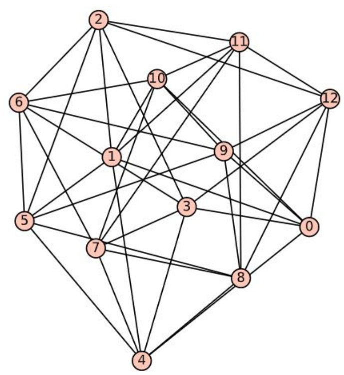

Figure 1: An undirected graph on 11 vertices

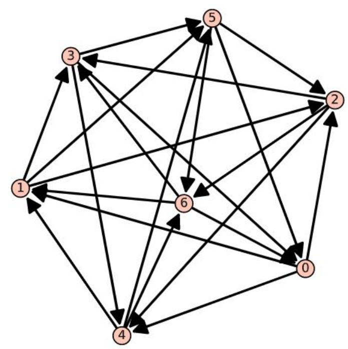

Figure 2: A directed graph on 7 vertices

The focus of this paper is a particularly important family of graphs called generalized Paley graphs. Consider a finite field of order $q = p^s$, denoted by $\mathbb{F}_q$, where p is a prime number, and s is a natural number greater than 0, and $q \equiv 1 \mod 4$. Let G be a graph with each vertex representing an element of $\mathbb{F}_q$. For each pair of distinct vertices $v_1, v_2 \in V$, associate an edge between v_1 and v_2 if $v_1 - v_2 \equiv x^2 \mod q$ for some $x \in \mathbb{F}_q$. The resultant graph, denoted by G_q, is called a **Paley graph**[2]. A **generalized Paley graph** has a vertex set defined in the same way as a Paley graph, but takes a parameter $m \in \mathbb{Z}^+$, and has $E = \{(v_1, v_2) \colon (v_1 - v_2) = k^m \text{ for some } k \in \mathbb{F}_p, v_1 \neq v_2\}$. Denote a generalized Paley graph by $G_{q,m}$ Paley graphs associate edges with *quadratic residues*, which generalized Paley graphs with *higher order residues.*[3]

A **walk** of length n on a graph is a sequence of adjacent oriented edges $W = a_1 a_2 ... a_n$.

The edges in a walk are oriented, even if the graph is undirected. If the first edge of a walk is $a_1 = (v_i, v_j)$, then v_i is called the **initial vertex** of the walk.If the last edge of a walk is $a_n = (v_i, v_j)$, then v_j is called the **terminal vertex** of the walk.

A **cycle** of length n on a graph is a walk of length n, in which the initial vertex of the walk is equal to the terminal vertex. If $a_k = (v_i, v_j)$ is an edge on a graph, then $a_k^{-1} = (v_j, v_i)$. A walk is said to have a **backtrack** at a_k if $a_{k+1} = a_k^{-1}$. A walk is said to have a tail at a_k if $a_k = a_1^{-1}$.[4]

A **prime cycle** is a cycle containing no backtracks or tails, where the cycle from initial vertex to the terminal vertex is completed only once.[4]

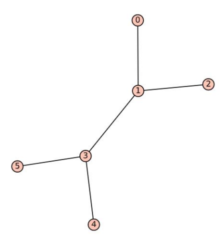

Figure 3: An undirected graph containing no prime cycles

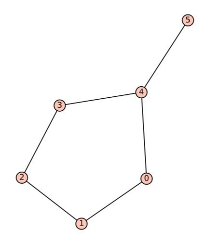

Figure 4: An undirected graph containing one prime cycle

In figure 4, the unique prime cycle, up to the choice of the initial edge, is given by $W = (0,1)(1,2)(2,3)(3,4)(4,0)$. No prime cycle on this graph could contain the edge $(4,5)$ or its inverse, as this would create a backtrack in the graph. Since the cycle from the initial to terminal vertex can be completed only once in a prime cycle, W is a prime cycle, while $2W = (0,1)(1,2)(2,3)(3,4)(4,0)(0,1)(1,2)(2,3)(3,4)(4,0)$ is not.

Spectral graph theory—

Graphs can be encoded by matrices, which allows for the use of techniques from linear algebra in studying their properties. For a Graph $G = (V, E)$ with $|V| = N$, the **adjacency Matrix** is the $N \times N$ matrix A with

$$A_{ij} = \begin{cases} 1 \text{ If there is an edge between vertices } i \text{ and } j \\ \\ 0 \text{ Otherwise} \end{cases}$$

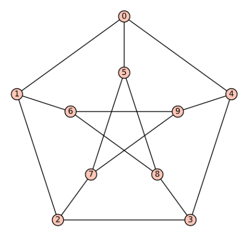

Figure 5: The Petersen Graph

```
[0 1 0 0 1 1 0 0 0 0]
[1 0 1 0 0 0 1 0 0 0]
[0 1 0 1 0 0 0 1 0 0]
[0 0 1 0 1 0 0 0 1 0]
[1 0 0 1 0 0 0 0 0 1]
[1 0 0 0 0 0 0 1 1 0]
[0 1 0 0 0 0 0 0 1 1]
[0 0 1 0 0 1 0 0 0 1]
[0 0 0 1 0 1 1 0 0 0]
[0 0 0 0 1 0 1 1 0 0]
```

Figure 6: The Adjacency Matrix of the Petersen Graph

The **adjacency spectrum** of a graph G is the set of eigenvalues of the associated adjacency matrix A, which are the roots, together with algebraic multiplicity, of the characteristic polynomial[5]

$$c_A(\lambda) = \det(A - \lambda I).$$

Spectral graph theory uses the adjacency matrix, spectrum, and eigenvectors of a related matrix of graph to draw conclusions about using algebraic methods. To illustrate the importance of graph spectra a selection of useful properties of graph spectra are described:

Property 1: A graph is called d-regular, if each vertex is connected to d edges. Whenever a graph is d-regular, the largest eigenvalue of the graph is equal to d, and all eigenvalues of the graph lie within the range $[-d, d]$.[1]

Property 2: Two Graphs are **isomorphic** if there is a bijection between the vertex sets of each graph, that preserves edges. Say V_1 denotes the set of vertices of G_1, and V_2 represents the set of vertices of G_2, then $G_1 \cong G_2$ iff there exists a bijection

$$\Phi : V_1 \to V_2 \text{ such that } \Phi(v_1) \text{ and } \Phi(v_2) \text{ are adjacent if and only if } v_1 \text{ and } v_2 \text{ are.}$$

Two graphs are isomorphic if they have the same adjacency matrix under some labelling of the vertices. If $|V| = n$. Graph spectra is an invariant under labelling, and so two graphs can only be isomorphic if they have the same spectrum.[1]

Property 3: The number of walks between vertices i, j denoted by $N_k(v_i, v_j)$, on a graph G is equal to $A^k_{v_i v_j}$, where A is the associated adjacency matrix.[1]

Property 4: The k-th spectral moment of a graph is defined as

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

i) The number of vertices of a graph is equal to the number of eigenvalues, multiplied by their respective algebraic multiplicities.

ii) The number of edges on a graph is equal to $\frac{s_2}{2}$.

iii) The average degree is equal to $\frac{s_2}{n}$

iv) The number of triangles is equal to $\frac{s_3}{6}$ [1]

Property 5: If a graph G is $d-$regular then the number of connected components of G is equal to the multiplicity of d as an eigenvalue of G.[1]

The graphs considered throughout the remainder of this paper will be undirected simple graphs, which will have real valued spectra.

We define $\lambda(G) = \max(|\lambda_i|)_{i \neq 1}$ A connected $d-$regular graph is called a **Ramanujan graph** if it satisfies

$$\lambda(G) \leq 2\sqrt{d-1}$$ [6]

The Ihara zeta function and the Riemann Hypothesis—

The **degree** of a vertex v in a graph is the number of edges connected to v.

The Ihara zeta function is given by

$$\zeta(s) = \prod_{p, \text{ a prime cycle}} \frac{1}{1 - q^{-s|p|}},$$ [4]

where G is $q+1$-regular, and $|p|$ denotes the length of the prime cycle. A pole of the Ihara zeta function of a graph is a complex number s, such that $q^s + q^{1-s}$ is an eigenvalue of the adjacency matrix of G.[6] A graph is said to satisfy the Riemann Hypothesis if all of the poles of the associated Ihara zeta function with real part between 0 and 1, have real part exactly equal to $\frac{1}{2}$.[4] Though this is called a *hypothesis*, it is actually just a property that *some* graphs have, named for its similarity to the classical Riemann hypothesis. It turns out that a graph satisfies the Riemann hypothesis if and only if it is Ramanujan, this fact is proven in the methodology section of the paper. The Ihara zeta function has played an important role in the fields of discrete mathematics and spectral graph theory, and is included in this paper for its fascinating connection to Ramanujan graphs.[4]

The Problem—

Paley graphs, and their generalizations, are graph representations of finite fields, and their residue structure, making them particularly useful in any area where finite fields relevant. Elliptic curves defined over finite fields are extremely important in number theory, and are the basis for elliptic curve cryptography.[7] Graphs which satisfy the Riemann Hypothesis are an important family of spectral expanders which have numerous applications, including to post-quantum elliptic curve cryptography.[8] All Paley graphs are Ramanujan. This makes Paley graphs an infinite family, and standard example of, Graphs which satisfy the Riemann Hypothesis. Not all generalized Paley graphs are Ramanujan. For instance, the generalized Paley graph $G_{25,6}$ shown in figure 7 is not Ramanujan. This paper will explore conditions for when a generalized Paley graph of the form $G_{q,3}$ is Ramanujan, with some explicit examples and computations.

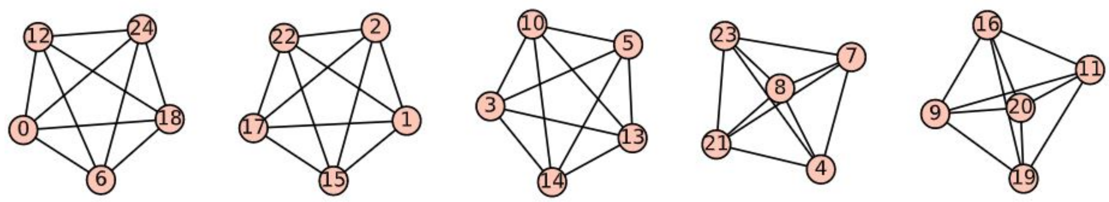

Figure 7: $G_{25,6}$ is an example of a non-Ramanujan generalized Paley Graph

Methodology

This section of the paper will cover known results about Paley graphs. An approach to the problem considered in this paper will also be described. I will also prove the important result that a graph satisfies the Riemann hypothesis if and only if it is Ramanujan, which allows us to conclude that all Paley graphs satisfy the Riemann hypothesis.

Results about Paley Graphs and Ramanujan Graphs—

We will need to make use of the Legendre symbol throughout this section.

$$\left(\frac{a}{q}\right) = \begin{cases} 0 & a = 0 \\ 1 & a \in \left(\mathbb{F}_q^\times\right)^2 \\ -1 & \text{otherwise} \end{cases}$$

The following lemma, as well as proposition 1, was proven in a note by one of my supervisors, Tung Nguyen.

Lemma 1. *The number of quadratic residues over* $\mathbb{F}_q$ *is* $\dfrac{q-1}{2}$.

Proposition 1. *If* G_q *is a Paley graph then:*

1) G_q *is an undirected simple graph*

2) G_q *is* k*-regular with* $k = \dfrac{q-1}{2}$

Proof.

1) If $(v_1, v_2) \in E_q$, where E_q is the edge set of G_q, then we have that $\left(\dfrac{v_1 - v_2}{q}\right) = \left(\dfrac{-1}{q}\right)\left(\dfrac{v_2 - v_1}{q}\right) = \left(\dfrac{v_2 - v_1}{q}\right)$, and so $(v_2, v_1) \in E$ if and only if (v_1, v_2) is, so G_q is undirected. G_q does not contain any loops, since $\left(\dfrac{v - v}{q}\right) = 0$ for all $v \in V_q$ (the vertex set of G_q), and the construction of G_q does not allow for multiple edges, hence G_q is simple.[9]

2) Fix an arbitrary vertex $v_i \in V_q$. Then for arbitrary $v_j \in V_q$, we have that

$$1 + \left(\frac{v_i - v_j}{q}\right) = \begin{cases} 1 & v_i = v_j \\ 2 & (v_i, v_j) \in \mathbb{F}_q \\ 0 & \text{otherwise} \end{cases}$$

Summing over all $v_j \in V_q$ we have that

$$\sum_{v_j \in V_q} \left[1 + \left(\frac{v_i - v_j}{q}\right)\right] = 1 + 2\deg(v_i).$$

We observe that

$$\sum_{v_j \in V_q} \left[1 + \left(\frac{v_i - v_j}{q}\right)\right] = q + \sum_{a} \left[\left(\frac{a}{q}\right)\right] = q \text{ by Lemma 1.}$$

Hence we have that $q = 1 + 2\deg(v_i)$, and so $\deg(v_i) = \dfrac{q-1}{2}$. Since this is true for arbitrary $v_i \in V_q$, G_q is $\dfrac{q-1}{2}$ regular. $\square$

Theorem 1. *The spectrum of a Paley graph G_q is*

$$\left\{\frac{q-1}{2}, \frac{-1+\sqrt{2}}{q}, \frac{-1+\sqrt{2}}{q}\right\}$$

Where the multiplicities of $\dfrac{q-1}{2}$ is 1, and the multiplicity of $\dfrac{-1+\sqrt{q}}{2}$ and $\dfrac{-1-\sqrt{q}}{2}$ are both $\dfrac{q-1}{2}$.[9]

Proposition 2. *All Paley graphs are Ramanujan*

Proof. By theorem 1, for a paley graph G_q, $\lambda(G_q) = \max_{i \neq 1} |\lambda_i| = \left|\dfrac{-1-\sqrt{q}}{2}\right| = \left|\dfrac{+1+\sqrt{q}}{2}\right|$, where $\cup_i \lambda_i$ is the adjacency spectrum of G_q. $\square$

The following proposition is stated and proven by Murty in "Ramanujan Graphs."[6]

Proposition 3. *A $q+1$-regular, connected simple graph is Ramanujan if and only if it satisfies the Riemann Hypothesis*

Proof. Recall that for a $q+1$-regular graph, Ihara zeta function of that graph is given by

$$\zeta(s) = \prod_{p,\text{a prime cycle}} \frac{1}{q^{-s|p|}}.$$

Then s is a pole of ζ if and only if $q^s + q^{1-s}$ is an eigenvalue of G (cite). Suppose that $s = a + bi$ is an eigenvalue of G, then since G is a undirected simple graph, it has only real eigenvalues, and so $\lambda = q^s + q^{1-s}$ is a real number. If $\mathrm{Re}(s) = \frac{1}{2}$, then

$$\lambda = q^{\frac{1}{2}+bi} + q^{\frac{1}{2}-bi} = \sqrt{(}q)\left(q^{ib} + q^{-ib}\right) = 2\sqrt{q}\cos(b\ln(q)).$$

If $\mathrm{Re}(s) \neq \frac{1}{2}$, then

$$\lambda^2 = q^{2-2a} + q^{2a} + 2q$$

Now, suppose that G does not satisfy the Riemann hypothesis. Then there exists a pole of ζ with $0 < \mathrm{Re}(s) < 1$, but $\mathrm{Re}(s) \neq \frac{1}{2}$. Then G has an eigenvalue λ such that $\lambda^2 = q^{2-2a} + q^{2a} + 2q$. The function $f(a) = q^{2-2a} + q^{2a} + 2q$, with $0 < a < 1$, obtains a unique minimum at $a = \frac{1}{2}$, where it takes the value of $4q$ and a maximum at $a \in \{0, 1\}$ of $(q+1)^2$. This gives the inequality

$$4q < \lambda^2 < (q+1)^2$$

and so

$$2\sqrt{q} < |\lambda| < q + 1$$

and so $\lambda(G) > \sqrt{q}$, and G is not Ramanujan.

Now, suppose that G satisfies the Riemann hypothesis. Then if $\lambda = q^s + q^{1-s}$, with $s = a + bi$, is an eigenvalue of G, one either has that $\mathrm{Re}(s) = \frac{1}{2}$, or $\mathrm{Re}(s) \notin (0, 1)$. If $\mathrm{Re}(s) = \frac{1}{2}$ then $\lambda = 2\sqrt{q}\cos(b\ln(q)) \leq 2\sqrt{q}$. If $\mathrm{Re}(s) \neq \frac{1}{2}$ then $\lambda = q^{2-2a} + q^{2a} + 2q$. Either

$a \leq 0$ or $a \geq 1$, and in either case, $|\lambda| \geq q+1$. Since all eigenvalues of a $q+1$-regular graph lie between $[-q-1, q+1]$, we must have that $|\lambda| = q+1$. Since the eigenvalues of a $q+1-$regular graph satisfy $\lambda_1 = q+1 > \lambda_2 \geq ... \geq \lambda_n \geq -q-1$, there are only two possibilities: either $\lambda = \lambda_1$, or G is a bipartite Ramanujan graph,[6] and in either case, G is Ramanujan.[6] □

Corollary 1. *All Paley graphs satisfy the Riemann hypothesis.*

The Approach to the Problem—

In this section we have provided characterization of the degree and spectrum of an arbitrary Paley graph. This allowed us to prove that all Paley graphs satisfy the Riemann hypothesis. In the next section, we consider two families of generalized Paley graphs. The first are of the form $G_{p,3}$, where p is a prime. The second family of generalized Paley graphs are of the form $G_{q,q^{\ell+1}}$, which I include because they have been most thoroughly studied in the literature.[10] In each case, we make a statement about the spectrum and degree of the graph, and see if the graphs satisfy the Riemann Hypothesis.

Results

In the introduction, I showed an example of a generalized Paley graph that did not satisfy the Riemann hypothesis. I will begin by defining an infinite family of generalized Paley graphs, for which there is a complete characterization of when they satisfy the Riemann hypothesis.

The following results were published by Podesta and Videla. Let

$$\mathcal{G}_{q,m} = \left\{ G_{q^m, q^{\ell+1}} : 1 \leq l \leq \frac{m}{2}, l|m \text{ and } \frac{m}{l} \text{ is even} \right\}$$

Theorem 2. *The generalized Paley graph $G_{q^m,q^{\ell+1}}$ satisfies the Riemann hypothesis if and only if $q \in 2, 3, 4$, $l = 1$, and $m \geq 4$.*[10]

Example 1. $G_{49,8}$. The field, $\mathbb{F}_{49}$ is constructed by taking $\mathbb{F}_7[X]/_f$, where f is an irreducible polynomial of degree 2 over $\mathbb{F}_7$.[11] The elements of this field are polynomials over $\mathbb{F}_7$

of degree at most 2. The 8^{th} residues in this field are given by $R_8 = \{1, 2, 3, 4, 5, 6\}$, so $G_{49,8}$ is a 6-regular graph. We can index the vertices as $v_1, .., v_{49}$, with each vertex representing a polynomial in $\mathbb{F}_7[X]/f$. Then $v_1 - v_2 \in E_{G_{49,8}}$ if $v_1 - v_2 \in R_8$. The resulting graph is

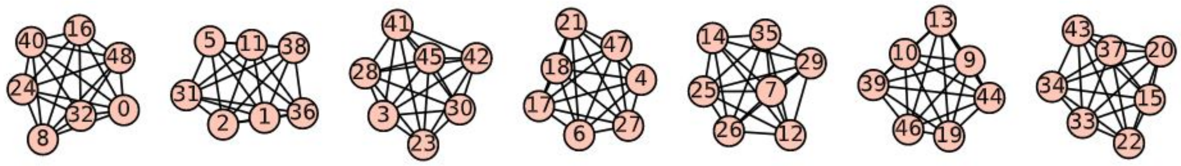

Figure 8: $G_{49,8}$

In general, the largest eigenvalue of a $d-$regular graph gives its degree.[1] The multiplicity of the largest eigenvalue shows the number of components of the graph, which we can observe here is 6. Whenever the multiplicity of the largest eigenvalue $\max(|\lambda_i|)$ of a d-regular graph G is greater than 1, then $\lambda(G) = \max(|\lambda_i|) = d$, so $\lambda(G) = d > 2\sqrt{d-1}$. Therefore $G_{49,8}$ does not satisfy the Riemann hypothesis.

Example 2. The infinite families of generalized Paley graphs $G_{2^{2t},4}, G_{3^{2t},9}, G_{4^{2t},16} t \geq 2$ satisfy the Riemann hypothesis.

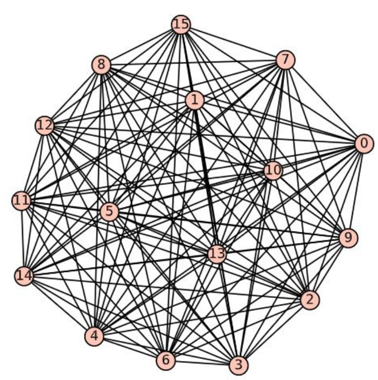

Figure 9: $G_{16,4}$ is a member of the first infinite family

Now I will focus on a simple family of generalized Paley graphs, those of the form $G_{p,3}$, where p is a prime with $p \equiv 1 \mod 4$.

Lemma 2. *Let p be a prime greater than 2. The number of cubic residues in a field $\mathbb{F}_p$ is* *given by*

$$R_{p,3} = \begin{cases} \dfrac{p-1}{3} & p \equiv 1 \mod 3 \\ p-1 & p \equiv 2 \mod 3 \end{cases}$$

[11]

Corollary 2. *The degree of any vertex v in generalized Paley graph of the form $G_{p,3}$ is given by*

$$\deg(v) = \begin{cases} \dfrac{p-1}{3} & p \equiv 1 \mod 3 \\ p-1 & p \equiv 2 \mod 3 \end{cases}$$

Proposition 4. *If $p \equiv 2 \mod 3$ then $G_{p,3}$ satisfies the Riemann hypothesis.*

Proof. If $p \equiv 2 \mod 3$, then by lemma 2, there are $p-1$ cubic residues in $\mathbb{F}_p$. Then for an arbitrary vertex v_i, every distinct vertex v_j is such that $v_i - v_j \in R_{p,3}$. Then $G_{p,3} \cong K_p$. The eigenvalues of a complete graph K_n are $\{n-1, -1\}$, where the multiplicity of $n-1$ is 1, and the multiplicity of -1 is $n-1$.[2] Therefore $\lambda(G_{p,3}) = -1$, so $\lambda(G) \leq 2\sqrt{p-1}$, and $G_{p,3}$ satisfies the Riemann hypothesis. $\square$

Remark 1. It has been shown by Lim and Praegar that a generalized Paley graph $G_{q,m}$, where $m = \dfrac{q-1}{k}$, with $k \geq 2$, that if $G_{q,m}$ is disconnected, then the connected components of $G_{q,m}$ are generalized Paley graphs over a proper subfield of $\mathbb{F}_q$.[12] This shows that the family of graphs of the form $G_{p,3}$, are at least connected graphs. So far, the only instances of of non-Ramanujan graphs found in the literature have been unions of generalized Paley graphs over proper subfields[12], so it is unlikely the $G_{p,m}$ with $p \equiv 1 \mod 3$ could ever fail to satisfy the Riemann hypothesis.

Conclusions—

In this paper we have shown that all Paley graphs satisfy the Riemann hypothesis, and several infinite families of generalized Paley graphs do as well. Particularly, generalized Paley graphs of the form $G_{q^m,q^{\ell+1}}$ where $q \in \{2,3,4\}$, $\ell = 1$, and $m \geq 4$ is even are Ramanujan.

Furthermore all generalized Paley graphs of the form $G_{p,3}$ where $p \equiv 2 \mod 3$ satisfy the Riemann hypothesis. The only known examples of generalized Paley graphs which do not are disconnected unions of Ramanujan generalized Paley graphs over proper subfields of the vertex set.

Discussion

Further investigation is needed to determine whether $G_{p,3}$ satisfies when $p \equiv 1 \mod 3$. Since there is a statement about the degree of such a graph, we need only determine the value of $\lambda(G)$ to conclude whether G is Ramanujan or not. Many of the results discussed in this paper are also discussed by Ricardo Podesta and Denis Videla in their paper "The Spectra of Generalized Paley Graphs of $(q^{\ell+1}) - th$ Powers and Applications." That paper is the most substantial investigation into generalized Paley graphs that I have encountered in the literature. Much of the background information in spectral graph theory came from "An Introduction to the Theory of Graph Spectra" by Cvetcović, Simic and Rowlinson, as well as "Graph Spectra for Complex Networks" by Piet Van Mieghem. The textbook "Zeta Functions of Graphs: a Stroll Through the Garden" by Audrey Terras is the quintessential source for all topics relating too zeta functions of graphs, and their applications, and was the primary source for the topics relating to the Riemann hypothesis for graphs.

Applications—

Ramanujan graphs are an important family of **expander** graphs. Expander graphs are not very easy to describe, but morally, they with strong connectivity properties. Expander graphs, and their properties, have been thoroughly surveyed by scholars in the fields of computational complexity, elliptic curve cryptography, and random graph theory. In fact, one survey "Research Directions in Number Theory" identified Ramnujan graphs in cryptography as one of the most relevant areas of research in number theory today.[13] One survey"Expander Graphs and their Applications," describes that "Expansion of a graph requires it to be simultaneosly sparse and highly connected".[8] Here "sparse" is opposite to "dense", where a dense graph has close to the maximum number of possible edges, and highly connected refers to the shortness minimal of walks between arbitrary vertex's on the graph. In general, for a graph to be sparse would suggest that it has weaker connectivity problems, making expander graphs, and Ramnanujan graphs in particular, noteworthy and useful. One particularly relevant application comes from a paper titled "Ramanujan Graphs for Post-Quantum Cryptography", which describes a cryptographic Hash function based on expander graphs[7]. The authors of that paper describe Ramanujan graphs as "an optimal structure of expander graphs." [7] The utility of this project, therefore, is in classifying known families of graphs as Ramanujan, marking them as ideal candidates for certain functions with substantial applications.

Appendix A: Definitions from Graph Theory

I have provided a list of definitions used throughout the paper. Some definitions were provided in the main text, but are included here for the convenience of the reader.

Adjacency matrix: a matrix representation of a graph given by

$$A_{ij} = \begin{cases} 1 \text{ If there is an edge between vertices } i \text{ and } j \\ 0 \text{ Otherwise.} \end{cases}$$

Backtrack: A walk is said to have a backtrack at a_k if $a_{k+1} = a_k^{-1}$.

Bipartite graph: A graph with vertex set $V = V_1 V_2$, where each vertex in V_1 is adjacent only to vertices in V_2, and each vertex in V_2 is adjacent only to vertices in V_1.

Complete graph: A graph where each vertex is connected to every other vertex.

Connected graph: A graph with only one component.

Component: A collection of vertices on a graph that are each connected by a walk.

Cycle: A walk on a graph where the initial vertex is equal to the terminal vertex.

Directed graph: A graph with oriented edges.

Finite field: A field with a finite number of elements.

Generalized Paley graph: A graph with vertex set representing a finite field, and edge set determined by m-th residues over that field.

Graph: An ordered pair $G = (V, E)$, with V a set of vertices and $E \subseteq V^2$ a set of edges.

Graph Isomorphism: Two graphs are isomorphic if there exists a bijection between their vertex sets that preserves edges.

Initial vertex: If (u, v) is the first oriented edge of a walk W, then u is the initial vertex of W.

Loop: An edge between a vertex and itself.

Paley graph:A graph with vertex set representing a finite field, and edge set determined by the quadratic residues over that field.

Pole: A root of the reciprocal of a function.

Prime cycle: A cycle which contains no tails or backtracks.

Ramanujan graph: A d-regular graph which has second largest eigenvalue λ_2 satisfying $\lambda_2 \leq \sqrt{d-1}$.

Simple graph: A graph containing no loops or multiple edges.

Tail: A walk is said to have a tail at a_k if $a_k = a_1.^{-1}$

Terminal vertex: If (u, v) is the last edge in a walk W, then v is called the terminal vertex of W.

Undirected graph: A graph with non-oriented edges.

Walk: A sequence of adjacent edges in a graph.

Appendix B: Sage Code

The following function can produce a generalized Paley graph object in sage by passing it two parameters: p, the size of the finite field, and m, the parameter we use to define a generalized Paley graph. This version produces generalized Paley graphs with vertex set equal to $\mathbb{F}_p$, where p is a prime.

```
def Generalized_Paley_prime(p,m):
    residues = set()
    for x in range(p):
        residues.add((x^m)%p)
    G = Graph(p)
    G.allow_loops(new = True)
    for i in range(p):
        for j in range(p):
            for residue in residues:
                if (i-j) == residue:
                    G.add_edges([(i,j)])
    G.remove_multiple_edges()
    G.remove_loops()
    return G
```

This code is a variation of the previous function, but produces a generalized Paley graph with vertex set equal to $\mathbb{F}_q$, where q is a power greater than one of a prime.

```
def Generalized_Paley_prime_power(p,m):
    G = Graph(p)
    k = GF(p, 'x')
    residues = set()
    for x in k:
        if x !=0:
            residues.add(x^m)
```

```
    for v1 in G.vertices():
        for v2 in G.vertices():
                if k.list()[v1]-k.list()[v2] in residues:
                    G.add_edges([(v1,v2)])
    return G
```

The following function can be used to check if a graph is Ramanujan in sage.

```
def is_Ramanujan(G):
    if G.is_regular():
        spec = []
        for eigenvalue in G.spectrum():
            spec.append(eigenvalue.abs())
        spec.sort()
    spectralGap = spec[-2]
    if  spectralGap <= 2*(G.average_degree()-1)^(1/2):
        return True
    else:
        return False
```

Literature Cited

1. Cvetkovic, D., Rowlinson, P. & Simic, S. *An Introduction to the Theory of Graph Spectra* (Cambridge University Press, 2010).
2. Godsil, C. & Royle, G. F. *Algebraic Graph Theory*. No. Book 207 in Graduate Texts in Mathematics (Springer, 2001).
3. Babai, L. Spectra of cayley graphs. *Journal of Combinatorial Theory, Series B* **27**, 180–189 (1979).

4. *Zeta Functions of Graphs: a Stroll Through the Garden, publisher=Cambridge University Press, year = 2011.*

5. Mieghem, P. v. *Graph Spectra for Complex Networks* (Cambridge University Press, 2010).

6. Murty, R. Ramanujan graphs. *Journal of the Ramanujan Mathematical Society* **18** (2003).

7. Jo, H., Sugiyama, S. & Yamasaki, Y. Ramanujan graphs for post-quantum cryptography. In Takagi, T. *et al.* (eds.) *International Symposium on Mathematics, Quantum Theory, and Cryptography*, 231–250 (Springer Singapore, Singapore, 2021).

8. Hoory, S., Linial, N. & Wigderson, A. Expander graphs and their applications. *Bull. Amer. Math. Soc.* **43**, 439–562 (2006).

9. Spielman, D. Lecture notes on cayley graphs (2018).

10. Podestá, R. A. & Videla, D. E. The spectra of generalized paley graphs of $q^\ell + 1$-th powers and applications (2018). URL https://arxiv.org/abs/1812.03332.

11. Wu, H.-L. & She, Y.-F. Cubes in finite fields and related permutations (2021). URL https://arxiv.org/abs/2105.09822.

12. Lim, T. K. & Praeger, C. E. On generalised paley graphs and their automorphism groups (2006). URL https://arxiv.org/abs/math/0605252.

13. Balakrishnan, J., Folsom, A., Lalín, M. & Manes, M. *Research Directions in Number Theory Women in Numbers IV: Women in Numbers IV* (2019).