The Expanding Constant, Ramanujan Graphs, and Winnie Li Graphs

Erin W. Kelly

Masters Thesis submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Master of Science
in
Mathematics

Dr. Peter Haskell, Chair
Dr. Gail Letzter
Dr. Charles Parry

May 10, 2006
Blacksburg, Virginia

Keywords: Expanding Constant, Ramanujan Graphs, Winnie Li Graphs

The Expanding Constant, Ramanujan Graphs, and Winnie Li Graphs

Erin W. Kelly

(ABSTRACT)

The expanding constant is a measure of graph connectivity that is important for certain applications. This paper discusses the mathematical foundations for the construction of Winnie Li's graphs and for the proof that Winnie Li's graphs are Ramanujan. The paper also establishes the implications of the Ramanujan property for the expanding constant.

Dedication

To Ryan, Mom & Dad, Megan, Logan, and Phelan

Acknowledgments

I would like to thank my family and friends who have provided me with continuous support and encouragement. In addition, I would like acknowledge my committee members for all their time and energy. In particular, thank you Dr. Haskell for your patience, for the countless hours of advising, explaining, re-explaining, and editing my paper, and for teaching me how to learn and appreciate mathematics.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

In this thesis, we will examine the relationships among the expanding constant of a graph, Ramanujan graphs, and Winnie Li's graphs. In order to discuss the expanding constant of a graph, we will first need to introduce some basic definitions.

Definition. A *graph*, X, is a set of vertices, V, connected by a set of edges, E, denoted $X = (V, E)$.

The graphs we will look at are undirected and connected. A graph is connected if there exists a path, i.e. a sequence of edges, between any two vertices. In particular, most of our graphs will be k-regular meaning that every vertex has k neighbors. In other words, there is exactly one edge between a vertex x and each of the k other distinct vertices. Now, we will define the boundary of a subset of the graph.

Definition. For the subset $F \subseteq V$, *the boundary of* F is the set of edges that connect a vertex in F with a vertex in $V - F$. The boundary of F is denoted ∂F.

The *expanding constant of* X is defined as

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

If we choose the subset to be at most half the vertices, then $\min\{|F|, |V - F|\} = |F|$. Therefore, an equivalent definition is

$$h(X) = \inf \left\{ \frac{|\partial F|}{|F|} \mid F \subseteq V, 0 < |F| \leq \frac{|V|}{2} < +\infty \right\}.$$

We will often use the latter of the two definitions, always assuming that the subset is at most half the vertices.

The expanding constant of the graph X is a measure of how efficiently connected the graph is with respect to subsets. If we view the graph as a network, this provides us with a strong motivation for studying the expanding constant of the graph. Networks are seen in almost every aspect of our daily lives. For example, consider a graph that represents the power grid for a neighborhood. We want the expanding constant to be a relatively large positive number. Since $h(X)$ is the infimum over all possible subsets, the worst case is when all the vertices of a subset are grouped together, with relatively few connections to vertices outside the subset, because the boundary of the subset is small while the number of edges may be large. The idea of keeping $|\partial F|$ large relative to $|F|$ is that one cannot isolate a relatively large number of vertices from the grid with a relatively small number of broken connections (edges). This prevents having a few mishaps leave lots of people without power. Although the power grid example is suggestive of the right issues and is an application of the ideas discussed, it is not a "pure" example because in a power grid, the vertex (or vertices) representing (or most closely attached to) the power source has a special status in the example.

An alternate example would be a communications network, such as the internet. There are no vertices (internet users) more important than others. In this example, we want to avoid having a relatively large number of vertices cut off from another relatively large number of vertices by a relatively small number of cut edges. In other words, we would want to make sure that in our network, a large group of internet users is not isolated from another large group of internet users by a small number of broken connections.

Our goal is to find a graph that is efficiently connected so that any large subset of the graph cannot be isolated from the rest of the graph by a relatively small number of disconnected edges. That is, we want to find a graph, or a family of graphs, that satisfies a fixed positive (preferably large) lower bound on the expanding constant, $h(X)$.

1.1 A Lower Bound on the Expanding Constant

Our goal, mentioned above, requires a lower bound on the expanding constant, $h(X)$ for the graph X. It turns out that we can find a bound on $h(X)$ in terms of the eigenvalues of a matrix that captures the geometry of the graph.

Definition. Suppose $X = (V, E)$ is a graph with n vertices, $V = \{x_1, x_2, \ldots, x_n\}$, and X has no multiple edges between vertices. Then the *adjacency matrix*, A, of the graph X is an $n \times n$ matrix consisting of 0's and 1's. In particular, $A = (a_{ij})$ where

$$a_{ij} = \left\{ \begin{array}{ll} 1 & \text{if there is an edge between } x_i \text{ and } x_j \\ 0 & \text{otherwise} \end{array} \right\}.$$

If X has no loops, i.e. an edge that begins and ends at the same vertex, then A has 0's

along the diagonal. Because we are working with an undirected graph, there is no distinction between a_{ij} and a_{ji}, and A is symmetric.

Remark 1.1. Suppose X is a graph with adjacency matrix A. When referring to the eigenvalues and eigenfunctions of the graph X, more precisely, we are referring to the eigenvalues and eigenfunctions of the adjacency matrix A that corresponds to the graph X.

In Chapter 3, we will prove that $\frac{(k-\mu_1)}{2}$ is a lower bound on the expanding constant where k and μ_1 are eigenvalues of the adjacency matrix of the graph. Since the bound on $h(X)$ involves the eigenvalues of the graph, we will want to consider Ramanujan graphs.

Definition. A finite, connected, k-regular graph X is Ramanujan if, for every eigenvalue μ of its adjacency matrix A, $\mu \neq \pm k$, we have that

$$|\mu| \leq 2\sqrt{k-1}.$$

From a result found in Davidoff, Sarnak and Valette's book [1], we are guaranteed that k is an eigenvalue of A since X is a k-regular graph.

The name Ramanujan refers to a self-trained Indian mathematician S. Ramanujan [1887-1919] ([9]). A Ramanujan conjecture proven by the mathematician P. Deligne was the foundation for some of the earliest interesting bounds on expanding constants for families of graphs. If X is a k-regular graph for $k > 2$, and X is Ramanujan, we note that $h(X) > 0$. Since X is Ramanujan, then all eigenvalues, μ, $\mu \neq k$, of the adjacency matrix satisfy

$$|\mu| \leq 2\sqrt{k-1}.$$

Now, using the lower bound for $h(X)$ and the upper bound on the eigenvalues of X, we have that

$$\begin{aligned}
\frac{(k-\mu_1)}{2} > 0 \iff & \frac{k-(2\sqrt{k-1})}{2} > 0 \\
\iff & k > 2\sqrt{k-1} \\
\iff & k^2 - 4k + 4 > 0 \\
\iff & (k-2)^2 > 0 \\
\iff & k > 2
\end{aligned}$$

Therefore, if X is a Ramanujan graph that is k-regular for $k > 2$, then the bounds on the eigenvalues guarantee a positive lower bound on $h(X)$. In addition, for a family of Ramanujan graphs where the regularity of the graph grows as the number of vertices grow, we see that $h(X)$ continues to grow as k grows, because

$$h(X) \geq \frac{k-2\sqrt{k-1}}{2},$$

which is an increasing function of the regularity, k.

1.2 The Expanding Constant of the Complete and Cyclic Graphs

The next two examples represent two extremes of the possible connectedness of a graph. First, consider the cyclic graph, C_n, on n vertices. In the cyclic graph, there is only one cycle through all n vertices. Figure 1.1 is the cyclic graph on 5 vertices. Note that the cyclic graph is a 2-regular graph with n vertices.

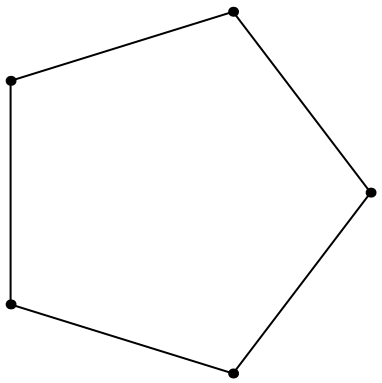

Figure 1.1: *Cyclic Graph,* C_5

Suppose $F \subseteq V$ such that $|F| = \frac{|V|}{2} = \frac{n}{2}$. Now if F is chosen so that every other vertex in the cycle is in F, then $|\partial F| \sim 2n$. If F is chosen to be a half-cycle, where all the vertices of F are grouped together, then $|\partial F| = 2$. Other choices of F give intermediate values. Therefore

$$h(C_n) = \inf\left\{\frac{|\partial F|}{|F|}\right\} = \frac{4}{n}.$$

Therefore, as $n \longrightarrow +\infty$ we see that $h(C_n) \longrightarrow 0$. In conclusion, the cyclic graph is not well-connected. Relating the cyclic graph to our communications network, the loss of two connections could isolate as many as half of the vertices from the other half.

The second example is the complete graph, K_n, with n vertices in which each vertex shares an edge with every other distinct vertex. Below is the complete graph on 5 vertices.

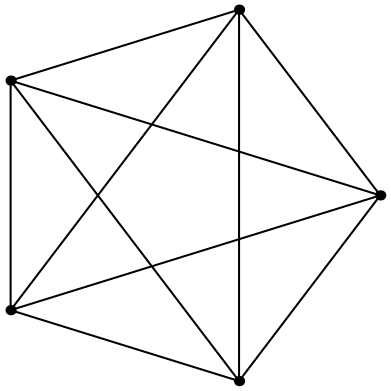

Figure 1.2: *Complete Graph,* K_5

For the graph K_n, because each vertex has $(n-1)$ edges, K_n is an $(n-1)$-regular graph. Let F be a subset of V such that $|F| \leq \frac{|V|}{2}$. For K_n, we know that $|V| = n$ and suppose $|F| = m$, then $|\partial F| = m(n-m)$. So,

$$h(K_n) = \inf\left\{\frac{|\partial F|}{\min\{|F|, |V-F|\}}\right\} = \inf\left\{\frac{|\partial F|}{|F|}\right\} = \frac{m(n-m)}{m} = (n-m).$$

For n even, $h(K_n) = \frac{n}{2}$. This expanding constant is good because it is greater than 0 for $n \geq 1$. In fact, the more vertices we add to the graph, the larger the expanding constant gets. Therefore, the complete graph will satisfy our goal, but with a high price to pay, specifically, the large number of edges in the graph. Therefore, it is not efficient to use the complete graph. In our communications network, this would mean that each internet user is directly connected to every other user on the internet.

1.3 A Family of Expanders

To achieve our goal, we can also consider families of graphs where each graph in the family is efficiently connected so that a relatively large subset of the graph cannot be isolated from another large subset of the graph with a relatively small number of broken edges. This criterion forces the expanding constant, $h(X)$, to be bounded away from 0 as the number of vertices in the graph goes to infinity.

An example of a family of graphs that fails the condition on $h(X)$ is a tiling of the plane. Consider a tiling of the plane by regular hexagons as shown in Figure 1.3. For each m, let $X_m = (V_m, E_m)$ be a finite, connected graph in the tiling of the plane such that for all m, as $m \to +\infty$, $|V_m| \to +\infty$. Each vertex of X_m has degree 3 except for the vertices "on the edge" of X_m. (The entire tiling represents a 3-regular graph, but an infinite graph.)

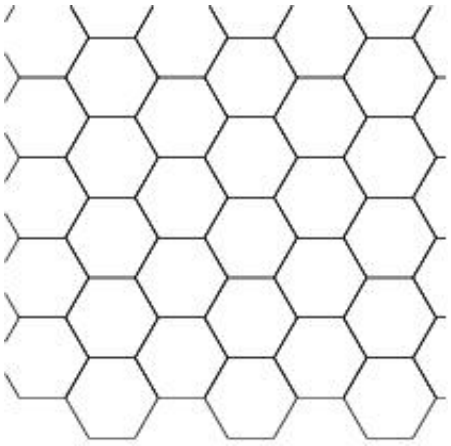

Figure 1.3: *Regular Hexagonal Tiling of the Plane*

When considering all possible subsets, F, of V_m, we will choose a subset that is grouped together. Hence it will have fewer edges in its boundary. Define the following subsets of X_m inductively where $F_1 = (\nu_1, \varepsilon_1)$ is the subset consisting of one center hexagon, and $F_2 = (\nu_2, \varepsilon_2)$ is a subset with an additional ring of hexagons around the center hexagon. For each m, define the subset $F_m = (\nu_m, \varepsilon_m)$ so there are $(m-1)$ rings around the center hexagon. Then $F_m = (\nu_m, \varepsilon_m)$ is a finite subset of the graph X_m with $\nu_m \subset V_m$ and $\varepsilon_m \subset E_m$ for all m. Recall that X_m is a finite, connected, 3-regular graph and $|V_m| \to +\infty$ as $m \to +\infty$. The expanding constant is defined to be

$$h(X) = \inf \left\{ \frac{|\partial F|}{|F|} \mid F \subseteq V, |F| \leq \frac{|V|}{2} \right\}.$$

To understand why $h(X_m) \to 0$ as $m \to +\infty$, we will consider the ratio of the "perimeter" versus the "area" of the subset F_m. This intuition comes from the definition of $h(X)$ by viewing $|\partial F|$, the boundary of F, as the perimeter and $|F|$, the number of vertices of F, as the area. Therefore,

$$\frac{|\partial F|}{|F|} \approx \frac{\text{Perimeter}}{\text{Area}}.$$

From our intuition about area and perimeter, we see that $|F_m|$ grows approximately like m^2 while $|\partial F_m|$ grows approximately like m. So,

$$h(X_m) \sim \frac{|\partial F_m|}{|F_m|} \sim \frac{m}{m^2} = \frac{1}{m},$$

thus as $m \to +\infty$, $h(X_m) \to 0$. This intuition can be developed into a rigorous proof. Hence, there is no positive lower bound on the expanding constant of the tiling of the plane by regular hexagons. This demonstrates that finding a family of graphs that satisfies the condition is no trivial task.

The terminology "family of expanders" refers to a family of graphs that satisfies a strong version of the condition.

Definition. Let $(X_m)_{m\geq 1}$ be a family of graphs $X_m = (V_m, E_m)$ indexed by $m \in \mathbb{N}$. Furthermore, fix $k \geq 2$. Such a family $(X_m)_{m\geq 1}$ of finite, connected, k-regular graphs is called a *family of expanders* if $|V_m| \to +\infty$ for $m \to +\infty$, and if there exists $\varepsilon > 0$, such that $h(X_m) \geq \varepsilon$ for every $m \geq 1$.

In a family of expanders, each graph is k-regular for a fixed $k \geq 2$ so the number of edges grows proportionately with the number of vertices. In addition, there is a uniform positive lower bound on $h(X_m)$ for all X_m in the family.

The next section will introduce a family of graphs called Winnie Li graphs. In its properties, the family of Winnie Li graphs lies between a family of expanders and the family of complete graphs. The Winnie Li graphs are k-regular, finite, connected graphs. However, they differ from a family of expanders because the regularity of the graph, k, is not fixed. As the number of vertices grows, both the regularity and the lower bound on the expansion constant grow, although, neither grows as fast as the corresponding quantity in the family of complete graphs.

1.4 Winnie Li's Graphs

In Chapter 5, we will describe a family of graphs that are defined using finite fields. For a prime p and $n \in \mathbb{N}$, the Winnie Li graphs are finite, connected, and $k = (\frac{p^n-1}{p-1})$-regular with p^n vertices. We will show that for the special case when $n = 2$, we know the eigenvalues of the adjacency matrix. A deep result shows that these eigenvalues satisfy a bound that makes these graphs Ramanujan. In order to understand the construction of the Winnie Li graphs, Chapter 4 will provide background information in Abstract Algebra, particularly about fields and Galois extensions. For the definition below, F_{p^n} is a finite field with p^n elements, and Θ_n is the kernel of a homomorphism that is defined using elements of the Galois group of the field extension F_{p^n}/F_p.

Definition. A *Winnie Li graph* is the Cayley graph $X = (F_{p^n}, \Theta_n)$ with vertices defined to be the elements of F_{p^n} and the edges of each vertex x given by $x + s$ for $s \in \Theta_n$. These are $k = (\frac{p^n-1}{p-1})$-regular graphs with p^n vertices.

For values of n that are even, Θ_n is a symmetric set of generators of F_{p^n}, and these graphs are non-directed graphs. In Chapter 5, we focus on examples of Winnie Li graphs with $n = 2$. Winnie Li's graphs are very interesting, and they achieve our goal for obtaining a positive lower bound on the expanding constant. In fact, the graphs are Ramanujan for $n = 2$, and as the number of vertices increases, the lower bound on the expanding constant increases. This differs from a true family of expanders, which has fixed regularity and a fixed lower

bound on the expanding constant for all the graphs in the family. However, Winnie Li graphs are not ideal. In general, as the number of vertices increases, we would prefer just to add additional edges to the graph, but with a Winnie Li graph $X = (F_{p^n}, \Theta_n)$, as $p \to +\infty$, we need to add edges and change the existing ones. Therefore, considering the Winnie Li graph as representing a communications network in our previous example, as soon as we add new users to the network we would need to completely change all existing connections, which could be very costly and cumbersome.

In Chapter 7, we will compute the eigenvalues of the adjacency matrix for the complete graph and for two examples of Winnie Li graphs. We will use these eigenvalues to explicitly find the lower bound on $h(X)$ and show that the graphs are Ramanujan. In addition, we will observe some interesting patterns in the characteristic polynomials of the Winnie Li graphs, for $n = 2$.

All of these concepts and examples have enabled us to illustrate the underlying ideas of working with eigenvalues to create useful bounds, specifically the Ramanujan bound and the expanding constant bound.

Chapter 2

Linear Algebraic Foundations

In Chapter 3, we will establish the lower bound on the expanding constant of a graph $X = (V, E)$ by using the eigenvalues of the adjacency matrix of $X = (V, E)$. Therefore, in this chapter we will provide the background information that is necessary for the proof. The proof in Chapter 3, works in the vector spaces of $\ell^2 V$ and $\ell^2 E$, which are the vector spaces of functions defined on the vertices and on the edges of a graph, respectively. In the current chapter, we will focus our discussion on orthonormal bases, linear maps and their adjoints, and self-adjoint matrices. All the results in this chapter are standard, (See e.g. 337-341, [6]), but we wrote many of the proofs without reference to any source.

Let V be a finite-dimensional vector space over $\mathbb{C}$ and let $\mathbf{x}, \mathbf{y} \in V$ such that $\mathbf{x} = (a_1, a_2, \ldots, a_n)$ and $\mathbf{y} = (b_1, b_2, \ldots, b_n)$, both represented with respect to a chosen basis of V. Define the inner product on V to be

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{n} a_i \overline{b_i}.$$

Then for all $\mathbf{x}, \mathbf{y}, \mathbf{z} \in V$ and $c \in \mathbb{C}$, the inner product of V has the following properties:
a) $\langle \mathbf{x} + \mathbf{y}, \mathbf{z} \rangle = \langle \mathbf{x}, \mathbf{z} \rangle + \langle \mathbf{y}, \mathbf{z} \rangle$
b) $\overline{\langle c\mathbf{x}, \mathbf{y} \rangle} = c\langle \mathbf{x}, \mathbf{y} \rangle$
c) $\overline{\langle \mathbf{x}, \mathbf{y} \rangle} = \langle \mathbf{y}, \mathbf{x} \rangle$, the complex conjugate
d) $\langle \mathbf{x}, \mathbf{x} \rangle > 0$ if and only if $\mathbf{x} \neq \mathbf{0}$
e) $\|\mathbf{x}\| = \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle}$, where $\|\mathbf{x}\|$ is the magnitude or length of $\mathbf{x}$
Recall that a linear map, $T : V \longrightarrow W$, acting on a vector space satisfies the following property: $T(c\mathbf{x} + \mathbf{y}) = cT(\mathbf{x}) + T(\mathbf{y})$ for all $\mathbf{x}, \mathbf{y} \in V$ and $c \in \mathbf{C}$.

Using the inner product of a vector space allows us to easily identify when two vectors are orthogonal.

Definition. For vectors $\mathbf{x}, \mathbf{y} \in V$, if $\langle \mathbf{x}, \mathbf{y} \rangle = 0$ then $\mathbf{x}$ is *orthogonal* to $\mathbf{y}$.

Definition. Let $\beta = \{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n\}$ be a set of vectors. Then β is called an *orthonormal* set of vectors if $\langle \mathbf{x_i}, \mathbf{y_j} \rangle = \left\{ \begin{array}{ll} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \end{array} \right\} = \delta_{i,j}$.

Remark 2.1. It is implicit in the coordinate-based definition of the inner product given on the preceding page that the basis of V is an orthonormal basis.

In an inner product space, it is convenient to work with an orthogonal or orthonormal basis. For example, an orthogonal set of vectors is always independent and with an orthonormal basis, we can use the inner product to write any vector in V as a linear combination of the basis vectors.

Lemma 2.2. *An orthogonal set of nonzero vectors in an inner product space is always independent.*

Proof. Let V be an inner product space and let $\beta = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ be an orthogonal set of nonzero vectors. For $a_1, a_2, \ldots, a_n \in F$, suppose $a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n = 0$ Then for an arbitrary i,

$$\begin{aligned} 0 &= \langle \mathbf{0}, \mathbf{v}_i \rangle \\ &= \langle a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n, \mathbf{v}_i \rangle \\ &= a_1\langle \mathbf{v}_1, \mathbf{v}_i \rangle + a_2\langle \mathbf{v}_2, \mathbf{v}_i \rangle + \cdots + a_n\langle \mathbf{v}_n, \mathbf{v}_i \rangle \end{aligned}$$

by the properties of the inner product. Since β is an orthogonal set, $\langle \mathbf{v}_i, \mathbf{v}_j \rangle = 0 \iff i \neq j$. Thus

$$0 = a_1\langle \mathbf{v}_1, \mathbf{v}_i \rangle + a_2\langle \mathbf{v}_2, \mathbf{v}_i \rangle \cdots + a_n\langle \mathbf{v}_n, \mathbf{v}_i \rangle = a_i\langle \mathbf{v}_i, \mathbf{v}_i \rangle.$$

By assumption, $\mathbf{v}_i \neq 0$ for all i, so $\langle \mathbf{v}_i, \mathbf{v}_i \rangle \neq 0$. Therefore, it must be that $a_i = 0$ for all i. That is, if $a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n = 0$ then $a_i = 0$ for $1 \leq i \leq n$. Thus $\beta = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ is a set of independent vectors. □

As mentioned above, in an inner product space with a chosen orthonormal basis, we can easily write an arbitrary vector as a linear combination of basis elements by using the inner product to find the coefficients.

Lemma 2.3. *Let V be an inner product space with orthonormal basis $\{\boldsymbol{v}_i\}_{i=1}^n$. Then for a vector $\boldsymbol{v} \in V$,*

$$\boldsymbol{v} = \sum_{j=1}^{n} \langle \boldsymbol{v}, \boldsymbol{v}_j \rangle \boldsymbol{v}_j.$$

Proof. Let V be an inner product space with orthonormal basis $\{\mathbf{v}_i\}_{i=1}^n$, then for each $\mathbf{v} \in V$, there exists a set of scalars $a_1, a_2, \ldots, a_n$ such that $\mathbf{v} = \sum_{i=1}^{n} a_i\mathbf{v}_i$. For each j,

$$\langle \mathbf{v}, \mathbf{v}_j \rangle = \langle \sum_{i=1}^{n} a_i\mathbf{v}_i, \mathbf{v}_j \rangle = \sum_{i=1}^{n} a_i\langle \mathbf{v}_i, \mathbf{v}_j \rangle$$

by the properties of the inner product space. Since $\{\mathbf{v}_i\}_{i=1}^n$ is an orthonormal basis, then $\langle \mathbf{v}_i, \mathbf{v}_j \rangle = \delta_{i,j}$. Hence,

$$\langle \mathbf{v}, \mathbf{v}_j \rangle = \sum_{i=1}^{n} a_i \langle \mathbf{v}_i, \mathbf{v}_j \rangle = \sum_{i=1}^{n} a_i \delta_{i,j} = a_j$$

Thus for each $\mathbf{v} \in V$, $\mathbf{v} = \sum_{j=1}^{n} \langle \mathbf{v}, \mathbf{v}_j \rangle \mathbf{v}_j$. □

This method of finding the coefficients for each basis vector of V is more convenient because it is easy to compute.

A linear map can be expressed as a matrix with respect to chosen bases. On the other hand, we can also choose a matrix, which then determines a unique linear map with respect to a chosen orthonormal basis.

Lemma 2.4. *Let V and W be finite-dimensional inner product spaces with chosen orthonormal bases $\{\boldsymbol{v}_i\}_{i=1}^m$ and $\{\boldsymbol{w}_j\}_{j=1}^n$. For any choice of $n \cdot m$ scalars a_{ji} there is one and only one map $L : V \longrightarrow W$ satisfying for all i and j, $\langle L(\boldsymbol{v}_i), \boldsymbol{w}_j \rangle = a_{ji}$.*

Proof. Choose $n \cdot m$ scalars a_{ji}. The linear map $L : V \longrightarrow W$ is uniquely determined by the images of the basis elements of V. So $L(\mathbf{v}_i)$ is a vector in W. We can use the method in Lemma 2.3, to write $L(\mathbf{v}_i)$ as a linear combination of orthonormal basis elements. That is, $\langle L(\mathbf{v}_i), \mathbf{w}_j \rangle = a_{ji}$, hence

$$L(\mathbf{v}_i) = \sum_{j=1}^{n} a_{ji} \mathbf{w}_j.$$

By determining the images of the basis elements of V, we have established the existence of the linear map L. Since the basis elements are independent and they span V, L is unique. □

Definition. Let $T : V \longrightarrow W$ be a linear map. The *adjoint* of T, noted by $T^* : W \longrightarrow V$, is defined by the property that for all $\mathbf{v} \in V$ and $\mathbf{w} \in W$,

$$\langle T(\mathbf{v}), \mathbf{w} \rangle_W = \langle \mathbf{v}, T^*(\mathbf{w}) \rangle_V,$$

or equivalently, $\langle T^*(\mathbf{w}), \mathbf{v} \rangle_V = \langle \mathbf{w}, T(\mathbf{v}) \rangle_W$.

Lemma 2.5. *Let $T : V \longrightarrow W$ be a linear map and let $T^* : W \longrightarrow V$ be its adjoint. Then T^* exists, is unique, and is linear.*

Proof. The linear map $T : V \longrightarrow W$ has determined the $n \cdot m$ scalars a_{ji} where $\langle L(\mathbf{v}_i), \mathbf{w}_j \rangle = a_{ji}$. By the property of the adjoint of T, $a_{ji} = \langle T(\mathbf{v}), \mathbf{w} \rangle = \langle \mathbf{v}, T^*(\mathbf{w}) \rangle$. Therefore, by Lemma

2.4, T^* exists and is unique. To show that T^* is linear, let $\mathbf{x}, \mathbf{y} \in W$ and $c \in \mathbb{C}$, then by the properties of the inner product,

$$\begin{aligned}\langle T^*(c\mathbf{x}+\mathbf{y}), \mathbf{v}\rangle &= \langle c\mathbf{x}+\mathbf{y}, T(\mathbf{v})\rangle \\ &= c\langle \mathbf{x}, T(\mathbf{v})\rangle + \langle \mathbf{y}, T(\mathbf{v})\rangle \\ &= c\langle T^*(\mathbf{x}), \mathbf{v}\rangle + \langle T^*(\mathbf{y}), \mathbf{v}\rangle \\ &= \langle cT^*(\mathbf{x}) + T^*(\mathbf{y}), \mathbf{v}\rangle.\end{aligned}$$

Therefore, $T^*(c\mathbf{x}+\mathbf{y}) = cT^*(\mathbf{x}) + T^*(\mathbf{y})$, so T^* is linear. □

We have seen how a linear map and its adjoint are related by examining inner products. However, we can also consider how they are related through their matrix representations with respect to orthonormal bases.

Lemma 2.6. *Let $\mathbb{R}^m$ and $\mathbb{R}^n$ have the standard $\mathbb{R}$-valued inner product. If $T : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ is represented by the matrix A with respect to the standard orthonormal bases, then T^* is represented by A^T, the transpose of A.*

Proof. Suppose $T : \mathbb{R}^m \longrightarrow \mathbb{R}^n$ is represented by the matrix A with respect to the standard orthonormal basis. Let $\{\mathbf{e}_i\}_{i=1}^m$ and $\{\mathbf{f}_j\}_{j=1}^n$ be the standard orthonormal bases for $\mathbb{R}^m$ and $\mathbb{R}^n$, respectively. Then $A\mathbf{e}_i = T(\mathbf{e}_i)$ for all i where $A\mathbf{e}_i$ is the ith column of A. Similarly, let A^* be the matrix representation of T^* with respect to the standard orthonormal basis. Then $A^*\mathbf{f}_j = T^*(\mathbf{f}_j)$ for all j, where $A^*\mathbf{f}_j$ is the jth column of A^*. So,

$$\langle T(\mathbf{e}_i), \mathbf{f}_j\rangle = \langle \mathrm{A}\mathbf{e}_i, \mathbf{f}_j\rangle = a_{ji}, \tag{2.1}$$

where a_{ij} is the jith entry of A. Alternatively, by definition of the adjoint,

$$\langle T(\mathbf{e}_i), \mathbf{f}_j\rangle = \langle \mathbf{e}_i, T^*(\mathbf{f}_j)\rangle = \langle \mathbf{e}_i, \mathrm{A}^*(\mathbf{f}_j)\rangle = \overline{a}^*_{ij}, \tag{2.2}$$

where $\overline{a}^*_{ij}$ is the ijth entry of $\overline{A}^*$. Since A and A^* are matrices with entries in $\mathbb{R}$, then $\overline{A} = A$ and $\overline{A}^* = A^*$, so $\overline{a}^*_{ij} = a^*_{ij}$. By the equality of equations 2.1 and 2.2, we have that for all i and j, $a_{ji} = a^*_{ij}$ which by definition means that $A^* = A^T$. Hence the matrix representation for T^* is A^T. □

Lemma 2.7. *Suppose $\mathbb{C}^m$ and $\mathbb{C}^n$ have the standard $\mathbb{C}$-valued inner products. If $T : \mathbb{C}^m \longrightarrow \mathbb{C}^n$ is represented by the matrix A with respect to the standard orthonormal bases, then T^* is represented by $\overline{A}^T$, the conjugate transpose of A.*

Proof. Suppose $T : \mathbb{C}^m \longrightarrow \mathbb{C}^n$ is represented by A with respect to the standard orthonormal bases. Let $\{\mathbf{e}_i\}_{i=1}^m$ and $\{\mathbf{f}_j\}_{j=1}^n$ be the standard orthonormal bases for $\mathbb{C}^m$ and $\mathbb{C}^n$, respectively. Then $\mathrm{A}\mathbf{e}_i = T(\mathbf{e}_i)$ for all i and note $\mathrm{A}\mathbf{e}_i$ is the ith column of A. So

$$\langle T(\mathbf{e}_i), \mathbf{f}_j\rangle = \langle \mathrm{A}\mathbf{e}_i, \mathbf{f}_j\rangle = a_{ji}, \tag{2.3}$$

where a_{ji} is the jith entry of A. Let A^* is the matrix representation of T^* with respect to $\{\mathbf{f}_j\}_{j=1}^n$. By the definition of the adjoint of T, we have that

$$\langle T(\mathbf{e}_i), \mathbf{f}_j \rangle = \langle \mathbf{e}_i, T^*(\mathbf{f}_j) \rangle = \langle \mathbf{e}_i, A^* \mathbf{f}_j \rangle = \overline{a}_{ij}^*, \tag{2.4}$$

where $\overline{a}_{ij}^*$ is the ijth entry of $\overline{A}^*$. Therefore, for all i and j,

$$a_{ji} = \overline{a}_{ij}^*.$$

Hence $\overline{A}^* = A^T \implies A^* = \overline{A}^T$. Hence the matrix representation for T^* is $\overline{A}^T$ in $\mathbb{C}^n$. □

Definition. A linear map , $T : V \longrightarrow V$ defined on an inner product space and satisfying, for all $\mathbf{x}, \mathbf{y} \in V$, $\langle T(\mathbf{x}), T(\mathbf{y}) \rangle = \langle \mathbf{x}, \mathbf{y} \rangle$ is called an *orthogonal* map in the real case and *unitary* in the complex case.

This linear map has various special properties, one being that its adjoint is its inverse.

Lemma 2.8. *If T is orthogonal/unitary then*
1) $\|T(\boldsymbol{x})\| = \|\boldsymbol{x}\|$
2) $T^{-1} = T^*$, T^{-1} *is also orthogonal/unitary*
3) $\{\boldsymbol{v}_i\}_{i=1}^n$ *is an orthonormal basis for* $V \iff \{T(\boldsymbol{v}_i)\}_{i=1}^n$ *is an orthonormal basis for* V

Proof. Let $T : V \longrightarrow V$ be orthogonal/unitary such that for all $\mathbf{x}, \mathbf{y} \in V$,

$$\langle T(\mathbf{x}), T(\mathbf{y}) \rangle = \langle \mathbf{x}, \mathbf{y} \rangle.$$

1): For $x \in V$, $\|\mathbf{x}\| = \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle} = \sqrt{\langle T(\mathbf{x}), T(\mathbf{x}) \rangle} = \|T(\mathbf{x})\|$ since T is orthogonal.
2): First, show that T is invertible. So the kernel of T is

$$\ker(T) = \{\mathbf{v} \in V \mid T(\mathbf{v}) = \mathbf{0}\}.$$

From part (1), $T(\mathbf{x}) = \mathbf{0} \iff \|T(\mathbf{x})\| = 0 \iff \|\mathbf{x}\| = 0$. Since T is orthogonal/unitary, we have that

$$\begin{aligned} \ker(T) &= \{\mathbf{v} \in V \mid \langle T(\mathbf{v}), T(\mathbf{w}) \rangle = 0 \text{ for all } \mathbf{w} \in V\} \\ &= \{\mathbf{v} \in V \mid \langle \mathbf{v}, \mathbf{w} \rangle = 0 \text{ for all } \mathbf{w} \in V\} \\ &= \{\mathbf{v} \in V \mid \mathbf{v} = \mathbf{0}\} \\ &= \{\mathbf{0}\}. \end{aligned}$$

Since $\ker(T) = \{\mathbf{0}\}$ then T is one-to-one, and since V is finite-dimensional, then T is onto. Therefore T is invertible, and hence T^{-1} exists. Now, we will show that T^{-1} is orthogonal/unitary and that is the adjoint of T. Since T is orthogonal/unitary, for all $\mathbf{x}, \mathbf{y} \in V$ we have,

$$\langle T^{-1}(\mathbf{x}), T^{-1}(\mathbf{y}) \rangle = \langle T(T^{-1}(\mathbf{x})), T(T^{-1}(\mathbf{y})) \rangle = \langle \mathbf{x}, \mathbf{y} \rangle.$$

Hence, T^{-1} is orthogonal/unitary. Therefore,

$$\langle T^{-1}(T(\mathbf{x})), T^{-1}(\mathbf{y})\rangle = \langle T(\mathbf{x}), \mathbf{y}\rangle.$$

But we can also rewrite the above as

$$\langle T^{-1}(T(\mathbf{x})), T^{-1}(\mathbf{y})\rangle = \langle \mathbf{x}, T^{-1}(\mathbf{y})\rangle.$$

So for all $\mathbf{x}, \mathbf{y} \in V$, $\langle T(\mathbf{x}), \mathbf{y}\rangle = \langle \mathbf{x}, T^{-1}(\mathbf{y})\rangle$, so T^{-1} satisfies the adjoint property of T and $T^{-1} = T^*$.
3): ($\Rightarrow$) Suppose $\{\mathbf{v}_i\}_{i=1}^n$ is an orthonormal basis for V. Then for all $\mathbf{v}_i, \mathbf{v}_j \in \{\mathbf{v}_i\}_{i=1}^n$, $\langle \mathbf{v}_i, \mathbf{v}_j\rangle = \delta_{ij}$. Since T is orthogonal/unitary then $\langle T(\mathbf{v}_i), T(\mathbf{v}_j)\rangle = \langle \mathbf{v}_i, \mathbf{v}_j\rangle = \delta_{ij}$. The inner product calculation shows that $\{T(\mathbf{v}_i)\}_{i=1}^n$ is an orthonormal set with the number of elements equal to the dimension of V, so this set must be a basis for V. Therefore, $\{T(\mathbf{v}_i)\}_{i=1}^n$ is an orthonormal basis for V.
($\Leftarrow$) Similarly, suppose $\{T(\mathbf{v}_i)\}_{i=1}^n$ is an orthonormal basis for V. Then for all $T(\mathbf{v}_i), T(\mathbf{v}_j) \in \{T(\mathbf{v}_i)\}_{i=1}^n$, $\langle T(\mathbf{v}_i), T(\mathbf{v}_j)\rangle = \delta_{ij}$. So $\langle \mathbf{v}_i, \mathbf{v}_j\rangle = \langle T(\mathbf{v}_i), T(\mathbf{v}_j)\rangle = \delta_{ij}$. By the same reasoning above, $\{\mathbf{v}_i\}_{i=1}^n$ is an orthonormal basis for V. □

Below is a useful result that enables us to identify when a map is orthogonal by looking at its matrix representation.

Corollary 2.9. *Let std be the standard ordered orthonormal basis for V and let $T : V \longrightarrow V$ be a linear map. The columns of $[T]_{std}$, viewed as standard column vectors of numbers form and orthonormal basis of $V \iff T$ is orthogonal/unitary.*

Proof. ($\Leftarrow$) Suppose T is orthogonal/unitary and consider $[T]_{std}$, the matrix representation of T with respect to $std = \{\mathbf{e}_i\}_{i=1}^n$. From Lemma 2.8, we know that $\{T(\mathbf{e}_i)\}_{i=1}^n$ is an orthonormal basis for V. Thus for all i and j, $\langle T(\mathbf{e}_i), T(\mathbf{e}_j)\rangle = \delta_{ij}$, and $T(\mathbf{e}_i) = \sum_{k=1}^n a_{ki}\mathbf{e}_k$. Since $\{\mathbf{e}_i\}$ is orthonormal,

$$\begin{aligned}\langle T(\mathbf{e}_i), T(\mathbf{e}_j)\rangle &= \langle \sum_{k=1}^n a_{ki}\mathbf{e}_k, \sum_{k=1}^n a_{kj}\mathbf{e}_k\rangle \\ &= \sum_{k=1}^n a_{ki}\overline{a}_{kj}\langle \mathbf{e}_k, \mathbf{e}_k\rangle \\ &= \sum_{k=1}^n a_{ki}\overline{a}_{kj},\end{aligned}$$

But from above,

$$\sum_{k=1}^n a_{ki}\overline{a}_{kj} = [T(\mathbf{e}_i)]_{std} \cdot \overline{[T(\mathbf{e}_j)]}_{std} = \delta_{ij}.$$

So $\{[T(\mathbf{e}_i)]_{std}\}_{i=1}^n$ is an orthonormal basis for V.
($\Rightarrow$) Suppose the columns of $[T]_{std}$ viewed as standard column vectors of numbers, form an orthonormal basis of V. That is, $\{[T(\mathbf{e}_i)]_{std}\}_{i=1}^n$ is an orthonormal basis for V. Thus $\langle T(\mathbf{e}_i), T(\mathbf{e}_j)\rangle = \delta_{ij} = \langle \mathbf{e}_i, \mathbf{e}_j\rangle$ for all i and j. Let $\mathbf{x}, \mathbf{y} \in V$ such that $\mathbf{x} = \sum_{i=1}^n a_i\mathbf{e}_i$ and $\mathbf{y} = \sum_{i=1}^n b_i\mathbf{e}_i$. Then

$$\langle \mathbf{x}, \mathbf{y}\rangle = \langle \sum_{i=1}^n a_i\mathbf{e}_i, \sum_{i=1}^n b_i\mathbf{e}_i\rangle = \sum_{i=1}^n a_i\overline{b}_i\langle \mathbf{e}_i, \mathbf{e}_j\rangle = \sum_{i=1}^n a_i\overline{b}_i$$

and

$$\begin{aligned}\langle T(\mathbf{x}), T(\mathbf{y})\rangle &= \langle T(\sum_{i=1}^n a_i\mathbf{e}_i), T(\sum_{i=1}^n b_i\mathbf{e}_i)\rangle \\ &= \sum_{i=1}^n a_i\overline{b}_i\langle T(\mathbf{e}_i), T(\mathbf{e}_i)\rangle \\ &= \sum_{i=1}^n a_i\overline{b}_i.\end{aligned}$$

Therefore, $\langle \mathbf{x}, \mathbf{y}\rangle = \langle T(\mathbf{x}), T(\mathbf{y})\rangle$, so T is orthogonal/unitary. □

Definition. For V an inner product space and a linear map $T : V \longrightarrow V$, T is *self-adjoint* if $T = T^*$. That is, for all $\mathbf{x}, \mathbf{y} \in V$, $\langle T(\mathbf{x}), \mathbf{y}\rangle = \langle \mathbf{x}, T(\mathbf{y})\rangle$. A matrix A is called self-adjoint if it represents (with respect to the standard ordered bases) a self-adjoint linear map.

We can also describe the matrix representations of $T = T^*$ with respect to a chosen basis. From previous results, Lemmas 2.6 and 2.7, if A is the matrix representation of T with respect to β, a basis of V, then the matrix representation of T^* is A^T and $\overline{A}^T$ in $\mathbb{R}^n$ and $\mathbb{C}^n$ respectively. Thus T is self-adjoint if and only if $A = A^T$ in $\mathbb{R}^n$ and $A = \overline{A}^T$ in $\mathbb{C}^n$. Since we now understand what the matrix representation of T will look like, we can investigate the eigenvalues and eigenvectors of a self-adjoint matrix.

Lemma 2.10. *If A is a self-adjoint matrix representing the linear map T, then*
1) all eigenvalues of A are real
2) if $\boldsymbol{x}$ and $\boldsymbol{y}$ are eigenvectors associated with distinct eigenvalues of A then $\langle \boldsymbol{x}, \boldsymbol{y}\rangle = 0$
3) if $\boldsymbol{x}$ is an eigenvector of A and $W = \{\boldsymbol{v} \in V \mid \langle \boldsymbol{v}, \boldsymbol{x}\rangle = 0\}$, then if $\boldsymbol{w} \in W$, then $T(\boldsymbol{w}) \in W$

Proof. 1): Suppose λ is an eigenvalue of A and $\mathbf{x}$ is its corresponding eigenvector, then $A\mathbf{x} = \lambda\mathbf{x}$. To show that λ is real, we must demonstrate that $\lambda = \overline{\lambda}$. So,

$$\langle T(\mathbf{x}), \mathbf{x}\rangle = \langle \lambda\mathbf{x}, \mathbf{x}\rangle = \lambda\langle \mathbf{x}, \mathbf{x}\rangle.$$

In addition, since T is self-adjoint,

$$\langle T(\mathbf{x}), \mathbf{x}\rangle = \langle \mathbf{x}, T(\mathbf{x})\rangle = \langle \mathbf{x}, \lambda\mathbf{x}\rangle = \overline{\lambda}\langle \mathbf{x}, \mathbf{x}\rangle.$$

Thus we have $\lambda\langle \mathbf{x}, \mathbf{x}\rangle = \overline{\lambda}\langle \mathbf{x}, \mathbf{x}\rangle \implies \lambda = \overline{\lambda}$. So λ is real.
2): Let $\mathbf{x}$ and $\mathbf{y}$ be eigenvectors corresponding to distinct eigenvalues α , β, respectively. Then $A\mathbf{x} = \alpha\mathbf{x} = T(\mathbf{x})$ and $A\mathbf{y} = \beta\mathbf{y} = T(\mathbf{x})$. Therefore,

$$\langle T(\mathbf{x}), \mathbf{y}\rangle = \langle \alpha\mathbf{x}, \mathbf{y}\rangle = \alpha\langle \mathbf{x}, \mathbf{y}\rangle.$$

Since T is self-adjoint,

$$\langle T(\mathbf{x}), \mathbf{y}\rangle = \langle \mathbf{x}, T(\mathbf{y})\rangle = \langle \mathbf{x}, \beta\mathbf{y}\rangle = \overline{\beta}\langle \mathbf{x}, \mathbf{y}\rangle = \beta\langle \mathbf{x}, \mathbf{y}\rangle,$$

by part (1). Hence $(\alpha - \beta)\langle \mathbf{x}, \mathbf{y}\rangle = 0$. Since we assumed α and β are distinct, $(\alpha - \beta) \neq 0$ thus $\langle \mathbf{x}, \mathbf{y}\rangle = 0$.
3): Suppose $\mathbf{x}$ is an eigenvector of A with corresponding eigenvalue λ and set

$$W = \{\mathbf{v} \in V \mid \langle \mathbf{v}, \mathbf{x}\rangle = 0\}.$$

Let $\mathbf{w} \in W$ and show that $T(\mathbf{w}) \in W$. Since $\mathbf{w} \in W$, $\langle \mathbf{w}, \mathbf{x}\rangle = 0$ and we want to show that $\langle T(\mathbf{w}), \mathbf{w}\rangle = 0$. Since T is self-adjoint and $\mathbf{x}$ is an eigenvector, then

$$\langle T(\mathbf{w}), \mathbf{x}\rangle = \langle \mathbf{w}, T(\mathbf{x})\rangle = \langle \mathbf{w}, \lambda\mathbf{x}\rangle.$$

By the properties of inner product, $\langle \mathbf{w}, \lambda\mathbf{x}\rangle = \overline{\lambda}\langle \mathbf{w}, \mathbf{x}\rangle = \overline{\lambda} \cdot 0 = 0$. Therefore $\langle T(\mathbf{w}), \mathbf{x}\rangle = 0$. So $T(\mathbf{w}) \in W$. □

Theorem 2.11. *If a linear map $T : V \longrightarrow V$ is self-adjoint, then V has an orthonormal basis of eigenvectors for T.*

Proof. (By Induction on $dim(V)$) Let T be a self-adjoint linear map from $V \longrightarrow V$, where V is an inner product space. Base case: Let $dim(V) = 1$. Since T is self-adjoint, then $\{1\}$ is a basis for V. In addition, the matrix representation of T is a 1×1 matrix, say A. For the eigenvalue λ of A, $A \cdot 1 = \lambda \cdot 1 \Leftrightarrow \lambda = A$ hence $\{1\}$is also an eigenvector for T. So the base case is true. Assume that T is self-adjoint and $dim(V) < 1$, then V has an orthonormal basis of eigenvectors. Show that this is true when $dim(V) = n$. Let λ be an eigenvalue for A, the self-adjoint matrix representation of T. Then there exists a corresponding eigenvector $\mathbf{x}$ such that $T(\mathbf{x}) = \lambda\mathbf{x}$. Let $W = \{\mathbf{v} \in V \mid \langle \mathbf{v}, \mathbf{x}\rangle = 0\}$. From Lemma 2.10, for all $\mathbf{w} \in W$ then $T(\mathbf{w}) \in W$. So $T\mid_W$ maps W into W. Now show that $T\mid_W$ is self-adjoint. That is, for all $\mathbf{w}$, $\mathbf{v} \in W$, $\langle T(\mathbf{w}), \mathbf{v}\rangle = \langle \mathbf{w}, T(\mathbf{v})\rangle$. Consider $\mathbf{w}$, $\mathbf{v} \in W$, then $T(\mathbf{w})$, $T(\mathbf{v}) \in W$. Since T is self-adjoint on V and $\mathbf{w}, \mathbf{v} \in W \subset V$, we know that $\langle T(\mathbf{w}), \mathbf{v}\rangle = \langle \mathbf{w}, T(\mathbf{v})\rangle$. However, since $T(\mathbf{w}), T(\mathbf{v}) \in W \subset V$ then $\langle T(\mathbf{w}), \mathbf{v}\rangle = \langle \mathbf{w}, T(\mathbf{v})\rangle$ is an inner product defined in W because all elements are in W. Therefore, T is self-adjoint on W. Now, $dim(W) = n - 1$ so by the inductive hypothesis, there exists an orthonormal basis of eigenvectors for W. Let $\{\mathbf{w}_i\}_{i=1}^{n-1}$ be the orthonormal basis of eigenvectors. Note that $\mathbf{x}$ is orthogonal to all $\mathbf{w}_i \in \{\mathbf{w}_i\}$. By Lemma 2.2, $\{\mathbf{x}\} \cup \{\mathbf{w}_i\}$ is an independent set of vectors. By a dimension argument, since $dim(\mathbf{x}) = 1$ and $dim(\{\mathbf{w}_i\}) = n - 1$, an n-dimensional independent set of vectors in V must span. So $\{\mathbf{x}\} \cup \{\mathbf{w}_i\}$ is an orthogonal basis for V of eigenvectors of T. Note that $\{\mathbf{w}_i\}$ is orthonormal set, so we can replace $\{\mathbf{x}\}$ by $\left\{\frac{\mathbf{x}}{\|\mathbf{x}\|}\right\}$ to make this an orthonormal basis for V. □

An immediate result of this Theorem is that if T is self-adjoint, then there is an orthonormal basis of eigenvectors for V, and the matrix representation of T with respect to this basis is a diagonal matrix with corresponding eigenvalues as diagonal entries.

Corollary 2.12. *If $T : V \longrightarrow V$ is a self-adjoint linear map with $[T]_\alpha$ its matrix representation with respect to the standard orthonormal basis, then there exists an orthogonal/unitary matrix Q such that $Q^*[T]_\alpha Q$ is a diagonal matrix.*

Proof. Let $T : V \longrightarrow V$ be a self-adjoint linear map. By Theorem 2.11, V has an orthonormal basis of eigenvectors, say $\beta = \{\mathbf{x}_i\}_{i=1}^n$. Let α be the standard bases for V, and write T as a matrix with respect to α, that is $[T]_\alpha$. Choose $Q = [I]_\beta^\alpha$ where I is the identity matrix. Note that

$$Q = [I]_\beta^\alpha = [I(\beta_1)I(\beta_2)\dots I(\beta_n)].$$

Since the columns of Q, $I(\beta_i)_\alpha$, form an orthonormal basis for V, then Q is orthogonal/unitary by Corollary 2.9. Since Q is orthogonal, $Q^{-1} = Q^*$. So by the change of basis formula,

$$Q^{-1}TQ = Q^*TQ = [I]_\alpha^\beta[T]_\alpha[I]_\beta^\alpha = [T]_\beta.$$

Since the matrix representation of T is now with respect to β, an orthonormal basis of eigenvectors of T, then $[T]_\beta$ is a diagonal matrix. □

Chapter 3

An Eigenvalue Bound on the Expanding Constant

In this chapter, we will prove that the eigenvalues of the adjacency matrix of a graph provide a bound for the expanding constant. We will use many of the results about linear maps, adjoints, and self-adjoint matrices from Chapter 2 in our proof. The discussion is an expansion of the proof given in [1].

Suppose $X = (V, E)$ is a k-regular graph on n vertices without loops. Then let A be the adjacency matrix of X. A is a symmetric $n \times n$ matrix consisting of 0's and 1's, hence A has n eigenvalues denoted $\mu_0 \geq \mu_1 \geq \cdots \geq \mu_{n-1}$. By a result found in Davidoff, Saranak, and Valette's book [1], we have the following result which enables us to order the eigenvalues of A and ensures us that if X is k-regular and connected, then k is an eigenvalue and $(k - \mu_1) \neq 0$.

Proposition 3.1. *Let $X = (V, E)$ be a finite k-regular graph with n vertices. Then*
1) $\mu_0 = k$
2) $k \geq |\mu_i|$ for $1 \leq i \leq n - 1$
3) $k = \mu_0 > \mu_1$ if and only if X is connected
4) μ_0 has multiplicity 1 if and only if X is connected.

Once we have ordered the eigenvalues of A, we are able to use them to find a bound on the expanding constant of X by the following Theorem.

Theorem 3.2. *Let $X = (V, E)$ be a finite connected k-regular graph on n vertices without loops. Let μ_1 be the first nontrivial eigenvalue of X, that is $k = \mu_0 > \mu_1 \geq \cdots \geq \mu_{n-1}$. Then*

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

In this thesis, we will not prove the upper bound on $h(X)$ because of the proof's advanced level of difficulty. Before we begin the proof for the lower bound on $h(X)$, we will explain

the motivation and organization of the proof. For the graph X, our goal is to find a useful lower bound on

$$h(X) = \inf\left\{ \frac{|\partial F|}{|F|} \mid F \subseteq V, |F| \leq \frac{|V|}{2} \right\},$$

without considering all possible subsets of the set of vertices. Since the adjacency matrix of the graph encodes the geometry of the graph, it must encode a way to reach our goal. In this chapter, we will see that the eigenvalues of the adjacency matrix, A, provide the bound on the expanding constant. Note that the adjacency matrix is both real and symmetric, hence its eigenvalues will be real.

The first step in making the connection is to observe that a function f defined on the the vertices, V, for which

$$f(x) = \left\{ \begin{array}{ll} 1 & \text{if } x \in F \\ 0 & \text{if } x \notin F \end{array} \right\} \tag{3.1}$$

will satisfy

$$\sum_{x \in V} f(x) = |F|.$$

For our example, we will give the set of edges a specific orientation. In particular, if e is an edge between F and $V - F$, then label the vertex in F as e^+ and the vertex in $V - F$ as e^- where e^+ is the origin and e^- is the extremity of the edge e. If e connects two vertices in both F or $V - F$, then any orientation will do. For any function, a difference construction defines a linear map on the edges such that

$$df(e) = f(e^+) - f(e^-).$$

By choosing the above orientation for the edges, if we apply d to function 3.1, then

$$\sum_{e \in E} df(e) = |\partial F|.$$

Thus df captures the size of the boundary of F. The eigenvalues of A are relevant to the comparison of f and df if we can make A act on the set of functions defined on the vertices in a way that is related to the difference construction. We will define the inner product structure on $\ell^2 V$, the vector space of functions defined on the vertices, and an analogous one on $\ell^2 E$, in a way that is related to the above sums. This permits us to use the definition of the adjoint d^* of d. We will verify that A is closely related to the self-adjoint linear map d^*d, thus providing the connection between the eigenvalues of A and the linear map d.

Proof. (of $\frac{k-\mu_1}{2} \leq h(X)$) Let $X = (V, E)$ be a k-regular graph. First, give E, the set of edges of X, an arbitrary chosen orientation. Then for all $e \in E$, e^- is its origin and e^+ is its extremity. Let $\ell^2 V$ be the vector space of functions defined on the set of vertices of X and similarly, let $\ell^2 E$ be the vector space of functions defined on the set of edges of X. We will use the bases $\{\delta_x\}$ and $\{\delta_e\}$ for the vector spaces, respectively.

We will now specify the map d that will capture the size of the boundary of F and decide the action of $\triangle = d^*d$. Define the "simplicial coboundary operator" $d : \ell^2V \longrightarrow \ell^2E$ where for $f \in \ell^2V$ and $e \in E$, $df(e) = f(e^+) - f(e^-)$.

Lemma 3.3. *The simplicial coboundary operator $d : \ell^2V \longrightarrow \ell^2E$ defined by $df(e) = f(e^+) - f(e^-)$ for $f \in \ell^2V$ and $e \in E$, is a linear map.*

Proof. Let $c \in \mathbb{C}$ and $f, g \in \ell^2V$ be functions on the vertices of X. Then,

$$\begin{aligned} d(cf+g)(e) &= (cf+g)(e^+) - (cf+g)(e^-) \\ &= [cf(e^+) + g(e^+)] - [cf(e^-) + g(e^-)] \\ &= [cf(e^+) - cf(e^-)] + [g(e^+) - g(e^-)] \\ &= cdf(e) + dg(e) \end{aligned}$$

□

By Lemma 3.3, d is a linear map. Define the inner product on ℓ^2V by

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

for $f, g \in \ell^2V$ and define an analogous one for ℓ^2E. By Lemma 2.5, since d is a linear map, we can define its adjoint, $d^* : \ell^2E \longrightarrow \ell^2V$ such that for all $f \in \ell^2V$ and $g \in \ell^2E$, $\langle df, g \rangle = \langle f, d^*g \rangle$. We will also define a function $\delta : V \times E \longrightarrow \{1, 0, -1\}$ by

$$\delta(x,e) = \left\{ \begin{array}{ll} 1 & \text{if } x = e^+ \\ -1 & \text{if } x = e^- \\ 0 & \text{otherwise} \end{array} \right\}$$

The function δ is an evaluation of whether a vertex, x, is an endpoint of an edge, e.

Remark 3.4. For $e \in E$ and $f \in \ell^2V$, we can define $df(e)$ as $\sum_{x \in V} \delta(x,e)f(x)$, which still corresponds to our original definition of $df(e) = f(e^+) - f(e^-)$. That is, for $x_i \in V$,

$$\delta(x_i,e)f(x_i) = \left\{ \begin{array}{ll} f(x_i) & \text{if } x_i = e^+ \\ -f(x_i) & \text{if } x_i = e^- \\ 0 & \text{otherwise} \end{array} \right\}.$$

If $x_i = e^+$ then $\delta(x_i, e) = f(e^+)$ and if $x_i = e^-$ then $\delta(x_i, e) = -f(e^-)$. In the graph X, each edge, e, has a distinct origin and extremity. Therefore for each $e \in E$, there is only one $x_i \in V$ such that $x_i = e^+$ and only one $x_j \in V$ such that $x_j = e^-$, where $i \neq j$. Then

$$\sum_{x \in V} \delta(x,e)f(x) = f(x_i) - f(x_j) = f(e^+) - f(e^-) = df(e)$$

by our original definition. So

$$df(e) = \sum_{x \in V} \delta(x, e) f(x).$$

Rewriting the function d will enable us to understand the action of $\triangle = d^*d$. For the same reason, we will show that we can rewrite the adjoint of d in a similar form.

Lemma 3.5. *For $x \in V$ and $g \in \ell^2 E$,*

$$d^*g(x) = \sum_{e \in E} \delta(x, e) g(e).$$

Proof. Recall that $\{\delta_{x_i}\}_{i=1}^n$ and $\{\delta_{e_i}\}_{i=1}^m$ are orthonormal bases for $\ell^2 V$ and $\ell^2 E$ respectively and that the defining property of the adjoint, d^*, is $\langle df, g\rangle = \langle f, d^*g\rangle$ for $f \in \ell^2 V$ and $g \in \ell^2 E$. To see how d^* acts on any given $g \in \ell^2 E$, it suffices to see how it acts on basis elements of $\ell^2 V$. So let $f \in \ell^2 V$, then

$$f = \sum_{i=1}^{n} a_i \delta_{x_i}.$$

Recall from Lemma 2.3 that $\langle f, \delta_{x_j}\rangle = a_j$ where a_j is the coefficient of δ_{x_j} in the linear combination of f. So for all $f \in \ell^2 V$,

$$f = \sum_{i=1}^{n} \langle f, \delta_{x_i}\rangle \delta_{x_i}. \tag{3.2}$$

Now for $\delta_{x_k} \in \{\delta_{x_i}\}_{i=1}^n$, $\langle d\delta_{x_k}, g\rangle = \langle \delta_{x_k}, d^*g\rangle$ by the property of the adjoint. Since $d^*g \in \ell^2 V$, then by equation 3.2,

$$d^*g = \sum_{k=1}^{n} \langle d^*g, \delta_{x_k}\rangle \delta_{x_k}.$$

Since d^* is linear, to know d^*g it suffices to know $d^*\delta_{e_i}$ where $\delta_{e_i} \in \{\delta_{e_i}\}_{i=1}^m$. Similar to above,

$$d^*\delta_{e_i} = \sum_{k=1}^{n} \langle d^*\delta_{e_i}, \delta_{x_k}\rangle \delta_{x_k}.$$

Since $\langle d^*\delta_{e_i}, \delta_{x_k}\rangle = \langle \delta_{e_i}, d\delta_{x_k}\rangle$ then

$$d^*\delta_{e_i} = \sum_{k=1}^{n} \langle \delta_{e_i}, d\delta_{x_k}\rangle \delta_{x_k}.$$

Our goal is to show that

$$d^*\delta_{e_i}(x) = \sum_{e \in E} \delta(x, e) \delta_{e_i}(e). \tag{3.3}$$

Therefore we will evaluate each side separately. First evaluate the left hand side of equation 3.3 at $x \in V$:

$$\begin{aligned} d^*\delta_{e_i}(x) &= \sum_{k=1}^{n} \langle \delta_{e_i}, d\delta_{x_k} \rangle \delta_{x_k}(x) \\ &= \sum_{k=1}^{n} \left(\sum_{e \in E} \delta_{e_i}(e) \overline{d\delta_{x_k}(e)} \right) \delta_{x_k}(x) \\ &= \sum_{k=1}^{n} \left(\sum_{e \in E} \delta_{e_i}(e) \big(\delta_{x_k}(e+) - \delta_{x_k}(e-) \big) \right) \delta_{x_k}(x) \\ &= \sum_{k=1}^{n} \delta(x_k, e_i) \delta_{x_k}(x) \\ &= \delta(x, e_i). \end{aligned}$$

Now we will evaluate the right hand side of equation 3.3 at $x \in V$:

$$\sum_{e \in E} \delta(x, e) \delta_{e_i}(e) = \delta(x, e_i).$$

Thus

$$d^*\delta_{e_i}(x) = \delta(x, e_i) = \sum_{e \in E} \delta(x, e) \delta_{e_i}(e).$$

Since the equality holds for an arbitrary δ_{e_i}, then it holds for all basis elements. Hence for all $g \in \ell^2 E$ and $x \in V$,

$$d^*g(x) = \sum_{e \in E} \delta(x, e) g(e).$$

□

Since we have chosen the linear map d and its adjoint d^* we can now define $\triangle$. So, define the combinatorial Laplace operator $\triangle := d^*d : \ell^2 V \longrightarrow \ell^2 V$. To show that $\triangle$ is self-adjoint, i.e that $\triangle = \triangle^*$, note that for $f, g \in \ell^2 V$, $\langle d^*df, g \rangle = \langle df, dg \rangle = \langle f, d^*dg \rangle$. So $(d^*d)^* = d^*d$. Hence $\triangle = d^*d$ is self-adjoint and we can utilize the results on self-adjoint matrices in Chapter 2.

Recall that for our graph $X = (V, E)$, the adjacency matrix, A, is an $n \times n$ matrix consisting of 0's and 1's since X has no loops. We will now verify the relationship between the adjacency matrix and the matrix representation of $\triangle$ in order to relate the eigenvalues of A to the eigenvalues of $[\triangle]$. More specifically, we will show that $[\triangle] = k \cdot Id - A$. Clearly,

$$k \cdot Id - A = \begin{bmatrix} k - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & k - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & k - a_{nn} \end{bmatrix}$$

Since $\triangle = d^*d : \ell^2V \longrightarrow \ell^2V$, by using $\{\delta_{x_i}\}$ and $\{\delta_{e_i}\}$ as bases for ℓ^2V and ℓ^2E, the matrix representation of $\triangle$ is

$$[\triangle]_{\{\delta_x\}} = [d^*]^{\{\delta_x\}}_{\{\delta_e\}} \cdot [d]^{\{\delta_e\}}_{\{\delta_x\}}.$$

Remark 3.6. We will simply refer to the matrix representation of $\triangle$ with respect to the basis $\{\delta_x\}$, as $[\triangle]$.

We will show that $[\triangle] = k \cdot Id - A$ by first analyzing the diagonal entries and then the remaining entries of the matrix. Consider $\triangle_{ii}$, the iith entry of $[\triangle]$. By using the properties of the inner product, we find that

$$\triangle_{ii} = \langle \triangle\delta_{x_i}, \delta_{x_i}\rangle = \langle d^*d\delta_{x_i}, \delta_{x_i}\rangle = \langle d\delta_{x_i}, d\delta_{x_i}\rangle = \sum_{e\in E} d\delta_{x_i}(e)\overline{d\delta_{x_i}(e)}$$

since $d\delta_{x_i}(e) \in \{-1, 0, 1\}$, then $d\delta_{x_i}(e) = \overline{d\delta_{x_i}(e)}$. Therefore,

$$\sum_{e\in E} d\delta_{x_i}(e)\overline{d\delta_{x_i}(e)} = \sum_{e\in E} \big(d\delta_{x_i}(e)\big)^2 = \sum_{e\in E} \big(\delta(x_i, e)\big)^2 = \left\{ \begin{array}{ll} 1 & \text{if } x_i \text{ is an endpoint of } e \\ 0 & \text{otherwise} \end{array} \right\}.$$

Since the graph X is k-connected, x_i is an endpoint to k edges. Thus $\triangle_{ii} = k$. Note that $(k \cdot Id - A)_{ii} = k - a_{ii}$ but since A has no loops, $a_{ii} = 0$ for all i. Therefore, $\triangle_{ii} = k = (k \cdot Id - A)_{ii}$. Now, consider the ijth entry of $[\triangle]$, $\triangle_{ij}$. By using the properties of the inner product, we have:

$$\triangle_{ij} = \langle \triangle\delta_{x_j}, \delta_{x_i}\rangle = \langle d^*d\delta_{x_j}, \delta_{x_i}\rangle = \langle d\delta_{x_j}, d\delta_{x_i}\rangle = \sum_{e\in E} d\delta_{x_j}(e)d\delta_{x_i}(e).$$

Recalling the definition of $df(e)$ for $e \in E$, we have

$$\begin{aligned}
&= \sum_{e\in E} d\delta_{x_j}(e)d\delta_{x_i}(e) \\
&= \sum_{e\in E} \big(\delta_{x_j}(e^+) - \delta_{x_j}(e^-)\big)\big(\delta_{x_i}(e^+) - \delta_{x_i}(e^-)\big) \\
&= \sum_{e\in E} \delta_{x_j}(e^+)\delta_{x_i}(e^+) - \delta_{x_j}(e^-)\delta_{x_i}(e^+) - \delta_{x_i}(e^-)\delta_{x_j}(e^+) + \delta_{x_i}(e^+)\big)\delta_{x_j}(e^-) \\
&= \sum_{e\in E} -\delta_{x_i}(e^+)\delta_{x_j}(e^-) - \delta_{x_i}(e^-)\delta_{x_j}(e^+) \\
&= \left\{ \begin{array}{ll} -1 & \text{if } x_i = e^+ \text{ and } x_j = e^- \\ 0 & \text{otherwise} \end{array} \right\} + \left\{ \begin{array}{ll} -1 & \text{if } x_i = e^- \text{ and } x_j = e^+ \\ 0 & \text{otherwise} \end{array} \right\}
\end{aligned}$$

Let E' be the set of edges such that x_i and x_j share an edge, $i \neq j$. Then

$$\triangle_{ij} = \sum_{e\in E'} -1 = -|E'|,$$

which by definition is $-a_{ij}$, the ijth entry of the adjacency matrix A. Thus $\triangle_{ij} = -a_{ij} = (k \cdot Id - A)_{ij}$. Hence $[\triangle] = k \cdot Id - A$. Note that $[\triangle]$ does not depend on the orientation of the edges of E.

Now that we have verified the relationship between $[\triangle]$ and A, we will relate the eigenvalues of A to the eigenvalues of $[\triangle]$. Since A is the adjacency matrix of the graph X, it has entries of either 0 or 1 and is symmetric. Since A is real and symmetric then $A = \overline{A}^T$, hence A is a self-adjoint matrix. Therefore, by Theorem 2.11, there is an orthonormal basis of eigenvectors of A, say $\{v_i\}_{i=1}^n = \beta$. Each eigenvector has a corresponding eigenvalue in the set $\{k, \mu_1, \mu_2, \ldots, \mu_{n-1}\}$ which are the eigenvalues of A. Then $[A]_\beta$ is a diagonal matrix with diagonal entries as the eigenvalues of A. That is,

$$[A]_\beta = \begin{bmatrix} k & 0 & \cdots & 0 \\ 0 & \mu_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \mu_{n-1} \end{bmatrix}.$$

Furthermore,

$$[\triangle]_\beta = k \cdot Id - [A]_\beta = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & k-\mu_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & k-\mu_{n-1} \end{bmatrix}.$$

After verifying the relationship between $[\triangle]$ and A, we now need to create the inequality that relates the eigenvalues of A to a function f and the linear map d. Once we have specified the carefully chosen function g, this inequality will then determine the bound on $h(X)$. So, let f be a function on V with

$$f = \sum_{i=0}^{n-1} a_i v_i$$

where $\beta = \{v_i\}$ is the orthonormal basis of eigenvectors for A. Suppose $\sum_{x \in V} f(x) = 0$, so f is orthogonal to the constant functions on $\ell^2 V$, hence $a_0 = 0$. Now,

$$\| df \|^2 = \langle df, df \rangle = \langle d^* df, f \rangle = \langle \triangle f, f \rangle.$$

Since $a_0 = 0$ for the function f, we can adjust the indices of the sum. Similarly, for $\triangle f$, the $i = 0$ term is $(k - \mu_0) = 0$ since $\mu_0 = k$. Therefore

$$\begin{aligned} f &= \sum_{i=1}^{n-1} a_i v_i \\ \triangle f &= \sum_{i=1}^{n-1} (k - \mu_i) a_i v_i \end{aligned}$$

We will now compute $\langle \triangle f, f\rangle$ and $\| f \|^2$ to get an inequality that involves the eigenvalues of A. So,

$$\begin{aligned}\langle \triangle f, f\rangle &= \langle \sum_{j=1}^{n-1}(k-\mu_j)a_j v_j, \sum_{i=1}^{n-1} a_i v_i\rangle \\ &= \sum_{i,j=1}^{n-1}(k-\mu_j)a_j\overline{a_i}\langle v_j, v_i\rangle\end{aligned}$$

Since $\{v_i\}$ is an orthonormal basis and $a_i \in \mathbb{R}$, we have

$$\langle \triangle f, f\rangle = \sum_{i,j=1}^{n-1}(k-\mu_j)a_j\overline{a_i}\delta_{i,j} = \sum_{i=1}^{n-1}(k-\mu_i)a_i^2 \tag{3.4}$$

Now, by the properties of the inner product,

$$\| f \|^2 = \langle f, f\rangle = \langle \sum_{j=1}^{n-1} a_j v_j, \sum_{i=1}^{n-1} a_i v_i\rangle = \sum_{i,j=1}^{n-1} a_j\overline{a_i}\langle v_j, v_i\rangle = \sum_{i,j=1}^{n-1} a_j a_i \delta_{i,j} = \sum_{i=1}^{n-1} a_i^2. \tag{3.5}$$

Recall that $\{k, \mu_1, \mu_2, \ldots, \mu_{n-1}\}$ are the eigenvalues of A in descending order, hence $\mu_1 \geq \mu_i$ for all i. Thus for all i, $k-\mu_i \geq k-\mu_1$ and

$$\frac{k-\mu_i}{k-\mu_1} \geq 1.$$

Now, by comparing equations 3.4 and 3.5, we have:

$$\langle \triangle f, f\rangle = \sum_{i=1}^{n-1}(k-\mu_i)a_i^2 = (k-\mu_1)\sum_{i=1}^{n-1}\frac{k-\mu_i}{k-\mu_1}a_i^2 \geq (k-\mu_1)\sum_{i=1}^{n-1} a_i^2 = (k-\mu_1)\| f \|^2 .$$

In conclusion, we have found that

$$\| df \|^2 \geq (k-\mu_1)\| f \|^2 . \tag{3.6}$$

This inequality relates the linear map, d, and a function f that is orthogonal to the constant functions, to the eigenvalues of A.

Our goal is to show that $h(X) \geq \frac{k-\mu_1}{2}$ where $h(X) = \inf = \{\frac{|\partial F|}{|F|} \mid F \subseteq V, |F| \leq \frac{|V|}{2}\}$. We will apply inequality 3.6 to a carefully chosen function on the vertices of the graph $X = (V, E)$. This function must be orthogonal to the constant functions and will essentially measure the size of F. Set

$$g(x) = \left\{ \begin{array}{ll} |V-F| & \text{if } x \in F \\ -|F| & \text{if } x \in V-F \end{array} \right\}$$

We want to make sure that $\sum_{x\in V} g(x) = 0$, i.e. that g is orthogonal to the constant functions in $\ell^2 V$. So

$$\sum_{x\in V} g(x) = \sum_{x\in F} g(x) + \sum_{x\in V-F} g(x) = |F||V-F| + |V-F|(-|F|) = 0.$$

Since g is orthogonal to the constant functions in $\ell^2 V$, we can use inequality 3.6 to put a bound on $h(X)$. First, evaluate

$$\| \, dg \, \|^2 = \langle dg, dg \rangle = \sum_{e\in E} dg(e)^2.$$

From our initial definition of $df(e)$, in general, $df(e) = f(e^+) - f(e^-)$. Hence for our function,

$$dg(e) = \left\{ \begin{array}{ll} 0 & \text{if } e \text{ connects 2 vertices in } F \text{ or in } V-F \\ \pm \mid V \mid & \text{if } e \text{ connects a vertex in } F \text{ with a vertex in } V-F \end{array} \right\}$$

Therefore,

$$\| \, dg \, \|^2 = \sum_{e\in E} dg(e)^2 = |V|^2 |\partial F| \tag{3.7}$$

where $|\partial F|$ is the boundary of F and by definition is the number of edges connecting F with $V - F$. Now we will evaluate $\| \, g \, \|^2$. So,

$$\begin{aligned} \| \, g \, \|^2 &= \langle g, g \rangle \\ &= \sum_{x\in V} g(x)\overline{g(x)} \\ &= \sum_{x\in V} g(x)^2 \\ &= \sum_{x\in V-F} g(x)^2 + \sum_{x\in F} g(x)^2 \\ &= |V-F| \, (-|F|)^2 + |F| \, (|V-F|)^2 \\ &= |F||V-F| \, (|F| + |V-F|) \\ &= |F||V-F||V| \end{aligned} \tag{3.8}$$

Again, since $\sum_{x\in V} g(x) = 0$ we know that $\| \, dg \, \|^2 \geq (k - \mu_1) \, \| \, g \, \|^2$. Now by substituting our evaluations of $\| \, dg \, \|^2$, equation 3.7, and $\| \, g \, \|^2$, equation 3.8 into inequality 3.6, we have

$$|V|^2 \, |\partial F| \geq (k - \mu_1)|F||V||V - F|$$

which implies that

$$\frac{|\partial F|}{|F|} \geq \frac{(k - \mu_1)|V - F|}{|V|}.$$

Note that the left hand side is precisely $h(X)$, assuming that $\frac{|V|}{2} \geq |F|$. So,

$$h(X) \geq \frac{(k-\mu_1)|V-F|}{|V|}.$$

Since $\frac{|V|}{2} \geq |F|$ then $|V-F| \geq \frac{|V|}{2}$. Hence we now have

$$h(X) \geq (k-\mu_1)\frac{|V|}{2}\frac{1}{|V|} = \frac{(k-\mu_1)}{2}.$$

Thus we have constructed the lower bound for the expanding constant, completing the proof. □

Chapter 4

Abstract Algebra Foundations

This chapter is the background information needed to construct and discuss the Winnie Li graphs, which involve finite field extensions and Galois groups. The material is standard. Our presentation and many of our proofs are based on those in [3], [7], [9], and [4]. We will begin our introduction of Abstract Algebra by defining the basic ring structure and then introduce key results about finite field extensions.

Definition. A set R is called a *ring* if it has two binary operations, written as addition and multiplication, satisfying the following axioms for all a, b, c in R:
1) $a + b = b + a$.
2) $a + (b + c) = (a + b) + c$.
3) An element 0 in R exists such that $0 + a = a$ for all a.
4) For each a in R and element $-a$ in R exists such that $a + (-a) = 0$.
5) $a(bc) = (ab)c$.
6) $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.
We will use the convention that R has multiplicative identity 1. In addition, R is called a commutative ring if and only if $ab = ba$ for all a, b in R.

Definition. If R is any ring, an element u in R is a *unit* if u has a multiplicative inverse in R. The set of all units of R, denoted $R^\times$, is a multiplicative group called the *group of units*.

We will primarily be focusing on finite fields through our discussion of Winnie Li's graphs.

Definition. A field, F, is a commutative ring such that every nonzero element in F is a unit in F. Note that this implies that F has no zero divisors. i.e. if $ab = 0$ in F, then $a = 0$ or $b = 0$.

4.1 Algebraic Extensions

Definition. Let K, F be fields such that K is an extension of F. $F[x]$ is a ring of polynomials in a variable x with coefficients in F. An element $\alpha \in K$ is *algebraic* over F if there exists $f(x) \in F[x]$, $f(x) \neq 0$, such that $f(\alpha) = 0$.

The polynomials in $F[x]$ are very important in our later constructions. Polynomials can be further characterized by the following definitions. Suppose F and K are fields such that $F \subseteq K$ and α is algebraic in K.

Definition. Let $f(x) \in F[x]$ with the degree of $f(x) \geq 1$.
1) $f(x)$ is *monic* if $f(x) = a_n x^n + \cdots + a_1 x + a_0$ where $a_n = 1$.
2) $f(x)$ is *irreducible* if $f(x) = g(x)h(x)$ then either $\deg g(x) = 0$ or $\deg h(x) = 0$.
3) $f(x)$ is *minimal* for $\alpha \in K$ if $f(x)$ is of minimal degree such that $f(\alpha) = 0$.
4) $f(x)$ is *separable* if all the roots of $f(x)$ are distinct.

Below is one of the central theorems about field extensions that helps us to better understand both the extension and how to work with its elements.

Theorem 4.1. *If $K \supseteq F$ are fields and $\alpha \in K$ is algebraic over F of degree n, then*
1) $F(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in F\} = \{f(\alpha) \mid f(x) \in F[x]\}$
2) $F(\alpha) \cong F[x]/(m(x))$ where $m(x)$ is the minimal polynomial of α over F.
3) $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is an F-basis of $F(\alpha)$, so $[F(\alpha) : F] = n = \deg m(x)$.

Proof. [7] Let $K \supseteq F$ be fields and $\alpha \in K$ be algebraic over F of degree n. Define $\Theta : F[x] \longrightarrow K$ by $\Theta(f(x)) = f(\alpha)$. Then Θ is a ring homomorphism and

$$\ker \Theta = \{f(x) \mid f(\alpha) = 0\} = (m(x)),$$

where $m(x)$ is the minimal irreducible polynomial of α over F. Then by the First Isomorphism Theorem,

$$\frac{F[x]}{(m(x))} \cong Im\Theta = \{f(\alpha) \mid f(x) \in F[x]\}.$$

So, $F(\alpha)$ is a field containing F and α and so contains $f(\alpha)$ for all $f(x) \in F[x]$. Hence $Im\Theta \subseteq F(\alpha)$. But $F[x]/(m(x))$ is a field because $m(x)$ is irreducible, so $Im\Theta$ is a field. Because $Im\Theta$ contains F and α, this shows that $F(\alpha) \subseteq Im\Theta$. Thus $F(\alpha) = Im\Theta$ which proves (1) and (2). It remains to show that $B = \{1, \alpha, \ldots, \alpha^{n-1}\}$ is an F-basis of $F(\alpha)$. To show that B is independent, for $a_i \in F$, let

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0.$$

Then $g(\alpha) = 0$ where $g(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ so $g(x) \neq 0$ in $F[x]$ which would contradict the choice of the minimal polynomial $m(x)$. Hence $g(x) = 0$, so $a_i = 0$ for all i.

Thus B is independent. Finally to show that B spans $F(\alpha)$, let $f(\alpha) \in F(\alpha)$ and write $f = qm + r$ in $F[x]$ where, sincedeg$(m(x))$=n, $r(x)$ has the form $r(x) = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}$, $b_i \in F$. As $m(\alpha) = 0$, we get $f(\alpha) = r(\alpha) = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$. Thus B spans $F(\alpha)$ and the proof is complete. □

Note that Theorem 4.1 shows us that the field, F, and the minimal polynomial, $m(x)$, of the algebraic element α determine the field extension $F[x]/(m(x)) = F(\alpha)$. Therefore, if α and β are two roots of the minimal polynomial $m(x)$, then $F(\alpha) \cong F(\beta)$.

Now, suppose $K \supseteq F$ are fields such that $\alpha_1, \alpha_2, \ldots, \alpha_n$, are elements of K. Then we can adjoin each root to F by a simple extension, that is $F(\alpha_1)$. In addition, note that $F(\alpha_1, \alpha_2) = F(\alpha_1)(\alpha_2)$. Hence we can adjoin each α_i for $1 \leq i \leq n$ to get $F(\alpha_1)(\alpha_2)\cdots(\alpha_n) = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. If $\alpha_1, \alpha_2, \ldots, \alpha_n$ are all the roots of some polynomial, $f(x) \in F[x]$, then the field $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is known as the splitting field of $f(x)$ over F.

Definition. Let $f(x) \in F[x]$ of degree $n \geq 1$ where F is a field. An extension $K \supseteq F$ is called a splitting field of $f(x)$ over F is the following are satisfied:
1) $f(x) = a(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)$, $a \in F$ and $\alpha_i \in K$ for each i.
2) $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Hence K is the smallest field containing F and all the roots of $f(x)$.

4.2 Finite Fields

In this section, we will prove results that are key in the set up of the field extensions used in the construction of Winnie's Li graphs.

Remark 4.2. A finite field is simply a field, F, such that $|F| < \infty$. The characteristic of F, char$F$, is some $p \in \mathbb{Z}^+$ where p is the smallest number such that $a \cdot p = 0$ for all $a \in F$. By a simple exercise, one can prove that the characteristic of any finite field is prime.

The following theorems enable us to characterize all finite fields.

Theorem 4.3. *If F is a finite field, then $|F| = p^n$ for $n \geq 1$ where charF $= p$.*

Proof. This proof can be found in [7], pg. 353, Theorem 1. □

Remark 4.4. When working with elements of a finite field of characteristic p, it is helpful to use the following facts. For all $a, b \in F$, char$F = p$:
1) $(a + b)^p = a^p + b^p$ by the Binomial Theorem
2) $(ab)^p = a^p\, b^p$ since F is commutative
3) $a^p \equiv a \bmod(p)$ by Fermat's Little Theorem

Definition. Let F be a finite field. The *Frobenius automorphism* is a map from $F \longrightarrow F$ defined by $\varphi(x) = x^p$ where $\text{char}F = p$.

Lemma 4.5. *The Frobenius automorphism, φ is a field automorphism.*

Proof. Let F be a finite field with characteristic p and define $\varphi : F \longrightarrow F$ by $\varphi(x) = x^p$. Let $x, y \in F$. Then $\varphi(x+y) = (x+y)^p = x^p + y^p$, by Remark 4.4, hence $x^p + y^p = \varphi(x) + \varphi(y)$. Now, consider $\varphi(xy) = (xy)^p = x^p y^p$, since F is commutative. So $x^p y^p = \varphi(x)\varphi(y)$. Now, $\ker\varphi = \{x \in F \mid \varphi(x) = 0\} = \{x \in F \mid x^p = 0\} = \{0\}$. Therefore φ is one-to-one. Since F is finite and φ is one-to-one, then that forces φ to be onto. Therefore φ is a field automorphism. □

Remark 4.6. Recall that a polynomial is separable if it has distinct roots. One way we can tell if a polynomial is separable, is if $f(x)$ and its derivative $f'(x)$ are relatively prime, that is $gcd(f(x), f'(x)) = 1$. We will be using the fact that $f(x) = x^{p^n} - x$ is separable often. Therefore, in characteristic p, simply note that $f'(x) = p^n x^{p^n - 1} - 1 = -1$, so $gcd(f(x), f'(x)) = gcd(x^{p^n} - x, -1) = 1$. Hence $f(x) = x^{p^n} - x$ is separable and has p^n distinct roots.

Theorem 4.7. *For p a prime and $n \geq 1$, let $f(x) = x^{p^n} - x$. F is a field with $|F| = p^n$ if and only if F is the splitting field of $f(x)$ over $\mathbb{Z}/p\mathbb{Z} \cong F_p$*

Proof. [7]($\Rightarrow$) Let p be a prime and n an integer, $n \geq 1$. Let $f(x) = x^{p^n} - x$ and suppose F is a field with $|F| = p^n$. Since the degree of $f(x)$ is p^n, $f(x)$ can have at most p^n roots in any field. Since $|F| = p^n$ then $f(x)$ must factor into p^n linear factors in F. That is, $f(x) = (x - a_1)(x - a_2)\cdots(x - a_{p^n})$ where a_i, $1 \leq i \leq p^n$, is a root of $f(x)$ in F. Therefore, F is the splitting field of $f(x)$ over F_p.
($\Leftarrow$) Suppose that F is the splitting field of $f(x)$ over F_p, the base field of F. Let $K = \{x \in F \mid f(x) = 0\}$ be the set of roots of $f(x)$ in F. By Remark 4.6, $f(x)$ has p^n distinct roots. So $|K| = p^n$. Since F is the splitting field of $f(x)$, it is generated by the roots of $f(x)$. That is, $F \subseteq K$. In order to show that $|F| = p^n$, we need to show that $K \subseteq F$. So, let $\varphi : F \longrightarrow F$ be the Frobenius automorphism in Lemma 4.5 defined by $\varphi(x) = x^p$ for all $x \in F$. Then $\varphi^n(x) = x^{p^n}$. So

$$\begin{aligned} K &= \{x \in F \mid f(x) = 0\} \\ &= \{x \in F \mid x^{p^n} - x = 0\} \\ &= \{x \in F \mid x^{p^n} = x\} \\ &= \{x \in F \mid \varphi^n(x) = x\}. \end{aligned}$$

Since φ^n is a field automorphism of F, then $K \subseteq F$. Since we have inclusion both ways, $K = F$ and $|F| = |K| = p^n$. □

In summary, for any prime p and $n \geq 1$, there exists a finite field, F, with p^n elements such that the elements of F are precisely the roots of $f(x) = x^{p^n} - x$, and F is unique up to isomorphism. Recall that $F^\times$ is the group of units of F. Since F is a field, then $F^\times = F - \{0\}$ and $|F^\times| = |F| - 1$.

Theorem 4.8. *For F a finite field, $F^\times = F - \{0\}$ is a cyclic group.*

Proof. [4] Suppose F is a finite field with group of units, $F^\times$. Since F is finite then $F^\times$ is finite. In addition, note that $F^\times$ contains 1 and for all $x \in F^\times$, the inverse of x is in $F^\times$. Suppose $x, y \in F^\times$ such that $x \neq 0$ and $y \neq 0$. Now, $xy \in F$ and $xy \in F^\times \iff xy \neq 0 \iff x \neq 0$ and $y \neq 0$. Hence, $F^\times$ is a group. Since $F^\times$ is a finite group, each of its elements have finite order. Let $P = \{k \in \mathbb{Z}^+ \mid x^k = 1 \text{ for some } x \in F^\times\}$, that is, let P be the the collection of all positive integers, k, such that k is the order of some element of $F^\times$. (i) Let $m \in P$ such that k divides m for some $k \in \mathbb{Z}^+$. Then there exists $x \in F^\times$ such that $x^m = 1$. Since k divides m, say $m = k \cdot d$, then $|x^{\frac{m}{k}}| = |x^d| = k$. Therefore, $k \in P$. (ii) If $r, s \in P$ such that $gcd(r, s) = 1$. Then there exists $x, y \in F^\times$ such that $|x| = r$ and $|y| = s$. So, $|xy| = \text{lcm}(r, s) = rs$ since $\gcd(r, s) = 1$. Hence $rs \in P$. By (i) and (ii), if $a, b \in P$ then the least common multiple of a and b is in P. Therefore, the least common multiple, M of all the elements of P is in P. So M is the largest integer in P and if $t \in P$ then t divides M. Therefore, $F^\times$ has an element z with order M. Hence $1, z, z^2, \ldots, z^{M-1}$ are all distinct and $z^M = 1$. If w is any element of $F^\times$ then $w^M = 1 \Longrightarrow w^M - 1 = 0$. Hence every element in $F^\times$ is a root of the polynomial $x^M - 1$ and we already have M distinct roots, $1, z, z^2, \ldots, z^{M-1}$. Since there cannot be more than M roots, each $w \in F^\times$ can be written as z^k for $1 \leq k \leq M$. So $F^\times$ is a cyclic group. □

Since $F^\times$ is a cyclic group, finding a generator of $F^\times$ will simplify working with the elements of $F^\times$ because multiplication will be reduced to addition of exponents. The next section describes in more detail an element of F that generates $F^\times$.

4.3 Primitive Elements

Definition. If F is a finite field, an element $\alpha \in F$ is a *primitive element* if α generates $F^\times$. The number of primitive elements for F is $\phi(q-1)$ where $q = |F|$ and ϕ is the Euler phi-function. If a primitive element, α, is a root of a monic irreducible polynomial $f(x)$, then $f(x)$ is a *primitive polynomial*.

The existence of a primitive element in a finite field F implies that F is a simple extension of $\mathbb{Z}/p\mathbb{Z} \cong F_p$. That is, $F = F_p(\alpha)$ where α is a primitive element. If we know that $f(x) \in F_p[x]$ is a primitive polynomial, then its roots are primitive elements. When creating the extension as in Section 4.1, it is most useful to choose $m(x)$ to be a primitive polynomial. However, primitive polynomials are not easy to find explicitly, so there are tables of primitive

polynomials available. When we are working with Winnie Li's graphs, we will check through brute force that the root α of the minimal irreducible polynomial we have chosen is in fact primitive by verifying that it generates $F^{\times}$.

4.4 Galois Extensions

Definition. Let K be a field. A *field automorphism*, $\sigma : K \longrightarrow K$, is a bijection such that $\sigma(x+y) = \sigma(x) + \sigma(y)$ and $\sigma(xy) = \sigma(x)\sigma(y)$ for all $x, y \in K$.

Definition. Let K be a finite field extension of F. The *Galois group*, $Gal(K/F)$ is the set of all field automorphisms $\sigma : K \longrightarrow K$ such that σ fixes F. i.e. $\sigma(x) = x$ for all $x \in F$. $Gal(K/F)$ is a subgroup of $Aut(K/F)$, hence the group operation is composition of automorphisms.

Definition. Let K be a finite field extension of F. K/F is a *Galois extension* if

$$\{x \in K \mid \sigma(x) = x \text{ for all } \sigma \in Gal(K/F)\} = F.$$

Remark 4.9. K is said to be *Galois* over F if K/F is a *Galois extension*. In addition, $|Gal(K/F)| = [K : F] = \deg(m(x))$ where $m(x)$ is the irreducible polynomial such that $K \cong F[x]/(m(x))$.

Let $K/F \cong F[x]/(m(x))$ be a finite field extension with monic irreducible polynomial $m(x)$. Then $K - F$ is the set of roots of $m(x)$. If K/F is Galois, then the automorphisms of the Galois group fix F and permute $K - F$, that is they permute the roots of $m(x)$.

Note that not all field extensions are Galois. If a field extension, K/F, is not Galois, then there exists an element of $K - F$ that is fixed by all field automorphisms of $Gal(K/F)$. The following theorem helps us determine when K/F is Galois and thus has a Galois group.

Theorem 4.10. *The extension K/F is Galois if and only if K is the splitting field of some separable polynomial over F.*

The proof of Theorem 4.10 can be found in [3], pg. 572, Theorem 13.

Theorem 4.11. *Let p be a prime, then*
1) $F_{p^r} \subseteq F_{p^s}$ if and only if r divides s.
2) In addition, $Gal(F_{p^s}/F_p)$ is cyclic of order s, generated by the Frobenius automorphism, φ.
3) Moreover, if $F_{p^r} \subseteq F_{p^s}$ then $Gal(F_{p^s}/F_{p^r})$ is cyclic of order s/r and generated by φ^r where $\varphi^r(x) = (x^p)^r$ for $x \in F_{p^s}$.

Proof. Let p be a prime.
1):[9] ($\Rightarrow$) Suppose $F_{p^r} \subseteq F_{p^s}$. Then F_{p^s} is a vector space over F_{p^r}. Hence the dimension of F_{p^s} over F_{p^r} is d where $p^s = (p^r)^d = p^{rd}$. Therefore, r divides s. ($\Leftarrow$) Suppose that r divides s. Then $(p^r - 1)$ divides $(p^s - 1)$, and $(x^{p^r-1} - 1)$ divides $(x^{p^s-1} - 1)$. By multiplying both factors by x we have that $(x^{p^r} - x)$ divides $(x^{p^s} - x)$. Therefore, the splitting field of $(x^{p^r} - x)$ is contained in the splitting field of $(x^{p^s} - x)$. By Theorem 4.7, F_{p^r} is the splitting field of $(x^{p^r} - x)$ and F_{p^s} is the splitting field of $(x^{p^s} - x)$, hence $F_{p^r} \subseteq F_{p^s}$.
2):[4] First note that F_{p^s}/F_p is Galois. Let $f(x) = x^{p^s} - x$ and note that $|F_{p^s}| = p^s$ then by Theorem 4.7, F_{p^s} is the splitting field of $f(x)$ over F_p. By Remark 4.6, $f(x)$ has p^s distinct roots and is thus separable. So, by Theorem 4.10, F_{p^s}/F_p is Galois. Now, consider the Frobenius map $\varphi : F_{p^s} \longrightarrow F_{p^s}$ defined by $\varphi(x) = x^p$. Set $G = \langle\varphi\rangle$, the cyclic group generated by φ. Then the fixed field of G is

$$\{x \in F_{p^s} \mid \varphi(x) = x\} = \{x \in F_{p^s} \mid x^p = x\}.$$

By Remark 4.4,

$$\{x \in F_{p^s} \mid x^p = x\} = F_p,$$

the base field of F_{p^s}. Hence $\varphi \in Gal(F_{p^s}/F_p)$. Since $Gal(F_{p^s}/F_p)$ is a group, then any power of φ is also in $Gal(F_{p^s}/F_p)$. Consider the sth power of the Frobenius automorphism, φ^s, defined by $\varphi^s(x) = x^{p^s}$. Then the fixed field of φ^s is

$$\begin{aligned}
\{x \in F_{p^s} \mid \varphi^s(x) = x\} &= \{x \in F_{p^s} \mid x^{p^s} = x\} \\
&= \{x \in F_{p^s} \mid x^{p^s} - x = 0\} \\
&= \{x \in F_{p^s} \mid f(x) = 0 \text{ where } f(x) = x^{p^s} - x\} \\
&= F_{p^s}
\end{aligned}$$

Therefore, φ^s is the identity on F_{p^s}. Recall that $|Gal(F_{p^s}/F_p)| = [F_{p^s} : F_p] = s$ by Remark 4.9. Therefore, $\langle\varphi\rangle \subseteq Gal(F_{p^s}/F_p)$. Now to show that $\varphi^k \neq 1$ for any $k < s$, suppose $\varphi^k = 1$ for $k < s$. Then for *all* $x \in F_{p^s}$,

$$\varphi^k(x) = x \Longleftrightarrow x^{p^k} = x \Longleftrightarrow x^{p^k} - x = 0.$$

Hence for all $x \in F_{p^s}$, x is a root of $f(x) = x^{p^k} - x$. But that says there are p^s roots for a polynomial of degree p^k, where $p^k < p^s$. A contradiction, thus $\varphi^k \neq 1$ for any $k < s$. Therefore, $Gal(F_{p^s}/F_p)$ is precisely the cyclic group generated by φ and has order s.
3): Suppose $F_{p^r} \subseteq F_{p^s}$, then r divides s, say $s = r \cdot d$. Then F_{p^s} is a finite extension of F_{p^r} of degree d. Let φ be the Frobenius map defined by $\varphi(x) = x^p$. Let φ^r be the rth power of the Frobenius map such that $\varphi^r(x) = x^{p^r}$. We will show that φ^r fixes F_{p^r}. Let $y \in F_{p^r}$, then $\varphi^r(y) = y^{p^r}$. Recall that F_{p^r} is the splitting field of $f(x) = x^{p^r} - x$ over F_p, so all of its elements are roots of $f(x)$. Therefore, since $y \in F_{p^r}$, $f(y) = y^{p^r} - y = 0 \Leftrightarrow y^{p^r} = y$. Hence $\varphi^r(y) = y^{p^r} = y$, so φ^r fixes all elements of F_{p^r}. Now we will show that F_{p^s} is Galois over F_{p^r}. Recall that $s = r \cdot d$ and F_{p^s} is a finite extension of degree d over F_{p^r}. By Theorem 4.7, F_{p^s} is the splitting field of $g(x) = x^{p^s} - x$ over F_p and hence unique. But since

$F_p \subseteq F_{p^r}$ it follows that F_{p^s} is the splitting field of $g(x) = x^{p^s} - x$ viewed as a polynomial over F_{p^r}. Therefore, by Theorem 4.10 and Remark 4.6, F_{p^s} is Galois over F_{p^r}. Note that $[F_{p^s} : F_{p^r}] = d = |Gal(F_{p^s}/F_{p^r})|$. By a similar argument as in the proof of (2), $|\varphi^r| = \frac{r}{s} = d$. Therefore, since we have shown that φ^r fixes F_{p^r}, then φ^r and all powers of the map are in $Gal(F_{p^s}/F_{p^r})$. In addition, since $|Gal(F_{p^s}/F_{p^r})| = d = |\varphi^r|$, then $Gal(F_{p^s}/F_{p^r}) = \langle\varphi^r\rangle$. So the Galois group is cyclic of order $\frac{r}{s} = d$ generated by φ^r. □

Remark 4.12. We will look specifically at F_{p^2}/F_p. By Theorem 4.11, $F_p \subseteq F_{p^2}$ and $Gal(F_{p^2}/F_p)$ is cyclic of order 2, generated by φ. Therefore, $Gal(F_{p^2}/F_p) = \{1, \varphi\}$ where $\varphi(x) = x^2$ for all $x \in F_{p^2}$.

4.5 The Trace and Norm of a Galois Extension

The Trace and Norm of a Galois extension are maps from from the finite field extension to the base field, as we will show. The Norm map will play a key role in determining the set of edges of the Winnie Li graphs.

Definition. Let K/F be a Galois extension. Define the Trace and Norm of K/F as follows for all $\alpha \in K$:

$$Tr_{K/F}(\alpha) = \sum_{\sigma \in Gal(K/F)} \sigma(\alpha)$$

$$N_{K/F}(\alpha) = \prod_{\sigma \in Gal(K/F)} \sigma(\alpha)$$

We will denote $Tr_{K/F}$ and $N_{K/F}$ by simply Tr and N, assuming the extension is clear.

Remark 4.13. For the extension, F_{p^n}/F_p, $Gal(F_{p^n}/F_p) = \langle\varphi\rangle$ where φ is the Frobenius map, $\varphi(x) = x^p$ by Theorem 4.11. Then for $x \in F_p$, the Norm of the extension is

$$N(x) = \prod_{i=1}^{n} \varphi^i(x) = x^p \cdot x^{p^2} \cdot x^{p^3} \cdots x^{p^n} = x^{1+p+p^2+\cdots+p^{n-1}}.$$

Note that $x^{p^n} = x$. Telescoping the sum, we have

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

Thus $N(x) = x^{\frac{(p^n-1)}{(p-1)}}$ for the extension F_{p^n}/F_p.

The next few theorems give us a better understanding of the properties of the Norm and Trace maps. In particular, their surjectivity and homomorphic behavior.

Theorem 4.14. *Tr is an additive homomorphism from $F_{p^n} \longrightarrow F_p$.*

Proof. Suppose F_{p^n}/F_p is a Galois extension and let G denote the Galois group, $Gal(F_{p^n}/F_p)$. First we will show that Tr maps F_{p^n} into the base field, F_p. So, for $x \in F_{p^n}$,

$$Tr(x) = \sum_{\sigma \in Gal(K/F)} \sigma(x),$$

which we will denote simply as $\sum \sigma(x)$. If for all $\hat{\sigma} \in G$, $\hat{\sigma}$ fixes $Tr(x) = \sum \sigma(x)$, then $\sum \sigma(x) \in F_p$, i.e. $\hat{\sigma}(\sum \sigma(x)) = \sum \sigma(x)$. So, let $\hat{\sigma} \in G$ be arbitrary. Then

$$\hat{\sigma}(\sum \sigma(x)) = \sum \hat{\sigma}(\sigma(x)) = \sum \hat{\sigma} \cdot \sigma(x).$$

Since G is a group then $\hat{\sigma} \cdot \sigma = \sigma'$ for some $\sigma' \in G$. So

$$\sum \hat{\sigma} \cdot \sigma(x) = \sum \sigma'(x).$$

Thus $\hat{\sigma}$ simply permutes the elements in the sum. Therefore,

$$\sum_{\sigma' \in G} \sigma'(x) = \sum_{\sigma \in G} \sigma(x).$$

So $\sum \sigma(x)$ is fixed by $\hat{\sigma} \in G$ thus $\sum \sigma(x) \in F_p$ and Tr maps elements into F_p. Now, we will show that Tr is an additive homomorphism. Let $x, y \in F_{p^n}$. So $Tr(x+y) = \sum \sigma(x+y)$. Since $\sigma \in G$ is a field automorphism, then

$$\sum \sigma(x+y) = \sum \sigma(x) + \sigma(y) = \sum \sigma(x) + \sum \sigma(y) = Tr(x) + Tr(y).$$

Thus Tr is an additive homomorphism. □

Lemma 4.15. *Moreover, if $n = 2$, Tr is surjective.*

Proof. Suppose $n = 2$. That is we are considering the Galois extension F_{p^2}/F_p. Let $x \in F_p$, then $Tr(x) = \sum \sigma(x)$. Since $x \in F_p$, for all $\sigma \in G$, $\sigma(x) = x$. Hence $Tr(x) = \sum \sigma(x) = |G|x = 2x$, as mentioned above in Remark 4.12. *Case 1*: Suppose p is odd. Then 2 does not divide p and hence 2 has an inverse in F_p. So for all $x \in F_p$, x can be written as $2 \cdot 2^{-1}x = 2y$ for some $y \in F_p \subseteq F_{p^2}$. Hence for all $x \in F_p$, there exists $y = 2^{-1}x \in F_{p^2}$ such that

$$Tr(y) = Tr(2^{-1}x) = \sum \sigma(2^{-1}x) = 2(2^{-1}x) = x.$$

Thus Tr is surjective. *Case 2*: Suppose p is even. Then by a construction in Section 5.1, $F_{p^2} = F_4 = \{0, 1, \alpha, \alpha+1\}$ with $\alpha^2 + \alpha + 1 = 0$. Thus $Gal(F_4/F_2) =< \varphi >$ where $\varphi(x) = x^2$ and for all $x \in F_4$,

$$Tr(x) = \sum \sigma(x) = x + \varphi(x) = x + x^2.$$

By explicitly evaluating Tr for values in F_4, we have $Tr(0) = 0$, and $Tr(\alpha) = \alpha + \alpha^2 = 2\alpha + 1 = 1$. So for all $x \in F_2$, there exists $y \in F_4$ such that $Tr(y) = x$. Hence Tr maps F_4 onto $F_2 = \{0, 1\}$. Therefore in both cases, Tr maps F_{p^2} onto F_p. □

Theorem 4.16. *N is a surjective, multiplicative homomorphism from $F_{p^n} \longrightarrow F_p$.*

Proof. Suppose F_{p^n}/F_p is a Galois extension with Galois group $Gal(F_{p^n}/F_p) = G$. For $x \in F_{p^n}$,

$$N(x) = \prod_{\sigma \in G} \sigma(x),$$

which we simply denote as $N(x) = \prod \sigma(x)$. First we will show that N maps F_{p^n} into the base field F_p. If for all $\hat{\sigma} \in G$, $\hat{\sigma}(\prod \sigma(x)) = \prod \sigma(x)$, then$\prod \sigma(x) \in F_p$. Let $G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$. Then $N(x) = \sigma_1(x)\sigma_2(x)\cdots\sigma_n(x)$. Let $\sigma_j \in G$ be arbitrary, then

$$\sigma_j(N(x)) = \sigma_j(\sigma_1(x)\sigma_2(x)\cdots\sigma_n(x)) = \sigma_j \cdot \sigma_1(x)\ \sigma_j \cdot \sigma_2(x)\cdots\sigma_j \cdot \sigma_n(x) \tag{4.1}$$

In a group, multiplication by a fixed group element simply permutes the group. In this case, the fixed element σ_j permutes the elements of G hence $\sigma_j \cdot \sigma_i = \sigma_k$, for $1 \leq k \leq n$. Reorder equation 4.1 if necessary, so

$$\sigma_j(N(x)) = \sigma_1(x)\sigma_2(x)\cdots\sigma_n(x) = N(x).$$

Hence $N(x)$ is fixed by an arbitrary $\sigma_j \in G$ so $N(x) \in F_p$. Next we will show that N is a multiplicative homomorphism. Let $x, y \in F_{p^n}$. Then $N(xy) = \prod \sigma(xy) = \prod \sigma(x)\sigma(y)$ since $\sigma \in G$ is a field automorphism. Thus

$$N(xy) = \prod \sigma(x)\sigma(y) = \prod \sigma(x) \prod \sigma(y) = N(x)N(y).$$

Finally, we will show that N is a surjective map. Recall from Remark 4.13 that for the extension F_{p^n}/F_p,

$$N(x) = x^{\frac{(p^n-1)}{(p-1)}}$$

for all $x \in F_{p^n}$. Set $\frac{(p^n-1)}{(p-1)} = k$. Note that $N(0) = 0^k = 0$, hence we will ignore this case and regard N as a multiplicative group homomorphism from $F_{p^n}^{\times} \longrightarrow F_p^{\times}$, where $|F_{p^n}^{\times}| = p^n - 1$ and $|F_p^{\times}| = p - 1$. So, $N(x) = x^k$ and

$$\ker N = \{x \in F_{p^n}^{\times} \mid N(x) = 1\} = \{x \in F_{p^n}^{\times} \mid x^k = 1\}.$$

We can then consider $\ker N$ to be the solutions of the equation $x^k - 1 = 0$. Since a polynomial of degree k can have at most k roots, $|\ker N| \leq k$. N is defined such that N maps $F_{p^n}^{\times}$ into $F_p^{\times}$, the range of N has at least $\frac{p^n-1}{k}$ elements by Lagrange's theorem, that is $|Im(N)| \geq p-1$. Since $Im(N) \subseteq F_p^{\times}$, then $|Im(N)| = p - 1$. Hence N maps onto $F_p^{\times}$, moreover, N maps onto F_p. □

Chapter 5

The Construction of Winnie Li's Graphs

Winnie Li graphs are specific Cayley graphs with the set of vertices defined to be the elements of the field F_{p^n}. These graphs are of interest to us because for $n = 2$, a Winnie Li graph is Ramanujan. This conclusion will be more thoroughly explained in Chapter 6. For $n = 2$, since the Winnie Li graphs are Ramanujan, we are able to use the eigenvalues of the adjacency matrix to get a bound on the expanding constant.

We will now begin the set up for the construction of the Winnie Li graphs. We follow and expand on the discussion in [9].

5.1 The Field Extension

Let F_{p^n} be a finite field with p^n elements and base field F_p. Let $m(x) \in F_p[x]$ be a monic irreducible polynomial of degree n and suppose $\alpha \in F_{p^n}$ is a root of $m(x)$. Thus $\alpha \in F_{p^n}$ is algebraic over F_p and by Theorem 4.1 we have the following results:

$$F_p[x]/(m(x)) \cong F_p(\alpha)$$

$$F_p(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in F_p \text{ for } 0 \leq i \leq n-1\}$$

$$[F_p(\alpha) : F_p] = \deg m(x) = n$$

Note that $|F_p(\alpha)| = p^n$ and $|F_{p^n}| = p^n$. Since all finite fields of order p^n are unique up to isomorphism by Theorem 4.7, then $F_p(\alpha) \cong F_{p^n}$.

Remark 5.1. When choosing the monic irreducible polynomial, $m(x)$, of degree n in $F_p[x]$, it is most useful to pick $m(x)$ to be a primitive polynomial. Then if $\alpha \in F_{p^n}$ is a root of $m(x)$,

α will be a primitive element and generate $F_{p^n}^{\times}$. Finding a monic irreducible polynomial in $F_p[x]$ is easy by utilizing Mathematica's "Algebra'FiniteFields'" package. This package that contains a command which will output an irreducible polynomial once you have specified the degree of the polynomial, the coefficients modulo a prime p, and the variable of representation, usually x. On the other hand, because finding a primitive polynomial is more difficult, extensive tables exist. In any specific case, to see whether a polynomial is primitive, take α to be a root of $m(x)$ and through brute force, see whether it generates $F_{p^n}^{\times}$.

Example. Let F_{2^2} be the finite field of 4 elements with base field $F_2 = \{0, 1\}$. Let α be a root to the minimal irreducible polynomial $m(x) = x^2 + x + 1$, hence $m(\alpha) = 0$. By the above conclusions:

$$F_2[x]/(x^2 + x + 1) \cong F_2(\alpha) \cong F_4$$

$$F_2(\alpha) = \{a_0 + a_1\alpha \mid a_0, a_1 \in F_2\} = \{0, 1, \alpha, \alpha + 1\}$$

$$[F_2(\alpha) : F_2] = \deg m(x) = 2$$

When reducing elements of $F_2[\alpha] \cong F_4$ modulo $m(x) = x^2 + x + 1$ and modulo 2, recall that

$$\alpha^2 + \alpha + 1 = 0 \Rightarrow \alpha^2 = -\alpha - 1 \Rightarrow \alpha^2 = \alpha + 1.$$

Now one can write out the Cayley Tables of F_4 with respect to addition and multiplication.

Table 5.1: *Additive Cayley Table of* $F_4 \simeq F_2(\alpha)$ *where* $\alpha^2 = \alpha + 1$

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

Table 5.2: *Multiplicative Cayley Table of* $F_4 \simeq F_2(\alpha)$ *where* $\alpha^2 = \alpha + 1$

$\times$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

Example. Let F_{3^2} be the finite field of 9 elements with base field $F_3 = \{0, 1, 2\}$. Let α be a root of the minimal irreducible polynomial $m(x) = x^2 + x + 2$, that is $m(\alpha) = 0$. We will show later that $m(x)$ is in fact primitive. By the conclusions above:

$$F_3[x]/(x^2 + x + 2) \cong F_3(\alpha) \cong F_9$$

$$F_3(\alpha) = \{a_0 + a_1\alpha \mid a_0, a_1 \in F_3\}$$

$$[F_3(\alpha) : F_3] = \deg m(x) = 2$$

When reducing elements of $F_3[\alpha] \cong F_9$ modulo $m(x) = x^2 + x + 2$ and modulo 3, recall that

$$\alpha^2 + \alpha + 2 = 0 \Rightarrow \alpha^2 = -\alpha - 2 \Rightarrow \alpha^2 = 2\alpha + 1.$$

The elements of F_9 are listed below, using the fact that $F_3(\alpha) = \{a_0 + a_1\alpha \mid a_0, a_1 \in F_3\}$. To gain practice working with the elements of F_9 one can create the Cayley Table of F_9 with respect to addition and multiplication as in the example of F_4 above.

Table 5.3: *Elements of* F_9

0	1	2
α	$\alpha + 1$	$\alpha + 2$
2α	2α +1	$2\alpha + 2$

Remark 5.2. To prove that a polynomial $m(x)$ in $F_p[x]$ is irreducible, one can divide $m(x)$ by all polynomials in $F_p[x]$ of smaller degree and conclude that $m(x)$ cannot be factored. Another technique is to use Mathematica's "IrreduciblePolynomial[s, p, d]" function that finds an irreducible polynomial of degree d over the integers mod prime p, expressed in terms of the symbol s which is in the Mathematica package <<Algebra‘FiniteFields‘, as previously mentioned.

5.2 Creating the Table of Logs for F_{p^n}

For choices of p and n as small as 7 and 2, we see that F_{p^n} has 49 elements which can be cumbersome to work with. In order to simplify working with the field, we will create a table of logs to represent the elements.

By Theorem 4.8, $F_{p^n}^{\times} = F_{p^n} - \{0\}$ is a cyclic group of order $p^n - 1$. For $\alpha \in F_{p^n}$, a root of $m(x)$, if α is a primitive element of F_{p^n} then $F_{p^n}^{\times} = \langle\alpha\rangle$ and we can develop a table of logs for the finite field $F_{p^n}^{\times}$ as shown below in Table 5.4 for $F_4^{\times}$. The table of logs allows us to identity each element of $F_{p^n}^{\times}$ by a power of α and by its coefficients when represented by the basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. In particular, i is the exponent of α that corresponds to the element

that is represented as a linear combination of powers of α, i.e. $\alpha^i = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$. We refer to the table as the table of logs because i is the $\log_\alpha(\text{row}_i)$.

The set of elements $\Theta_n \subset F_{p^n}$ will create the edges of the Winnie Li graph. Therefore, representing the elements of $F_{p^n}^\times$ in the form α^i enables us to easily identify the elements of Θ_n because this is a calculation done in the multiplicative group, $F_{p^n}^\times$. However, representing each element as $\sum_{k=1}^{(n-1)} a_k\alpha^k$ captures the additive operations by which elements of Θ_n connect the vertices of the graph. The table of logs condenses this information and simplifies computations in the field.

Table 5.4: *Table of Logs for* $F_4^\times \simeq F_2(\alpha)^\times$ *where* $\alpha^2 = \alpha + 1$ *and* $\alpha^i = a_0 + a_1\alpha$

i	a_0	a_1
0	1	0
1	0	1
2	1	1

To more easily compute the table of logs, we use a linear feedback shift register. First, define $\tau : F_{p^n}^\times \longrightarrow F_{p^n}^\times$ by $\tau(y) = \alpha y$ where $y \in F_{p^n}^\times$ and α is the primitive element of F_{p^n}. Since $y \in F_{p^n}^\times$ then $y = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ for $a_i \in F_p$. Hence

$$\tau(y) = \tau(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$$

reduced modulo $m(x)$ and modulo p, where $b_i \in F_p$. Now, define the feed back shift register $\sigma : F_p \times F_p \times \cdots \times F_p \longrightarrow F_p \times F_p \times \cdots \times F_p$ by

$$\sigma(a_0, a_1, \ldots, a_{n-1}) = (b_0, b_1, \ldots, b_{n-1}).$$

Note that each b_i is a linear combination of the a_j's. Therefore to make the table of logs of $F_{p^n}^\times$, we use τ once for the element $\alpha^0 = 1$ and then σ recursively to find $\alpha, \alpha^2, \ldots, \alpha^{p^n-1}$ in terms of their coefficients.

Example. In this example, we will construct the linear feedback shift register for $F_9^\times$. Define $\tau : F_9^\times \longrightarrow F_9^\times$ by

$$\begin{aligned} \tau(a_0 + a_1\alpha) &= \alpha(a_0 + a_1\alpha) \\ &= a_0\alpha + a_1\alpha^2 \\ &= a_0\alpha + a_1(2\alpha + 1) \\ &= a_1 + (a_0 + 2a_1)\alpha \end{aligned}$$

Thus, the feedback shift register σ, is defined as

$$\sigma(a_0, a_1) = (a_1, a_0 + 2a_1).$$

For instance, to find $\alpha^2 = \tau(\alpha)$, we take $(0,1)$ which corresponds to α and $\sigma(0,1) = (1, 0+2\cdot 1)$ thus $\alpha^2 = 1 + 2\alpha$. Similarly, $\alpha^3 = \tau(\alpha^2) = \tau(1+2\alpha)$. Then $\sigma(1,2) = (2, 1+2\cdot 2) = (2,2)$, hence $\alpha^3 = 2 + 2\alpha$.

If α generates the group $F_{p^n}^\times$ then α is a primitive element. In the example below, we complete the table of logs for $F_9^\times$ using the feedback shift register, σ. Since α generates $F_9^\times$ then α is a primitive element of F_9.

Example. For the field F_9, we have constructed the table of logs for $F_9^\times$ below using the map σ as defined in the previous example to be $\sigma(a_0, a_1) = (a_1, a_0 + 2a_1)$.

Table 5.5: *Table of Logs for* $F_9^\times \simeq F_3(\alpha)^\times$ *where* $\alpha^2 = 2\alpha + 1$ *and* $\alpha^i = a_0 + a_1\alpha$

i	a_0	a_1
0	1	0
1	0	1
2	1	2
3	2	2
4	2	0
5	0	2
6	2	1
7	1	1

5.3 Defining the Set of Edges

The edges of the Winnie Li graph associated with F_{p^n} are determined by calculations with the Galois group and the Norm map of the field extension F_{p^n}/F_p.

Recall from Theorem 4.11 that F_{p^n}/F_p is a Galois extension with Galois group, $Gal(F_{p^n}/F_p) = \langle\varphi\rangle$ where φ is the Frobenius automorphism defined by $\varphi(x) = x^p$ for all $x \in F_{p^n}$. Note that $|Gal(F_{p^n}/F_p)| = [F_{p^n} : F_p] = n$.

We will now use the Norm map of the extension F_{p^n}/F_p to form the set of edges of the graph. First, set $k = \frac{p^n-1}{p-1}$. Now, recall from Remark 4.13 that for all $x \in F_{p^n}$, the Norm of the extension F_{p^n}/F_p is

$$N(x) = \prod_{i=1}^{n} \varphi^i(x) = x \cdot x^p \cdots x^{p^n} = x^k.$$

Define Θ_n to be the following set:

$$\Theta_n = \ker N = \{x \in F_{p^n} \mid N(x) = 1\} = \{x \in F_{p^n} \mid x^k = 1\}.$$

Since the Norm maps F_{p^n} onto F_p by Theorem 4.16, $|\ker N| = |\Theta_n| = k$. The elements of Θ_n will form the set of edges of the Winnie Li graph.

Lemma 5.3. *For the Galois extension F_{p^n}/F_p and Θ_n as defined above, Θ_n is a cyclic group of order k generated by α^{p-1} where α is the primitive element of F_{p^n}.*

Proof. Let F_{p^n}/F_p be a Galois extension with the Galois group generated by φ, the Frobenius automorphism. By Theorem 4.16, the Norm map, N, is a surjective homomorphism from $F_{p^n} \longrightarrow F_p$. Since $N(0) = 0$, we can regard N mapping $F_{p^n}^{\times} \longrightarrow F_p^{\times}$. Recall from Remark 4.13 that $N(x) = x^k$ where $k = \frac{p^n-1}{p-1}$ and $|kerN| = |\Theta_n| = k$. Since $\Theta_n = kerN$, Θ_n is a subgroup of the cyclic group $F_{p^n}^{\times} = \langle\alpha\rangle$ where α is the primitive element of F_{p^n}. Since a subgroup of a cyclic group is itself cyclic, then $\Theta_n = \langle\alpha^i\rangle$ where $|\alpha^i| = k$. Thus

$$\alpha^{ik} = 1 = \alpha^{p^n-1}.$$

Find i, $0 \leq i \leq p^n - 1$ such that

$$ik = p^n - 1 \Longrightarrow \frac{i(p^n-1)}{p-1} = p^n - 1 \Longrightarrow i = p - 1.$$

So $\Theta_n = \langle\alpha^{p-1}\rangle$. □

In the examples below, we will find the elements of Θ_2 of $F_9 \cong F_3(\alpha)$.

Example. For the Galois extension, F_9/F_3, we have that $[F_9 : F_3] = 2$ and $k = \frac{p^n-1}{p-1} = \frac{3^2-1}{3-1} = 4$ For all $x \in F_9$, we know that $N(x) = x^4$, hence

$$\Theta_2 = \{x \in F_9 \mid x^4 = 1\}.$$

By Lemma 5.3, $\Theta_2 = \langle\alpha^2\rangle = \{\alpha^2, \alpha^4, \alpha^6, \alpha^8 = 1\}$. By using Table 5.5 we can write the elements of Θ_2 in the form $a_0 + a_1\alpha$. Hence

$$\Theta_2 = \{1, 1 + 2\alpha, 2, 2 + \alpha\}.$$

Example. For the Galois extension F_4/F_2, $k = \frac{2^2-1}{2-1} = 3$ and by Lemma 5.3, $\Theta_2 = \langle\alpha^{2-1}\rangle$. Note that for this extension, $F_4^{\times} = \langle\alpha\rangle = \Theta_2$, hence

$$\Theta_2 = \{1, \alpha, \alpha + 1\}.$$

5.4 A Winnie Li Graph

Definition. A *Winnie Li graph* is the Cayley graph $X = (F_{p^n}, \Theta_n)$ with vertices defined to be the elements of F_{p^n} and the edges of each vertex x given by $x + s$ for $s \in \Theta_n$. These are $k = (\frac{p^n-1}{p-1})$-regular graphs with p^n vertices.

For values of n that are even, Θ_n is a symmetric set of generators of F_{p^n}. Since Θ_n is symmetric, our graphs will be non-directed graphs. In our later discussions of Winnie Li's graphs in Chapter 6 we will take $n = 2$.

Remark 5.4. For a group G, with the operation written as multiplication, and $S \subseteq G$ a set of group elements such that $1 \notin S$, *a Cayley graph* (G, S) is defined to be the directed graph having one vertex associated with each group element and directed edges (g, h) whenever $g = sh$ for $s \in S$.

5.5 Examples of Completed Winnie Li Graphs

In this section, we will compile all the information we have found in the examples throughout the chapter to construct the Winnie Li graph for the finite fields F_4 and F_9. In addition, we will construct from start to finish the Winnie Li graph for F_{25}.

Construction of $X = (F_4, \Theta_2)$. We have the field extension $F_4 \cong F_2(\alpha)$ where α is the root of the monic irreducible polynomial $m(x) = x^2 + x + 1$. As shown in Section 5.2, α is a primitive element and thus generates the group $F_4^\times$. So,

$$F_4 = \{0,\ 1,\ \alpha,\ \alpha + 1\}$$

are the vertices of the graph. In Section 5.3, we found that

$$\Theta_2 = \langle \alpha \rangle = \{1,\ \alpha,\ \alpha + 1\}.$$

Hence we find the edges of the graph by adding the elements of Θ_2 to each element of F_4. Using the Additive Cayley Table for F_4, Table 5.1, we notice that we simply connect each vertex to all other vertices to construct the graph below. Notice that this is precisely the complete graph K_4, which has an edge between every set of vertices.

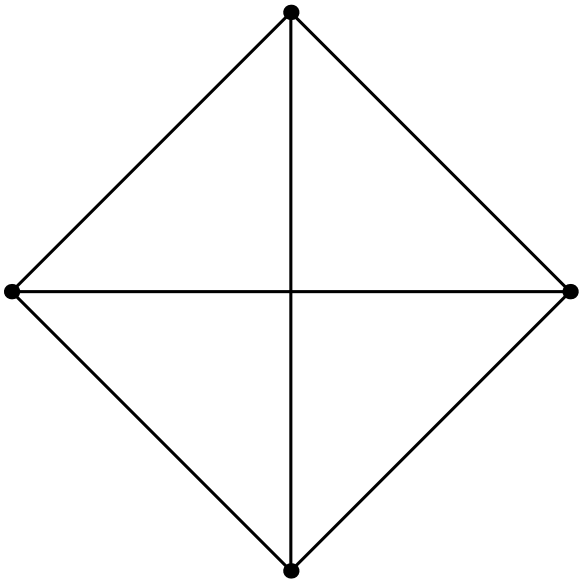

Figure 5.1: *Winnie Li's Graph* $X = (F_4, \Theta_2)$

Construction of $X = (F_9, \Theta_2)$. Now we are working with the field extension $F_9/F_3 \cong F_3(\alpha)$ where α is the root of the monic irreducible polynomial $m(x) = x^2 + x + 2$. By our example in Section 5.2, we know that $m(x)$ is a primitive polynomial of $F_9[x]$ and hence α, a root of $m(x)$, generates $F_9^{\times}$. Again, using Table 5.3, the elements of F_9 and the vertices of the graph are precisely,

$$F_9 = \{0,\ 1,\ 2,\ \alpha,\ \alpha + 1,\ \alpha + 2,\ 2\alpha,\ 2\alpha + 1,\ 2\alpha + 2\}.$$

In Section 5.3, we showed that

$$\Theta_2 = \langle \alpha^2 \rangle = \{1,\ 1 + 2\alpha,\ 2,\ 2 + \alpha\}.$$

To find the edges of $X = (F_9, \Theta_2)$, we need to add all the elements of Θ_2 to each element of F_9. Therefore we have the following graph of $X = (F_9, \Theta_2)$, Figure 5.2.

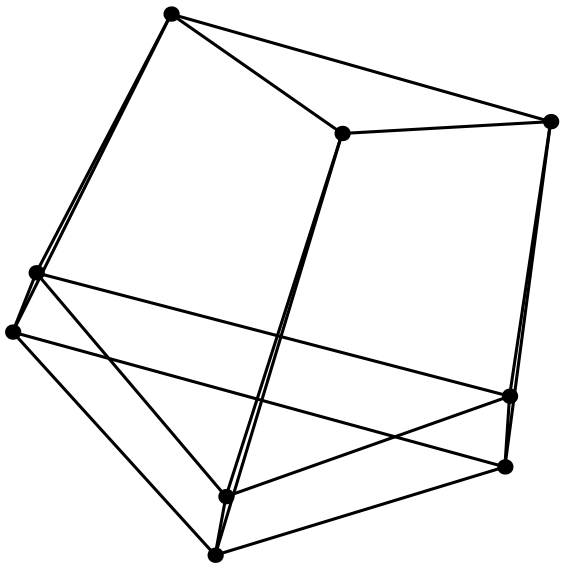

Figure 5.2: *Winnie Li's Graph* $X = (F_9, \Theta_2)$

Construction of $X = (F_{25}, \Theta_2)$. Let F_{25} be a finite field with 25 elements and base field F_5. Let $m(x) = x^2 + x + 2$ be the monic irreducible polynomial in $F_5[x]$ with α as root of $m(x)$. Then by Section 5.1 we know that

$$F_{25} \cong F_5(\alpha) = \{a_0 + a_1\alpha \mid a_1 \in F_5, \alpha^2 = 4\alpha + 3\}.$$

By computing the linear feedback shift register, $\sigma(a_0, a_1) = (4a_1 + a_0, 3a_1)$, we can compute the table of logs for F_{25} as below in Table 5.6 and conclude that since α generates $F_{25}^{\times}$ then α is a primitive element of F_{25}.

Table 5.6: *Elements of* $F_{25}^{\times} \simeq F_5(\alpha)^{\times}$ *where* $\alpha^2 = 4\alpha + 3$ *and* $\alpha^i = a_0 + a_1\alpha$

i	a_0	a_1	i	a_0	a_1
0	1	0	12	4	0
1	0	1	13	0	4
2	3	4	14	2	1
3	2	4	15	3	1
4	2	3	16	3	2
5	4	4	17	1	1
6	2	0	18	3	0
7	0	2	19	0	3
8	1	3	20	4	2
9	4	3	21	1	2
10	4	1	22	1	4
11	3	3	23	2	2

The elements of $F_{25} \cong F_5(\alpha)$ will be the vertices of our graph. Now we will find Θ_2 which will form the set of edges for the graph. First, note that $k = \frac{p^n-1}{p-1} = 6$ so $|\Theta_2| = 6$ and by Lemma 5.3, Θ_2 is generated by $\alpha^{p-1} = \alpha^4$. That is,

$$\begin{aligned} \Theta_2 = \langle \alpha^4 \rangle &= \{\alpha^4, \alpha^8, \alpha^{12}, \alpha^{16}, \alpha^{20}, \alpha^{24} = 1\} \\ &= \{1,\ 2+3\alpha,\ 1+3\alpha,\ 4,\ 3+2\alpha,\ 4+2\alpha\} \end{aligned} \tag{5.1}$$

Now to complete the graph, one needs to add each element of Θ_2 to each vertex of F_{25} to find the edges of each vertex. The graph is 6-regular with 25 vertices. Table 5.7 is the adjacency matrix of the graph, where a 1 in the ijth entry matrix means there is an edge between the ith and jth vertex. The ijth entry of the matrix represents the edge between α^{i-2} and α^{j-2}. Note that the first column and first row represent the edges between 0 and $F_{25}^{\times}$. In addition, Figure 5.3 is the graph of F_{25}.

Table 5.7: *Adjacency Matrix of* $X = (F_{25}, \Theta_2)$

0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0
1	0	0	0	0	1	0	1	1	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0
0	0	0	0	1	0	0	0	0	0	1	1	1	0	0	0	0	0	1	0	0	0	0	1	0
0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	1	0	0	1	0	0	1	0	0	0
0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0
1	1	0	0	0	0	0	0	0	1	0	1	1	0	0	0	1	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	0	1	0	0	0	0	0	1	1	1	0	0	0	0	0	1	0	0
0	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	1	0	0	1	0	0
0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0
1	0	0	0	0	1	0	0	0	0	0	0	0	1	0	1	1	0	0	0	1	0	0	0	0
0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	1	1	1	0	0	0	0
0	0	1	0	0	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	1	0
0	1	1	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	1	1	0	0	0	1
0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	1	1	1
0	0	0	1	0	0	1	0	0	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0
0	0	0	0	0	1	1	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0
1	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	1	1
0	0	1	1	1	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0
0	0	0	0	0	0	0	1	0	0	1	0	0	1	0	0	0	0	0	0	1	0	1	0	1
0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0	0	1	1	0	0	0	0	0
1	1	0	1	1	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
0	0	0	0	0	0	1	1	1	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1
0	0	1	0	1	0	0	0	0	0	0	1	0	0	1	0	0	1	0	0	0	0	0	0	1
0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0	0	1	1	0

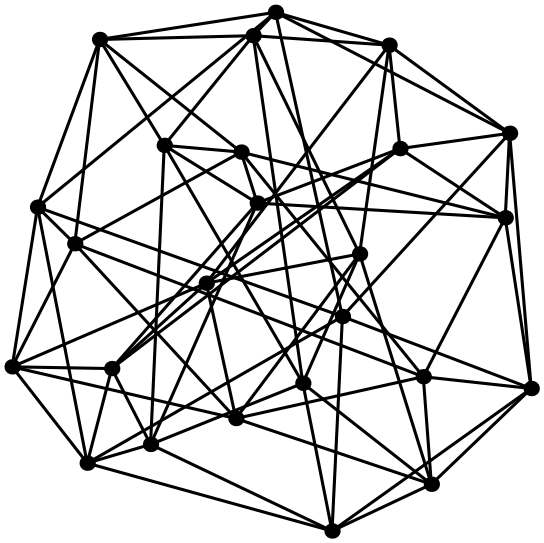

Figure 5.3: *Winnie Li's Graph* $X = (F_{25}, \Theta_2)$

We have used Mathematica's "DiscreteMath‘Combinatorica'" package to graph Winnie Li's graphs from their adjacency matrix. In addition, once we have the adjacency matrix for the Winnie Li graph, we can also use Mathematica to find the eigenvalues of the matrix and use those values to construct a bound on the expanding constant as in Chapter 3. In the next chapter, for a field extension F_{p^n} where $n = 2$, we will exhibit the eigenvalues and eigenfunctions for the Winnie Li graph, $X = (F_{p^2}, \Theta_2)$. In addition, it has been shown through more advanced mathematics that the Winnie Li graph is Ramanujan, for $n = 2$.

Chapter 6

Spectral Decomposition of the Adjacency Matrix

For the special case of Winnie Li graphs when $n = 2$, we will establish that we know the eigenfunctions and eigenvalues of the adjacency matrix of the graph. From estimates on the eigenvalues, it has been shown that these Winnie Li graphs are Ramanujan. In this chapter, we will first define the eigenfunctions and prove that they are a complete set of orthogonal functions in $L^2(F_{p^2})$. We will then define and prove that we know the eigenvalues of the graph, $X = (F_{p^2}, \Theta_2)$. Our discussion is an expansion of the outline given in [9].

Definition. For each $a \in F_{p^2}$, define $\varphi_a : F_{p^2} \longrightarrow T = \{z \in \mathbb{C} \mid |z| = 1\}$ such that for all $x \in F_{p^2}$,

$$\varphi_a(x) = exp\left(\frac{2\pi i Tr(ax)}{p}\right).$$

Remark 6.1. We will show later that φ_a is a group homomorphism. Recall that Tr maps elements into F_p, the base field of F_{p^2}. Hence we may regard $Tr(ax) \in \{0, 1, 2, \ldots, p-1\}$. We will use this convention to treat $Tr(ax)$ as an integer. Thus $exp\big(\frac{2\pi i Tr(ax)}{p}\big)$ is evaluated in $\mathbb{C}$ as usual.

Theorem 6.2. *The functions φ_a, for $a \in F_{p^2}$, form a complete orthogonal set of functions in $L^2(F_{p^2})$.*

Proof. Let $\varphi_a, \varphi_b \in \{\varphi_i \mid i \in F_{p^2}\} = K$. We will show that K forms a complete orthogonal set of functions on $L^2(F_{p^2})$. That is, for all $a, b \in F_{p^2}$, $\langle \varphi_a, \varphi_b \rangle = p^2 \delta_{a,b}$. Recall that

$$\langle \varphi_a, \varphi_b \rangle = \sum_{x \in F_{p^2}} \varphi_a(x) \overline{\varphi_b(x)}.$$

First, show that $\langle \varphi_a, \varphi_a \rangle \neq 0$. So,

$$\begin{aligned}
\langle \varphi_a, \varphi_a \rangle &= \sum_{x \in F_{p^2}} \varphi_a(x)\overline{\varphi_a(x)} \\
&= \sum_{x \in F_{p^2}} exp\left(\frac{2\pi i Tr(ax)}{p}\right)\overline{exp\left(\frac{2\pi i Tr(ax)}{p}\right)} \\
&= \sum_{x \in F_{p^2}} exp\left(\frac{2\pi i Tr(ax)}{p}\right)exp\left(\frac{-2\pi i Tr(ax)}{p}\right) \\
&= \sum_{x \in F_{p^2}} exp\left(\frac{2\pi i\big(Tr(ax) - Tr(ax)\big)}{p}\right) \\
&= \sum_{x \in F_{p^2}} exp(0) \\
&= \sum_{x \in F_{p^2}} 1 = p^2.
\end{aligned}$$

Therefore, $\langle \varphi_a, \varphi_a \rangle \neq 0$. Moreover, $\langle \frac{\varphi_a}{p}, \frac{\varphi_a}{p} \rangle = 1$. Now, we will show that $\langle \varphi_a, \varphi_b \rangle = 0$ where $a \neq b$. So,

$$\begin{aligned}
\langle \varphi_a, \varphi_b \rangle &= \sum_{x \in F_{p^2}} \varphi_a(x)\overline{\varphi_b(x)} \\
&= \sum_{x \in F_{p^2}} exp\left(\frac{2\pi i\big(Tr(ax) - Tr(bx)\big)}{p}\right).
\end{aligned}$$

Recall that $Tr(ax) = ax + (ax)^p = ax + a^p x^p$ since we are in a field. Similarly, $Tr(bx) = bx + b^p x^p$. So $Tr(ax) - Tr(bx) = ax + a^p x^p - bx - b^p x^p = x(a-b) + x^p(a^p - b^p)$. So by Remark **??**,

$$Tr(ax) - Tr(bx) = x(a-b) + x^p(a-b)^p = Tr\big((a-b)x\big).$$

Let $y = (a-b)x \in F_{p^2}$. Note that Tr is a surjective additive homomorphism from $F_{p^2} \longrightarrow F_p$ by Lemma 4.15. By the First Isomorphism Theorem, $F_{p^2}/\ker(Tr) \cong F_p$. Thus the order of each coset in $F_{p^2}/\ker(Tr)$ is p and there are p distinct cosets. That is, for each $q \in F_p$ there is a distinct coset of $F_{p^2}/\ker(Tr)$ that Tr maps to q. So in the sum, $\sum_{y \in F_{p^2}} exp\big(\frac{2\pi i Tr(y)}{p}\big)$, $Tr(y)$ takes on each value $q \in F_p$, p times. So

$$\sum_{y \in F_{p^2}} exp\left(\frac{2\pi i Tr(y)}{p}\right) = p\sum_{q=0}^{p-1} exp\left(\frac{2\pi i q}{p}\right).$$

One may then notice that $exp(\frac{2\pi i}{p})$ is the primitive p^{th} root of unity and thus generates the cyclic group of roots to the polynomial $f(x) = x^p - 1$ in $\mathbb{Z}[x]$. Hence $exp(\frac{2\pi i q}{p})$, for

$0 \leq q \leq p-1$, are all solutions to the equation $x^p - 1 = 0$. If we factor $f(x)$ completely in $\mathbb{C}[x]$ which contains the splitting field of $f(x)$ over $\mathbb{Q}$, then

$$f(x) = (x-\lambda_0)(x-\lambda_1)\cdots(x-\lambda_{p-1}) = x^p - 1$$

where each $\lambda_q = exp(\frac{2\pi iq}{p})$, $\lambda_q \in \mathbb{C}$. Note that the coefficient of x^{p-1} is

$$-\sum_{q=0}^{p-1} \lambda_q = -\sum_{q=0}^{p-1} exp(\frac{2\pi iq}{p}) = 0.$$

Thus

$$\langle \varphi_a, \varphi_b \rangle = \sum_{y \in F_{p^2}} exp\left(\frac{2\pi i Tr(y)}{p}\right) = p\sum_{q=0}^{p-1} exp(\frac{2\pi iq}{p}) = p \cdot 0 = 0.$$

So $\langle \varphi_a, \varphi_b \rangle = 0$ if $a \neq b$. Hence $\langle \varphi_a, \varphi_b \rangle = p^2\delta_{a,b}$ and $K = \{\varphi_a \mid a \in F_{p^2}\}$ forms an orthogonal basis for $L^2(F_{p^2})$. □

Theorem 6.3. *For $a \in F_{p^2}$, φ_a is an eigenfunction for Winnie Li's graphs $X(F_{p^2}, \Theta_2)$ corresponding to the eigenvalue*

$$\lambda_a = \sum_{s \in \Theta} \varphi_a(s) = \sum_{s \in \Theta} exp\left(\frac{2\pi i\big(as + (as)^p\big)}{p}\right).$$

Proof. For $a \in F_{p^2}$ and $x \in F_{p^2}$, let $\varphi_a : F_{p^2} \longrightarrow F_p$ be defined by

$$\varphi_a(x) = exp\left(\frac{2\pi i Tr(ax)}{p}\right).$$

Define the set $\Theta_2 = \{s \in F_{p^2} \mid N(s) = 1\}$ where N is the norm of F_{p^2}. For the extension F_{p^2}/F_p,

$$N(s) = \prod_{\sigma \in Gal(F_{p^2}/F_p)} \sigma(s) = s(s^p) = s^{p+1}.$$

Hence $\Theta_2 = \{s \in F_{p^2} \mid s^{p+1} = 1\}$. Now, let $f \in \ell^2 V$, $x \in V$, and $s \in \Theta_2 \subseteq V$, where V is the set of vertices of the graph X. Define $(s \cdot f)(x) = f(x-s)$. Since $\{\delta_{v_i}\}$ is a basis for $\ell^2 V$, we can write f as a linear combination of the basis elements. Note that

$$\begin{aligned} (s \cdot \delta_{v_i})(x) \neq 0 &\Leftrightarrow \delta_{v_i}(x-s) \neq 0 \\ &\Leftrightarrow x - s = v_i \\ &\Leftrightarrow x = v_i + s. \end{aligned}$$

Therefore $s \cdot \delta_{v_i} = \delta_{v_i+s}$. Let

$$f = \sum_{i=1}^{n} c\delta_{v_i} \Longrightarrow s \cdot f = \sum_{i=1}^{n} c\delta_{v_i+s}.$$

The defining property of an eigenfunction is that $Ax = \lambda x$, hence we will show that $A\varphi_a = \lambda_a\varphi_a$ for all $a \in F_{p^2}$ where A is the adjacency matrix for $X(F_{p^2}, \Theta)$. To better understand the action of A on f, note that A is a symmetric matrix with a 1 in the a_{ij} and a_{ji} entry if there is an $s \in \Theta$ such that $v_i + s = v_j$ or $v_j + s = v_i$, i.e. there is an edge between v_i and v_j. So if we use $\{\delta_{v_i}\}$ as a basis for A, then

$$\delta_{v_i} \longmapsto \sum_{s\in\Theta} s \cdot \delta_{v_i}.$$

Hence A represents the linear operator that takes f to $\sum_{s\in\Theta} s \cdot f$ for $f \in \ell^2 V$. Now we will show that $A\varphi_a = \lambda_a\varphi_a$. So $A\varphi_a = \sum_{s\in\Theta} s \cdot \varphi_a$ and as defined above,

$$A\varphi_a(x) = \sum_{s\in\Theta} s \cdot \varphi_a(x) = \sum_{s\in\Theta} \varphi_a(x - s).$$

$$\begin{aligned}
\sum_{s\in\Theta} \varphi_a(x-s) &= \sum_{s\in\Theta} exp\left(\frac{2\pi i Tr(a(x-s))}{p}\right) \\
&= \sum_{s\in\Theta} exp\left(\frac{2\pi i[a(x-s) + a^p(x-s)^p]}{p}\right) \\
&= \sum_{s\in\Theta} exp\left(\frac{2\pi i[ax + a^p x^p - as - a^p s^p]}{p}\right) \qquad (6.1)
\end{aligned}$$

Lemma 6.4. *If F_{p^2} is a degree 2 extension over F_p, then Θ_2 is a symmetric set of elements.*

Proof. Suppose that $s \in \Theta_2$ and we will show that $-s \in \Theta_2$. Since $s \in \Theta_2$ then by definition of Θ_2, $s^{p+1} = 1$. So,

$$(-s)^{p+1} = (-1)^{p+1}s^{p+1} = (-1)^{p+1}.$$

If p is an odd prime, then $(-1)^{p+1} = 1$. If $p = 2$, then $(-1)^{p+1} = -1 = 1 \mod 2$. Hence in either case, $-s \in \Theta_2$. □

By Lemma 6.4, if $s \in \Theta_2$ then $-s \in \Theta_2$. So $-s = \hat{s}$ for some $\hat{s} \in \Theta_2$. In equation 6.1, replace $-s$ by $\hat{s}$. Then,

$$\begin{aligned}
&\sum_{s\in\Theta_2} exp\left(\frac{2\pi i[ax + (ax)^p + a\hat{s} + (a\hat{s})^p]}{p}\right) \\
= &\sum_{s\in\Theta_2} exp\left(\frac{2\pi i Tr(ax)}{p}\right) exp\left(\frac{2\pi i Tr(a\hat{s})}{p}\right) \\
= &\ \varphi_a(x)\left[\sum_{\hat{s}\in\Theta_2} \varphi_a(\hat{s})\right] \\
= &\ \lambda_a\varphi_a(x).
\end{aligned}$$

Thus φ_a is an eigenfunction of the adjacency operator for Winnie Li's graphs $X(F_{p^2}, \Theta_2)$ corresponding to the eigenvalue λ_a. □

Theorem 6.2 only identifies the eigenvalues of the Winnie Li graph, $X(F_{p^2}, \Theta_2)$. The eigenvalue estimates showing that Winnie Li's graphs are Ramanujan are consequences of results of P. Deligne [2]. Because these results involve some of the most sophisticated algebraic geometry done in the twentieth century, including a generalization of algebraic topology that applies over fields of characteristic p, these results are not discussed in this thesis. However, it is interesting to note why the eigenvalues of Winnie Li's graphs fit into such a sophisticated algebraic framework. Let F_{p^2} be an additive group and $\mathbb{C} - \{0\}$ be the multiplicative group of nonzero complex numbers. Define the group homomorphism $\varepsilon : F_{p^2} \longrightarrow \mathbb{C} - \{0\}$ by

$$\varepsilon(w) = exp\left(\frac{2\pi i w}{p}\right).$$

Such homomorphisms are known as characters. The eigenvalue, λ_a, as defined in Theorem 6.2 is a "character sum", and in fact a Kloosterman sum. That is,

$$\lambda_a = \sum_{s \in \Theta} \varepsilon\left(\frac{2\pi i Tr(as)}{p}\right) = \sum_{b \in F_{p^2},\ s \in \Theta,\ b = as} \varepsilon\left(\frac{2\pi i Tr(b)}{p}\right).$$

Kloosterman sums are famous exponential sums that are frequently studied in number theory. (See [9], pg. 76).

As mentioned in Remark 6.1, below is the proof that φ_a is in fact a group homomorphism.

Lemma 6.5. *For $a \in F_{p^2}$, $\varphi_a :\longrightarrow T = \{z \in \mathbb{C} \mid |z| = 1\}$, defined by*

$$\varphi_a(x) = exp\left(\frac{2\pi i Tr(ax)}{p}\right)$$

is a group homomorphism.

Proof. Let $a \in F_{p^2}$ and $x, y \in F_{p^2}$. Recall that T is a multiplicative group and F_{p^2} is an additive group. So,

$$\begin{aligned}
\varphi_a(x)\varphi_a(y) &= exp\left(\frac{2\pi i Tr(ax)}{p} + \frac{2\pi i Tr(ay)}{p}\right) \\
&= exp\left(\frac{2\pi i[ax + a^p x^p + ay + a^p y^p]}{p}\right) \\
&= exp\left(\frac{2\pi i(a(x+y) + a^p(x+y)^p)}{p}\right) \\
&= exp\left(\frac{2\pi i Tr(a(x+y))}{p}\right) \\
&= \varphi_a(x+y).
\end{aligned}$$

Thus φ_a is a group homomorphism. □

Chapter 7

Eigenvalue Estimates

In this chapter, we will look at examples of the complete graph and Winnie Li graphs, their eigenvalues, and the bounds these eigenvalues create on the expanding constant $h(X)$. During our research, we observed an interesting fact about the characteristic polynomials of the Winnie Li graphs which turns out to be true in general, (for $n = 2$).

Suppose $X = (V, E)$ is a finite, connected, k-regular graph with n vertices. Then A is the $n \times n$ adjacency matrix of X with set of eigenvalues, $\{\mu_0, \mu_1, \ldots, \mu_{n-1}\}$. By Proposition 3.1 we can order the eigenvalues of A such that $k = \mu_0 > \mu_1 \geq \mu_2 \geq \cdots \geq \mu_{n-1} \geq -k$. From Chapter 3, recall that we established a bound on $h(X)$ where

$$\frac{k - \mu_1}{2} \leq h(X) \leq \sqrt{2k(k - \mu_1)}. \tag{7.1}$$

(As mentioned in Chapter 3, due to the advanced mathematics in the proof of the upper bound, we have only concentrated on the lower bound.)

In addition, from Chapter 1, a graph is Ramanujan if for every eigenvalue μ of A, $\mu \neq |k|$,

$$|\mu| \leq 2\sqrt{k - 1}. \tag{7.2}$$

There are a few reasons for the choice of the bound defining the Ramanujan graph. One reason is that the bound falls naturally out of the Deligne estimate mentioned in Chapter 6. However, a more compelling argument for the Ramanujan bound may come from a theorem in [1] that describes a family of graphs with bounds on the eigenvalues of the adjacency matrices. In particular, for a family of connected, k-regular (k fixed), finite graphs, $(X_m)_{m \geq 1}$ such that as $m \to +\infty$, $|V_m| \to +\infty$, we have that

$$\liminf_{m \to +\infty} \mu_1(X_m) \geq 2\sqrt{k - 1} \tag{7.3}$$

(Note that μ_1 is the largest nontrivial eigenvalue, $\mu_1 \neq k$.) As Terras describes, the above theorems show that "the Ramanujan bound is optimal for an infinite sequence of k-regular

graphs with number of vertices going to infinity" ([9]). As mentioned in Chapter 1, if a graph is Ramanujan then it satisfies a positive lower bound on $h(X)$. In particular, $k - \mu_1 > 0$ where $k - \mu_1$ is also known as the spectral gap of a graph, (k is the regularity of the graph and μ_1 is the largest nontrivial eigenvalue). Therefore, if the spectral gap is large for each graph in the family of expanders, then the family of expanders is of better quality because the spectral gap forces the lower bound on $h(X)$ to be large and hence the family more ideal.

In the next sections, we will look at examples of graphs, their eigenvalues, and the bounds these eigenvalues create on the expanding constant $h(X)$.

7.1 The Complete Graph

Definition. A *complete graph*, K_n is a graph with n vertices in which each vertex is connected to every other distinct vertex. The graph is undirected and has $\frac{n(n-1)}{2}$ edges. Figure 7.1 is the graph of K_6.

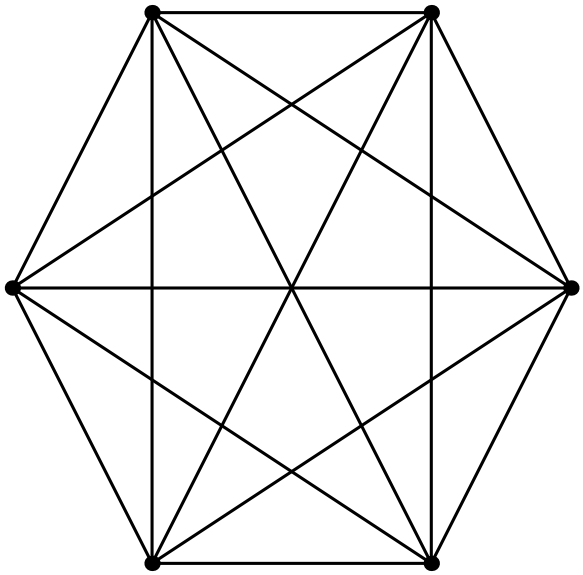

Figure 7.1: *Complete Graph,* K_6

Since each pair of distinct vertices has an edge between them, then the a_{ij} entry of the adjacency matrix of K_n is 1 if $i \neq j$ and 0 if $i = j$.

Proposition 7.1. *Let $X = K_n$ the complete graph with n vertices. Then the n eigenvalues of the adjacency matrix of X are $\{(n-1), -1, -1, \ldots, -1\}$.*

Proof. Recall that complete graph, K_n has n vertices and is $(n-1)$-regular. Therefore, the following is the adjacency matrix, A, of the graph K_n.

$$A = \begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 0 \end{bmatrix}.$$

Since K_n is $(n-1)$-regular, then $(n-1)$ is an eigenvalue of the matrix A. In addition, its corresponding eigenvector is $\mathbf{v_1} = (1, 1, \ldots, 1)$ since

$$A\mathbf{v_1} = \begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} = \begin{bmatrix} (n-1) \\ (n-1) \\ \vdots \\ (n-1) \end{bmatrix} = (n-1)\mathbf{v_1}.$$

Now, when looking for the eigenvectors, $\mathbf{v_i}$, associated with the eigenvalue -1, we want to find $\mathbf{v_i}$ such that

$$A\mathbf{v_i} = -\mathbf{v_i} \iff A\mathbf{v_i} + \mathbf{v_i} = 0 \iff (A + Id)\mathbf{v_i} = 0.$$

Since $(A + Id) = B$ where B is the matrix with a 1 in every entry, the search boils down to finding x_j such that

$$\sum_{j=1}^{n} x_j = 0 \tag{7.4}$$

where $\mathbf{v_i} = (x_1, x_2, \ldots, x_n)$. Therefore, the following are $(n-1)$ independent vectors that satisfy equation 7.4:

$$\begin{gathered} v_2 = (-1, 1, 0, \ldots, 0, 0) \\ v_3 = (-1, 0, 1, \ldots, 0, 0) \\ \vdots \\ v_{n-1} = (-1, 0, 1, \ldots, 1, 0) \\ v_n = (-1, 0, 0, \ldots, 0, 1) \end{gathered}$$

So, the above vectors are $(n-1)$ independent eigenvectors with corresponding eigenvalue -1. Hence the spectrum of A, or the set of n eigenvalues of A, is $\{(n-1), -1, -1, \ldots, -1\}$. □

Recall that K_n is $(n-1)$-regular, so $k = (n-1)$. By Proposition 7.1, $\mu_1 = -1$. Hence using equation 7.1 we have that

$$\begin{aligned} \frac{(n-1)-(-1)}{2} &\leq h(K_n) \leq \sqrt{2(n-1)((n-1)-(-1))} \\ \frac{n}{2} &\leq h(K_n) \leq \sqrt{2(n-1)n} \\ \frac{n}{2} &\leq h(K_n) \leq \frac{3n}{2} \end{aligned} \tag{7.5}$$

Hence, we have the desired eigenvalue bound on the expanding constant, $h(K_n)$. In addition, from Section 1.2, we observed through a hands-on calculation that $h(K_n) = \frac{n}{2}$. Thus, the bounds on $h(K_n)$ given by the eigenvalue bound is a tight bound. Since we know the eigenvalues of the adjacency matrix for K_n, we can also show that for $n > 2$, K_n is Ramanujan by using equation 7.2. By Proposition 7.1, for all eigenvalues μ of A, $\mu \neq (n-1)$, we note that $|\mu| = 1$. Hence for $n \geq 3$,

$$1 = |\mu| \leq 2\sqrt{(n-1)-1} = 2\sqrt{n-2}.$$

7.2 Winnie Li Graphs

From Chapter 5 we defined a Winnie Li graph, $X = (F_{p^n}, \Theta_n)$ to be the Cayley graph with vertices defined to be the elements of F_{p^n} and the edges of each vertex x given by $x + s$ for $s \in \Theta_n$. These graphs are $k = (\frac{p^n-1}{p-1})$-regular graphs with p^n vertices. In Chapter 6, we exhibited the eigenvalues of $X = (F_{p^2}, \Theta_2)$, by Theorem 6.3. In addition, $X = (F_{p^2}, \Theta_2)$ is a Ramanujan graph.

Theorem 7.2. *[5] For each prime p, the Winnie Li graph $X = (F_{p^2}, \Theta_2)$ is a Ramanujan graph.*

Proof. By a proof that is beyond the reach of this paper, P. Deligne ([2]) shows that $\mu_1 \leq 2\sqrt{p} = 2\sqrt{k-1}$. □

For the examples of the Winnie Li graphs we constructed in Section 5.5 we will explicitly demonstrate the eigenvalue bounds on $h(X)$. Since $X = (F_4, \Theta_2)$ is the complete graph, we will concentrate on $X = (F_9, \Theta_2)$ and $X = (F_{25}, \Theta_2)$.

Example. Let $X = (F_9, \Theta_2)$. During the construction of the graph, we created the adjacency matrix of X in order to use Mathematica to graph $X = (F_9, \Theta_2)$. Table 7.1 is the adjacency matrix and we have used Mathematica to find the eigenvalues of the matrix which are

$$\{4, 1, 1, 1, 1, -2, -2, -2, -2\}.$$

Recall that a Winnie Li Graph is a k-regular graph where $k = (\frac{p^n-1}{p-1})$. Hence for $X = (F_9, \Theta_2)$, $k = 4$ and by our calculation above, $\mu_1 = 1$ where μ_1 is the first nontrivial eigenvalue of X not equal to k.

Using equation 7.1, we have

$$\begin{aligned} \frac{(4)-(1)}{2} &\leq h(X) \leq \sqrt{2(4)((4)-(1))} \\ \frac{3}{2} &\leq h(X) \leq 2\sqrt{6} \end{aligned}$$

Table 7.1: *Adjacency Matrix of* $X = (F_9, \Theta_2)$

$$\left|\begin{array}{ccccccccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \end{array}\right|$$

In addition, to see that $X = (F_9, \Theta_2)$ is Ramanujan, we will use equation 7.2. First note that for all eigenvalues μ of the adjacency matrix ($\mu \neq k$), $|\mu| \leq 2$. Hence the Ramanujan inequality 7.2 is satisfied,

$$|\mu| \leq 2\sqrt{4-1} = 2\sqrt{3} \approx 3.46410.$$

Example. Let $X = (F_{25}, \Theta_2)$. As in the last example we used the adjacency matrix of X, Table 5.7, to graph $X = (F_9, \Theta_2)$ in Mathematica. Again, we have used Mathematica to find the eigenvalues of X which are

$$\begin{array}{llllll} 6, & & & & & \\ 1+\sqrt{5}, & 1+\sqrt{5}, & 1+\sqrt{5}, & 1+\sqrt{5}, & 1+\sqrt{5}, & 1+\sqrt{5}, \\ 1-\sqrt{5}, & 1-\sqrt{5}, & 1-\sqrt{5}, & 1-\sqrt{5}, & 1-\sqrt{5}, & 1-\sqrt{5}, \\ \frac{1}{2}(-3+\sqrt{5}), & \frac{1}{2}(-3+\sqrt{5}), & \frac{1}{2}(-3+\sqrt{5}), & \frac{1}{2}(-3+\sqrt{5}), & \frac{1}{2}(-3+\sqrt{5}), & \frac{1}{2}(-3+\sqrt{5}), \\ \frac{1}{2}(-3-\sqrt{5}), & \frac{1}{2}(-3-\sqrt{5}), & \frac{1}{2}(-3-\sqrt{5}), & \frac{1}{2}(-3-\sqrt{5}), & \frac{1}{2}(-3-\sqrt{5}), & \frac{1}{2}(-3-\sqrt{5}) \end{array}$$

In decimal form, the eigenvalues are

$$\begin{array}{llllll} 6, & & & & & \\ 3.23607, & 3.23607, & 3.23607, & 3.23607, & 3.23607, & 3.23607, \\ -1.23607, & -1.23607, & -1.23607, & -1.23607, & -1.23607, & -1.23607, \\ -0.381966, & -0.381966, & -0.381966, & -0.381966, & -0.381966, & -0.381966, \\ -2.61803, & -2.61803, & -2.61803, & -2.61803, & -2.61803, & -2.61803 \end{array}$$

Hence $k = 6$, since X is a 6-regular graph, and $\mu_1 = 1 + \sqrt{5} \approx 3.23607$. Using equation 7.1 we can calculate the bound on $h(X)$.

$$\begin{aligned} \frac{(6) - (1+\sqrt{5})}{2} &\leq h(X) \leq \sqrt{2(6)((6) - (1+\sqrt{5}))} \\ \frac{5-\sqrt{5}}{2} &\leq h(X) \leq 2\sqrt{3(5-\sqrt{5})} \\ 1.38197 &\leq h(x) \leq 5.75909 \end{aligned}$$

In addition, we show that $X = (F_{25}, \Theta_2)$ is Ramanujan by noticing that for all eigenvalues μ of the adjacency matrix ($\mu \neq k$), $|\mu| \leq (1 + \sqrt{5}) \approx 3.23607$ and hence the Ramanujan inequality 7.2 is satisfied:

$$|\mu| \leq 2\sqrt{6-1} = 2\sqrt{5} \approx 4.47214.$$

The characteristic polynomials of $X = (F_4, \Theta_2)$, $X = (F_9, \Theta_2)$, and $X = (F_{25}, \Theta_2)$ which are respectively,

$$(x-3)(x+1)^3 \tag{7.6}$$
$$-(x-4)(x^2+x-2)^4 \tag{7.7}$$
$$-(x-6)(x^4+x^3-9x^2-14x-4)^6 \tag{7.8}$$

suggest an observation that is in fact true in general. First, recall that for an extension of degree 2 over F_p and,

$$k = \frac{(p^2-1)}{(p-1)} = (p+1) = |\Theta_2|.$$

Since each of these graphs are k-regular and we have established by Proposition 3.1 that k is an eigenvalue, clearly each characteristic polynomial has a factor of $(x-k)$. Proposition 7.3 proves that the eigenvalues, other than k all have multiplicity at least k.

Proposition 7.3. *For a prime p, let $X = (F_{p^2}, \Theta_2)$ be a Winnie Li graph. Let β be the set of eigenvalues of the graph X. If $\mu \in \beta$ such that $\mu \neq k$, then μ has multiplicity at least $k = (p+1)$ in β.*

Proof. For a prime p, suppose that $X = (F_{p^2}, \Theta_2)$ is a Winnie Li graph. From Theorem 6.3, recall that for $a \in F_{p^2}$, φ_a is an eigenfunction of X with corresponding eigenvalue λ_a, defined by

$$\varphi_a(x) = exp\left(\frac{2\pi i Tr(ax)}{p}\right) \tag{7.9}$$
$$\lambda_a = \sum_{s\in\Theta} \varphi_a(s) = \sum_{s\in\Theta} exp\left(\frac{2\pi i\big(as + (as)^p\big)}{p}\right) \tag{7.10}$$

From Section 4.5 we know that Tr is a surjective, additive homomorphism and $N : F_{p^2}^{\times} \longrightarrow F_p^{\times}$ is a surjective multiplicative homomorphism. Recall that $\Theta_2 = \{s \in F_{p^2} \mid N(s) = 1\} = \ker N$ and $|\Theta| = k = (p-1)$. By the First Isomorphism Theorem, $F_{p^2}^{\times}/\ker N \cong F_p^{\times}$ since $N : F_{p^2}^{\times} \longrightarrow F_p^{\times}$ and N is onto. Therefore, $F_{p^2}^{\times}$ separates into $(p-1) = [F_{p^2}^{\times} : \ker N]$ cosets of $\ker N$ with $k = (p+1) = |\ker N|$ elements in each coset. To show the multiplicity of each eigenvalue, we will take advantage of the symmetry of the graph and the fields in which

it is defined. First, note that λ_0 is the special case for which $\lambda_0 = k$ and hence only has multiplicity 1. That is, for $0 \in F_{p^2}$ and for all $x \in F_{p^2}$,

$$\varphi_0(x) = exp\left(\frac{2\pi i Tr(0x)}{p}\right) = exp\left(\frac{2\pi i \cdot 0}{p}\right) = exp(0) = 1$$

hence the corresponding eigenvalue is

$$\lambda_0 = \sum_{s\in\Theta} \varphi_0(s) = \sum_{s\in\Theta} 1 = k$$

since $|\Theta| = k$. Now suppose that $a \in F_{p^2}, a \neq 0$. For $a, s \in F_{p^2}$ we know that

$$\{as \in F_{p^2} \mid N(s) = 1\} = \{b \in F_{p^2} \mid N(a) = N(b)\},$$

because N is a multiplicative homomorphism. In addition,

$$\begin{aligned} N(b) = N(a) &\iff N(a)^{-1}N(b) = 1 \\ &\iff N(a^{-1}b) = 1 \\ &\iff a^{-1}b \in \ker N \end{aligned}$$

Hence $b \in a\ker N \iff ba^{-1} \in \ker N$ and

$$|\{as \in F_{p^2} \mid N(s) = 1\}| = |\{b \in F_{p^2} \mid N(a) = N(b)\}| = |\ker N| = k.$$

Therefore, for all $b \in a\ker N$,

$$\begin{aligned} \lambda_a &= \sum_{s\in\Theta} \varphi_a(s) \\ &= \sum_{s\in\Theta} exp\left(\frac{2\pi i\big(as + (as)^p\big)}{p}\right) \\ &= \sum_{b\in a\ker N} exp\left(\frac{2\pi i\big(b + b^p\big)}{p}\right) \end{aligned} \tag{7.11}$$

For $c \in a\ker N$, $a\ker N = c\ker N$, hence the sum 7.11 is the same as the sum defining

$$\lambda_c = \sum_{b\in c\ker N = a\ker N} exp\left(\frac{2\pi i\big(b + b^p\big)}{p}\right).$$

Therefore, $\lambda_a = \lambda_c$ for each of the $k = (p+1)$ elements c in $a\ker N$. Therefore, λ_a has multiplicity at least k. □

The characteristic polynomial of a Winnie Li graph $X = (F_{p^2}, \Theta_2)$ is in the form $\pm(x - k)(p(x))^k$ for some $p(x) \in \mathbb{Z}[x]$. The degree of $p(x)$ is

$$\frac{|F_{p^2}| - 1}{k} = \frac{|F_{p^2}^{\times}|}{k} = \frac{p^2 - 1}{p + 1} = (p - 1).$$

The $p - 1$ roots of $p(x)$ are the remaining eigenvalues of the adjacency matrix, other than k. Since they all have multiplicity k by the above result, the adjacency matrix has at most $(p - 1) + 1 = p$ distinct eigenvalues. Therefore, rather than finding the characteristic polynomial of the adjacency matrix, it might be possible to take a different route towards identifying the first nontrivial eigenvalue of the matrix. That is, if we can find $p(x)$ and hence the roots of $p(x)$, we need only to identify the largest root of $p(x)$ which would then be the first nontrivial eigenvalue of the adjacency matrix. Once we have μ_1 we can use the bound for $h(X)$ described in Chapter 3. Although Proposition 7.3 greatly reduces the degree of the polynomial defining μ_1, it apparently does not lead to a more elementary proof of the bound on μ_1.

7.3 Comparison of Vertices vs. Edges

In this section, we will compare the ratio of vertices to edges of the complete and Winnie Li graphs in order to compare how efficient they are as the number of vertices grows towards infinity. That is, we will be considering this ratio for the graphs K_n and $X = (F_{p^2}, \Theta_2)$ and the rate at which it grows as $n, p \longrightarrow \infty$.

Remark 7.4. Let E and V be the set of edges and the set of vertices for a graph respectively. We will refer to the number of edges of a graph by $|E|$ and the number of vertices of a graph as $|V|$.

The graph K_n has n vertices and $\frac{n(n-1)}{2}$ edges since they are $(n - 1)$-regular graphs. Then the ratio of edges to vertices is

$$\frac{|E|}{|V|} = \frac{\frac{n(n-1)}{2}}{n} \sim \frac{n^2}{n} \sim n$$

Therefore the rate at which $|E|$ grows is approximately $|V|^2$. In addition, as $n \longrightarrow \infty$, then

$$\frac{|E|}{|V|} \sim n \longrightarrow \infty.$$

The Winnie Li graph $X = (F_{p^2}, \Theta_2)$ has p^2 vertices and the total number of edges is $(p^2 \cdot \frac{p^2-1}{(p-1)} \cdot \frac{1}{2}) = (p^2 \cdot (p + 1) \cdot \frac{1}{2})$. Now, the ratio of edges to vertices is

$$\frac{|E|}{|V|} = \frac{p^2(p+1)\frac{1}{2}}{p^2} \sim \frac{\frac{p^3}{2}}{p^2} \sim \frac{p}{2}.$$

Therefore the rate at which $|E|$ grows is approximately $\frac{|V|^{\frac{3}{2}}}{2}$. As $p \longrightarrow \infty$, then

$$\frac{|E|}{|V|} \sim \frac{p}{2} \longrightarrow \infty.$$

However, when comparing $|E_K|$ for K_n with $n = p^2$ to $|E_X|$ for $X = (F_{p^2}, \Theta_2)$ we see that $|E_K|$ exceeds $|E_X|$ by a factor of $(p-1)$. Therefore, when analyzing which family of graphs would be more efficient for networking purposes, for example, we see that even though the ratio of edges to vertices of the Winnie Li graph will go to infinity as p goes to infinity, it is still more efficient than the complete graph.

Bibliography

[1] G. Davidoff, P. Sarnak, A. Valette; *Elementary Number Theory, Group Theory, and Ramanujan Graphs*. London Mathematical Society, Student Texts **55**; Cambridge University Press: New York, 2003.

[2] P. Deligne; *Cohomologie étale* (SGA 4 1/2). *Springer Lecture Notes*, **569**, Springer-Verlag, Berlin, 1997.

[3] D. S. Dummit, R. M. Foote; *Abstract Algebra*, Third Edition. John Wiley and Sons, Inc.: New York, 2004.

[4] D. Farkas; Lecture Notes, Virginia Tech, Blacksburg, VA. Spring 2006.

[5] W. Li; Character Sums and Abelian Ramanujan Graphs, *J. Number Theory*, **41** (1992)

[6] S. H. Friedberg, A. J. Insel, L. E. Spence; *Linear Algebra*, Third Edition. Prentice Hall: New Jersey, 1997.

[7] W. K. Nicholson; *Introduction to Abstract Algebra*, Second Edition. John Wiley and Sons, Inc.: New York, 1999.

[8] S. Pemmaraju, S. Skiena; *Computational Discrete Mathematics: Combinatorics and Graph Theory with Mathematica*. Cambridge University Press: New York, 2003.

[9] A. Terras; *Fourier Analysis on Finitie Groups and Applications*, London Mathematical Society, Student Texts **43**; Cambridge University Press: New York, 1999.