UNIVERSITY OF CALIFORNIA,
IRVINE

Extended Wenger Graphs

DISSERTATION

submitted in partial satisfaction of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

in Mathematics

by

Michael B. Porter

Dissertation Committee:
Professor Daqing Wan, Chair
Assistant Professor Nathan Kaplan
Professor Karl Rubin

2018

DEDICATION

To Jesus Christ, my Lord and Savior.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGMENTS

I would like to thank my advisor, Daqing Wan, for giving me guidance, even when I didn't think I needed it.

I would also like to thank my wife, Natalia, for her love, support, encouragement, and patience.

CURRICULUM VITAE

Michael B. Porter

EDUCATION

Doctor of Philosophy in Mathematics **2018**
University of California *Irvine, California*

Master of Science in Mathematics **2012**
California State University *Long Beach, California*

Master of Engineering in
Electrical Engineering and Computer Science **1984**
University of California *Berkeley, California*

Bachelor of Science in
Electrical Engineering and Computer Science **1982**
University of California *Berkeley, California*

TEACHING EXPERIENCE

Teaching Assistant **2013–2018**
University of California *Irvine, California*

Teaching Associate **2011–2012**
California State University *Long Beach, California*

ABSTRACT OF THE DISSERTATION

Extended Wenger Graphs

By

Michael B. Porter

Doctor of Philosophy in Mathematics

University of California, Irvine, 2018

Professor Daqing Wan, Chair

Wenger graphs were originally introduced as examples of dense graphs that do not have cycles of a given size. Graphs with similar properties were known at the time, but Wenger graphs are based on algebraic relations in finite fields, and as such are easier to understand and analyze.

Wenger graphs are bipartite, with the vertices consisting of two copies of the vector space of dimension m+1 over the finite field of order q. These two sets of vertices are called points and lines, with a point vertex connected to a line vertex if the equations $p_k + l_k = l_1 f_k(p_1)$ are satisfied for k = 2, 3, ..., m+1. In the original Wenger graph, the function $f_k(x)$ was given by $f_k(x) = x^{k-1}$.

Since their introduction in 1991, the original Wenger graph concept has been extended to include linearized and jumped Wenger graphs, and some results are known for extensions in general. In this dissertation, another extension, the extended Wenger graph, is introduced and analyzed, and a new result about polynomial root patterns is proven.

Chapter 1

Introduction

Paul Erdös conjectured in 1964 that for every k there is a c such that any graph on n vertices with $cn^{1+\frac{1}{k}}$ edges has a cycle of length $2k$[16]. His conjecture was later proved by Bondy and Simonovits[5]. Explicit constructions of graphs with no C_4, C_6, and C_{10} were given by Reiman, Brown, and Benson[2, 6, 42], but these constructions all used finite projective geometry.

Wenger graphs were initially introduced[51] to provide a construction based on simple algebraic equations. They have been studied extensively since then[1, 3, 5, 7, 10–15, 17–20, 25–36, 39–41, 43–48, 53, 54]. Some extensions of Wenger graphs have been proposed[7, 47]. In this dissertation, another extension, the extended Wenger graph, is introduced and analyzed, and a new result about polynomial root patterns is proven.

I start by giving an overview of graph theory to define the terms and concepts used. This is chapter 2. For a more thorough introduction, there are many good books on graph theory, e.g. Bondy and Murty[4].

In chapter 3, some of the results from the literature on Wenger graphs (as originally de-

fined) are given. They are, by design, examples of graphs with the maximum number of edges without cycles of a given length. These original Wenger graphs have been extensively analyzed, and results are given for the diameter, girth, and spectrum.

One idea for extending the equations of definition for Wenger graphs is by using functions of the form x^{p^i}. The resulting graphs, called linearized Wenger graphs, are somewhat different from the original Wenger graphs, and results from the literature for the diameter, girth, and spectrum are in chapter 4.

In order to vary the properties of the graph like diameter and girth, it is important to have parameters to vary. Both the original and linearized Wenger graphs have equations that are fixed after choosing the size q of the field and the dimension m of the set of vertices.

In chapter 5 the extended Wenger graph is introduced. For fixed q and m, instead of just one graph, there is a family of graphs indexed by the parameter d, which is introduced into the last equation that defines the graph. The idea is that by allowing more flexibility in the definition, we can have more control over the properties of the graph.

Recently, the jumped Wenger graph was introduced in [47]. Both the jumped and extended Wenger graphs are treated in chapter 5.

The results for the spectrum of extended Wenger graphs are incomplete. The missing parts of the spectrum depend on the distribution of polynomials with a given number of roots over a finite field. I was not able to prove the result I needed to give an expression for the rest of the spectrum. The result I need has to do with polynomials of the form $x^m +$ (degree-n polynomial) with i roots, where $i \geq m$.

I was able to prove a very interesting related result, which has to do with polynomials of the form $x^m +$ (degree-n polynomial) with m roots. This analysis is given in chapter 6.

The equations of definition for Wenger graphs can be generalized even further, but less is

known about these more general extensions. Chapter 7 contains some ideas for future work analyzing the various extensions of Wenger graphs.

Chapter 2

Graph Theory Overview

This chapter contains graph-theoretical ideas used in later chapters.

2.1 Graph Definitions

A graph consists of set V of vertices, also called nodes, and a subset $E \subseteq V \times V$ of edges between these vertices. We will require the sets V and E to be finite. For a graph $G = (V, E)$, the vertex set will be denoted $V(G)$ and the edge set $E(G)$. The order of a graph is the number of vertices, and the size of a graph is the number of edges.

Note that the above definition does not allow two edges in the same direction between the same two vertices. These are called multiple edges, which might be used, for example, to model a pair of cities with two roads going from one to the other. To define a graph with multiple edges, instead of $E \subseteq V \times V$, we have a set E and a function $E \to V \times V$. We will restrict ourselves to graphs without multiple edges.

Suppose that for each $(v_1, v_2) \in E$, (v_2, v_1) is also in E. This means that for every edge

between two vertices, there is also an edge between the same two vertices going in the opposite direction. In this case, we consider the pair of edges to be one undirected edge, and the graph is called undirected.

Edges of the form (v, v) for some $v \in V$ are called loops; they are edges from a vertex to itself. If a graph is undirected and has no multiple edges or loops, it is called simple. We will consider only simple graphs.

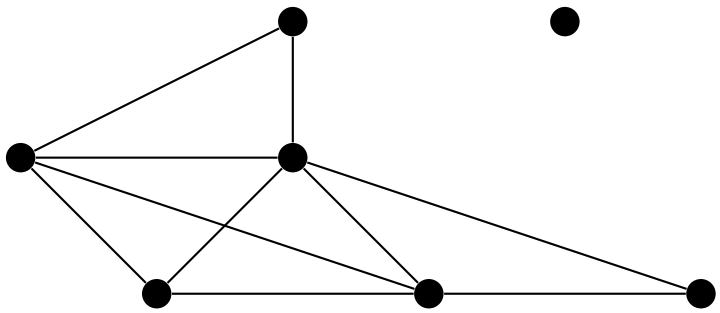


Figure 2.1: Example of a simple graph

A complete graph K_n is a graph with n vertices which has an edge from every vertex to every other vertex.

A graph is bipartite if the vertex set is the disjoint union of two sets V_1 and V_2, and all of the edges are between elements of V_1 and elements of V_2. So every edge coming from a vertex in V_1 goes to a vertex in V_2; there are no edges between vertices in V_1 or between vertices in V_2. A complete bipartite graph $K_{n,m}$ is a bipartite graph with $|V_1| = n$ and $|V_2| = m$, and an edge from every vertex in V_1 to every vertex in V_2.

A path is a finite sequence $v_1, v_2, \ldots, v_s$ of vertices for which there is an edge from v_i to v_{i+1}, $i = 1, 2, \ldots, s-1$. A path is simple if all the vertices and edges are distinct; we will assume that paths are simple. The length of a path is the number of its edges. A graph is connected

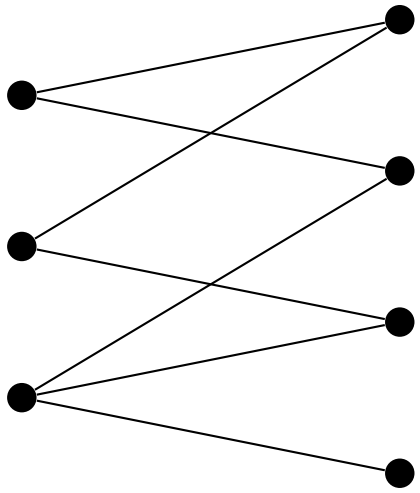


Figure 2.2: Example of a bipartite graph

if there is a path from every vertex to every other vertex. It is easy to prove that a graph is disconnected if and only if it can be partitioned into connected components.

The distance between two vertices v_i and v_j is the number of edges in the shortest path joining v_i and v_j. If there is no path between v_i and v_j, the distance is undefined. Some authors define the distance to be infinity in this case.

The diameter of a connected graph is the maximum distance between any two vertices. Note that by our definition, the diameter of an unconnected graph is undefined. A graph with diameter 3 is shown in Figure 2.3 with two paths of length 3.

A cycle is a path from a vertex to itself. Note that the length of a cycle must be at least three. A cycle of length two would be a path from v_1 to v_2 and back to v_1, which would not have distinct edges. A cycle of length one would just be a loop. The girth of a graph is the length of the shortest cycle in the graph. A graph with girth 4 is shown in Figure 2.4

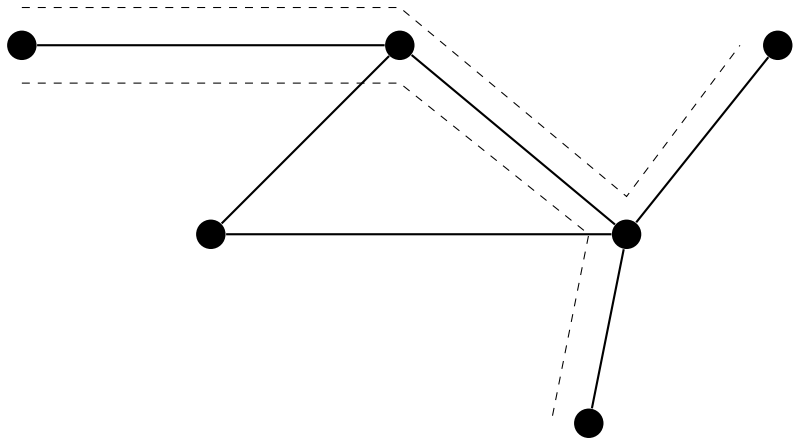


Figure 2.3: A graph with diameter 3

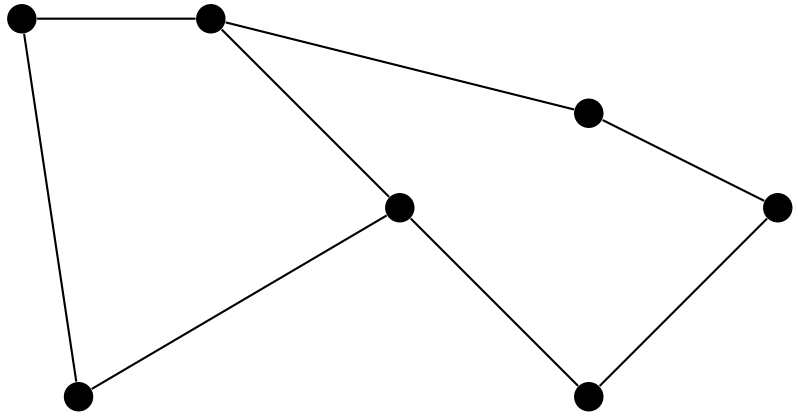


Figure 2.4: A graph with girth 4

A connected graph with no cycles is called a tree. A forest is the disjoint union of finitely many trees. The girth of a tree is undefined.

The degree of a vertex is the number of edges connected to it. A graph is regular if there are the same number of edges connected to every vertex, i.e. the degree of every vertex is the same. If the degree of every vertex is k, the graph is called k-regular. A 0-regular graph is a set of disconnected vertices. A 1-regular graph is a set of disconnected edges, and a 2-regular graph is a set of disconnected cycles. For $k \geq 3$, things get more interesting. A 3-regular graph is called cubic; an example is shown in Figure 2.5.

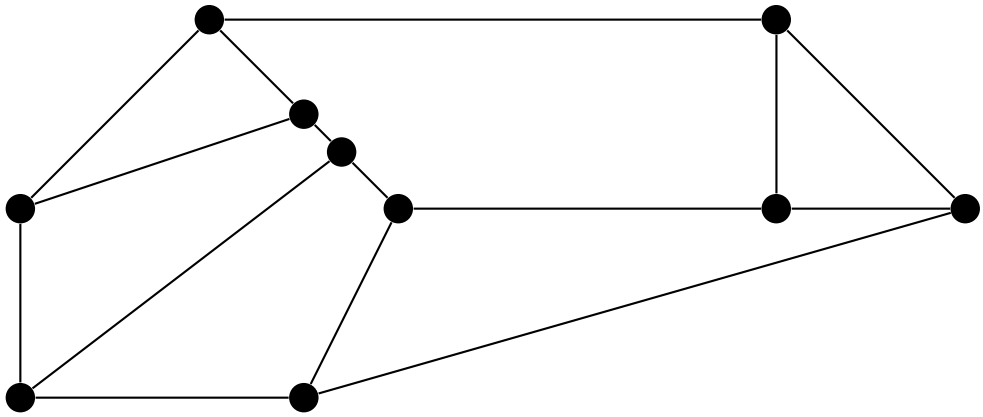


Figure 2.5: A 3-regular, or cubic, graph

2.2 Subgraphs, Isomorphism, and Planarity

Let $G = (V, E)$ be a graph. If $V' \subseteq V$ and $E' \subseteq E \cap (V' \times V')$, then $H = (V', E')$ is a subgraph of G. So a subgraph consists of vertices of the original graph and edges of the original graph between those vertices. If $H \neq G$, it is called a proper subgraph, and if $V = V'$, it is called a spanning subgraph.

If H is a tree (so G is connected), H is called a spanning tree. Spanning trees are important in many applications of graph theory.

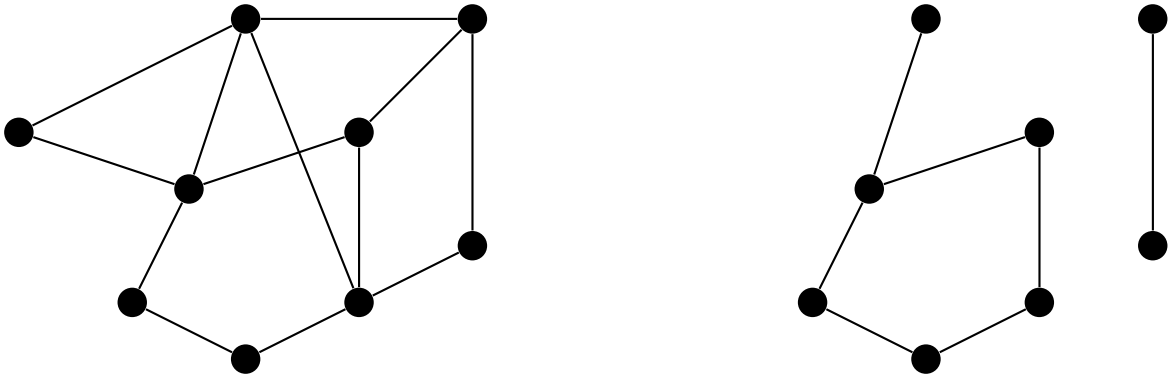


Figure 2.6: A graph and one of its subgraphs

An isomorphism between two graphs G and H is a bijective map $\phi : V(G) \to V(H)$ such

that there is an edge between $\phi(v_1)$ and $\phi(v_2)$ if and only if there is an edge between v_1 and v_2. An example of two isomorphic graphs is shown in Figure 2.7. An automorphism of G is an isomorphism between G and itself. The automorphisms of a graph form a group under composition.

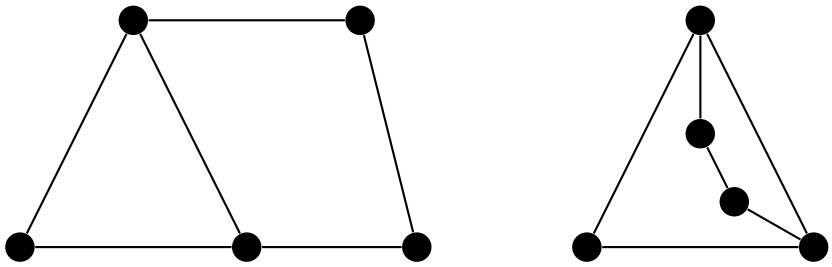


Figure 2.7: Two isomorphic graphs

A simple example of a non-identity automorphism is for the cycle graph C_n with vertex set $\mathbb{Z}/n\mathbb{Z}$ and an edge between vertex i and vertex j whenever $j = i + 1$ (or $i = j + 1$). The map that takes vertex i to vertex $i + k$ for some fixed $k \in \mathbb{Z}/n\mathbb{Z}$ is an automorphism.

The Turán number $\mathrm{ex}(n, H)$ is the largest number of edges in a graph with order n containing no subgraph isomorphic to H. Much is known about the Turán number when H is a complete graph on k vertices. Wenger graphs were initially introduced as part of the investigation into Turán numbers where H is the cycle graph, C_4, C_6, or C_{10}. A Turán graph is a graph with the maximum number of edges.

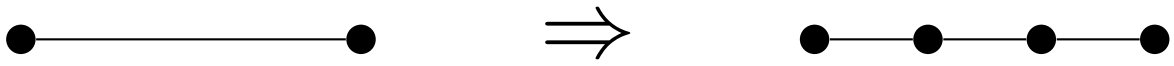


Figure 2.8: A subdivided edge

An edge can be subdivided by adding vertices of degree 2 along the edge. In many applications, this is essentially no change. For example, if the graph represents a map, where

the edges are roads and the vertices are cities, subdividing an edge is equivalent to adding a marker which says that you are halfway from one city to another. A graph is subdivided by subdividing its edges.

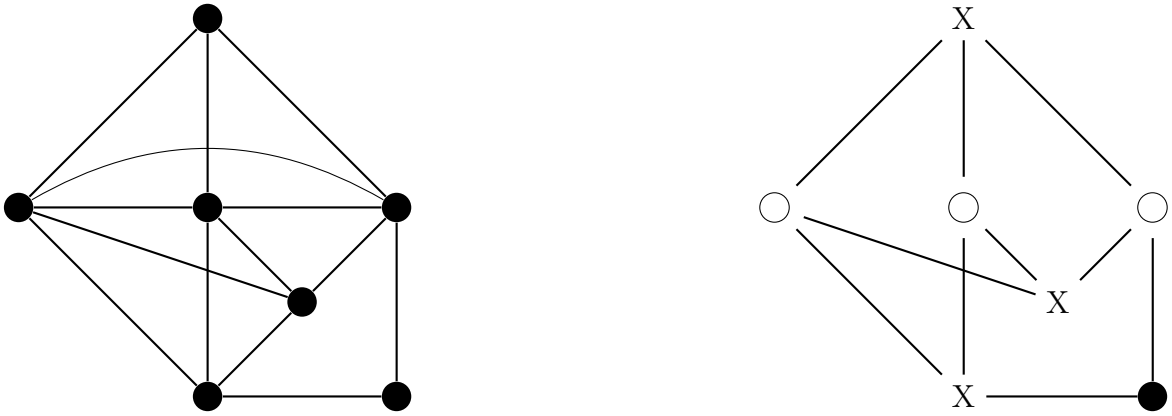


Figure 2.9: A nonplanar graph with its subdivision of $K_{3,3}$

A graph is planar if it can be drawn in the plane so that the edges only intersect at the vertices. Planar graphs are characterized by Kuratowski's theorem: a graph is planar if and only if it does not contain a subgraph that is a subdivision of K_5, the complete graph on five vertices, or $K_{3,3}$, the complete bipartite graph on two sets of three vertices. An example of a nonplanar graph is shown in Figure 2.9 with its subdivision of $K_{3,3}$.

2.3 Transitivity and Matrices

A graph is called vertex transitive if the automorphism group acts transitively on the vertices. That is, for every pair of vertices v_1 and v_2, there is an automorphism that takes v_1 to v_2. So all the vertices are equivalent in the sense that the graph looks the same when viewed from each vertex. Note that all vertex transitive graphs are regular, but it is not necessarily true that all regular graphs are vertex transitive.

For Wenger graphs, the vertices are divided into two groups, points and lines. It is called point transitive if the automorphism group acts transitively on the set of points and line transitive if the automorphism group acts transitively on the set of lines. Note that a graph can be both point and line transitive, but still not be vertex transitive.

A graph is called edge transitive if the automorphism group acts transitively on the edges. So there is an automorphism that takes every edge to every other edge. Edge transitive graphs look the same when viewed from every edge.

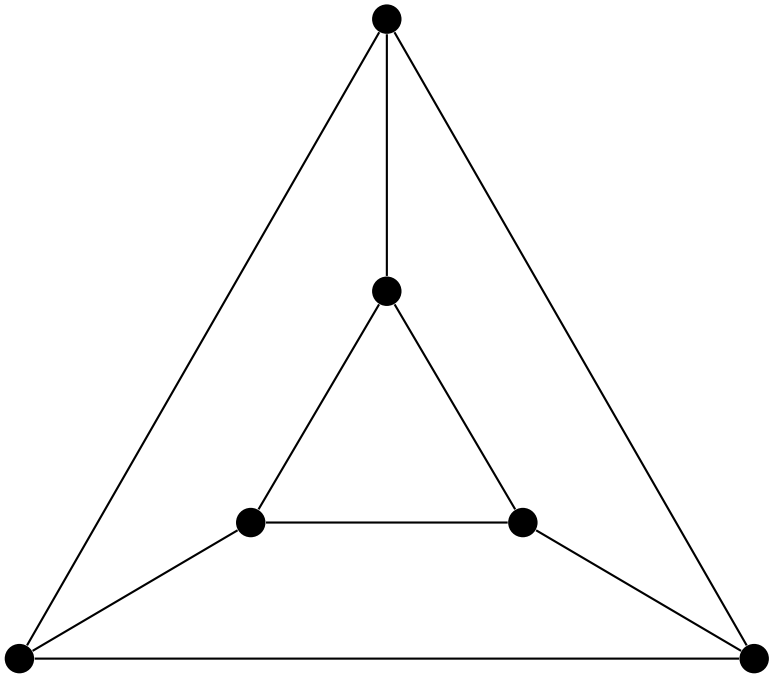


Figure 2.10: A graph that is vertex transitive but not edge transitive

The graph in Figure 2.10 is vertex transitive, since each vertex is the vertex of a triangle which is connected by three edges to another triangle. It is not edge transitive, though, since six edges are a side of a triangle, but the other three are not the side of a triangle.

It is not hard to construct a graph which is edge transitive but not vertex transitive, but it can be difficult to construct such a graph if we also require it to be regular. Such graphs are

called semisymmetric.

A path in a graph that visits every edge exactly once is called an Euler path, and if it begins and ends at the same vertex, it is called a Euler tour. A graph is called Eulerian if it has an Euler tour, and semi-Eulerian if it has an Euler path but not an Euler tour. A connected graph is Eulerian if and only if all vertices have even degree, and it is semi-Eulerian if it has exactly two vertices with odd degree. In the latter case, the two vertices with odd degree are the endpoints of the Euler path.

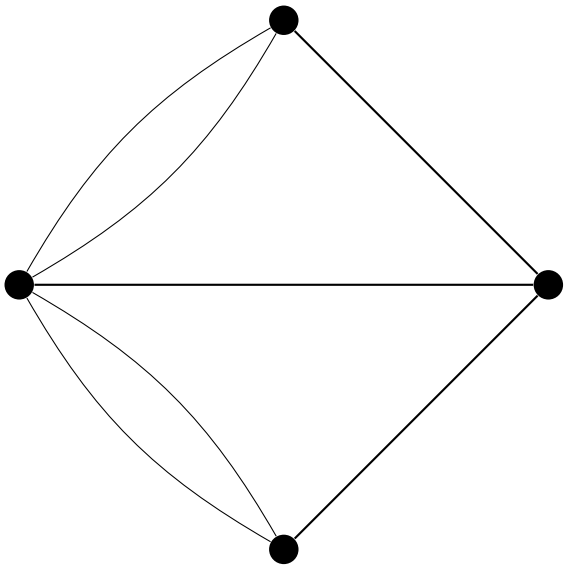


Figure 2.11: Graph for the bridges of Königsberg problem

The bridges of Königsberg problem is one of the oldest problems in graph theory[50]. The town of Königsberg was built on both sides of a river, and there are two islands. Seven bridges were built, and the problem is to plan a tour of the town crossing all seven bridges exactly one time. The mathematical equivalent is to find an Euler tour of the graph in Figure 2.11 (note that the graph has multiple edges). Euler solved the problem in 1736, proving that such a tour is impossible.

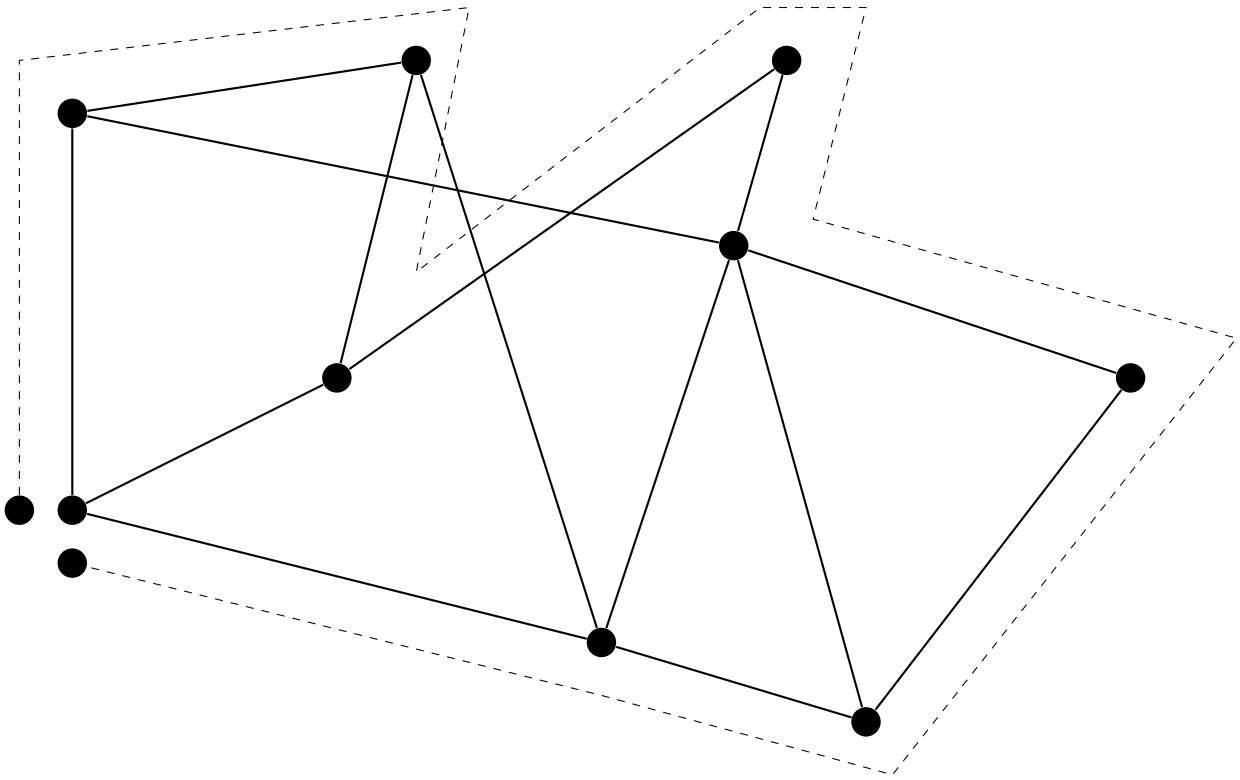
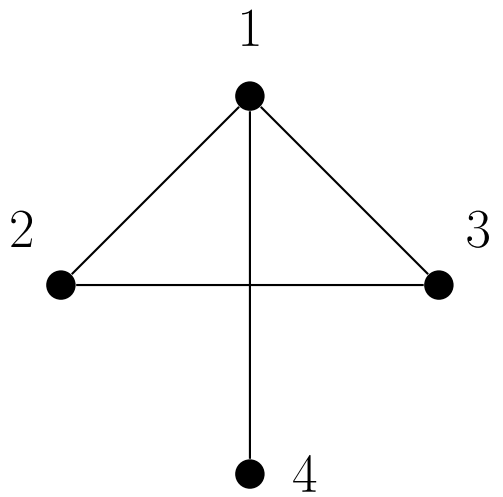


Figure 2.12: A graph with a Hamilton cycle

A path in a graph that visits every vertex exactly once is called a Hamilton path, and if it begins and ends at the same vertex, it is called a Hamilton cycle. If a graph has a Hamilton cycle, it is called Hamiltonian. A graph with one of its Hamilton cycles is shown in Figure 2.12. The computation of a Hamiltonian cycle is a well-known NP-complete problem, and the traveling salesman problem, which is the weighted version of the same problem, has been extensively studied.

Graphs can often be analyzed through use of an adjacency matrix. Every vertex is assigned a row and the corresponding column. The (i, j) entry is 1 if there's an edge from vertex i to vertex j and 0 if there's no edge from vertex i to vertex j. The matrix is symmetric (for undirected graphs), so all the eigenvalues are real. The eigenvalues (with their associated multiplicities) are called the spectrum of the graph.



$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

Figure 2.13: A graph with its adjacency matrix

2.4 Finite Fields

A field F is a set of elements for which addition and multiplication are defined with $(F, +)$ and $(F - \{0\}, *)$ being abelian groups. Also, the distributive law $a(b + c) = ab + ac$ must hold for all $a, b, c \in F$. A finite field is a field with finitely many elements.

We can define a ring homomorphism $\mathbb{Z} \to F$ by taking the multiplicative identity 1 and adding it to itself n times. Since $\mathbb{Z}$ is infinite and F is not, the kernel can not be trivial, but it must be a prime ideal since the image is a subring of a field and therefore an integral domain. So the kernel must be of the form $p\mathbb{Z}$ for some prime p. This p is the characteristic of the field F. In other words, the characteristic is the minimum number of times you have to add 1 to itself to get zero as a sum.

Finite fields must have prime power order. Since 1 has order p in the group $(F, +)$, p divides $|F|$. Suppose there were a different prime q dividing $|F|$. Then there is an element $x \neq 0$ in F whose additive order is q. Then $px = qx = 0$, where kx represents x added to itself k times. Since p and q are relatively prime, there are integers a and b such that $ap + bq = 1$. But this means $x = 1x = (ap + bq)x = apx + bqx = 0 + 0 = 0$, a contradiction. Thus, p is

the only prime factor of $|F|$.

The integers modulo p, where p is a prime, form a field $\mathbb{F}_p$. It can be shown that irreducible polynomials of any degree over $\mathbb{F}_p$ exist, so let $f(x)$ be an irreducible polynomial of degree e over $\mathbb{F}_p$. Then $\mathbb{F}_p/(f(x))$ is a field of order $q = p^e$. It can also be shown that all fields of order q are isomorphic to this one. As a result, $\mathbb{F}_q$ can be described as "the" finite field of order q.

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$*$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Table 2.1: Addition and Multiplication in $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)$

In the finite field construction in Table 2.1, the field elements have the form $a = a_{e-1}x^{e-1} + \cdots + a_1 x + a_0$. We can associate a vector $\begin{pmatrix} a_{e-1} \\ \vdots \\ a_1 \\ a_0 \end{pmatrix}$ with this field element. This assumes the basis $\{1, x, x^2, \ldots, x^{e-1}\}$ is being used, but the definition that follows will be independent of basis. Multiplication by a given field element b is then a linear transformation, which is equivalent to multiplication by a matrix M_b. We then define the trace $\mathrm{Tr}(b)$ to be the trace of M_b and the norm $N(b)$ to be the determinant of M_b. An example is given in Table 2.2.

$$
\begin{aligned}
(x+1)(ax+b) &= ax^2 + (a+b)x + b \\
&= bx + (a+b)
\end{aligned}
$$

$$
\begin{pmatrix} b \\ a+b \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}
$$

$$
\begin{aligned}
\mathrm{Tr}(x+1) &= \mathrm{Tr} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = 1 \\
\mathrm{N}(x+1) &= \det \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = -1 = 1
\end{aligned}
$$

Table 2.2: Multiplication by $x+1$ in $\mathbb{F}_4$

Chapter 3

Wenger Graphs

Wenger graphs were introduced in 1991[51] as a family of graphs with many edges but no small cycles. Let p be a prime, e a positive integer, and $\mathbb{F}_q$ the finite field with $q = p^e$ elements.

The Wenger graph $W_m(q)$ is defined as follows. It is bipartite with the two sets of vertices being two copies $\mathfrak{P}$ and $\mathfrak{L}$ of $\mathbb{F}_q^{m+1}$. There is an edge from $P = (p_1, p_2, \ldots, p_{m+1}) \in \mathfrak{P}$ to $L = (l_1, l_2, \ldots, l_{m+1}) \in \mathfrak{L}$ whenever

$$\begin{aligned} l_2 + p_2 &= p_1 l_1 \\ l_3 + p_3 &= p_1^2 l_1 \\ &\vdots \\ l_{m+1} + p_{m+1} &= p_1^m l_1 \end{aligned}$$

This creates a graph with $2q^{m+1}$ vertices and q^{m+2} edges. An example of a small Wenger graph is shown in Figure 3.1. Two of the 27 edges are shown with the calculation corresponding to the defining equation $l_2 + p_2 = p_1 l_1$.

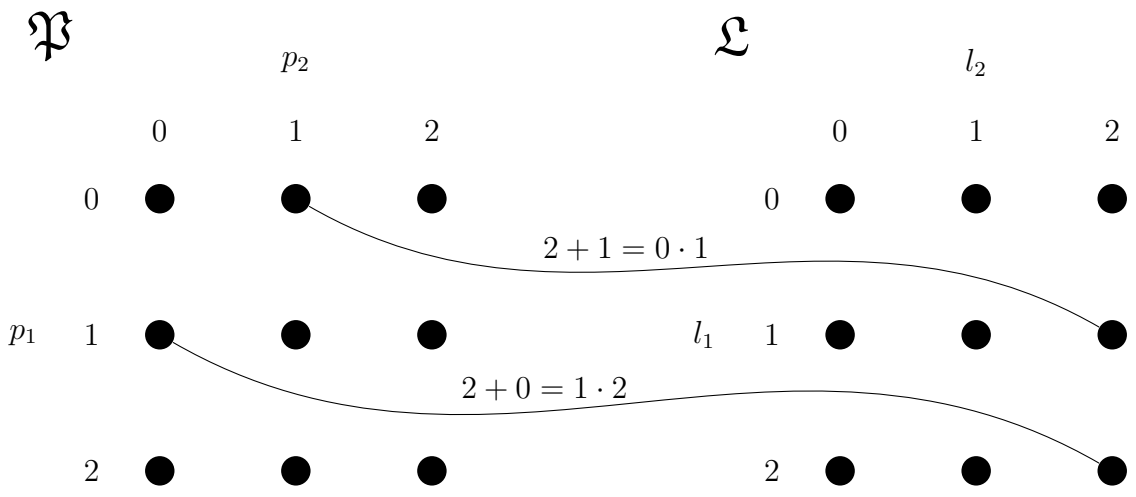


Figure 3.1: Vertices of Wenger graph $W_1(3)$ with two example edges

It is possible to generalize the definition of Wenger graphs by replacing $p_1, p_1^2, \ldots, p_1^m$ with other functions of p_1. For example, the functions $p_1, p_1^p, p_1^{p^2}, \ldots, p_1^{p^{m-1}}$ have been studied[7, 45, 54]. These are called linearized Wenger graphs, and some of the results are described in Chapter 4.

For $k = 2$, 3, or 5, Wenger graphs are examples of graphs on a given vertex set with the largest possible number of edges without a cycle of length $2k$[12, 30, 51]. Cycles of length $2k$ for $k = 4$ and $k \geq 6$ are known to exist[43]. Wenger graphs are also known to be expander graphs[12], which have found many applications[9, 21–23, 38, 52]. The diameter of Wenger graphs, when they're connected, is known to be $2m + 2$[46]. The eigenvalues of Wenger graphs are also known[12].

Wenger's original paper[51] uses a different definition from the one above. He also assumed

the field was a prime field $\mathbb{F}_p$ (i.e. $e = 1$). I will use the label $H_k(p)$ for this description. The vertices are two copies of $\mathbb{F}_p^k$ with vertices $(a_0, a_1, \ldots, a_{k-1})$ and $(b_0, b_1, \ldots, b_{k-1})$ having an edge between them if:

$b_j = a_j + a_{j+1} b_{k-1},\ j = 0, 1, \ldots, k-2$

There is a third description by Lazebnik and Ustimenko[30]; I will use the label $H'_n(q)$ for this description. The vertices are two copies of $\mathbb{F}_q^{n-1}$ with vertices $(p_2, p_3, \ldots, p_n)$ and $(l_1, l_3, \ldots, l_n)$ having an edge between them if

$l_k - p_k = l_1 p_{k-1},\ k = 3, \ldots, n$

All three of these representations are isomorphic. The isomorphisms are[12]:

$\phi : H_k(p) \to H'_{k+1}(p)$

$(a_0, a_1, \ldots, a_k - 1) \mapsto (a_{k-1}, a_{k-2}, \ldots, a_0)$

$(b_0, b_1, \ldots, b_{k-1}) \mapsto (b_{k-1}, b_{k-2}, \ldots, b_0)$

and

$\psi : H'_{m+2}(q) \to W_m(q)$

$(p_2, p_3, \ldots, p_{m+2}) \mapsto (p_2, p_3, \ldots, p_{m+2})$

$(l_1, l_3, \ldots, l_{m+2}) \mapsto (-l_1, -l_3, \ldots, -l_{m+1})$

The representation $W_m(q)$ first appeared in Lazebnik and Viglione[34]. This is the description that is currently used. In terms of this description, $H_k(p)$ is isomorphic to $W_{k-1}(p)$ and $H'_n(q)$ is isomorphic to $W_{n-2}(q)$. A comparison of the various descriptions is shown in Table 3.1.

Wenger's original paper showed that for any prime p, $W_1(p)$ has no cycles of length 4, $W_2(p)$ has no cycles of length 6, and $W_4(p)$ has no cycles of length 10. He also showed that $W_2(p)$

	Wenger[51]	Lazebnik & Ustimenko[30]	recent papers
Name of Graph	$H_k(p)$	$H'_n(q)$	$W_m(q)$
Size of Field	p	$q = p^e$	$q = p^e$
Dimension of $\mathfrak{P}$ and $\mathfrak{L}$	k	$n-1$	$m+1$
Number of Vertices	$2p^k$	$2q^{n-1}$	$2q^{m+1}$
Number of Edges	p^{k+1}	q^n	q^{m+2}
Range of p-subscripts	0 to $k-1$	2 to n	1 to $m+1$
Range of l-subscripts	0 to $k-1$	1, 3 to n	1 to $m+1$

Table 3.1: Comparison of Wenger graph descriptions

has girth 8. Note that the graph $W_{k+1}(p)$ has $2p^k$ vertices and p^{k+1} edges.

It was shown in [30] that the automorphism group of $W_m(q)$ acts transitively on the P vertices, on the L vertices, and on the set of edges. In [34] it was shown that the automorphism group acts transitively on the whole set of vertices of $W_1(q)$ for all q and of $W_2(q)$ in characteristic 2.

Another result of [34] is that $W_m(q)$ is connected if $1 \leq m \leq q-1$, and if $m \geq q$, it has q^{m-q+1} components, each isomorphic to the graph with $m = q-1$. For this reason, the restriction $m < q$ is often used.

In [43], it is shown that if $m \geq 2$, given any integer l, $l \neq 5$, $4 \leq l \leq 2p$ and any vertex v in $W_m(q)$, there is a cycle of length $2l$ passing through v.

The Wenger graph with $m = 2$ and $q = 3$ is isomorphic to the Gray graph, shown in Figure 3.2. The Gray graph is constructed from a 3x3x3 grid of points, and the 27 lines parallel to the coordinate axes through these points. There is a vertex for each point and each line, and there is an edge between a point-vertex and a line-vertex if the corresponding point is on the corresponding line. The Gray graph is the only cubic semisymmetric graph of order $2p^3$[40], and is the smallest cubic semisymmetric graph[39].

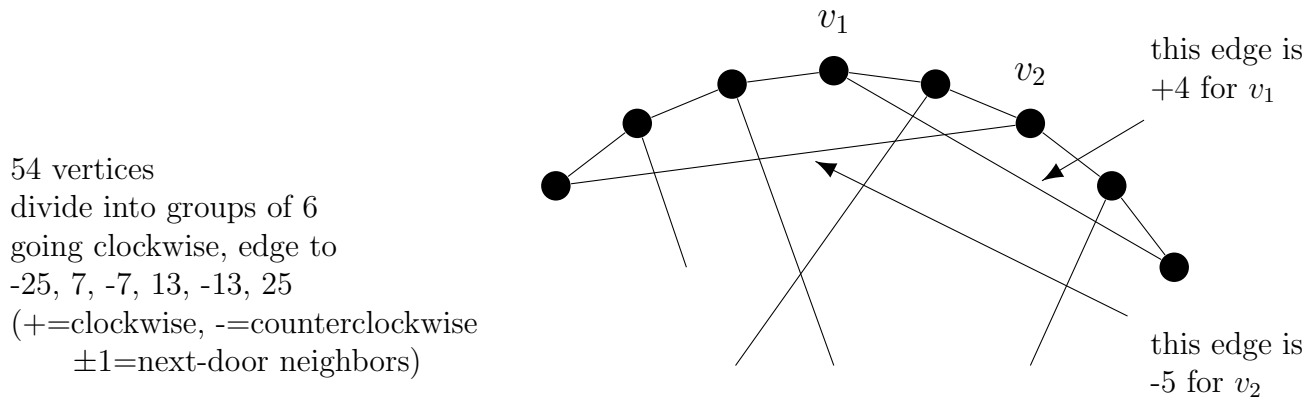


Figure 3.2: The Gray graph, $W_2(3)$[49]

It is shown in [34] that $W_m(q)$ is semisymmetric if $m \geq 3$ and $q \geq 3$ or if $m = 2$ and q is odd, and is vertex transitive if $m = 1$ or if $m = 2$ and q is even. The case $q = 2$, $m \geq 3$ is not mentioned.

It is shown in [30] that the girth of the Wenger graph $W_m(q)$ is 8 for $m \geq 2$. They also extended Wenger's original result that $W_4(p)$ has no cycles of length 10 from primes to powers of primes.

For any integer k and any vertex v in the Wenger graph, there is a cycle of length 2k passing through v if $m \geq 2$, $k \neq 5$, and $4 \leq k \leq 2p$[43].

The diameter of the Wenger graph is $2m + 2$ if $1 \leq m \leq q - 1$[46].

The spectrum of Wenger graphs was calculated in [12]. Their result is:

Theorem 3.1. *For all prime power q and $1 \leq m \leq q - 1$, the eigenvalues of the Wenger graph are $\pm q$ and $\pm\sqrt{qi}$ where $0 \leq i \leq m$. The multiplicity of $\pm q$ is 1, and the multiplicity of $\pm\sqrt{qi}$ is:*

$$(q-1)\binom{q}{i}\sum_{d=i}^{m}\sum_{k=0}^{d-i}(-1)^k\binom{q-i}{k}q^{d-i-k}$$

The proof is similar to the one given for a general Wenger graph (Theorem 5.5, or Theorem 2.2 of [7]). The multiplicities are calculated to be equal to the number of polynomials of degree at most m having i distinct roots in $\mathbb{F}_q$. The expression in the result comes from [24].

i	eigenvalues	multiplicity
-	3, -3	1, since $1 \leq m \leq q-1$
2	$\sqrt{6}$, $-\sqrt{6}$	6
1	$\sqrt{3}$, $-\sqrt{3}$	12
0	0	16

sum of multiplicities = 1+6+12+16+12+6+1 = 54 = # of vertices

Table 3.2: Spectrum of the Gray graph

As an example, the spectrum of the Gray graph is calculated. The results are shown in Table 3.2. The eigenvalues 3 and -3 are a special case: the multiplicity of q and $-q$ is the number of connected components, which is 1 if $1 \leq m \leq q-1$, and q^{m-q+1} if $m \geq q$.

For $\sqrt{6}$ and $-\sqrt{6}$, the multiplicity is:

$$\begin{aligned}(3-1)\binom{3}{2}\sum_{d=2}^{2}\sum_{k=0}^{d-2}(-1)^k\binom{3-2}{k}3^{d-2-k} &= 6\sum_{k=0}^{0}(-1)^k\binom{1}{k}3^{-k} \\ &= 6(1) = 6\end{aligned}$$

For $\sqrt{3}$ and $-\sqrt{3}$, the multiplicity is:

$$(3-1)\binom{3}{1}\sum_{d=1}^{2}\sum_{k=0}^{d-1}(-1)^k\binom{3-1}{k}3^{d-1-k}$$
$$= 6\left(\sum_{k=0}^{0}(-1)^k\binom{2}{k}3^{-k}+\sum_{k=0}^{1}(-1)^k\binom{2}{k}3^{1-k}\right)$$
$$= 6(1+(3-2)) = 12$$

And for 0, we calculate:

$$(3-1)\binom{3}{0}\sum_{d=0}^{2}\sum_{k=0}^{d}(-1)^k\binom{3-0}{k}3^{d-k}$$
$$= 2\left(\sum_{k=0}^{0}(-1)^k\binom{3}{k}3^{-k}+\sum_{k=0}^{1}(-1)^k\binom{3}{k}3^{1-k}+\sum_{k=0}^{2}(-1)^k\binom{3}{k}3^{2-k}\right)$$
$$= 2(1+(3-3)+(9-9+3)) = 8$$

but the formula gives a multiplicity for 0 and -0 separately, so the actual multiplicity of 0 is 16.

The following theorem is well-known:

Theorem 3.2. *The diameter of a graph G is less than the number of distinct eigenvalues of its adjacency matrix.*

Proof. Let A be the adjacency matrix, and let ϕ be the minimal polynomial of A. Then $\deg(\phi) = k$, the number of distinct eigenvalues. By the Cayley-Hamilton Theorem, $\phi(A) = 0$, so A^k is a linear combination of $A^{k-1}, \ldots, A, I$. Suppose the diameter of G is greater than or equal to k. Then there are vertices u and v such that the distance between u and v is exactly

k. So the (u, v) component of A^k is positive, while the (u, v) components of $A^{k-1}, \ldots, A, I$ are all zero. This contradicts A^k being a linear combination.

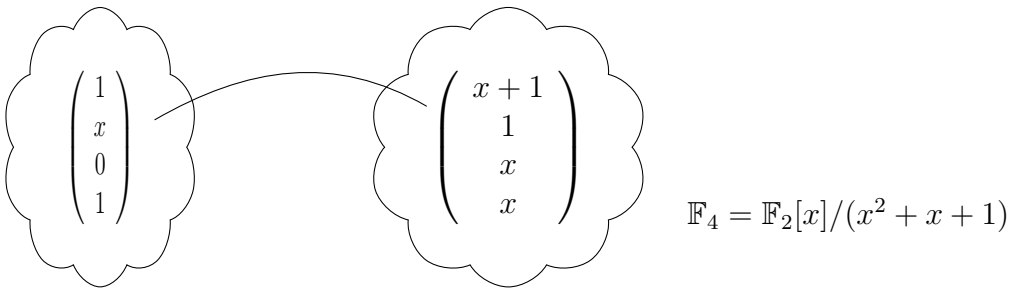
□

Since there are $2m+3$ distinct eigenvalues and the diameter of the Wenger graph was shown to be $2m+2$, the Wenger graph has the minimum number of eigenvalues for a given diameter.

Chapter 4

Linearized Wenger Graphs

If the functions f_k of a Wenger graph are given by $f_k(x) = x^{p^{k-2}}$, where p is the characteristic of $\mathbb{F}_q$, the Wenger graph is called a linearized Wenger graph. These graphs are studied in [7]. An example of the calculations for an edge is shown in Figure 4.1.



$l_1 = 1$ so

$p_2 + l_2 = x + 1$ $\quad l_1 p_1 = p_1 = x + 1$

$p_3 + l_3 = 0 + x = x$ $\quad l_1 p_1^2 = p_1^2 = x^2 + 1 = (x+1) + 1 = x$

$p_4 + l_4 = 1 + x = x + 1$ $\quad l_1 p_1^4 = p_1^4 = x^2 = x + 1$

Figure 4.1: Example of edge in $L_3(4)$

The spectrum of linearized Wenger graphs is stated in the following two theorems, the first by Cao et al.[7] for the case $m \geq e$ (where e is the exponent in $q = p^e$) and the second by Yan and Liu[53] for the case $m < e$.

Theorem 4.1. *Let $m \geq e$. The linearized Wenger graph has q^{m-e} components. The eigenvalues are 0 and $\pm\sqrt{qp^i}$ where $0 \leq i \leq e$. The multiplicity of the eigenvalues $\pm\sqrt{qp^i}$ is given by:*

$$\frac{q^{m-e+1}}{p^i}\frac{\prod_{j=0}^{e-i-1}(p^e-p^j)^2}{\prod_{j=0}^{e-i-1}(p^{e-i}-p^j)}$$

and the multiplicity of eigenvalue 0 is given by:

$$2q^{m-e}\sum_{i=1}^{e}(p^e-p^{e-i})\frac{\prod_{j=0}^{e-i-1}(p^e-p^j)^2}{\prod_{j=0}^{e-i-1}(p^{e-i}-p^j)}$$

The "2" in the multiplicity of eigenvalue 0 is due to contributions from both $+0$ and -0. For the second theorem, the Gaussian binomial coefficients are required:

$$\binom{n}{k}_q = \begin{cases} \prod_{t=0}^{k-1}\frac{q^n-q^t}{q^k-q^t} & 1 \leq k \leq n \\ 1 & k = 0 \\ 0 & k > n \end{cases}$$

where n and k are nonnegative integers. This is the number of k-dimensional subspaces of $\mathbb{F}_q^n$.

Theorem 4.2. *Let $m < e$. The eigenvalues of the linearized Wenger graph $L_m(q)$ are:*

$$0, \pm q, \pm\sqrt{qp^r}, 0 \leq r \leq m-1$$

Moreover, the multiplicities of the eigenvalues $\pm q$ are 1, the multiplicities of the eigenvalues $\pm\sqrt{qp^r}$ are $p^{e-r}n_r$, and the multiplicity of the eigenvalue 0 is:

$$2\left(q^{m+1}-1-\sum_{r=0}^{m-1}p^{e-r}n_r\right)$$

where

$n_r = \binom{e}{r}_p \sum_{i=0}^{m-r-1} (-1)^i p^{i(i-1)/2} \binom{e-r}{i}_p (q^{m-r-i} - 1)$.

The spectrum of the linearized Wenger graph $L_3(4)$ is given in Table 4.1.

$m = 3$, $p = 2$, $e = 2$, $q = 4$

Nonzero eigenvalues:

i	eigenvalues	multiplicity
0	± 2	96
1	$\pm 2\sqrt{2}$	72
2	± 4	4^*

*double-check: there are $q^{m-e} = 4$ components

eigenvalue 0 has multiplicity 84

double-check: number of eigenvalues $= 96 \cdot 2 + 72 \cdot 2 + 4 \cdot 2 + 84 = 512$
number of vertices $= 2q^{m+1} = 2 \cdot 4^4 = 512$

Table 4.1: Spectrum of $L_3(4)$

As an example of the calculations involved, the multiplicity of $\pm 2\sqrt{2}$ is calculated as follows:

We have $m = 3$, $p = 2$, $e = 2$, so $q = 4$, and $i = 1$ so that the eigenvalue is $\sqrt{qp^i} = 2\sqrt{2}$. The multiplicity is calculated as:

$$\frac{q^{m-e+1}}{p^i} \frac{\prod_{j=0}^{e-i-1} (p^e - p^j)^2}{\prod_{j=0}^{e-i-1} (p^{e-i} - p^j)}$$

$$= \frac{4^2}{2^1} \frac{\prod_{j=0}^{0} (p^2 - p^j)^2}{\prod_{j=0}^{0} (p^1 - p^j)}$$

$$= 8 \frac{(4-1)^2}{(2-1)} = 72$$

For the diameter of the linearized Wenger graph, we have the following theorem[7]:

Theorem 4.3. *If $m \leq e$, then the diameter of the linearized Wenger graph is $2(m + 1)$.*

If $m > e$, then the linearized Wenger graph is not connected. Based on Theorem 4.1, it has q^{m-e} connected components. Each of these components is isomorphic to the graph with $m = e$.

All linearized Wenger graphs are 4-cycle free. The linearized Wenger graph with $m = 1$ is the same as the (original) Wenger graph, and it is known to be free of 4-cycles[36]. The authors also observed that adding functions to the list will not decrease the girth. As a result, all linearized Wenger graphs have girth at least 6.

The results for girth of linearized Wenger graphs are given in the following two theorems from [7]

Theorem 4.4. *If $p \neq 2$, or if $p = 2$, $m = 1$, and $e \geq 2$, then the girth of the linearized Wenger graph is 6.*

Proof. A cycle of length 6 is constructed for both cases. For $p \neq 2$,

$$P_1 = (0, 0, \ldots, 0)$$
$$L_1 = (1, 0, \ldots, 0)$$
$$P_2 = (-1, -1, \ldots, 0)$$
$$L_2 = (-1, 2, \ldots, 2)$$
$$P_3 = (-2, 0, \ldots, 0)$$
$$L_3 = (0, 0, \ldots, 0)$$
$$P_1 = (0, 0, \ldots, 0)$$

For the case $p = 2$, $m = 1$, and $e \geq 2$, choose $\beta \neq 0$ with $\mathrm{Tr}(\beta) \neq 0$. So there is a solution

$\alpha \neq 0$ to $\alpha^2 + \alpha = \beta$. Then the cycle is:

$$P_1 = (0, 0)$$
$$L_1 = (0, 0)$$
$$P_2 = (\alpha^2, 0)$$
$$L_2 = (\alpha^{-1}\beta, \alpha\beta)$$
$$P_3 = (\beta, \beta)$$
$$L_3 = (1, 0)$$
$$P_1 = (0, 0)$$

The cycle is shown in Table 4.2 for the case $e = 3$.

□

$p = 2$, $m = 1$, $e = 3$, $q = 8$

$\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3 + x + 1)$ $\qquad$ $\alpha = x$, $\beta = x^2 + x$

$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} x^2 \\ 0 \end{pmatrix}$	$\begin{pmatrix} x+1 \\ x^2+x+1 \end{pmatrix}$	$\begin{pmatrix} x^2+x \\ x^2+x \end{pmatrix}$	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$
P	L	P	L	P	L	P
l_1p_1: 0	0	$x^3 + x^2 = x^2 + x + 1$	$x^3 + 2x^2 + x = 1$	$x^2 + x$	0	

equation: $p_2 + l_2 = l_1p_1$

Table 4.2: Example of 6-cycle for $L_1(8)$

Theorem 4.5. *If $p = 2$, $m = 1$, and $e = 1$, or if $p = 2$ and $m \geq 2$, then the girth of the linearized Wenger graph is 8.*

Proof. In the original paper by Wenger[51], it is shown that the Wenger graph with $m = 1$

and $e = 1$ has no 4-cycles or 6-cycles. So by the observation in [36], the girth is at least 8 for $e = 1$ and $m \geq 1$.

If there is no 6-cycle for $p = 2$, $m = 2$, and $e \geq 2$, then by that same observation, this extends to $m \geq 2$, which is all the remaining cases. So we will show that there is no 6-cycle for $p = 2$, $m = 2$, and $e \geq 2$.

If there were a 6-cycle $P_1L_1P_2L_2P_3L_3P_1$, then since P_1 and P_2 share a common neighbor L_1, setting $c_1 = l_1$ and $u_1 = p_1^{(1)} - p_1^{(2)}$) and remembering that $x^p - y^p = (x - y)^p$, we get:

$$P_1 - P_2 = (u_1, c_1u_1, c_1u_1^p, \ldots, c_1u_1^{p^{m-1}})$$

and similarly,

$$P_2 - P_3 = (u_2, c_2u_2, c_2u_2^p, \ldots, c_2u_2^{p^{m-1}})$$

$$P_3 - P_1 = (u_3, c_3u_3, c_3u_3^p, \ldots, c_3u_3^{p^{m-1}})$$

so that:

$$u_1 + u_2 + u_3 = 0$$

$$c_1u_1 + c_2u_2 + c_3u_3 = 0$$

$$c_1u_1^2 + c_2u_2^2 + c_3u_3^2 = 0$$

eliminating c_1 in the last equation gives:

$$u_1 + u_2 + u_3 = 0$$

$$c_1u_1 + c_2u_2 + c_3u_3 = 0$$

$$c_2(u_2^2 - u_2u_1) + c_3(u_3^2 - u_3u_1) = 0$$

Since we're in characteristic 2 and $u_1 + u_2 + u_3 = 0$, we have $u_2^2 - u_2u_1 = u_2(u_2 - u_1) =$

$(u_1 + u_3)(u_1 + u_3 - u_1) = (u_3 - u_1)u_3 = u_3^2 - u_3u_1$, so the expressions in parentheses are equal, and must also be nonzero, since $u_2^2 - u_2u_1 = u_2(u_2 - u_1) = u_2u_3$ and $u_2, u_3 \neq 0$. So we have:

$u_1 + u_2 + u_3 = 0$

$c_1u_1 + c_2u_2 + c_3u_3 = 0$

$c_2 + c_3 = 0$

But this means that $c_2 = c_3$, which would make $L_2 = L_3$. So there can be no 6-cycle.

We have shown that the girth is at least 8 in all cases, so it remains to be shown that the girth is at most 8, i.e. that there is a cycle of length 8. Here is such a cycle:

$P_1 = (0, 0, \ldots, 0)$

$L_1 = (0, 0, \ldots, 0)$

$P_2 = (1, 0, \ldots, 0)$

$L_2 = (1, 1, \ldots, 1)$

$P_3 = (0, 1, \ldots, 1)$

$L_3 = (0, 1, \ldots, 1)$

$P_4 = (1, 1, \ldots, 1)$

$L_4 = (1, 0, \ldots, 0)$

$P_1 = (0, 0, \ldots, 0)$

□

Wang[48] was able to prove that cycles exist in the linearized Wenger graph with even lengths between 6 and $2p^2$. Of course, odd cycles do not exist since Wenger graphs are bipartite.

Theorem 4.6. *Let q be the power of an odd prime p. For any integer k with $3 \leq k \leq p^2$, $L_m(q)$ contains cycles of length $2k$.*

Corollary 4.1. *If p is an odd prime, $L_1(p)$ is Hamiltonian.*

Proof. It has $2p^2$ vertices, and by the theorem, there is a path of length $2p^2$. □

A Hamiltonian cycle for $L_1(5)$ (which is the same as $W_1(5)$) is shown in Figure 4.2. Hamiltonian cycles are difficult to find in general (the decision problem is NP-complete), but here I just constructed a path of length 10 from $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ to $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ using $p_1 = 1, 2, 3, 4$ and $l_1 = 0, 1, 2, 3, 4$. Then I repeated the same p_1 and l_1 values, so that the p_2 values are 1 greater and the l_2 values are 1 less. Repeating for a total of 5 of these blocks gives a path of length 50 with no vertices repeated, and ending at $\begin{pmatrix} 0 \\ 5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$.

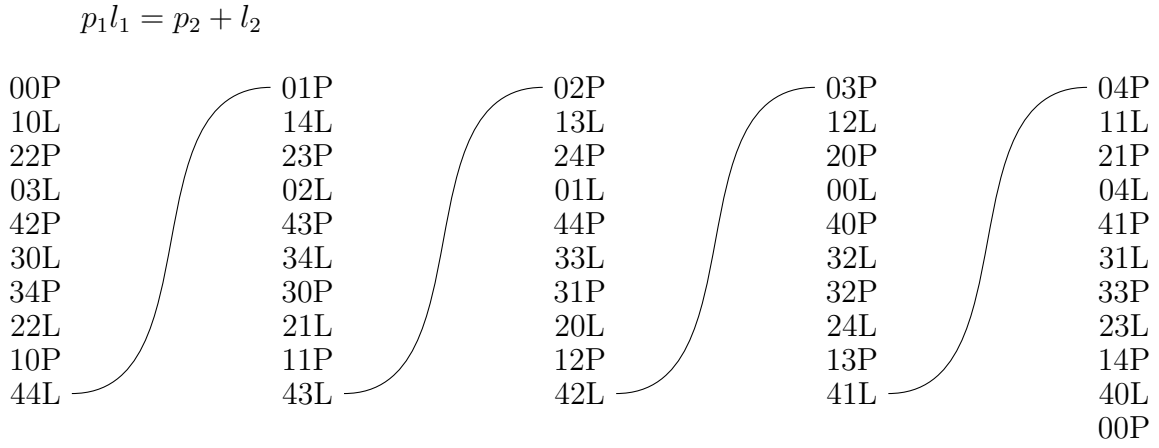


Figure 4.2: Hamiltonian cycle in $L_1(5)$

Chapter 5

Extended Wenger Graphs

In this chapter, the definition of Wenger graphs is extended by making minor adjustments to the set of exponents of p_1. There are two types of adjustments. In the first type of graph, the exponent of p_1 in the last equation is changed from m to $m+d$, where d is a nonnegative integer. If $m+d \geq q$, then $m+d$ can be reduced (mod $q-1$), so there is no harm in assuming that $m+d < q$. This first type of graph is called an extended Wenger graph, and is denoted $G_d(m,q)$. In the second type of graph, two "jumps" are inserted in the list of exponents, skipping x^i and x^j, so the functions f are given by $(f_1(x), f_2(x), \ldots, f_{m+1}(x)) = (1, x, \ldots, x^{i-1}, x^{i+1}, \ldots, x^{j-1}, x^{j+1}, \ldots, x^{m+2})$ where $m+2 < q$. These are called jumped Wenger graphs, denoted $J_m(q,i,j)$, and are analyzed in [47].

Note that if $d=0$, the extended Wenger graph becomes an original Wenger graph, described in Chapter 3. Also, if $0 \leq d \leq 2$, the extended Wenger graph can be interpreted as a jumped Wenger graph. For $d=0$, set $(i,j) = (m+1, m+2)$, for $d=1$, set $(i,j) = (m, m+2)$, and for $d=2$, set $(i,j) = (m, m+1)$.

We first look at the number of connected components of $G_d(m,q)$. By Theorem 2.2 of [7], the number of connected components is:

$q^{m+1-\text{rank}_{\mathbb{F}_q}(1,x,x^2,\ldots,x^{m-1},x^{m+d})}$

where $\text{rank}_{\mathbb{F}_q}(1, x, x^2, \ldots, x^{m-1}, x^{m+d})$ is the rank of the $(m+1) \times q$ matrix consisting of the values of these $m+1$ functions for the q possible values of x. This will be 1, and therefore the graph will be connected, if:

$\text{rank}_{\mathbb{F}_q}(1, x, x^2, \ldots, x^{m-1}, x^{m+d}) = m+1$

Since $m+1 \leq q$, this is possible, and will happen when the functions $1, x, x^2, \ldots, x^{m-1}$, and x^{m+d} are linearly independent. This condition is stated in more general terms in [7].

In our case, since $m-1 < q$, the functions $1, x, x^2, \ldots, x^{m-1}$ are indeed linearly independent, and since $m \leq m+d \leq q-1$, the function x^{m+d} is linearly independent of the others. Therefore, $G_d(m, q)$ is connected.

If $m+2 < q$ the jumped Wenger graph $J_m(q, i, j)$ is also connected for all $i < j < m+1$[47].

5.1 Diameter

In this section, the diameter of the graphs $G_d(m, q)$ and $J_m(q, i, j)$ is analyzed.

Two lines $L = (l_1, \ldots, l_{m+1})$ and $L' = (l'_1, \ldots, l'_{m+1})$ that share a point $P = (p_1, \ldots, p_{m+1})$ will satisfy:

$l_k - l'_k = (l_1 - l'_1) f_k(p_1)$

and note that if $l_1 = l'_1$, the two lines are identical.

Two points $P = (p_1, \ldots, p_{m+1})$ and $P = (p'_1, \ldots, p'_{m+1})$ that share a line $L = (l_1, \ldots, l_{m+1})$ will similarly satisfy:

$p_k - p'_k = l_1(f_k(p_1) - f_k(p'_1))$

and similarly note that if $p_1 = p'_1$, the two points are identical.

Theorem 5.1. *If the functions $f_k(p_1)$ are linearly independent, the diameter of the Wenger graph is at most $2(m+1)$.*

Proof. Consider a path of the form $L_1 P_1 \dots P_{m+1} L_{m+2}$. Since L_{h+1} and L_h share the point P_h,

$l_k^{(h+1)} - l_k^{(h)} = (l_1^{(h+1)} - l_1^{(h)}) f_k(p_1^{(h)})$ for $1 \le h \le m+1$ and $1 \le k \le m+1$

Set $t_h = l_1^{(h+1)} - l_1^{(h)}$ and $x_h = p_1^{(h)}$. Then $L_{h+1} - L_h = t_h \begin{pmatrix} f_1(x_h) \\ \vdots \\ f_{m+1}(x_h) \end{pmatrix}$

where $L_h = \begin{pmatrix} l_1^{(h)} \\ \vdots \\ l_{m+1}^{(h)} \end{pmatrix}$.

Summing over h gives

$$L_{m+2} - L_1 = \sum_{h=1}^{m+1} t_h \begin{pmatrix} f_1(x_h) \\ \vdots \\ f_{m+1}(h) \end{pmatrix} = \begin{pmatrix} \sum_{h=1}^{m+1} t_h f_1(x_h) \\ \vdots \\ \sum_{h=1}^{m+1} t_h f_{m+1}(x_h) \end{pmatrix} = M \begin{pmatrix} t_1 \\ \vdots \\ t_{m+1} \end{pmatrix}$$

where $M = \begin{pmatrix} f_1(x_1) & f_1(x_2) & \dots & f_1(x_{m+1}) \\ f_2(x_1) & f_2(x_2) & \dots & f_2(x_{m+1}) \\ \vdots & \vdots & \ddots & \vdots \\ f_{m+1}(x_1) & f_{m+1}(x_2) & \dots & f_{m+1}(x_{m+1}) \end{pmatrix}$.

The x_i can be chosen so that the columns of M are independent, so M is invertible, and there will be a solution for any (L_{m+2}, L_1).

A similar argument applies to paths of the form $P_1 L_1 \dots L_{m+1} P_{m+2}$.

Now consider paths between a vertex $P \in \mathfrak{P}$ and $L \in \mathfrak{L}$. Choose a vertex L_1 adjacent to P, and look at paths from L_1 to L that pass through P. This can be done by setting x_1 to the first coordinate of P. The rest of the x_i can be chosen so that M is invertible, so there is a path from L_1 to L of length $2(m+1)$ passing through P, and therefore a path of length $2m+1$ from P to L.

Since a path exists in all three cases, the diameter of the graph is less than or equal to $2(m+1)$. □

For $J_m(q,i,j)$ with $(i,j) = (m, m+1)$, $(m, m+2)$, or $(m+1, m+2)$, we consider a path of length $2s$ where $s \leq m$. Set $L_{s+1} - L_1$ to $\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$. The first s rows of M form a Vandermonde matrix, and so the solution must have $t_1 = t_2 = \cdots = t_s = 0$. But this makes the last row zero, so there is no solution. Therefore, there is no path from L_1 to L_{s+1} of length s, and the diameter is exactly $2(m+1)$. A similar argument applies to $G_d(m,q)$, so the diameter of $G_d(m,q)$ is also exactly $2(m+1)$.

5.2 Girth

The girth of a wide class of Wenger graphs is less than or equal to 8, as shown by the following theorem.

Theorem 5.2. *Let G be a generalized Wenger graph given by the equations:*

$l_2 + p_2 = l_1 p_1^{e_2}$

$l_3 + p_3 = l_1 p_1^{e_3}$

$\vdots$

$l_{m+1} + p_{m+1} = l_1 p_1^{e_{m+1}}$

where the e_i are positive integers. Then the girth of G is less than or equal to 8.

Proof. A cycle of length 8 is given in Table 5.1.

L_1	P_1	L_2	P_2	L_3	P_3	L_4	P_4	L_1
0	0	1	1	0	0	-1	1	0
0	0	0	1	-1	1	-1	0	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
0	0	0	1	-1	1	-1	0	0
0	0	1	0	0	0	-1	0	

Table 5.1: Cycle of length 8

Since p_1 is always 0 or 1, all powers are the same, so that in the equation to determine if an edge exists becomes $l_k + p_k = l_1 p_1$. The product $l_1 p_1$ is zero except for the edges $L_2 P_2$ where it is 1, and $L_4 P_4$ where it is -1. So the p_k and l_k are as given.

In characteristic 2, the same path works. Even though -1 and 1 are equal, the vertices are distinct, and on the edge $L_4 P_4$, $l_1 p_1 = l_k + p_k = 1$. □

There are cases where the girth of a jumped Wenger graph is 4 or 6. The girth is 4 if:

- $m = 1, 2$, q is not a power of 2, and $(i, j) = (1, 3)$
- $m = 1$, $q - 1$ is divisible by 3, and $(i, j) = (1, 2)$

and the girth is 6 if:

- $m = 1$, q is a power of 2, and $(i, j) = (1, 3)$
- $m = 1$, $q - 1$ is not divisible by 3, and $(i, j) = (1, 2)$
- $m = 1$, q is not 2 or 3, and $(i, j) = (2, 3)$
- $m = 2$, q is neither 3 nor an odd power of 2, and $(i, j) = (1, 2)$
- $m = 2$, q is neither 3 nor an odd power of 2, and $(i, j) = (2, 3)$
- $m = 2$, q is not 2, 3, or 5, and $(i, j) = (1, 4)$
- $m = 2$, q is not 2, and $(i, j) = (2, 4)$
- $m = 3, 4, 5$, $q - 1$ is divisible by 3, and $(i, j) = (1, 4)$
- $m = 3, 4, 5, 6$, $q - 1$ is divisible by 3, and $(i, j) = (2, 5)$

The girth is 8 in all other cases. The proof can be found in [47]. I will give a few examples of the special cases.

Set $m = 1$, $(i, j) = (1, 3)$, and the characteristic is not 2. The girth should be 4. A cycle of length 4 is given in Table 5.2.

Since $(i, j) = (1, 3)$, the equation to determine if an edge exists is $p_2 + l_2 = l_1 p_1^2$. Since $p_1 = \pm 1$, this reduces to $p_2 + l_2 = l_1$, which can be easily verified.

Note that if it were characteristic 2, P_1 would be the same as P_2 and L_1 the same as L_2, so the cycle would just go back and forth between two vertices. But since the characteristic is not 2, the four vertices are distinct.

Let $m = 2$, $q = 7$, and $(i, j) = (1, 4)$. The girth should be 6. A cycle of length 6 is given in Table 5.2.

$m = 1$, $p \neq 2$, $(i, j) = (1, 3)$

P_1	L_1	P_2	L_1	P_1
1	1	-1	-1	1
0	1	0	-1	0

1	1	-1	-1

$m = 2$, $q = 7$, $(i, j) = (1, 4)$

P_1	L_1	P_2	L_2	P_3	L_3	P_1
1	1	2	0	4	3	1
0	1	3	4	3	3	0
0	1	0	0	0	3	0

1	4	0	0	6	3
1	1	0	0	3	3

P_1	L_1	P_2	L_2	P_1
p_1	l_1	p_2	l_2	p_1
0	a	b	c	0
0	—	—	—	0

Table 5.2: Cycles in jumped Wenger graphs

Since $(i, j) = (1, 4)$, the equations to determine if an edge exists are $p_2 + l_2 = l_1 p_1^2$ and $p_3 + l_3 = l_1 p_1^3$. For the cubes, $1^3 = 2^3 = 4^3 = 1 \pmod 7$, so $p_3 + l_3 = l_1$ and the sequence of p_3 and l_3 becomes $0, l_1^{(1)}, 0, l_1^{(2)}, 0, l_1^{(3)}, 0$.

The squares can be just calculated directly: $p_1 = 1, 2, 2, 4, 4, 1$ and $l_1 = 1, 1, 0, 0, 3, 3$, so the sum $p_2 + l_2$ is $l_1 p_1^2 = 1, 4, 0, 0, 6, 3$, and the sequence of l_2 and p_2 is $0, 1, 3, -3, 3, 3, 0$.

There can be no cycle of length 4. A cycle of length 4 would have to be as shown in Table 5.2. The latter two elements of P_1 can be set to $0, 0$ without loss of generality since the calculation applies only to the sums $p_2 + l_2$ and $p_3 + l_3$. Thus:

$a = l_1 p_1^2$

$b = l_1 p_2^2 - l_1 p_1^2$

$c = l_2 p_2^2 - l_1 p_2^2 + l_1 p_1^2$

$0 = l_2 p_1^2 - l_2 p_2^2 + l_1 p_2^2 - l_1 p_1^2$

A similar calculation for the third element gives the same equation with squares replaced by cubes:

$0 = l_2p_1^3 - l_2p_2^3 + l_1p_2^3 - l_1p_1^3$

Combining terms in the two equations gives:

$0 = (l_2 - l_1)(p_1^2 - p_2^2)$

$0 = (l_2 - l_1)(p_1^3 - p_2^3)$

If $l_2 = l_1$, then $L_1 = L_2$ since they are both connected to P_2 (and P_1). So divide by $l_2 - l_1$ giving $p_1^2 = p_2^2$ and $p_1^3 = p_2^3$. But these imply $p_1 = p_2$, which means $P_1 = P_2$ since they are both connected to L_1 (and L_2).

The following describes the girth of extended Wenger graphs $G_d(m, q)$. The next theorem is about generalized Wenger graphs.

Theorem 5.3. *Given a generalized Wenger graph G of order $2q^{m+1}$ with equations:*

$p_2 + l_2 = g_2(p_1, l_1)$

$p_3 + l_3 = g_3(p_1, l_1)$
$\vdots$

$p_{m+1} + l_{m+1} = g_{m+1}(p_1, l_1),$

suppose that there is a path in G of length k. Then the graph G' of order $2q^m$ given by removing one equation from the equations for G has a corresponding path of length k. In particular, if G has a cycle of length k, then G' has a cycle of length less than or equal to k.

Proof. Without loss of generality, assume that the equation removed from the list for G is the last one, since re-arranging the equations gives an isomorphism of the corresponding

graphs. Consider an edge between $\begin{pmatrix} l_1 \\ l_2 \\ \vdots \\ l_{m+1} \end{pmatrix}$ and $\begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_{m+1} \end{pmatrix}$ in G. There is a corresponding edge in G' between $\begin{pmatrix} l_1 \\ l_2 \\ \vdots \\ l_m \end{pmatrix}$ and $\begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_m \end{pmatrix}$ in G' since the defining equations are the same. Edges with a common vertex in G will give corresponding edges in G' that have a common vertex, so a path in G corresponds to a path in G'.

A cycle in G with length k will give a cycle of length k in G' if all the vertices remain distinct. But two vertices in G might map to the same vertex in G'. Since P vertices map to P vertices and L vertices map to L vertices, if this happens, the vertices in G must be an even number of steps apart in the path. If the distance is always 4 or greater, then the cycle in G maps to a set of cycles of length 4 or greater in G'. But if the distance can be 2, the cycle can collapse: for example, the cycle $P_1L_1P_2L_2P_1$ in G could map to $P_1'L_1'P_1'L_1'P_1'$ in G', which is not a cycle, but a trip back and forth twice on the same edge. So the distance-2 case needs to be resolved. Two vertices with distance 2 in a path can be of the form $P_1L_1P_2$ or $L_1P_1L_2$.

Suppose $P_1L_1P_2$ is part of a cycle in G with P_1 and P_2 mapping to the same vertex in G'. Then $p_1^{(1)} = p_1^{(2)}$, so that $P_1 = P_2$, contradicting that $P_1L_1P_2$ is part of a cycle. A similar argument applies to parts of a cycle of the form $L_1P_1L_2$. Therefore, consecutive edges in G' are still distinct, and true cycles are always created in G'. Of course, these cycles must have length less than or equal to k. □

All graphs $G_d(m, q)$ have the 8-cycle which is given in Table 5.1, so that the girth is less

than or equal to 8.

Since $W_m(q)$ has girth 8 for $m \geq 2$, $G_d(m,q)$ has girth 8 for $m \geq 3$. Also, since original Wenger graphs have no 4-cycles, the girth is 6 or 8 for $m = 2$. So the cases to be analyzed are cycles of length 4 or 6 with $m = 1$ and cycles of length 6 with $m = 2$.

Theorem 5.4. *The graph $G_d(1,q)$ has cycles of length 4 if and only if $d+1$ divides $q-1$.*

Proof. Consider a cycle $P_1L_1P_2L_2P_1$ of length 4. Combine the defining equations to get:

$l_2^{(2)} - l_2^{(1)} = (l_1^{(2)} - l_1^{(1)})(p_1^{(2)})^{d+1}$

$l_2^{(1)} - l_2^{(2)} = (l_1^{(1)} - l_1^{(2)})(p_1^{(1)})^{d+1}$

If $l_1^{(1)} = l_1^{(2)}$ then L_1 and L_2 are the same vertex. So $l_1^{(1)} \neq l_1^{(2)}$, and dividing by $l_1^{(1)} - l_1^{(2)}$ gives $(p_1^{(1)})^{d+1} = (p_1^{(2)})^{d+1}$. But since P_1 and P_2 must be distinct, $p_1^{(1)} \neq p_1^{(2)}$. This can only happen if $d+1$ divides $q-1$.

Conversely, if $d+1$ divides $q-1$, then there are nonzero $p_1^{(1)}$ and $p_1^{(2)}$ which are not equal but their $d+1$ powers are equal. Then

$P_1 = (p_1^{(1)}, 0)$

$L_1 = (1, (p_1^{(1)})^{d+1})$

$P_2 = (p_1^{(2)}, 0)$

$L_2 = (0,0)$

$P_1 = (p_1^{(1)}, 0)$

is a cycle of length 4. □

Next to analyze are cycles of length 6 with $m = 1$ and characteristic 2.

If $d+1 \neq q-1$, then $a \in \mathbb{F}_q$ can be chosen so that $a^{d+1} \neq 1$, $a \neq 0$. Then there is the cycle of length 6 given in Table 5.3.

The case $d+1 = q-1$ is a little strange. Since $a^{d+1} = a^{q-1} = 1$ when $a \neq 0$ and $a^{d+1} = 0$ when $a = 0$, the defining equation for the graph becomes:

$$p_2 + l_2 = \begin{cases} l_1, & p_1 \neq 0 \\ 0, & p_1 = 0 \end{cases}$$

If $e \neq 1$, then there is the 6-cycle given in Table 5.3.

When $e = 1$, $q = 2$, and the only choice for d is $d = 0$, so that $d+1 = q-1$. In this case, the graph is the cycle graph with 8 vertices, so clearly there is no 6-cycle.

The next case is $m = 1$ and characteristic greater than 2. If $d+1$ is odd, there is the 6-cycle given in Table 5.3.

When the characteristic is not 2, $q-1$ is even, so when $d+1$ is even, the strange case $d+1 = q-1$ is one of the possibilities. If $d+1 \neq q-1$, $a \in \mathbb{F}_q$ can be chosen so that $a^{d+1} \neq 1$ and $a \neq 0$. Then there is the 6-cycle given in Table 5.3.

In the $d+1 = q-1$ case, if $q > 3$, then there are three distinct non-zero elements of $\mathbb{F}_q$, a, b, and c. The 6-cycle is in Table 5.3.

In the last case, $q = 3$, $d+1 = q-1 = 2$, there are not three distinct non-zero elements, so the method above doesn't work. In fact, there are no 6-cycles in this case.

The three entries $p_1^{(1)}$, $p_1^{(2)}$, and $p_1^{(3)}$ must be distinct, since otherwise the points P_1, P_2, and P_3 will not be distinct, but the vertices must be distinct to construct a 6-cycle. There are only three elements in the field, and since the labels on the P-vertices can be rotated and their order can be reversed, it is possible without loss of generality to assume that $p_1^{(1)} = 0$, $p_1^{(2)} = 1$, and $p_1^{(3)} = -1$. Now the vertices can be calculated, leaving $p_2^{(1)}$, $l_1^{(1)}$, $l_1^{(2)}$, and $l_1^{(3)}$ as

unknowns:

$P_1 = (0, p_2^{(1)})$

$L_1 = (l_1^{(1)}, -p_2^{(1)})$

$P_2 = (1, p_2^{(1)} + l_1^{(1)})$

$L_2 = (l_1^{(2)}, l_1^{(2)} - p_2^{(1)} - l_1^{(1)})$

$P_3 = (-1, p_2^{(1)} + l_1^{(1)})$

$L_3 = (l_1^{(3)}, l_1^{(3)} - p_2^{(1)} - l_1^{(1)})$

$P_1 = (0, p_2^{(1)} + l_1^{(1)} - l_1^{(3)})$

To close the loop, $l_1^{(1)} - l_1^{(3)}$ must be zero. But then $-p_2^{(1)} = l_1^{(3)} - p_2^{(1)} - l_1^{(1)}$, so L_1 and L_3 are the same vertex, a contradiction.

The last case is cycles of length 6 when $m = 2$. If $p \neq 2$ and $d + 2$ is odd, then the $m = 1$ case can be extended, so there is the 6-cycle in Table 5.4.

This fails when $p = 2$, since then $-1 = 1$ so that $P_3 = P_2$ and $L_3 = L_1$. So the cycle becomes a round trip on a path of length 3.

The method also fails when $p \neq 2$ and $d + 2$ is even, since then $l_1^{(3)}(p_1^{(3)})^{d+2}$ is -1, not 1, so the edge from P_3 to L_3 does not exist.

It seems likely that cycles of length 6 exist in most cases, but I have not been able to find a proof. An example for the case $q = 7$ and $d + 2 = 4$ is given in Table 5.4.

The existence of a 6-cycle is equivalent to the matrix $\begin{pmatrix} 1 & x_1 & x_1^4 \\ 1 & x_2 & x_2^4 \\ 1 & x_3 & x_3^4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 5 \\ 1 & 3 & 4 \\ 1 & 4 & 3 \end{pmatrix}$ being

singular, since in the first coordinate:

$$0 = (l_1^{(3)} - l_1^{(2)}) + (l_1^{(2)} - l_1^{(1)}) + (l_1^{(1)} - l_1^{(3)}) = t_3 + t_2 + t_1,$$

in the second coordinate:

$$0 = (l_1^{(3)} - l_1^{(2)})p_1^{(3)} + (l_1^{(2)} - l_1^{(1)})p_1^{(2)} + (l_1^{(1)} - l_1^{(3)})p_1^{(1)} = t_3x_3 + t_2x_2 + t_1x_1,$$

and in the third coordinate:

$$0 = (l_1^{(3)} - l_1^{(2)})(p_1^{(3)})^4 + (l_1^{(2)} - l_1^{(1)})(p_1^{(2)})^4 + (l_1^{(1)} - l_1^{(3)})(p_1^{(1)})^4 = t_3x_3^4 + t_2x_2^4 + t_1x_1^4,$$

so that $\begin{pmatrix} t_1 \\ t_2 \\ t_3 \end{pmatrix}$ is in the null space of the transpose.

Looking at it another way, $(2, 5)$, $(3, 4)$, and $(4, 3)$ are on the same line in the x-y plane (if $(a\ b\ c)^T$ is in the null space, then all three points satisfy $a + bx + cy = 0$).

It also corresponds to the fact that $x^4 + x + 4$ has 3 (or more) distinct roots. The powers of the roots form the rows of the matrix, and the null space vector $(4\ 1\ 1)^T$ gives the coefficients. Checking, $(x - 2)^2(x - 3)(x - 4) = x^4 - 11x^3 + 44x^2 - 76x + 48 = x^4 + x + 4 \pmod{11}$, so it's x^4 plus a linear polynomial.

If there were no polynomials of the form $x^4 + ax + b$ with 3 or more distinct roots, then there would be no x_1, x_2, x_3 that make the matrix singular, so there would be no nontrivial solution to the coordinate equations, and therefore no cycle of length 6. As a result, the girth would be 8.

5.3 Spectrum

In this section, the spectrum of the extended Wenger graph $G_d(m, q)$ is analyzed.

The degree of every vertex of $G_d(m, q)$ is q. This is true since in the equations defining the graph,

$$\begin{aligned} l_2 + p_2 &= p_1 l_1 \\ l_3 + p_3 &= p_1^2 l_1 \\ &\vdots \\ l_m + p_m &= p_1^{m-1} l_1 \\ l_{m+1} + p_{m+1} &= p_1^{m+d} l_1 \end{aligned}$$

if $p_1, p_2, \ldots, p_{m+1}$ are given, then there are q possible values of l_1, and then $l_2, l_3, \ldots, l_{m+1}$ are uniquely determined. Similarly, if $l_1, l_2, \ldots, l_{m+1}$ are given, then there are q possible values of p_1, and $p_2, p_3, \ldots, p_{m+1}$ are uniquely determined. The jumped Wenger graphs $J_m(q, i, j)$ are also q-regular[47].

Since the graph is q-regular, the incidence matrix will have q ones in each row, with the rest zero. Therefore the all-one vector will be an eigenvector with eigenvalue q. Furthermore, since the graph is bipartite, the incidence matrix will have the form $A = \begin{pmatrix} 0 & N \\ N^T & 0 \end{pmatrix}$ so that the vector with the first half all 1 and the second half all -1 will be an eigenvector with eigenvalue $-q$.

Conversely, suppose that $e = \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}$ is an eigenvector with eigenvalue q. Suppose that e_i is the largest element of e (i.e. that $e_j \leq e_i$ for all j). Then taking the i-th row of $Ae = qe$ gives $\sum_{j=1}^{n} A_{ij}e_j = qe_i$. Since e_i is the largest and $\sum_{j=1}^{n} A_{ij} = q$, it must be that every e_j for which $A_{ij} = 1$ is equal to e_i. Since the graph is connected, the process can be continued to show that every e_i is equal, so the only eigenvector with eigenvalue q is the all-one vector. A similar argument shows that the only eigenvector with eigenvalue $-q$ is the vector with the first half all 1 and the second half all -1.

The following is a very important result from [7] that equates the eigenvalue multiplicity with the number of polynomials with a given number of distinct roots.

Theorem 5.5 (Theorem 2.2 of [7])**.** *Let G be a generalized Wenger graph defined by the equations:*

$$p_2 + l_2 = l_1 f_2(p_1)$$

$$p_3 + l_3 = l_1 f_3(p_1)$$
$$\vdots$$

$$p_{m+1} + l_{m+1} = l_1 f_{m+1}(p_1)$$

and assume that the mapping $u \mapsto (1, f_2(u), \ldots, f_{m+1}(u))$ is injective. Then the eigenvalues of G are $\pm\sqrt{qi}$, where $0 \leq i \leq q$ with multiplicity given by:

$$n_i = |\{w = (w_1, w_2, \ldots, w_{m+1}) \in \mathbb{F}_q^{m+1} : N_{F_w} = i\}|$$

where $N_{F_w} = |\{u \in \mathbb{F}_q : F_w(u) = 0\}|$ and $F_w(u) = w_1 + w_2 f_2(u) + \cdots + w_{m+1} f_{m+1}(u)$.

So to calculate the spectrum of a given Wenger graph, the functions $F_w(u)$ are listed, and the number of roots of each is calculated. Then the multiplicity of $\pm\sqrt{qi}$ is the number of

functions with i roots.

The largest eigenvalues $\pm q$ always have nonzero multiplicity since if $w_0 = w_1 = \cdots = w_m = 0$, F_w will be identically zero and therefore have exactly q roots.

For eigenvalues other than $\pm q$, it is not so easy to calculate the multiplicity. Since the degree of F_w is $m + d$, F_w can not have more than $m + d$ roots, and the multiplicity of eigenvalues $\pm\sqrt{qi}$ is zero if $m + d < i < q$. So the eigenvalues with the largest possible absolute value are $\pm\sqrt{q(m + d)}$.

The next result is about the multiplicity of the eigenvalues $\pm\sqrt{q(m + d)}$. For the case $d = 0$, the graph is the original Wenger graph $W_m(q)$ and the multiplicity of $\pm\sqrt{qm}$ is given by Theorem 3.1. So it is assumed that $d > 0$ in the following analysis.

Theorem 5.6. *Let $G_d(m, q)$ be an extended Wenger graph.*

If $q > ((m+d)(m+d+2)!)^2$ and $m \geq 2$, then the second largest eigenvalue is $\pm\sqrt{q(m + d)}$.

The multiplicity N_{m+d} of $\pm\sqrt{q(m + d)}$ is bounded by:

$$\left| N_{m+d} - \tfrac{1}{q^m}\binom{q}{m+d} \right| \leq \binom{q/p+(m-1)\sqrt{q}+m+d-1}{m+d}$$

For any $\epsilon > 0$, there is a constant $c_\epsilon > 0$ such that if $d < \epsilon\sqrt{m + d}$ and $4\epsilon^2 \ln^2 q < m+d \leq c_\epsilon q$, then the second largest eigenvalue is $\pm\sqrt{q(m + d)}$.

Proof. The eigenvalues $\pm\sqrt{q(m + d)}$ have multiplicity given by:

$$n_{m+d} = |\{(w_0, w_1, \ldots, w_{m-1}, w_m) \in \mathbb{F}_q^{m+1} : F_w \text{ has m+d distinct roots in } \mathbb{F}_q\}|$$

where $F_w = w_0 + w_1 x + \cdots + w_{m-1}x^{m-1} + w_m x^{m+d}$. If $w_m = 0$, then the polynomial has degree $m - 1$, so it can not have $m + d$ roots. Dividing by w_m gives:

$$n_{m+d} = (q-1)|\{(a_0, a_1, \ldots, a_{m-1}) \in \mathbb{F}_q^{m} : F_a \text{ has m+d distinct roots in } \mathbb{F}_q\}|$$

where now $F_a = a_0 + a_1 x + \cdots + a_{m-1}x^{m-1} + x^{m+d}$. If $c_1, c_2, \ldots, c_{m+d}$ are the roots of F_a, then since they can appear in any order:

$$n_{m+d} = \frac{q-1}{(m+d)!}|\{(c_1, c_2, \ldots, c_{m+d}) \in \mathbb{F}_q^{m+d} : \\ (x-c_1)(x-c_2)\ldots(x-c_{m+d}) = x^{m+d} + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0, c_i \text{ distinct}\}|$$

Setting $N_{m+d} = \frac{(m+d)!}{q-1} n_{m+d}$ and re-arranging the polynomial gives:

$$N_{m+d} = |\{(c_1, c_2, \ldots, c_{m+d}) \in \mathbb{F}_q^{m+d} : \\ (1-c_1x)(1-c_2x)\ldots(1-c_{m+d}x) = 1+a_{m-1}x^{d+1}+\cdots+a_1x^{m+d-1}+a_0x^{m+d}, c_i \text{ distinct}\}|$$

$$N_{m+d} = |\{(c_1, c_2, \ldots, c_{m+d}) \in \mathbb{F}_q^{m+d} : \\ (1-c_1x)(1-c_2x)\ldots(1-c_{m+d}x) \equiv 1 \pmod{x^{d+1}}, c_i \text{ distinct}\}|$$

If $N_{m+d} > 0$, then $\pm\sqrt{q(m+d)}$ are the eigenvalues with the second largest absolute value. The first result now follows from Cohen[13], and the other two results follow from Li and Wan[37].

□

The following is an example of the spectrum of an extended Wenger graph: $G_d(m, q)$ with

$m = 1$, $q = 3$, and $d = 1$. The graph has $2q^{m+1} = 18$ vertices. There is an edge from $\begin{pmatrix} p_1 \\ p_2 \end{pmatrix}$ to $\begin{pmatrix} l_1 \\ l_2 \end{pmatrix}$ whenever $p_2 + l_2 = l_1 p_1^2$. The edges for the graph are computed in Table 5.5.

The adjacency matrix is easily calculated from this table, and it is $A = \begin{pmatrix} 0 & N \\ N^T & 0 \end{pmatrix}$, where N is given in Table 5.6.

A can be viewed as a matrix over the real numbers, and the eigenvalues and eigenvectors can be calculated. Note that the matrix is symmetric, so all of the eigenvalues are real, and the matrix is diagonalizable, so it should have a full complement of eigenvectors - in this case, since it's an 18x18 matrix, it will have 18 eigenvectors. The eigenvalues are $-1, -\sqrt{6}, -\sqrt{3}, 0, \sqrt{3}, \sqrt{6}$, and 3 with multiplicities $1, 2, 2, 8, 2, 2$, and 1, respectively. The eigenvectors are given in Tables 5.7 and 5.8.

The multiplicity of the eigenvectors is related to the number of roots of polynomials over $F_w \in \mathbb{F}_3[u]$. In this case, there are 9 polynomials to look at, and the number of roots of each is in Table 5.9.

The multiplicity of ± 3 is 1, the number of equations with 3 roots. The multiplicity of $\pm\sqrt{6}$ is 2, the number of equations with 2 roots. The multiplicity of $\pm\sqrt{3}$ is 2, the number of equations with 1 root. There are 4 equations with no roots, so the multiplicity of 0 is 8, since we count $+0$ and -0.

The following theorem shows that the multiplicities of the smaller eigenvalues of $G_d(m, q)$ are nonzero.

Theorem 5.7. *Given an extended Wenger graph $G_d(m, q)$, if $i < m$ the multiplicities of the eigenvalues $\pm\sqrt{qi}$ are nonzero.*

Proof. By Theorem 5.5, the multiplicity of $\pm\sqrt{qi}$ is given by

$$n_i = |\{(w_0, w_1, \ldots, w_{m-1}, w_m) \in \mathbb{F}_q^{m+1} | F_w \text{ has exactly } i \text{ distinct roots in } \mathbb{F}_q\}|$$

where $F_w = w_m x^{m+d} + w_{m-1} x^{m-1} + \cdots + w_1 x + w_0$.

For the multiplicity to be positive, there only needs to be one such F_w. So choose $w_m = w_{m-1} = \cdots = w_{i+1} = 0$. Note that since $i < m$, this list is not empty.

Now choose any distinct $x_1, x_2, \ldots, x_i \in \mathbb{F}_q$, and set $w_i = 1$ and $w_{i-1}, \ldots, w_0$ so that $F_w = (x - x_i)(x - x_{i-1}) \ldots (x - x_1)$. Clearly, then, F_w has exactly i roots. □

L_1	P_1	L_2	P_2	L_3	P_3	L_1	$m = 1$, characteristic 2
0	a	1	0	a^{d+1}	1	0	$d + 1 \neq q - 1$
0	0	a^{d+1}	a^{d+1}	a^{d+1}	0	0	
0	a^{d+1}	0	0	a^{d+1}	0		

P_1	L_1	P_2	L_2	P_3	L_3	P_1	$m = 1$, characteristic 2
1	0	x	1	$x + 1$	$x + 1$	1	$d + 1 = q - 1$
0	0	0	1	0	$x + 1$	0	
0	0	1	1	$x + 1$	$x + 1$		

P_1	L_1	P_2	L_2	P_3	L_3	P_1	$m = 1$, $p \neq 2$
0	1	1	0	-1	-1	0	$d + 1$ odd
0	0	1	-1	1	0	0	
0	1	0	0	1	0		

P_1	L_1	P_2	L_2	P_3	L_3	P_1	$m = 1$, $p \neq 2$
0	1	a	0	1	a^{d+1}	0	$d + 1$ even
0	0	a^{d+1}	-a^{d+1}	a^{d+1}	0	0	$d + 1 \neq q - 1$
0	a^{d+1}	0	0	a^{d+1}	0		

P_1	L_1	P_2	L_2	P_3	L_3	P_1	$m = 1$, $p \neq 2$
a	0	b	1	c	-1	a	$d + 1 = q - 1$
0	0	0	1	0	-1	0	
0	0	1	1	-1	-1		

Table 5.3: Cycles of length 6 in $G_d(1, q)$

P_1	L_1	P_2	L_2	P_3	L_3	P_1	$m = 2$, $p \neq 2$
0	1	1	0	-1	-1	0	$d + 2$ odd
0	0	1	-1	1	0	0	
0	0	1	-1	1	0	0	
0	1	0	0	1	0		
0	1	0	0	1	0		

P_1	L_1	P_2	L_2	P_3	L_3	P_1	example
2	10	3	1	4	0	2	$m = 2$, $q = 11$
0	9	10	4	0	0	0	$d + 2 = 4$
0	6	1	3	0	0	0	
9	8	3	4	0	0		
6	7	4	3	0	0		

Table 5.4: Cycles of length 6 in $G_d(2, q)$

			$l_1 p_1^2 - p_2$ $(= l_2)$			connections
p_1	p_2	p_1^2	$l_1 = 0$	$l_1 = 1$	$l_1 = 2$	$l_1 l_2 =$
0	0	0	0	0	0	00, 10, 20
0	1	0	2	2	2	02, 12, 22
0	2	0	1	1	1	01, 11, 21
1	0	1	0	1	2	00, 11, 22
1	1	1	2	0	1	02, 10, 21
1	2	1	1	2	0	01, 12, 20
2	0	1	0	1	2	00, 11, 22
2	1	1	2	0	1	02, 10, 21
2	2	1	1	2	0	01, 12, 20

Table 5.5: Calculations for edges of $G_1(1, 3)$

$N =$

p_1p_2 \ l_1l_2	00	01	02	10	11	12	20	21	22
00	1	0	0	1	0	0	1	0	0
01	0	0	1	0	0	1	0	0	1
02	0	1	0	0	1	0	0	1	0
10	1	0	0	0	1	0	0	0	1
11	0	0	1	1	0	0	0	1	0
12	0	1	0	0	0	1	1	0	0
20	1	0	0	0	1	0	0	0	1
21	0	0	1	1	0	0	0	1	0
22	0	1	0	0	0	1	1	0	0

Table 5.6: Adjacency matrix for $G_1(1,3)$

$\lambda = -3$: $\begin{pmatrix} -1 \\ -1 \\ -1 \\ -1 \\ -1 \\ -1 \\ -1 \\ -1 \\ -1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$ $\lambda = 3$: $\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$ $\lambda = \sqrt{6}$: $\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \sqrt{6}/2 \\ -\sqrt{6}/2 \\ 0 \\ \sqrt{6}/2 \\ -\sqrt{6}/2 \\ 0 \\ -1 \\ 1 \\ 1 \\ 0 \\ -1 \\ -1 \\ 1 \\ 0 \end{pmatrix}$ $\begin{pmatrix} 0 \\ 0 \\ 0 \\ \sqrt{6}/2 \\ 0 \\ -\sqrt{6}/2 \\ \sqrt{6}/2 \\ 0 \\ -\sqrt{6}/2 \\ 1 \\ -1 \\ 0 \\ 0 \\ 1 \\ -1 \\ -1 \\ 0 \\ 1 \end{pmatrix}$

$\lambda = -\sqrt{6}$: $\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ -\sqrt{6}/2 \\ \sqrt{6}/2 \\ 0 \\ -\sqrt{6}/2 \\ \sqrt{6}/2 \\ 0 \\ -1 \\ 1 \\ 1 \\ 0 \\ -1 \\ -1 \\ 1 \\ 0 \end{pmatrix}$ $\begin{pmatrix} 0 \\ 0 \\ 0 \\ -\sqrt{6}/2 \\ 0 \\ \sqrt{6}/2 \\ -\sqrt{6}/2 \\ 0 \\ \sqrt{6}/2 \\ 1 \\ -1 \\ 0 \\ 0 \\ 1 \\ -1 \\ -1 \\ 0 \\ 1 \end{pmatrix}$ $\lambda = \sqrt{3}$: $\begin{pmatrix} -\sqrt{3} \\ 0 \\ \sqrt{3} \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -1 \\ 1 \\ 0 \\ -1 \\ 1 \\ 0 \\ -1 \\ 1 \\ 0 \end{pmatrix}$ $\begin{pmatrix} -\sqrt{3} \\ \sqrt{3} \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -1 \\ 0 \\ 1 \\ -1 \\ 0 \\ 1 \\ -1 \\ 0 \\ 1 \end{pmatrix}$

Table 5.7: Eigenvectors for $G_1(1, 3)$

$\lambda = -\sqrt{3}$:	$\begin{pmatrix} \sqrt{3} \\ 0 \\ -\sqrt{3} \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -1 \\ 1 \\ 0 \\ -1 \\ 1 \\ 0 \\ -1 \\ 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} \sqrt{3} \\ -\sqrt{3} \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -1 \\ 0 \\ 1 \\ -1 \\ 0 \\ 1 \\ -1 \\ 0 \\ 1 \end{pmatrix}$	$\lambda = 0$:	$\begin{pmatrix} -1 \\ -1 \\ -1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \\ 0 \\ -1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

$\lambda = 0$ (cont.):	$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ -1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} -1 \\ -1 \\ -1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -1 \\ -1 \\ -1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -1 \\ -1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ -1 \\ -1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -1 \\ 0 \\ -1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

Table 5.8: Eigenvectors for $G_1(1, 3)$

$w \in \mathbb{F}_3^2$	$F_w(u)$	roots in $\mathbb{F}_3$
00	0	3
01	u^2	1
02	$2u^2$	1
10	1	0
11	u^2+1	0
12	$2u^2+1$	2
20	2	0
21	u^2+2	2
02	$2u^2+2$	0

Table 5.9: Number of Roots of F_w

Chapter 6

Polynomial Root Patterns

Li and Wan[37] calculated $N_m(k,b)$, the number of products $(1+x_1t)(1+x_2t)\dots(1+x_kt)$ with distinct x_i which are congruent to $1+b_1t+\cdots+b_mt^m \pmod{t^{m+1}}$. In this chapter, their result is extended to the case where the x_i are not necessarily distinct. The Li and Wan result is presented in Section 6.1 and the new result is in Section 6.2.

6.1 Distinct Roots

Let D be a finite set, and $X \subseteq D^k$. So the elements of X are of the form $(x_1, x_2, \dots, x_k)$ with $x_i \in D$. Let $\overline{X}$ be the set of elements with distinct x_i (so $x_i \neq x_j$ if $i \neq j$).

For any $\tau \in S_k$, let $(i_1 i_2 \dots i_{a_1})(j_1 j_2 \dots j_{a_2}) \dots (l_1 l_2 \dots l_{a_s})$ be its disjoint cycle representation. Then define $X_\tau = \{(x_1, x_2, \dots, x_k) \in X : x_{i_1} = \cdots = x_{i_{a_1}}, \dots, x_{l_1} = \cdots = x_{l_{a_s}}\}$, the set of components of X which are invariant under τ.

Theorem 6.1 (Theorem 1.1 of [37]). *The number of elements of $\overline{X}$ is given by*

$|\overline{X}| = \sum_{\tau \in S_k} \operatorname{sign}(\tau) |X_\tau|$

If X is invariant under permutation of the coordinates x_i, then the sum can be grouped by conjugacy class:

$|\overline{X}| = \sum_{\tau \in C_k} \text{sign}(\tau) C(\tau) |X_\tau|$

where C_k is the set of conjugacy classes of S_k, and $C(\tau)$ is the number of permutations in S_k conjugate to τ.

They use this theorem to count $N_m(k, b)$, the number of un-ordered k-tuples $x = (x_1, \ldots, x_k)$ with distinct coordinates $x_i \in \mathbb{F}_q$ such that $1 + b_1 t + \cdots + b_m t^m \equiv \prod_{i=1}^{k} (1 + x_i t) \pmod{t^{m+1}}$.

Theorem 6.2 (Theorems 1.3 and 1.4 of [37])**.** *For all $b \in \mathbb{F}_q^m$,*

$|N_m(k, b) - \frac{1}{q^m}\binom{q}{k}| \leq \binom{q/p + (m-1)\sqrt{q} + k - 1}{k}$

Furthermore, for any $\epsilon > 0$, there is a constant $c_\epsilon > 0$ such that if $m < \epsilon k^{1/2}$ and $4\epsilon^2 (\ln q)^2 < k \leq c_\epsilon q$, then $N_m(k, b) > 0$ for all $b \in \mathbb{F}_q^m$.

6.2 General Case

As in the beginning of Section 6.1, let D be a finite set, and $X \subseteq D^k$.

Let $p = \{S_1, S_2, \ldots, S_l\}$ be a partition of $\{1, 2, \ldots, k\}$, so that $S_1 \cup S_2 \cup \cdots \cup S_l = \{1, 2, \ldots, k\}$ and $S_i \cap S_j = \emptyset$ for $i \neq j$.

Theorem 6.3. *The number of elements of X for which $x_i = x_j$ if and only if i and j are in the same set in p is given by:*

$$|X_p| = |\overline{X_l}| = \sum_{\tau \in S_l} \text{sign}(\tau) |X_\tau| \tag{6.1}$$

where if $(i_1 i_2 \dots i_{a_1}) \dots (j_1 j_2 \dots j_{a_s})$ *is the cycle decomposition of* τ, $X_\tau = \{(x_1, \dots, x_l) \in X_l | x_{i_1} = x_{i_2} = \dots = x_{i_{a_1}}, \dots, x_{j_1} = x_{j_2} = \dots = x_{j_{a_s}}\}$.

If the elements of X_p *are invariant under the action of* S_l,

$$|X_p| = \sum_{\tau \in C_l} \text{sign}(\tau) C(\tau) |X_\tau| \tag{6.2}$$

where C_l *is a set of representatives of the conjugacy classes of* S_l *and* $C(\tau)$ *is the size of the conjugacy class containing* τ.

Proof. Let $\alpha_i = |S_i|$ for $i = 1, 2, \dots, l$, so that $\sum_{i=1}^{l} \alpha_i = k$.

Consider the set $X_{(p)} = \{(x_1, x_2, \dots, x_k) \in X | x_i = x_j$ if i and j are in the same set in $p\}$.

Let $X_p = \{(x_1, x_2, \dots, x_k) \in X | x_i = x_j$ if and only if i and j are in the same set in $p\}$. The difference between $X_{(p)}$ and X_p is that $X_{(p)}$ has "if" in the definition, and X_p has "if and only if". So $|X_p| \leq |X_{(p)}|$ since we have removed elements for which $x_i = x_j$ even though i and j are in different sets in p.

Let X_l be the set $X_{(p)}$ with the elements corresponding to each S_i in p collapsed into one element. There is clearly a bijective relationship between X_l and $X_{(p)}$. Let $\overline{X_l}$ be the subset of X_l for which the coordinates $(x_1, x_2, \dots, x_l)$ are distinct. There is also a bijective relationship between $\overline{X_l}$ and X_p since corresponding elements are removed.

By Theorem 6.1,

$|X_p| = |\overline{X_l}| = \sum_{\tau \in S_l} \text{sign}(\tau) |X_\tau|$

If the elements of X_p are invariant under the action of S_l, the terms can be grouped by

conjugacy classes to get

$|X_p| = \sum_{\tau \in C_l} \text{sign}(\tau) C(\tau) |X_\tau|$

□

The following is an example of Theorem 6.3.

Let $X = \mathbb{F}_3^6$ and $p = \{\{1,3,4\},\{2,5\},\{6\}\}$. So $D = \mathbb{F}_3$, and X is everything in D^6. And $|X_p|$, the result of the calculation, is the number of X for which $x_1 = x_3 = x_4$, $x_2 = x_5$, with the x_i being otherwise distinct. Note that $l = 3$, the number of sets in p.

There are $3^6 = 729$ elements in X, and fixing $x_3 = x_1$, $x_4 = x_1$, and $x_6 = x_2$ brings this down to 27 elements in $X_{(p)}$ and X_l. They look like:

$X_{(p)} = (a, b, a, a, b, c)$ with $a, b, c \in \mathbb{F}_3$

$X_l = (a, b, c)$ with $a, b, c \in \mathbb{F}_3$.

τ	$\lvert X_\tau \rvert$	$\text{sign}(\tau)$
1	27	+1
(12)	9	-1
(13)	9	-1
(23)	9	-1
(123)	3	+1
(132)	3	+1

Table 6.1: Size of X_τ for $\tau \in S_3$

The results for $|X_\tau|$ are in Table 6.1 for $\tau \in S_3$. As an example, if $\tau = (12)$, we choose the elements of X_l with $x_1 = x_2$ (or $a = b$). So there are 9 elements, and since (12) is the product of 1 transposition, $\text{sign}((12)) = -1$.

Plugging in to Equation 6.1 gives $|X_p| = 27 - 9 - 9 - 9 + 3 + 3 = 6$ and there are indeed 6 elements in X_p:

$(0, 1, 0, 0, 1, 2)$

$(0, 2, 0, 0, 2, 1)$

$(1, 0, 1, 1, 0, 2)$

$(1, 2, 1, 1, 2, 0)$

$(2, 0, 2, 2, 0, 1)$

$(2, 1, 2, 2, 1, 0)$

This completes the example. The following is an analysis of polynomials with a given pattern of roots.

Theorem 6.4. *Let $N_m(k, b, p)$ be the number of ordered k-tuples $(x_1, \ldots, x_k) \in \mathbb{F}_q^k$ such that*

$$\prod_{i=1}^{k}(1 + x_i t) \equiv 1 + b_1 t + \cdots + b_m t^m \pmod{t^{m+1}} \tag{6.3}$$

and $x_i = x_j$ if and only if i and j are in the same set in p. Set $b(t) = 1 + b_1 t + \cdots + b_m t_m$ and let l be the number of sets in p. In the symmetric group S_l, for any permutation τ, let r be the number of cycles of τ, and let c_i be the sum of the α_i corresponding to cycle i of τ, $i = 1, 2, \ldots, r$. Then:

$$q^m N_m(k, b, p) = \frac{q!}{(q-l)!} + \sum_{\chi \neq 1} \chi^{-1}(b(t)) \sum_{\tau \in S_l} \operatorname{sign}(\tau) \prod_{i=1}^{r} \sum_{a \in \mathbb{F}_q} \chi^{c_i}(1 + at) \tag{6.4}$$

As an example of the definition of r and c_i, if $\tau = (13)(245)(6) \in S_6$, $r = 3$, and $c_1 = \alpha_1 + \alpha_3$, $c_2 = \alpha_2 + \alpha_4 + \alpha_5$, and $c_3 = \alpha_6$. Note that $\sum_{i=1}^{r} c_i = \sum_{j=1}^{l} \alpha_j = k$.

Proof. Let $A = \mathbb{F}_q[t]/(t^{m+1})$, and let A^* be the group of units of A. A character is a group homomorphism $\chi : A^* \to \mathbb{C}^*$ into the nonzero complex numbers. The characters form a group $\hat{A^*}$ under multiplication ($(\chi_1\chi_2)(a) = \chi_1(a)\chi_2(a)$). Let G be the subgroup for which $\chi(\mathbb{F}_q^*) = 1$. Note that $|G| = q^m$. In Theorem 6.3, set:

$X = \mathbb{F}_q^k$,

$X_{(p)} = \{(x_1, \ldots, x_k) \in X | x_i = x_j \text{ if } i \text{ and } j \text{ are in the same set in } p\}$,

$X_p = \{(x_1, \ldots, x_k) \in X | x_i = x_j \text{ if and only if } i \text{ and } j \text{ are in the same set in } p\}$.

$X_l = \{(x_1, \ldots, x_l) \in \mathbb{F}_q^l | x_i \text{ distinct}\}$

So $|X| = q^k$, $|X_{(p)}| = q^l$, and $|X_p| = \frac{q!}{(q-l)!}$. Note also that there are bijections between $X_{(p)}$ and $\mathbb{F}_p^l$ and between X_p and X_l. Thus:

$$\begin{aligned} N_m(k, b, p) &= \frac{1}{q^m} \sum_{x \in X_l} \sum_{\chi \in G} \chi \left(\frac{(1 + x_1 t)^{\alpha_1} \ldots (1 + x_l t)^{\alpha_l}}{1 + b_1 t + \cdots + b_m t_m} \right) \\ &= \frac{1}{q^m} \sum_{x \in X_l} \sum_{\chi \in G} \chi^{-1}(1 + b_1 t + \cdots + b_m t_m) \chi(\prod_{i=1}^{l} (1 + x_i t)^{\alpha_i}) \end{aligned}$$

For $\chi \in G$, set $f_\chi(x) = \chi \left(\prod_{i=1}^{l} (1 + x_i t)^{\alpha_i} \right)$ so

$q^m N_m(k, b, p) = \sum_{\chi \in G} \chi^{-1}(b(t)) \sum_{x \in X_l} f_\chi(x_1, \ldots, x_l)$

Applying equation 6.1 gives:

$$
\begin{aligned}
q^m N_m(k,b,p) &= \sum_{\chi \in G} \chi^{-1}(b(t)) \sum_{\tau \in S_l} \operatorname{sign}(\tau) F_\tau(\chi) \\
&= \frac{q!}{(q-l)!} + \sum_{\chi \neq 1} \chi^{-1}(b(t)) \sum_{\tau \in S_l} \operatorname{sign}(\tau) F_\tau(\chi)
\end{aligned}
$$

where

$$
F_\tau(\chi) = \sum_{x \in X_\tau} f_\chi(x_1, \ldots, x_l) = \sum_{x \in X_\tau} \chi \left(\prod_{i=1}^{l} (1 + x_i t)^{\alpha_i} \right) \tag{6.5}
$$

Equation 6.5 factors into:

$$
\begin{aligned}
F_\tau(\chi) &= \sum_{x \in X_\tau} \prod_{i=1}^{l} \chi^{\alpha_i}(1 + x_i t) \\
&= \left(\sum_{a \in \mathbb{F}_q} \chi^{c_1}(1 + at) \right) \left(\sum_{a \in \mathbb{F}_q} \chi^{c_2}(1 + at) \right) \ldots \left(\sum_{a \in \mathbb{F}_q} \chi^{c_l}(1 + at) \right) \\
&= \prod_{i=1}^{r} \sum_{a \in \mathbb{F}_q} \chi^{c_i}(1 + at)
\end{aligned}
$$

Substituting this in gives the required result. □

This is an exact result for $N_m(k,b,p)$.

As an example, the triples $(x_1, x_2, x_3) \in \mathbb{F}_3^3$ with $x_1 = x_2 \neq x_3$ for which $\prod_{i=1}^{3}(1 + x_i t) \equiv 1 \pmod{t^2}$ are counted.

So $p = \{\{1,2\},\{3\}\}$, $k = 3$, $m = 1$, $l = 2$, $\alpha_1 = 2$, and $\alpha_2 = 1$.

And $A = \mathbb{F}_3[t]/(t^2)$ and $|A| = q^{m+1} = 9$. The group of units A^* consists of everything with nonzero constant term, $|A^*| = q^m(q-1) = 6$, $A^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. We can use the generators 2 and $t+1$ with orders 2 and 3 to generate the group.

Defining $\omega = e^{2\pi i/3}$, $\chi(2)$ is either 1 or -1, and $\chi(t+1)$ is 1, ω, or ω^2. So the group of characters has order 6 as expected. The subgroup $G = \{\chi \in A^* | \chi(2) = 1\}$ has only 3 elements. We have $\tau \in S_l = S_2 = \{1, (12)\}$.

$1^2 \cdot 1 = 1$	$(t+1)^2 \cdot 1 = 2t+1$	$(2t+1)^2 \cdot 1 = t+1$
$1^2 \cdot (t+1) = t+1$	$(t+1)^2 \cdot (t+1) = 1$	$(2t+1)^2 \cdot (t+1) = 2t+1$
$1^2 \cdot (2t+1) = 2t+1$	$(t+1)^2 \cdot (2t+1) = t+1$	$(2t+1)^2 \cdot (2t+1) = 1$

Table 6.2: Calculation of $N_m(k,b,p)$ example

$N_m(k,b,p)$ can be calculated directly, as shown in Table 6.2. It is zero, since the product is 1 only when all three factors are equal.

Now $N_m(k,b,p)$ will be calculated using Equation 6.4. The calculation of $F_\tau(\chi)$ for all $\tau \in S_l$ and all $\chi \in G$ is done in Table 6.3.

τ	r	c_1	c_2	Expression for $F_\tau(\chi)$
1	2	$\alpha_1 = 2$	$\alpha_2 = 1$	$\left(\sum_{a\in\mathbb{F}_3} \chi^2(1+at)\right)\left(\sum_{a\in\mathbb{F}_3} \chi(1+at)\right)$
(12)	1	$\alpha_1 + \alpha_2 = 3$	-	$\sum_{a\in\mathbb{F}_3} \chi^3(1+at)$

$\chi(1)$	$\chi(t+1)$	$\chi(2t+1) = \chi(t+1)^2$	$\sum_{a\in\mathbb{F}_3} \chi(1+at)$	$\sum_{a\in\mathbb{F}_3} \chi^2(1+at)$	$F_1(\chi)$	$F_{(12)}(\chi)$
1	1	1	3	3	9	3
1	ω	ω^2	0	0	0	3
1	ω^2	ω	0	0	0	3

Table 6.3: Calculation of $F_\tau(\chi)$

Note that $\text{sign}(1) = 1$ and $\text{sign}((12)) = -1$. The first term is $\frac{q!}{(q-l)!} = \frac{3!}{(3-2)!} = 6$. The other

term is $\sum_{\chi \neq 1} \sum_{\tau \in S_l} \text{sign}(\tau) F_\tau(\chi) = \sum_{\chi \neq 1} (F_1(\chi) - F_{(12)}(\chi)) = -6$. So the result is zero as expected.

The next step is to estimate the right-hand side of Equation 6.4.

Corollary 6.1. *Using the notation in this chapter, and assuming* $m + 1 \leq \sqrt{q}$,

$$\left| N_m(k, b, p) - \tfrac{q!}{q^m (q-l)!} \right| < l! (m+1)^{l - \frac{k}{p}} q^{\frac{l}{2} + \frac{k}{2p}}$$

Proof. In Equation 6.4, if $\chi^{c_i} = 1$, then $\sum_{a \in \mathbb{F}_q} \chi^{c_i}(1 + at) = q$, and if $\chi^{c_i} \neq 1$, the Weil bound:

$$|\sum_{a \in \mathbb{F}_q} \chi^{c_i}(1 + at)| \leq (m+1)\sqrt{q}$$

can be used. Removing $\chi^{-1}(b(t))$ and $\text{sign}(\tau)$ further bounds the sum:

$$\left| q^m N_m(k, b, p) - \tfrac{q!}{(q-l)!} \right| \leq \sum_{\chi \neq 1} \sum_{\tau \in S_l} \prod_{i=1}^{r} \begin{cases} q, & \chi^{c_i} = 1 \\ (m+1)\sqrt{q}, & \chi^{c_i} \neq 1 \end{cases}$$

Since the group is a p-group, the order of $\chi \neq 1$ is at least p. Since $\sum_{i=1}^{r} c_i = k$, there are at most $\frac{k}{p}$ values of c_i for which χ^{c_i} is trivial. Since q is greater than $(m+1)\sqrt{q}$, this gives:

$$\left| q^m N_m(k, b, p) - \tfrac{q!}{(q-l)!} \right| \leq \sum_{\chi \neq 1} \sum_{\tau \in S_l} q^{\frac{k}{p}} ((m+1)\sqrt{q})^{r - \frac{k}{p}}$$

Since $r \leq l$,

$$\left| q^m N_m(k, b, p) - \tfrac{q!}{(q-l)!} \right| \leq \sum_{\chi \neq 1} \sum_{\tau \in S_l} q^{\frac{k}{p}} ((m+1)\sqrt{q})^{l - \frac{k}{p}} = (q^m - 1)(l!) q^{\frac{k}{p}} ((m+1)\sqrt{q})^{l - \frac{k}{p}}$$

Replacing $q^m - 1$ with q^m and dividing by q^m gives:

$$\left| N_m(k, b, p) - \tfrac{q!}{(q-l)! q^m} \right| < l! ((m+1)\sqrt{q})^{l - \frac{k}{p}} q^{\frac{k}{p}} = l! (m+1)^{l - \frac{k}{p}} q^{\frac{l}{2} + \frac{k}{2p}}$$ □

Chapter 7

Future Work

In this chapter, I will outline the some of the things that are still unknown about Wenger graphs. I will start with some of the cases where I have not yet found results for extended Wenger graphs.

For the girth of extended Wenger graphs, $m = 2$, there are two cases remaining:

- characteristic 2
- $p > 2$, $d + 2$ even

The case $p > 2$, $d + 2$ even is an interesting case. It essentially asks the following question: Given a set of polynomials $x^n + ax + b \in \mathbb{F}_q[x]$, can one with 3 roots in $\mathbb{F}_q$ always be found?

The results for the spectrum of extended Wenger graphs are incomplete. For eigenvalues with $i < m$, Theorem 5.7 states that the multiplicity is positive, but it would be nice to have a formula for the multiplicity. It would also be nice to have results in the $i \geq m$ case. To make progress, a result about polynomials similar to the one needed for the girth seems to be required.

I have recently become aware of a paper by Cesaratto et al. [8] which seems to address this question about roots of polynomials. Specifically, consider the set of monic polynomials of degree n in $\mathbb{F}_q[x]$. Let $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_n)$ be a set of positive integers satisfying $\lambda_1 + 2\lambda_2 + \cdots + n\lambda_n = n$. A polynomial is said to have factorization pattern λ if it has exactly λ_i irreducible factors with degree i, $1 \leq i \leq n$. Let $T(\lambda)$ be the proportion of permutations in S_n with cycle pattern λ (i.e. permutations which are the product of λ_i disjoint cycles of length i). Let A be the subset of monic polynomials of degree n with the coefficients of $x^{i_1}, x^{i_2}, \ldots, x^{i_m}$ fixed (so $|A| = q^{n-m}$), and A_λ the subset of A with factorization pattern λ. Then their result is:

$$|A_\lambda| = T(\lambda)q^{n-m} + O(q^{n-m-1})$$

where the constant implied by $O(q^{n-m-1})$ is given in terms of λ and $i_1, i_2, \ldots, i_m$.

The authors of [8] use methods from algebraic geometry to get some of their results. Even if their results are not directly applicable, it might be useful to think of the problem differently, i.e. instead of counting polynomials in a subset of $\mathbb{F}_q[x]$ with a given number of roots, think about counting $\mathbb{F}_q$-rational points on an algebraic variety.

There are a few questions that would be good to answer about existing versions of Wenger graphs:

- The diameter of most Wenger graphs is known, which gives the maximum distance from vertex to vertex, but what is the distribution of distances between vertices? For any even number between 2 and the diameter, is there always a pair of vertices with that distance?
- Under what circumstances is a Wenger graph Hamiltonian? There are a few results in the literature, but they are not extensive. Is there an example of a non-Hamiltonian Wenger graph?

- There is little known about the automorphism groups of Wenger graphs.
- As far as I know, there are no results on the spectrum of jumped Wenger graphs.

There is a natural connection between Wenger graphs and certain linear codes. For example, Theorem 3.1 can be interpreted in terms of the Hamming weight enumerator of a certain Reed-Solomon code. Many of the references mention coding as a possible application for Wenger graphs, and the paper by Yan and Liu [53] takes advantage of this connection to prove results for both Reed-Solomon codes and Wenger graphs. This is an interesting topic for future study.

The defining equations of the graphs can be generalized. First, allow the use of any power of p_1, so the equations become:

$p_2 + l_2 = l_1 p_1^{e_2}$

$p_3 + l_3 = l_1 p_1^{e_3}$

$\vdots$

$p_{m+1} + l_{m+1} = l_1 p_1^{e_{m+1}}$

with the exponents e_i being any nonnegative integers.

The theorem that gives a cycle of length 8, Theorem 5.2, is at this level of generality.

Note that if two of the powers are the same, there are just q copies of the graph without one of the redundant powers. For example, if we have equations $l_3 + p_3 = l_1 p_1^5$ and $l_4 + p_4 = l_1 p_1^5$, then $l_3 - l_4 = -(p_3 - p_4)$, so that this is a constant over a connected component. Thus, there is a connected component for each possible value.

The following is an example to show how vertices are connected with this type of graph. Let $q = 7$ and $m = 5$. So the vertices correspond to 5-tuples of elements taken from $\mathbb{F}_7$, giving

$2 * 7^5 = 33614$ vertices. The following equations will be used to define an edge:

$p_2 + l_2 = l_1 p_1^5$

$p_3 + l_3 = l_1 p_1$

$p_4 + l_4 = l_1 p_1^4$

$p_5 + l_5 = l_1 p_1^3$

Table 7.1 lists the edges connected to an example "L" vertex and an example "P" vertex.

$$\text{connections to } P_1 = \begin{pmatrix} 4 \\ 3 \\ 2 \\ 4 \\ 2 \end{pmatrix}$$

$p_1^5 = 2 \quad p_1 = 4 \quad p_1^4 = 4 \quad p_1^3 = 1$

l_1	$l_i + p_i$	L-vertex
0	0000	(04535)
1	2441	(16206)
2	4112	(21640)
3	6553	(33311)
4	1224	(45052)
5	3665	(50423)
6	5336	(62164)

$$\text{connections to } L_1 = \begin{pmatrix} 2 \\ 1 \\ 6 \\ 4 \\ 0 \end{pmatrix}$$

	$l_1 f_i(p_1) =$				
p_1	$2p_1^5$	$2p_1$	$2p_1^4$	$2p_1^3$	P-vertex
0	0	0	0	0	(06130)
1	2	2	2	2	(11352)
2	1	4	4	2	(20502)
3	3	6	1	5	(32045)
4	4	1	1	2	(43242)
5	6	3	4	5	(55405)
6	5	5	2	5	(64655)

Table 7.1: Edges connected to two example vertices

Now a path will be calculated between two vertices, specifically a path of length 10 between

the vertices $L_0 = \begin{pmatrix} 1 \\ 6 \\ 1 \\ 1 \\ 2 \end{pmatrix}$ and $L_5 = \begin{pmatrix} 5 \\ 2 \\ 5 \\ 1 \\ 3 \end{pmatrix}$. The calculation is done two steps at a time, using the combined equations $l_k - l'_k = (l_1 - l'_1)f_k(p_1)$. Define $f_1(x)$ to be the constant 1 function, so the values for $f_k(p_1)$ are in Table 7.2.

		p_1						
k	$f_k(x)$	0	1	2	3	4	5	6
1	1	1	1	1	1	1	1	1
2	x^5	0	1	4	5	2	3	6
3	x	0	1	2	3	4	5	6
4	x^4	0	1	2	4	4	2	1
5	x^3	0	1	1	6	1	6	6

Table 7.2: Values of $f_k(p_1)$

These columns are a spanning set of $\mathbb{F}_7^5$, so there is a path. The difference between the start and end vector is $L_5 - L_0 = \begin{pmatrix} 4 \\ 3 \\ 4 \\ 0 \\ 1 \end{pmatrix}$. This can be expressed as:

$$\begin{pmatrix} 4 \\ 3 \\ 4 \\ 0 \\ 1 \end{pmatrix} = 4 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + 5 \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} + 3 \begin{pmatrix} 1 \\ 4 \\ 2 \\ 2 \\ 1 \end{pmatrix} + 3 \begin{pmatrix} 1 \\ 5 \\ 3 \\ 4 \\ 6 \end{pmatrix} + 3 \begin{pmatrix} 1 \\ 2 \\ 4 \\ 4 \\ 1 \end{pmatrix}$$

The rest of the calculations are in Table 7.3.

coefficients $= l_1^{(k)} - l_1^{(k-1)}$

$$\begin{array}{lcccccc} & 4 & 5 & 3 & 3 & 3 & \\ l_1 = & 1 & 5 & 3 & 6 & 2 & 5 \end{array}$$

vectors $\rightarrow p_1$ values 0, 1, 2, 3, 4

Path:

L_0	P_0	L_1	P_1	L_2	P_2	L_3	P_3	L_4	P_4	L_5
1	0	5	1	3	2	6	3	2	4	5
6	1	6	6	4	1	2	0	3	1	2
1	6	1	4	6	0	5	6	0	1	5
1	6	1	4	6	0	5	5	3	5	1
2	5	2	3	0	3	3	5	0	2	3

Table 7.3: Calculations for path from L_0 to L_5

The next level of generalization is from powers of p_1 to any function of p_1, and the equations become:

$p_2 + l_2 = l_1 f_2(p_1)$

$p_3 + l_3 = l_1 f_3(p_1)$

$\vdots$

$p_{m+1} + l_{m+1} = l_1 f_{m+1}(p_1)$

There has been some progress in evaluating the spectrum of a Wenger graph in this case. This proposition is from [7].

Proposition 7.1. *The general Wenger graph is q-regular, that is, every vertex has degree q.*

Proof. Given a vertex $P = (p_1, p_2, \ldots, p_{m+1})$ and $l_1 \in \mathbb{F}_q$, the rest of the l_k are given by $l_k = l_1 f_k(p_1) - p_k$. Since l_1 can be chosen freely, there are q L-vertices connected to P.

Similarly, given $L = (l_1, l_2, \ldots, l_{m+1})$ and $p_1 \in \mathbb{F}_q$, the rest of the p_k are given by $p_k = l_1 f_k(p_1) - l_k$. □

The main theorem about eigenvalues and roots of polynomials, Theorem 5.5, and the theorem giving an upper bound on the diameter, Theorem 5.1, are at this level of generality.

Unless all the functions are constant, the girth is less than or equal to 8. Table 7.4 gives the calculation. Since not all the functions are constant, there are p_0 and p_1 such that for some i, $f_i(p_0) \neq f_i(p_1)$. So the path in Table 7.4, is valid if the vertices are distinct. If the characteristic is not 2, this is pretty clear since $f(p_1) - f(p_0)$ is not zero. In characteristic 2, $1 = -1$, but still L_2 and L_4 are distinct, since $f(p_1) - f(p_0) = f(p_1) + f(p_0)$ is not zero.

L_1	P_1	L_2	P_2	L_3	P_3	L_4	P_4	L_1
0	p_1	1	p_0	0	p_1	-1	p_0	0
0	0	$f(p_1)$	$f(p_0)-$ $f(p_1)$	$f(p_1)-$ $f(p_0)$	$f(p_0)-$ $f(p_1)$	$-f(p_0)$	0	0
0	$f(p_1)$	$f(p_0)$	0	0	$-f(p_1)$	$-f(p_0)$	0	

Table 7.4: Cycle of length 8 in generalized Wenger graph

In fact, the girth is 4 if all the functions are constant. If $f_i(x) = c_i$, then a cycle of length 4 is:

$L_1 = (1, 0)$

$P_1 = (0, c_i)$

$L_2 = (0, -c_i)$

$P_2 = (1, c_i)$

$L_1 = (1, 0)$.

The final generalization is to any function of p_1 and l_1. The equations are now:

$p_2 + l_2 = g_2(l_1, p_1)$

$p_3 + l_3 = g_3(l_1, p_1)$

$\vdots$

$p_{m+1} + l_{m+1} = g_{m+1}(l_1, p_1)$

There is a result known for this type of graph. If the girth of the graph with functions $g_2, g_3, \ldots, g_k$ is known to be g, then the girth of the graph with functions $g_2, g_3, \ldots, g_k, g_{k+1}, \ldots, g_m$ is at least g, regardless of how the functions $g_{k+1}, \ldots, g_m$ are chosen[36]. Theorem 5.3 also compares paths in smaller graphs to those in larger graphs.

Bibliography

[1] James Alexander. *Selected results in combinatorics and graph theory.* PhD thesis, University of Delaware, 2016.

[2] Clark T Benson. Minimal regular graphs of girth eight and twelve. *Canad. J. Math*, 18(1):94, 1966.

[3] Greg Bodwin, Michael Dinitz, Merav Parter, and Virginia Vassilevska Williams. Optimal vertex fault tolerant spanners (for fixed stretch). *arXiv preprint arXiv:1710.03164*, 2017.

[4] J Bondy and U Murty. Graph theory (graduate texts in mathematics vol 244), 2008.

[5] John A Bondy and Miklós Simonovits. Cycles of even length in graphs. *Journal of Combinatorial Theory, Series B*, 16(2):97–105, 1974.

[6] William G Brown. On graphs that do not contain a thomsen graph. *Canad. Math. Bull*, 9(2):1–2, 1966.

[7] Xiwang Cao, Mei Lu, Daqing Wan, Li-Ping Wang, and Qiang Wang. Linearized wenger graphs. *Discrete Mathematics*, 338(9):1595–1602, 2015.

[8] Eda Cesaratto, Guillermo Matera, and Mariana Pérez. The distribution of factorization patterns on linear families of polynomials over a finite field. *Combinatorica*, 37(5):805–836, 2017.

[9] Denis X Charles, Kristin E Lauter, and Eyal Z Goren. Cryptographic hash functions from expander graphs. *Journal of Cryptology*, 22(1):93–113, 2009.

[10] Xiaoyan Cheng, Wenbing Chen, and Yuansheng Tang. On the conjecture for the girth of the bipartite graph d (k, q). *Discrete Mathematics*, 339(9):2384–2392, 2016.

[11] Xiaoyan Cheng, Yuansheng Tang, and Huaxiong Wang. On a generalization of the bipartite graph $d(k, q)$. *arXiv preprint arXiv:1707.01633*, 2017.

[12] Sebastian M Cioabă, Felix Lazebnik, and Weiqiang Li. On the spectrum of wenger graphs. *Journal of Combinatorial Theory, Series B*, 107:132–139, 2014.

[13] Stephen D Cohen. Polynomial factorisation and an application to regular directed graphs. *Finite Fields and Their Applications*, 4(4):316–346, 1998.

[14] Karl Däubel, Yann Disser, Max Klimm, Torsten Mütze, and Frieder Smolny. Distance-preserving graph contractions. *arXiv preprint arXiv:1705.04544*, 2017.

[15] Vasyl Dmytrenko, Felix Lazebnik, and Jason Williford. On monomial graphs of girth eight. *Finite Fields and Their Applications*, 13(4):828–842, 2007.

[16] Paul Erdös. Extremal problems in graph theory. In Miroslav Fiedler, editor, *Theory of Graphs and its Applications*. Academic Press, New York, 1964.

[17] Vyacheslav Futorny and Vasyl Ustimenko. On small world semiplanes with generalised schubert cells. *Acta Applicandae Mathematicae*, 98(1):47–61, 2007.

[18] Dániel Gerbner, Ervin Győri, Abhishek Methuku, and Máté Vizer. Generalized turán problems for even cycles. *arXiv preprint arXiv:1712.07079*, 2017.

[19] António Girão, Teeradej Kittipassorn, and Kamil Popielarz. Partite saturation of complete graphs. *arXiv preprint arXiv:1708.01607*, 2017.

[20] Lior Gishboliner and Asaf Shapira. A generalized turán problem and its applications. *arXiv preprint arXiv:1712.00831*, 2017.

[21] Oded Goldreich. Candidate one-way functions based on expander graphs. *IACR Cryptology ePrint Archive*, 2000:63, 2000.

[22] Shlomo Hoory, Nathan Linial, and Avi Wigderson. Expander graphs and their applications. *Bulletin of the American Mathematical Society*, 43(4):439–561, 2006.

[23] Sina Jafarpour, Weiyu Xu, Babak Hassibi, and Robert Calderbank. Efficient and robust compressed sensing using optimized expander graphs. *IEEE Transactions on Information Theory*, 55(9):4299–4308, 2009.

[24] Arnold Knopfmacher and John Knopfmacher. Counting polynomials with a given number of zeros in a finite field. *Linear and Multilinear Algebra*, 26(4):287–292, 1990.

[25] Dániel Korándi and Benny Sudakov. Saturation in random graphs. *Random Structures & Algorithms*, 51(1):169–181, 2017.

[26] Thomas Lam. Graphs without cycles of even length. *Bulletin of the Australian Mathematical Society*, 63(3):435–440, 2001.

[27] Thomas Lam. A result on 2k-cycle free bipartite graphs. *Australasian Journal of Combinatorics*, 32:163–170, 2005.

[28] Felix Lazebnik, Shuying Sun, and Ye Wang. Some families of graphs, hypergraphs and digraphs defined by systems of equations: a survey. *Lecture Notes of Seminario Interdisciplinare di Matematica, vol. 14*, pages 105–142, 2017.

[29] Felix Lazebnik and Vasiliy Ustimenko. Some algebraic constructions of dense graphs of large girth and of large size. *DIMACS series in Discrete Mathematics and Theoretical Computer Science*, 10:75–93, 1993.

[30] Felix Lazebnik and Vasiliy A Ustimenko. New examples of graphs without small cycles and of large size. *European Journal of Combinatorics*, 14(5):445–460, 1993.

[31] Felix Lazebnik and Vasiliy A Ustimenko. Explicit construction of graphs with an arbitrary large girth and of large size. *Discrete Applied Mathematics*, 60(1-3):275–284, 1995.

[32] Felix Lazebnik, Vasiliy A Ustimenko, and Andrew J Woldar. Properties of certain families of 2k-cycle-free graphs. *Journal of Combinatorial Theory, Series B*, 60(2):293–298, 1994.

[33] Felix Lazebnik, Vasiliy A Ustimenko, and Andrew J Woldar. A new series of dense graphs of high girth. *Bulletin of the American mathematical society*, 32(1):73–79, 1995.

[34] Felix Lazebnik and Raymond Viglione. An infinite series of regular edge-but not vertex-transitive graphs. *Journal of Graph Theory*, 41(4):249–258, 2002.

[35] Felix Lazebnik and Ye Wang. On some cycles in wenger graphs. *Acta Math. Appl. Sin. Engl., to appear*, 5, 2014.

[36] Felix Lazebnik and Andrew J Woldar. General properties of some families of graphs defined by systems of equations. *Journal of Graph Theory*, 38(2):65–86, 2001.

[37] Jiyou Li and DaQing Wan. A new sieve for distinct coordinate counting. *Science China Mathematics*, 53(9):2351–2362, 2010.

[38] Alexander Lubotzky. Expander graphs in pure and applied mathematics. *Bulletin of the American Mathematical Society*, 49(1):113–162, 2012.

[39] Aleksander Malnič, Dragan Marušič, Primož Potočnik, and Changqun Wang. An infinite family of cubic edge-but not vertex-transitive graphs. *Discrete Mathematics*, 280(1):133–148, 2004.

[40] Aleksander Malnič, Dragan Marušič, and Changqun Wang. Cubic edge-transitive graphs of order 2p 3. *Discrete Mathematics*, 274(1):187–198, 2004.

[41] Monika Polak and Vasyl Ustimenko. Examples of ramanujan and expander graphs for practical applications. In *Computer Science and Information Systems (FedCSIS), 2013 Federated Conference on Computer Science and Information Systems*, pages 499–505. IEEE, 2013.

[42] Istvan Reiman. Über ein problem von k. zarankiewicz. *Acta Mathematica Hungarica*, 9(3-4):269–273, 1958.

[43] Jia-yu Shao, Chang-xiang He, and Hai-ying Shan. The existence of even cycles with specific lengths in wengers graph. *Acta Mathematicae Applicatae Sinica, English Series*, 24(2):281–288, 2008.

[44] Jacques Verstraëte. Extremal problems for cycles in graphs. In *Recent Trends in Combinatorics*, pages 83–116. Springer, 2016.

[45] Raymond Viglione. *Properties of some Algebraically Defined Graphs*. PhD thesis, University of Delaware, 2002.

[46] Raymond Viglione. On the diameter of wenger graphs. *Acta Applicandae Mathematicae*, 104(2):173–176, 2008.

[47] Li-Ping Wang, Daqing Wan, Weiqiong Wang, and Haiyan Zhou. On jumped wenger graphs. *arXiv preprint arXiv:1702.03102*, 2017.

[48] Ye Wang. On some cycles in linearized wenger graphs. *Discrete Mathematics*, 340(12):2782–2788, 2017.

[49] Eric W. Weisstein. "Gray Graph." From MathWorld—A Wolfram Web Resource. `http://mathworld.wolfram.com/GrayGraph.html` Last visited on Feb. 2, 2018.

[50] Eric W. Weisstein. "Königsberg Bridge Problem." From MathWorld—A Wolfram Web Resource. `http://mathworld.wolfram.com/KoenigsbergBridgeProblem.html` Last visited on Dec. 22, 2017.

[51] Rephael Wenger. Extremal graphs with no c4's, c6's, or c10's. *Journal of Combinatorial Theory, Series B*, 52(1):113–116, 1991.

[52] Weiyu Xu and Babak Hassibi. Efficient compressive sensing with deterministic guarantees using expander graphs. In *Information Theory Workshop, 2007. ITW'07. IEEE*, pages 414–419. IEEE, 2007.

[53] Haode Yan and Chunlei Liu. Linearized reed-solomon codes and linearized wenger graphs. *arXiv preprint arXiv:1502.01885*, 2015.

[54] Haode Yan and Chunlei Liu. A note on the spectrum of linearized wenger graphs. *Discrete Mathematics*, 340(5):1050–1053, 2017.