A Generalization of Cayley Graphs for Finite Fields

Dawn M. Jones
Western Michigan University

Follow this and additional works at: https://scholarworks.wmich.edu/dissertations

Part of the Algebra Commons, and the Applied Mathematics Commons

Recommended Citation
https://scholarworks.wmich.edu/dissertations/1553

This Dissertation-Open Access is brought to you for free and open access by the Graduate College at ScholarWorks at WMU. It has been accepted for inclusion in Dissertations by an authorized administrator of ScholarWorks at WMU. For more information, please contact wmu-scholarworks@wmich.edu.
A GENERALIZATION OF CAYLEY GRAPHS
FOR FINITE FIELDS

by

Dawn M. Jones

A Dissertation
Submitted to the
Faculty of The Graduate College
in partial fulfillment of the
requirements for the
Degree of Doctor of Philosophy
Department of Mathematics
and Statistics

Western Michigan University
Kalamazoo, Michigan
August 1998
A central question in the area of topological graph theory is to find the genus of a given graph. In particular, the genus parameter has been studied for Cayley graphs. A Cayley graph is a representation of a group and a fixed generating set for that group. A group is said to be planar if there is a generating set which produces a planar Cayley graph. We say that a group is toroidal if there is a generating set that produces a toroidal Cayley graph and if there are no generating sets which produce a planar Cayley graph. Characterizations for the planar finite groups and the toroidal groups are known. In this dissertation we study graphs which model another algebraic structure, namely, the finite field.

A graph which models a finite field is called a generalized Cayley graph. This graph is produced by taking a generating set for the finite field which consists of the standard basis of additive generators for a single fixed multiplicative generator. We characterize those finite fields that have multiplicative generators which yield planar graphs. We also
characterize the toroidal finite fields. To accomplish these tasks we first obtain a genus bound for the prime order finite fields. To do this we find a bound for the number of $i$-sided regions for $1 \leq i \leq 4$. Next, we use known genus results for certain classes of graphs to get bounds for the remaining finite fields. We also use these genus results to rule out potential planar and toroidal finite fields. To complete the characterizations we use various ad hoc methods.

In addition, we find the maximum genus for all generalized Cayley graphs for finite fields and, in the process, we show that the maximum genus is independent of the multiplicative generator for that finite field. In general, finding the genus of a finite field is not easy. However, we present some asymptotic results for the genus of certain classes of finite fields. We also prove that there is a finite number of finite fields, for each given genus.
INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.
ACKNOWLEDGMENTS

There are so many people who have helped me over the past five years that I cannot possibly list them all. First, I would like to thank my family for all the love and support they have given me throughout my life. My parents Lynda and Joseph and my step-mother Susan have been a great source of guidance and for that I thank them. I thank my wonderful in-laws Robert and Anita as well. I would also like to recognize my brothers and sisters Gerard, Julie, Lori, Joseph and Sara. I am grateful for the love and support of my grandparents as well: Frederick, Ruth, Lyndsay, Edith, Paul, Shirley, Charles and Hannalore.

Secondly, I wish to express my gratitude for the friends that have helped me along the way. A special thanks is owed to Esther Tesar who is like a big sister to me; she gave me advice and guidance since the first day I arrived at Western. I owe a special thanks to Ramón Figueroa-Centeno. He is responsible for the wonderful figures which are found in this dissertation. I would also like to thank Margo and Pearl who helped me keep a clear head, especially in these last few months. I am especially grateful to all my friends in Tae Kwon Do. I wish I could list them all, but I am fortunate in that there are too many to count.
Acknowledgments-continued

Thanks also to the teachers and mentors that I have had along the way. I am grateful for the advice and guidance I have received from my advisor Arthur T. White. I feel very fortunate that I have been able to do research under his direction. I also appreciate the guidance of Yousef Alavi who has given me many opportunities to use my talents. Thanks also to the other members of my committee John Martino and Ping Zhang who gave me a lot of advice and support along the way. Finally, I wish to thank Gary Chartrand, Allen Schwenk and John Petro for the many ways in which they have helped me.

Lastly, I wish to thank my husband Michael who has been my greatest source of inspiration and support. There are no words to express how fortunate I am to have him in my life. Thanks also to Alexander for waiting to be born until this dissertation was done.

Dawn M. Jones
# TABLE OF CONTENTS

ACKNOWLEDGMENTS................................................................................................. ii

LIST OF TABLES.................................................................................................... vi

LIST OF FIGURES................................................................................................... vii

CHAPTER

I. INTRODUCTION ................................................................................................ 1

  1.1 History........................................................................................................ 1

  1.2 Graph Theory Definitions........................................................................ 2

  1.3 Topological Graph Theory......................................................................... 4

  1.4 Cayley Color Graphs and the Genus of a Group ............................... 11

  1.5 Field Theory: Definitions and Results.................................................. 16

  1.6 Generalized Cayley Graphs................................................................. 17

II. STRUCTURALRESULTS AND VARIOUS PARAMETERS................................... 20

  2.1 Various Parameters................................................................................ 20

  2.2 The Chromatic Number and Edge Chromatic Number....................... 26

  2.3 Automorphism Groups........................................................................... 29

III. THE PLANAR FINITE FIELDS........................................................................ 35

  3.1 Genus Bounds for Finite Fields............................................................ 35

  3.2 The Characterization of the Planar Finite Fields............................... 55
Table of Contents—continued

CHAPTER

IV. THE TOROIDAL FINITE FIELDS ................................................................. 61
  4.1 The Genus of $\mathbb{F}_{39}$ Is 2 ......................................................... 61
  4.2 The Genus of $\mathbb{F}_{23}$ Is at Least 2 .................................. 79
  4.3 The Characterization of the Toroidal Finite Fields ......................... 84

V. OTHER GENUS RESULTS ........................................................................ 88
  5.1 Asymptotic Results ................................................................. 88
  5.2 The Maximum Genus of a Finite Field .................................. 92
  5.3 Finite Number of Finite Fields of a Given Genus ....................... 94

VI. CONCLUSIONS .................................................................................... 97
  6.1 Conclusions and Open Problems ........................................... 97

APPENDICES

  A. Rotational Imbedding Schemes for $\mathbb{F}_8$, $\mathbb{F}_{11}$, and $\mathbb{F}_{13}$ .... 101
  B. The Graphs $\mathcal{C}(\mathbb{F}_{19}, g)$ and $\mathcal{C}(\mathbb{F}_{23}, g)$ ................. 105
  C. Rotational Imbedding Schemes for $\mathbb{F}_{19}$ .............................. 114

REFERENCES ............................................................................................ 118
LIST OF TABLES

1. The Element $\alpha$ as a Generator of $\mathbb{F}_q^*$ ................................................... 18
2. Possible Region Distributions for $C(\mathbb{F}_{19}, 2) < S_1$ .......................... 72
# LIST OF FIGURES

1. $K_4$ and $K_{2,3}$ are Planar ............................................................... 5
2. The Sphere, the Torus and the Double Torus ..................................... 6
3. An Imbedding of $K_{2,3}$ ................................................................... 9
4. The Cayley Color Graph $C_4(S_3)$ .................................................. 12
5. The Cayley Graph $G_4(S_3)$ ............................................................... 14
6. A Multiplicative Edge in $C(F_q, g)$ .................................................. 18
7. An Additive Edge in $C(F_q, g)$ .......................................................... 18
8. The Graph $C(F_8, \alpha)$ ................................................................. 19
9. The Graph $C(F_2, 1)$ ....................................................................... 21
10. $K_3$ as a Subgraph of $C(F_p, g)$ ...................................................... 22
11. $K_4$ With 4 Multiplicative Edges ..................................................... 23
12. The Graph $C(F_5, 2)$ ...................................................................... 23
13. $K_4$ as in Subcase 2.1 ..................................................................... 24
14. $K_4$ as in Subcase 2.2 ..................................................................... 25
15. $K_4$ With Exactly Two Multiplicative Edges ................................. 25
16. The Graph $C(F_4, \alpha)$ ................................................................. 32
17. An Imbedding of $C(F_{2^r}, \alpha + 1)$ on the Torus .......................... 34
18. An Imbedding of $C(F_{1,7})$ on $S_3$ ............................................... 36
List of Figures–Continued

19. A Subgraph of $C(F_{11}, 2)$ Homeomorphic With $K_{3,3}$................................. 37
20. A Digon With Two Multiplicative Edges................................................................. 38
21. The Graph $C(F, 2)$.................................................................................................. 38
22. Two Digons With Two Distinct Additive Generators............................................ 39
23. A Digon With Two Additive Edges and the Same Generator.............................. 39
24. Two Digons With One Additive and One Multiplicative Generator........................ 40
25. The 3-cycle as in Subcase 1.1 ................................................................................ 41
26. The 3-cycles as in Subcase 1.2 .............................................................................. 42
27. The 3-cycle as in Subcase 1.3 .............................................................................. 42
28. The 3-cycles as in Subcase 2.1 .............................................................................. 43
29. The 3-cycle as in Subcase 2.2 .............................................................................. 44
30. The 3-cycles as in Case 3.................................................................................... 45
31. The 4-cycles as in Case 1.................................................................................... 47
32. The 4-cycle as in Subcase 2.1 .............................................................................. 47
33. The 4-cycle as in Subcase 2.2 .............................................................................. 48
34. The 4-cycle as in Subcase 2.3 .............................................................................. 48
35. The 4-cycle as in Subcase 2.4 .............................................................................. 49
36. The 4-cycle as in Subcase 2.5 .............................................................................. 49
37. A 4-cycle as in Subcase 2.6 .............................................................................. 50
List of Figures—Continued

38. Another 4-cycle as in Subcase 2.6........................................................... 50
39. The 4-cycle as in Case 3............................................................................ 51
40. Imbeddings of $C(\mathbb{F}_2, 1)$, $C(\mathbb{F}_3, 2)$ and $C(\mathbb{F}_5, 2)$ on $S_0$........ 51
41. A Subgraph of $C(\mathbb{F}_8, \alpha)$ ............................................................. 56
42. A Subgraph of $C(\mathbb{F}_8, \alpha^2)$ .............................................................. 57
43. A Subgraph of $C(\mathbb{F}_8, \alpha^3)$ .............................................................. 57
44. A Subgraph of $C(\mathbb{F}_{13}, 2)$................................................................. 58
45. A Subgraph of $C(\mathbb{F}_{13}, 6)$................................................................. 58
46. An Imbedding of $C(\mathbb{F}_7, 3)$................................................................. 59
47. Two Copies of $K_{2,3}$ in $C(\mathbb{F}_{19}, 3)$.................................................... 62
48. Two Copies of $K_{2,3}$ in $C(\mathbb{F}_{19}, 14)$.................................................... 63
49. A Partial Imbedding of $C(\mathbb{F}_{19}, 3)$....................................................... 67
50. A Partial Imbedding of $C(\mathbb{F}_{19}, 3)$ With $\rho_{12} = (17, 13, 11, 4)$........ 68
51. The 4-sided Regions in $C(\mathbb{F}_{19}, 2)$....................................................... 70
52. A Partial Imbedding of $C(\mathbb{F}_{19}, 2)$....................................................... 73
53. Another Partial Imbedding of $C(\mathbb{F}_{19}, 2)$............................................. 74
54. 16-13-7-8-16 is Not a 4-sided Region......................................................... 75
55. Some Regions Containing Vertex 6............................................................ 76
56. 13-7-6-12-12 and Other 4-sided Regions.................................................. 77
List of Figures--Continued

57. The Regions for Case 2 ................................................................. 77
58. The Regions for Case 3 ................................................................. 78
59. The Regions for Case 4 ................................................................. 78
60. The Triangles in C(F_{23}, 11) ...................................................... 81
61. The 4-sided Regions for $g = 5, 15, \text{ and } 17$ ..................... 82
62. The 3-gons and 4-gons in C(F_{23}, 7) ......................................... 82
63. A Digon Replaced With an Edge .............................................. 89
CHAPTER I

INTRODUCTION

1.1 History

Topological graph theory is an area of graph theory that has been widely studied. Many teachers introduce the subject of topological graph theory by asking if a given graph is planar, that is, by asking if it is possible to draw (or imbed) a given graph in the plane in such a way that none of its edges cross. This is a classical question and we will give examples of this phenomenon in the upcoming section on topological graph theory.

It has long been known that we can model the algebraic structure called a group by a graph that we call the Cayley color graph, or simply Cayley graph, of the group. Another classical question that has been studied asks which of these groups have a Cayley graph that is planar. Of course there are many other questions that could be asked and we will address these later.
1.2 Graph Theory Definitions

We start by reviewing some basic graph theory definitions. For a more complete treatment see Chartrand and Lesniak [5], or White [17].

A graph, denoted by $G$, is a finite nonempty set of vertices, denoted by $V(G)$, together with a set of unordered pairs of vertices called edges, denoted by $E(G)$. The cardinality of the vertex set is the order of a graph and the size of a graph refers to the cardinality of the edge set. Two vertices, $u$ and $v$, of a graph are said to be adjacent if there is an edge between them, say $e = \{u, v\}$. Two edges are said to be adjacent if they share a common vertex. The set of vertices that are adjacent to a vertex $v$ is called the neighborhood of $v$ and is denoted by $N(v)$. We say that the vertex $u$ is incident with the edge $e$, as is the vertex $v$. The degree of a vertex $v$, denoted by $\deg(v)$, is the number of edges incident with vertex $v$. If each vertex in a graph has the same degree, say $\deg(v) = r$, we say that the graph is regular of degree $r$, or simply regular. The maximum degree among the vertices of $G$ is given by $\Delta(G)$. The minimum degree among the vertices of $G$ is given by $\delta(G)$. A loop is an edge of the form $\{v, v\}$. A multiple edge is an edge that appears more than once in $E(G)$. A multigraph is a graph where we allow multiple edges. We say that a graph is a pseudograph if we allow multiple edges and loops. A directed edge or arc is an ordered pair of vertices. A directed graph or digraph has every
edge directed. The multigraph graph corresponding to the digraph with all the directions deleted is referred to as the underlying graph.

A walk in a graph is an alternating sequence of vertices and edges which starts and ends with a vertex and such that each edge is incident with the two vertices immediately preceding and following it. A path is a walk in the graph such that no vertex is repeated. We say that a graph is connected if there is a path between every pair of vertices in the graph. The distance, \(d(u, v)\), between two vertices \(u\) and \(v\) is the length of a shortest path joining them, if such a path exists. If no such path exists we say that \(d(u, v) = \infty\).

If every two vertices in a graph are adjacent we say that the graph is a complete graph. A complete graph of order \(n\) is denoted by \(K_n\). A graph is called a bipartite graph if it is possible to partition the vertex set into two disjoint sets, called partite sets, such that every edge is incident to a vertex from each partite set. A complete bipartite graph is a bipartite graph such that there is an edge between every two vertices that are from different partite sets. If the partite sets of a complete bipartite graph have orders \(a\) and \(b\), then we denote the graph by \(K_{a,b}\).

There are many ways to create a new graph from a given graph. Let \(G\) be a graph. If \(e\) is an edge of \(G\), then the graph \(G - e\) is the graph with vertex set \(V(G)\) and with edge set \(E(G) - \{e\}\). Let \(v\) be a vertex of \(G\). By the graph \(G - v\) we mean the graph with vertex set \(V(G) - v\) and edge set \{\(e \in E(G) | e \neq v\}\).
$E(G)$: $e$ is not incident with $v$. Now suppose $G$ is a nonempty graph. The
line graph $L(G)$ of $G$ is the graph whose vertices can be put in one-to-one
 correspondence with the edges of $G$ in such a way that two vertices of
$L(G)$ are adjacent if and only if the corresponding edges of $G$ are adjacent.

Let $H$ be a graph. The cartesian product $G \times H$ has $V(G \times H) = V(G) \times
V(H)$, and two vertices $(g_1, h_1)$ and $(g_2, h_2)$ of $G \times H$ are adjacent if and
only if

$$g_1 = h_1 \text{ and } h_1 h_2 \in E(H)$$

or

$$g_2 = h_2 \text{ and } g_1 g_2 \in E(G).$$

An important class of graphs is defined using the cartesian product. The $n$-
cube $Q_n$ is the graph $K_2$ if $n = 1$, while for $n > 1$, $Q_n$ is defined recursively
as $Q_{n-1} \times K_2$. The cycle on $n$ vertices is denoted by $C_n$. The repeated
cartesian product of $t$ such $n$-cycles is denoted by $(C_n)^t$.

1.3 Topological Graph Theory

In Section 1.1 we mentioned one of the central questions in
topological graph theory, that is, the question of whether or not a given
graph is planar. Now we turn to define this and many other concepts. A
graph is said to be planar if it is possible to draw the graph in the plane so
that the edges only intersect at their common vertices. In such a case we say that the graph is *imbedded* in the plane. Later we shall give a careful definition of the term *imbedding*. Below we show examples of the planar graphs $K_4$ and $K_{3,3}$ in Figure 1. If a graph is imbedded in the plane we call it a *plane* graph.

![Figure 1. $K_4$ and $K_{3,3}$ are Planar.](image)

We see that imbedding a graph in the plane is equivalent to imbedding it on the sphere through the use of stereographic projection (see White [17, p. 45]). We denote the sphere by $S_0$. In general, if $k \geq 0$, the space $S_k$ denotes the surface of genus $k$, which one may think of as a sphere with $k$ handles attached. To be more precise, a *surface* is a 2-manifold. In Figure 2 below we show the sphere $S_0$, the torus $S_1$, and the double torus $S_2$. 

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
Now we carefully define the term "imbedding". We say that a graph $G$ *imbeds* on $S_k$ if there exists a homeomorphism of $G$ as a finite 1-complex in $\mathbb{R}^3$ with a subspace of $S_k$. If a pseudograph $G$ is imbedded on a surface $S_k$, the components of $S_k - (\text{image of } G)$ are called *regions*. A region is a 2-cell if it is homeomorphic to 2-dimensional Euclidean space (equivalently, to an open disk). If every region in an imbedding is a 2-cell, then we say that it is a 2-cell imbedding. If $G$ is 2-cell imbedded on $S_k$ then we write $G \preceq S_k$. It is clear that no imbedding of a disconnected graph is a 2-cell imbedding. From now on all imbeddings will be 2-cell imbeddings.

In Figure 1, our imbedding of $K_4$ has $n = 4$, $m = 6$ and $r = 4$, where $n$, $m$, and $r$ refer to the order, size and the number of regions, respectively. We note that when we calculate the value of the expression $n - m + r$ we obtain 2. In fact, the value of that expression will always equal 2 for a graph imbedded on the sphere. This phenomenon is not
restricted to the sphere, in fact, we have the following more general result below.

**Theorem 1.A** If $G$ is a connected graph of order $n$ and size $m$ that is imbedded on $S_k$ with $r$ regions, then

\[(1.1) \quad n - m + r = 2 - 2k.\]

We refer to equation (1.1) as Euler's identity [7]. The constant value $2 - 2k$ is called the Euler characteristic or simply the characteristic of the surface $S_k$. Quite often we wish to find the genus of the surface on which $G$ has been imbedded, so we solve for $k$ in the Euler identity to get

\[(1.2) \quad k = 1 + \frac{1}{2}(m - n - r),\]

which we will refer to as Euler's Formula.

The genus of a pseudograph $G$, denoted by $\gamma(G)$, is the minimum nonnegative integer $k$ such that $G$ imbeds on $S_k$. We have seen that $K_4$ can be imbedded on the sphere and so $\gamma(K_4) = 0$. If a connected pseudograph $G$ has been imbedded on $S_{\chi(G)}$, then, necessarily, the imbedding is a 2-cell imbedding (see [19]). The genus parameter has been determined for many classes of graphs. In particular Ringel and Youngs [13] have found this parameter for the complete graphs. The genus of the
n-cube has been found by both Ringel [14] and Beineke and Harary [1]. We state these here for future reference.

**Theorem 1.B** For \( n \geq 3 \), \( \gamma(K_n) = \frac{(n-3)(n-4)}{12} \).

**Theorem 1.C** For \( n \geq 2 \), \( \gamma(Q_n) = 1 + 2^{n-3}(n-4) \).

The previous theorem tells us the genus of a given graph. One may also ask what graphs have a particular genus? In particular which graphs are planar graphs or toroidal graphs; that is, which have genus 0 or 1? In the famous theorem of Kuratowski [9] we know the answer for genus zero as stated below.

**Theorem 1.D** A graph \( G \) is planar if and only if it contains no subgraph homeomorphic with either \( K_5 \) or \( K_{3,3} \).

In general, it is difficult to determine the genus of a graph simply by looking at various drawings. However, we are fortunate in that there is an algebraic way of describing 2-cell imbeddings of graphs. For a connected graph \( G \), a rotational imbedding scheme (or simply a rotation scheme) \( \mathcal{P} \) is a collection of cyclic permutations \( \rho_v : N(v) \to N(v) \) for each \( v \in V(G) \), where \( N(v) \) denotes the neighborhood of \( v \). For example, let us consider the 2-cell imbedding of the graph \( K_{2,3} \) shown in Figure 3. We find that the rotation scheme is given by

\[
\mathcal{P} = \{ \rho_1 = (2, 4, 3), \rho_2 = \rho_3 = \rho_4 = (1, 5), \rho_5 = (2, 3, 4) \},
\]
where we have imposed a clockwise orientation on $S_0$.

Figure 3. An Imbedding of $K_{2,3}$.

We can see that a 2-cell imbedding of a labeled graph yields a rotation scheme. As it turns out, the converse is also true. That is, for a connected graph $G$ with $V(G)=\{1, 2, \ldots, n\}$, each collection $\{\rho_i: N(i)\to N(i) \mid 1 \leq i \leq n\}$ of cyclic permutations determines a 2-cell imbedding of $G$ on some surface. To find the genus we trace out the region boundaries and then use Euler's formula. For more details on this process including examples see White [17, p. 70]. Thus, there is a one-to-one correspondence between 2-cell imbeddings of $G$ and the rotation schemes of the graph. This result is due to Edmonds [6].

**Theorem 1.E** Let $G$ be a connected graph with $V(G)=\{1, 2, \ldots, n\}$. If $G$ is imbedded on $S_k$, then this 2-cell imbedding uniquely determines a rotation scheme $\mathcal{P} = \{\rho_i: N(i)\to N(i) \mid 1 \leq i \leq n\}$. Conversely, each such
rotation scheme uniquely determines a 2-cell imbedding of $G$ on some surface.

Since we can count the number of distinct rotation schemes for a given labeled graph $G$, we know how many different labeled 2-cell imbeddings $G$ has. In fact there are

$$\prod_{i=1}^{n} (\text{deg}(i) - 1)!$$

such imbeddings of $G$. Since there is a finite number of 2-cell imbeddings of a given graph there must be a surface of maximum genus on which the graph can be imbedded. We define the maximum genus, $\gamma_m(G)$, of a graph $G$ to be the maximum genus among all surfaces in which $G$ can be 2-cell imbedded. This parameter has been found for many classes of graphs (see White [17, p. 68]). Fortunately, it is not difficult to determine an upper bound for the maximum genus of a graph.

**Theorem 1.F** Let $G$ be a connected graph of order $n$ and size $m$. Then,

$$\gamma_m(G) \leq \left\lfloor \frac{m - n + 1}{2} \right\rfloor.$$  

Moreover, we have equality if and only if this imbedding has 1 or 2 regions, according as $m - n + 1$ is even or odd, respectively.

A graph $G$ is said to be upper imbeddable if the inequality in equation (1.3) is actually an equality. A splitting tree of a connected graph
$G$ is a spanning tree $T$ for $G$ such that at most one component of $G - E(T)$ has odd size. The following characterization of upper imbeddable graphs is due, independently, to Jungerman [8] and Xuong [18].

**Theorem 1.1** A graph $G$ is upper imbeddable if and only if $G$ has a splitting tree.

There are many other topological parameters that can be associated with a graph. We will introduce these as needed.

1.4 Cayley Color Graphs and the Genus of a Group

Previously we had mentioned the notion of a Cayley color graph and we now carefully define this graph. After this we define what we mean by the genus of a group. Let $\Gamma$ be a finite group and let $\Delta$ be a generating set for $\Gamma$. The vertices of the Cayley color graph correspond to the group elements. To assist in defining the edge set we imagine that the generators of the group have been assigned colors. Let $g_1$ and $g_2$ be two group elements. There is a directed edge in the Cayley color graph from $g_1$ to $g_2$, colored with the color of generator $h$, if and only if $g_1 h = g_2$. We denote the Cayley color graph for the group $\Gamma$ with generating set $\Delta$ by $C_\Delta(\Gamma)$. We note that this is a labeled, directed graph with a color assigned to each edge. Now let us look at an example of a Cayley color graph. Let $\Gamma = S_3$, and let $\Delta = \{a = (123), b = (12)\}$. This graph is depicted in Figure 4 below. Note that this is actually an imbedding of this graph in the sphere, $S_3$. For
a generator $\delta$ of order 2 we shall represent the two directed edges $(g, g\delta)$ and $(g\delta, g)$ in our Cayley color graph with a single undirected edge colored with the color of $\delta$. This may be seen in our example below since the generator $b$ has order 2 in $S_3$.

![Diagram of the Cayley Color Graph $C_3(S_3)$](image)

Figure 4. The Cayley Color Graph $C_3(S_3)$.

Next we wish to define what we mean by the genus of a group. We have already constructed a way to represent groups by graphs. Now we wish to imbed these graphs. However, we notice that these graphs have properties that are not important when discussing topological results. We note our Cayley color graphs have directed edges. We also have the
possibility that our graphs have multiple edges and loops. To avoid such instances we have some requirements for our generating set \( \Delta \) as follows:

(i) \( e \in \Delta \), where \( e \) is the identity element of \( \Gamma \),

(ii) if \( \delta \in \Delta \), then \( \delta^{-1} \in \Delta \), unless \( \delta \) has order two, and

(iii) we also continue to replacing each pair of directed edges \((g, g\delta)\) and \((g\delta, g)\) in our Cayley color graph with a single undirected edge whenever \( \delta \in \Delta \) has order 2.

If we follow these three conventions and if we suppress the colors and directions on the edges of the Cayley color graph we in fact have a graph. So, if our generating set \( \Delta \) satisfies the three conditions above, then the underlying graph of \( C_3(\Gamma) \) is called a Cayley graph and is denoted by \( G_3(\Gamma) \). It is clear that no topological properties are lost. Thus we can use the Cayley graph to define the genus of a group. Below is the Cayley graph of the group \( S_3 \) with the same generating set as the Cayley color graph above (Figure 5). We note that this graph is simply the graph which is given by \( K_2 \times C_3 \).

We define the genus of a group \( \Gamma \) to be

\[ \chi(\Gamma) = \min(\chi(G_3(\Gamma))) \],

where the minimum is taken over all generating sets \( \Delta \) for \( \Gamma \). We have already seen that we have a generating set for \( S_3 \) that yields a planar graph. Thus, \( \chi(S_3) = 0 \). A group \( \Gamma \) is said to be planar if \( \chi(\Gamma)=0 \).
Figure 5. The Cayley Graph $G_3(S_3)$.

It is natural to ask which groups are planar. In particular, which finite groups are planar? This question has been answered by Maschke [10].

**Theorem 1.H** The finite group $G$ is planar if and only if $G \cong G_1 \times G_2$, where $G_1 = \mathbb{Z}$ or $\mathbb{Z}$ and $G_2 = \mathbb{Z}_n, D_n, S_n, A_4$ or $A_5$.

Thus, the planar finite groups have been characterized. We say that a group is *toroidal* if $\gamma(\Gamma) = 1$. It turns out that the toroidal groups have been characterized as well. This task was completed by Proulx [12]. In this dissertation we model another algebraic structure, finite fields, and try to answer similar genus questions. To do this we first need some background information concerning finite fields.
1.5 Field Theory: Definitions and Results

We have just finished our discussion of modeling groups by graphs. Groups are algebraic structures that have one operation. Here we turn our attention to algebraic structures, called finite fields, which have two operations. A division ring is a ring with unity $1 \neq 0$ in which every nonzero element is invertible. A field is a commutative division ring. A finite field is a field with a finite number of elements. Let $R$ be a ring and let $x$ be a variable. We define a ring $R[x]$, called the polynomial ring, as follows. The elements of this ring are formal sums $r_n x^n + r_{n-1} x^{n-1} + \ldots + r_1 x + r_0$, where $t$ is a nonnegative integer and each $r_i \in R$. Rather than writing this sum we simply write $f(x)$. If $r_0 \neq 0$, we say $f(x)$ has degree $t$ and that $r_0$ is its leading coefficient. We add and multiply in this ring in the expected way. A nonzero polynomial $f$ is reducible in $R[x]$ if there are elements $g$ and $h$ in $R[x]$ such that $f = gh$ and such neither $g$ nor $h$ is a unit. We say a polynomial is irreducible if it has positive degree and is not reducible. Now we record some results which may be found in almost any algebra text.

Let $F$ be a finite field. Suppose that $g$ is a polynomial of degree $t$ in $F[x]$. Let $E = F[x]/(g(x))$. If $F$ has $p$ elements, then $E$ has $p'$ elements, the polynomials of degree at most $t - 1$ over $F$. Now, if $F$ is a finite field with $q$ elements and characteristic $p$, then $q = p'^t$, where $t$ is a positive
integer. That is, the order of a finite field is a prime power. To construct a finite field with $p'$ elements we find an irreducible polynomial $\pi(x)$ of degree $t$ in $\mathbb{Z}_p[x]$ and construct $\mathbb{Z}_p[x]/\pi(x)$. As it turns out we may find such a polynomial among the factors of $x^q - x$, where $q = p'$. We also note that for each prime power there is a unique isomorphism class of fields for that prime power. So we refer to a finite field with $p'$ elements as the finite field of order $p'$, denoted by $\mathbb{F}_q$, where $q = p'$. We note that a finite field is also referred to as a Galois Field. We choose to denote the finite field of order $q$ as $\mathbb{F}_q$ rather than $GF(q)$ as it is denoted in many algebra texts.

The set of nonzero elements in a field forms a multiplicative group. If $\mathbb{F}$ is a field we denote the set of nonzero elements by $\mathbb{F}^*$. As we have just mentioned, we construct a finite field $\mathbb{F}$ with $q = p'$ elements by finding an irreducible polynomial of degree $t$ in $\mathbb{Z}_p[x]$. For this polynomial we may find an element $g$ in $\mathbb{F}$ such that $g$ generates $\mathbb{F}^*$. That is, the set of nonzero elements of a finite field forms a cyclic group, under multiplication.

1.6 Generalized Cayley Graphs

Now we are in a position to define what we mean by a generalized Cayley graph. Let $p$ be a prime, $t$ be a positive integer and let $q = p^t$. Let $\mathbb{F}_q$ denote the finite field of order $q$. As we have seen in the previous
section, the set of nonzero elements of a finite field forms a cyclic group. In order to model the multiplicative structure of our finite field we choose a generator $g$ for this cyclic group. To model the additive structure we use the standard basis for $\mathbb{Z}_p^*$ for that multiplicative generator $g$. That is, we use the generating set $\{\alpha^{-i} : 1 \leq i \leq l\}$ to model the additive structure.

The generalized Cayley graph for the finite field $F_q$ is defined as follows. The vertices of our graph correspond to our field elements. Next we think of each generator, as explained above, as associated with distinct colors. Suppose the vertices of our graph $v_1$ and $v_2$ correspond to the field elements $f_1$ and $f_2$. We have two kinds of edges, one kind corresponding to addition, the other to multiplication. There is a directed edge from $v_1$ to $v_2$ colored $g$ if and only if $f_1 g = f_2$ (see Figure 6 below). We shall later refer to this kind of edge as a multiplicative edge. There is an additive edge from $v_1$ to $v_2$ colored $\alpha^i$ if and only if $f_1 + \alpha^i = f_2$ (see Figure 7 below). Since we use the standard basis depending on our multiplicative generator $g$ to model the additive structure, we denote the generalized Cayley graph modeling the finite field of order $q$ by $C(F_q, g)$. We note that $C(F_q, g)$ is a directed psuedograph with labels on both the edge and vertices. The underlying graph of $C(F_q, g)$, that is the graph where we ignore directions and colors on the edges, is denoted by $G(F_q, g)$. 

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
As an example, let us construct a generalized Cayley graph to model the finite field of order $8$. We find $f(x) = x^3 + x + 1$ is an irreducible polynomial. Let $\alpha$ be a root of this polynomial; so that $\alpha^3 = \alpha + 1$; in fact $\alpha$ is a primitive root. As one sees below, $\alpha$ generates $F_8^\times$ (see Table 1.) The graph $C(F_8, \alpha)$ is given in Figure 8. In Chapter II we shall discuss some properties of these graphs, such as the order, size and the degrees of the vertices, just to name a few.

<table>
<thead>
<tr>
<th>$\alpha^i$</th>
<th>$\alpha^j$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha^2$</td>
<td>$\alpha^2$</td>
</tr>
<tr>
<td>$\alpha^3$</td>
<td>$\alpha + 1$</td>
</tr>
<tr>
<td>$\alpha^4$</td>
<td>$\alpha^2 + \alpha$</td>
</tr>
<tr>
<td>$\alpha^5$</td>
<td>$\alpha^2 + \alpha + 1$</td>
</tr>
<tr>
<td>$\alpha^6$</td>
<td>$\alpha^2 + 1$</td>
</tr>
<tr>
<td>$\alpha^7$</td>
<td>$1$</td>
</tr>
</tbody>
</table>
Figure 8. The Graph $C(F_s, \alpha)$. 

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
CHAPTER II

STRUCTURAL RESULTS AND VARIOUS PARAMETERS

2.1 Various Parameters

There are, of course, many parameters that one can investigate for any given class of graphs. In this section, we shall look at a few of these. First, let $q$ be a prime power, say $q = p'$, and let $g$ be a generator for $\mathbb{F}_q$. Since each vertex in the graph $C(\mathbb{F}_q, g)$ corresponds to a field element, the order of this graph is $q$. Each vertex in this graph is incident with 2 multiplicative arcs and $2t$ additive arcs. We note that we do not identify the two additive arcs for the finite fields of order $2^t$ as we do with Cayley graphs. The two multiplication arcs come from multiplication by $g$ and by $g^{-1}$. The irreducible polynomial that we use to construct the finite field had degree $t$ and this polynomial gives a basis for the additive structure of this graph. Thus for each element in this basis we get two additive arcs incident with each vertex. This tells us that this graph is $(2t + 2)$-regular. Since we know the order of $C(\mathbb{F}_q, g)$ and we know the degree of each vertex, we use the first theorem of graph theory to find the size. In fact, the size of $C(\mathbb{F}_q, g)$ is $(t + 1)p'$, or $(t + 1)q$. So the prime order finite field of order $p$ yields a graph of order $p$ and size $2p$; this graph is 4-regular.
Next, we shall investigate the clique number of the generalized Cayley graph. The clique number of a graph $G$ is the maximum order among the complete subgraphs of $G$, denoted by $\omega(G)$. We note that the graph for the finite field of order 2 (see Figure 9 below) does not contain $K_n$ as a subgraph for any $n \geq 3$. Since $C(F_2, 1)$ does contain edges we can see $\omega(C(F_2, 1)) = 2$.

![Figure 9. The Graph $C(F_2, 1)$](image)

**Theorem 2.1** If $p \geq 3$, then $\omega(C(F_p, g)) = 3$.

**Proof** In order to show that the clique number is equal to three we must do two things. First, we show that $K_3$ is a subgraph of $C(F_p, g)$. Secondly, we show that $K_4$ is not a subgraph of $C(F_p, g)$.

To show $K_3$ is a subgraph of $C(F_p, g)$ we show that the $K_3$ shown in Figure 10 is subgraph of $C(F_p, g)$. First, note that since $p \geq 3$, $g \neq 1$. This implies that $(g-1)^{-1}$ exists. Let $a = 2(g-1)^{-1}$. This would imply $a$ is unique. In turn, this tells us that the following is a subgraph of $C(F_p, g)$, see Figure 10. That is, this figure gives us an equation, in terms of the generators, that we can solve in order to find the values for each vertex. The equation that we get is $ag = a + 2$. Solving for $a$ we find $a = 2(g-1)^{-1}$. 

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
Thus we know that $\omega(C(\mathbb{F}_p, g)) \geq 3$. Later we will see that this is not the only $K_3$ that is a subgraph of $C(\mathbb{F}_p, g)$. In fact, in Chapter III, we will show that there are four such subgraphs.

\[ \begin{array}{c}
\text{a+1} \\
\downarrow \\
a \\
\downarrow \\
a+2
\end{array} \]

Figure 10. $K_3$ as a Subgraph of $C(\mathbb{F}_p, g)$.

Now we need to show that $K_4$ is not a subgraph of $C(\mathbb{F}_p, g)$. We assume, to the contrary that $K_4$ is a subgraph of $C(\mathbb{F}_p, g)$. We know that each vertex of $C(\mathbb{F}_p, g)$ is incident with exactly two multiplicative and two additive edges. Therefore, in the subgraph isomorphic to $K_4$, each vertex is incident with at least one multiplicative and one additive edge. We consider the following cases.

**Case 1.** Suppose our subgraph contains four multiplicative edges. Then each vertex must be incident with exactly two such edges (see Figure 11 below). This implies that the set of nonzero elements forms a cyclic group of order four. Thus, our finite field has order 5. However we may examine the graph for the finite field of order 5 and find that there is no such subgraph (Figure 12).
Case 2. The subgraph contains exactly three multiplicative edges. This implies that there are exactly three additive edges as well. We consider what this subgraph could look like. We find that there are two cases.

Subcase 2.1 The subgraph is as in Figure 13 below. From this figure we get the following three equations:
\[ a \cdot g = a + 3 \]
\[ (a + 2) \cdot g = a \]
\[ (a + 3) \cdot g = a + 1. \]

Since \((a + 2) \cdot g = a\), \((a + 2) \cdot g + 1 = a + 1\). Thus our third equation above tells us that \((a + 3)g = (a + 2)g + 1\). Simplifying this we find \(g = 1\). However, this is a contradiction as we know that \(p \neq 2\).

\[ \text{Figure 13. } K_4 \text{ as in Subcase 2.1.} \]

\textit{Subcase 2.2} The subgraph is as in Figure 14 below. As in the previous subcase, we get three equations as below:
\[ a \cdot g = a + 2 \]
\[ a = (a + 3) \cdot g \]
\[ a + 3 = (a + 1) \cdot g. \]

So \(a \cdot g = a + 2\) implies that \(a \cdot g + 1 = a + 3\). So using equation three above we have \(a \cdot g + 1 = (a + 1) \cdot g\). This implies \(g = 1\), which is a contradiction.
Case 3. Our subgraph contains exactly two multiplicative edges. This implies that each vertex is incident with two multiplicative edges as below in Figure 15. This implies that our finite field has order four. However, we are assuming that our finite field has prime order, a contradiction.

![Figure 14](image1)

**Figure 14.** $K_4$ as in Subcase 2.2.

![Figure 15](image2)

**Figure 15.** $K_4$ With Exactly Two Multiplicative Edges.

The clique numbers of the other generalized Cayley graphs are yet unknown. To find these we simply have to add more cases to the proof above. We will use the previous theorem in the next section when we discuss the chromatic number of these graphs.
2.2 The Chromatic Number and Edge Chromatic Number

A coloring of a graph $G$, or a proper coloring, is an assignment of colors to the vertices of $G$, one color to each vertex, such that adjacent vertices are assigned different colors. If we have a coloring of $G$ using $n$ colors, we call it an $n$-coloring. The minimum number for which a graph $G$ is $n$-colorable is called the vertex chromatic number, or simply the chromatic number. The chromatic number of a graph $G$ is denoted by $\chi(G)$. The following theorem due to Brooks [4] gives us an upper bound for the chromatic number.

**Theorem 2.A.** If $G$ is a connected graph that is neither an odd cycle nor a complete graph, then

$$\chi(G) \leq \Delta(G).$$

The clique number of a graph gives us a lower bound for the chromatic number. Thus, $\omega(G) \leq \chi(G)$. These theorems give us bounds for the chromatic number of the generalized Cayley graph $C(F_q, g)$. We record these in the following two corollaries.

**Corollary 2.3** Let $p$ be a prime, let $t$ be a positive integer and let $q = p^t$. Let $g$ be a generator for $F_p^\times$. Then

$$\chi(C(F_q, g)) \leq 2t + 2.$$
Corollary 2.4 Let $p \geq 3$ be a prime and let $g$ be a generator for $\mathbb{F}_p^*$. Then

$$\chi(C(F_p, g)) = 3 \text{ or } 4.$$ 

Proof For $p \geq 3$, we know that $\omega(C(F_p, g)) = 3$. From Corollary 2.3 above we know that $\chi(C(F_p, g)) \leq 4$. Together these tell us $\chi(C(F_p, g)) = 3$ or 4. □

We note that $\chi(C(F_2, 1)) = 2$. It is possible to show that $\chi(C(F_p, g)) = 3$ for all $p \leq 23$. At this time, the chromatic numbers for the other generalized Cayley graphs are not known.

Thus far, we have been discussing coloring the vertices of a graph. One may also discuss edge colorings. An edge coloring of a nonempty graph $G$ is an assignment of colors to the edges of $G$ so that adjacent edges are assigned different colors. If we use $n$ colors in an edge coloring of $G$, we say $G$ is $n$-edge colorable. The minimum number $n$ for which $G$ is $n$-edge colorable is called the edge chromatic number and is denoted by $\chi_e(G)$. We note that

$$\chi_e(G) = \chi(L(G)).$$

Again, we have a bound in terms of the maximum degree. This result is due to Vizing [16].

Theorem 2.8 If $G$ is nonempty, then

$$\chi_e(G) \leq \Delta(G) + 1.$$
Since it is clear that the maximum degree of a graph is a lower bound for the edge chromatic number we know that for a graph $G$, $\chi_e(G) = \Delta(G)$ or $\Delta(G) + 1$. We say a graph is of class one if $\chi_e(G) = \Delta(G)$ and of class two if $\chi_e(G) = \Delta(G) + 1$. We have the following result due to Beineke and Wilson [2], which gives us a sufficient condition for a graph to be of class two. This condition is in terms of the maximum degree and the edge independence number. An independent set of edges in a graph $G$ is a set of edges, each two of which are independent (nonadjacent). The edge independence number $\beta_1(G)$ of a graph $G$ is the maximum cardinality among the independent sets of edges of $G$. 

**Theorem 2.5** Let $G$ be a graph of size $m$. Then $G$ is of class two if 

$$m > \Delta(G) \beta_1(G).$$

This gives us the following result. 

**Theorem 2.5** Let $t$ be odd, $p \geq 3$ be a prime and let $q = p^t$. Let $g$ be a generator for $\mathbb{F}_q^\times$. Then $C(\mathbb{F}_q, g)$ is of class two. 

**Proof** Let $G = C(\mathbb{F}_q, g)$. We know that $G$ has $(t+1)p^t$ edges and $\Delta(G) = 2t + 2$. Since there is a cycle of length $p^t - 1$ in $G$, $\beta_1(G) = (p^t - 1)/2$. So then 

$$m = (t+1)p^t > (t + 1)(p^t - 1) = (2t + 2)(p^t - 1)/2 = \Delta(G) \beta_1(G)$$

implies that $G$ is of class two. \[\square\]
2.3 Automorphism Groups

Now we wish to discuss the automorphisms of our generalized Cayley graphs. An isomorphism of a graph $G$ is a bijection from $V(G)$ to itself that preserves adjacency. An automorphism of a graph $G$ is an isomorphism of $G$ with itself. The set of all such automorphisms forms a group, $\mathcal{A}(G)$, called the automorphism group of $G$. Let $p$ be a prime, let $t$ be a positive integer and let $q = p^t$. Let $g$ be a generator for $\mathbb{F}_q^*$, and let $D = \mathcal{C}(\mathbb{F}_q, g)$. We know that $D$ is a directed pseudograph with labeled, or colored, edges. If we compute the automorphism group of $D$, that is the automorphism group where we preserve directions, colors and adjacency, we find that $\mathcal{A}(D) = 1$, the trivial group, for all $q \neq 2$. This is shown in Theorem 2.6. When $q = 2$, we have that $\mathcal{A}(D) = \mathbb{Z}_2$, as shown in Theorem 2.9.

Theorem 2.6 For $q \neq 2$, $\mathcal{A}(D) = 1$.

Proof We note that since $0 \cdot g = 0$, for any element $g$, there is always a loop at the zero vertex colored with the color $g$. Suppose, to the contrary, there is another multiplicative loop at the vertex labeled $a$. Then this implies that $ag = a$. Thus, $a(g - 1) = 0$. Since $\mathbb{F}_q$ is an integral domain, this tells us that either $a = 0$ or $g = 1$. Since $\mathbb{F}_2$ is the only finite field such that $1$ is a multiplicative generator, $\mathcal{C}(\mathbb{F}_2, 1)$ is the only generalized Cayley graph with more than one multiplicative loop; in fact it has exactly two such
loops. However, we are assuming that \( q \neq 2 \). We may note that there are no additive loops in \( D \) since zero is not an additive generator. This tells us that any automorphism of \( D \) must send the zero vertex to itself.

Now let us consider the additive arcs leaving the zero vertex. There is one such arc for each additive generator. Any automorphism fixes the colors on the additive arcs and so the neighborhood of the zero vertex is fixed by any automorphism. Since this argument may be applied to the neighborhood of the zero vertex and so on, we see that any automorphism of \( D \) fixes each vertex. Thus, \( \mathcal{A}(D) = 1 \). \( \square \)

When we examine these graphs we note that there are some symmetries if we ignore such things as colors and directions. This brings us to the following definitions. The first automorphism group, denoted by \( \mathcal{A}'(D) \), is the automorphism group of the graph \( D \) if we ignore the directions and respect the colors of the edges. The second automorphism group, denoted by \( \mathcal{A}''(D) \), is the automorphism group of the graph \( D \) if we ignore the directions and ignore the colors of the edges as well. By these definitions, it is clear that \( \mathcal{A}'(D) \) is a subgroup of \( \mathcal{A}''(D) \). We also note that \( \mathcal{A}(D) \) is a subgroup of \( \mathcal{A}'(D) \). We could also define a third automorphism group where we ignore the colors yet respect the directions. We leave this automorphism group for future study.

Theorem 2.7 When \( q = 2 \), \( \mathcal{A}(D) = \mathcal{A}'(D) = \mathcal{A}''(D) = \mathbb{Z}_2 \).
Proof The automorphism which exchanges zero with one is an automorphism regardless of colors or directions. This is the only possible non-trivial automorphism since there are only two vertices. □

Theorem 2.8 For the prime order finite fields, \( \mathcal{A}'(D) = \mathbb{Z}_2 \).
Proof Here we shall prove the result for primes \( p \geq 3 \); the case when \( p = 2 \) is taken care of in Theorem 2.9. As we have noted before, the only loop in \( D \) occurs at the zero vertex. Hence, any automorphism must send zero to itself. We want to find non-trivial automorphisms that disregard directions yet preserve colors. So any such automorphism must send zero to itself yet it must permute the neighbors of zero. Since the only neighbors of zero are 1 and \( p - 1 \), this automorphism must permute these two. Since we are still preserving colors, this forces 2 to be sent to \( p - 2 \). In general, the vertex \( v \) is sent to \(-v\). This automorphism preserves the multiplication edges as well since \( ag = b \) if and only if \(-ag = -b\). Since this is the only non-trivial automorphism we must conclude that \( \mathcal{A}'(D) = \mathbb{Z}_2 \). □

Theorem 2.9 For the finite field of order 4, \( \mathcal{A}''(D) = \mathbb{Z}_2 \).
Proof Here we use the irreducible polynomial \( f(x) = x^2 + x + 1 \). By examining the figure below (Figure 16) we may see that the only non-trivial automorphism exchanges vertex 1 with vertex \( \alpha \). This preserves all the edges and so \( \mathcal{A}''(D) = \mathbb{Z}_2 \). □
Theorem 2.10 Let \( t \geq 2 \), with \( q = 2^t \). Then, \( \mathcal{A}(D) = \mathbb{Z}_t \).

**Proof** Let \( \alpha' \) be an additive generator. Since this additive generator has order two, we may replace any digon formed by two edges labeled \( \alpha' \) with a single edge. Note this will not effect the computation of the first automorphism group. Thus, each vertex in this graph would be incident with exactly one edge labeled with the color \( \alpha' \). Again, any automorphism must send zero to itself. Now this vertex is incident with exactly one edge labeled \( \alpha' \) for each \( i \) from 0 to \( t-1 \). So any automorphism which fixes colors must also fix the neighborhood of zero. This same argument may be applied to the vertices adjacent to zero. If we continue in this manner, we find that the only automorphism is the trivial automorphism. \( \Box \)
Now that we have computed these automorphism groups for various generalized Cayley graphs we see that most of these groups are isomorphic to the trivial group or the cyclic group of order two. These are not the only groups that appear as the automorphism group, as seen in the following result.

**Theorem 2.11** For the finite field of order nine we have \( \mathcal{A}'(C(F_9, \alpha+1)) = \mathbb{Z}_2 \) and \( \mathcal{A}''(C(F_9, \alpha+1)) = \mathbb{Z}_4 \).

**Proof** For the finite field of order 9 we use the irreducible polynomial \( f(x) = x^2 + 1 \). In Figure 17 below we have an imbedding of \( C(F_9, \alpha+1) \) on the torus. Let us first compute the first automorphism group. Any automorphism must send the zero vertex to itself because of the loop. If we ignore the arrows but keep the colors, we see that the only non-trivial automorphism would send vertex 1 to vertex 2. Then the digons at those vertices force where the remaining vertices must be sent under this automorphism. This automorphism may be thought of as a rotation of the diagram below by 180°. Thus, \( \mathcal{A}'(C(F_9, \alpha+1)) = \mathbb{Z}_2 \).

The second automorphism group allows us to ignore both direction and color. Thus, we have other automorphisms in addition to the one mentioned above. One such automorphism sends 1 to \( \alpha \), \( \alpha \) to 2, 2 to \( 2\alpha \), and \( 2\alpha \) to 1. This forces where the rest of the vertices are sent. In terms of the figure below, one may think of this automorphism as a counterclockwise rotation of 90° about vertex 0. Other automorphisms can
be thought of as rotations by $180^\circ$ and $270^\circ$. One can easily check that these are the only non-trivial automorphisms. This tells us that the second automorphism group is given by $\mathcal{A}'(C(\mathbb{F}_q, \alpha+1)) = \mathbb{Z}_4$. □

Figure 17. An Imbedding of $C(\mathbb{F}_q, \alpha+1)$ on the Torus.
CHAPTER III

THE PLANAR FINITE FIELDS

3.1 Genus Bounds for Finite Fields

As we have mentioned, the characterization of the finite planar groups is well known, as given in theorem 1.H. Now we wish to characterize those finite fields that are planar. We define the genus of a finite field $\mathbb{F}$ to be

$$\gamma(\mathbb{F}) = \min \{\gamma(C(\mathbb{F}, g))\}$$

where the minimum is taken over all $g$ that generate $\mathbb{F}$. A finite field $\mathbb{F}$ is said to be planar if $\gamma(\mathbb{F}) = 0$. We should note that it is possible to have two generalized Cayley graphs that model the same finite field and such that these graphs have different genera. We note the finite field of order 11 has $\gamma(C(\mathbb{F}_{11}, 7)) = 0$ and $\gamma(C(\mathbb{F}_{11}, 2)) = 1$. In Figure 18 below we may see an imbedding of $C(\mathbb{F}_{11}, 7)$ on the plane. The graph $C(\mathbb{F}_{11}, 2)$ is not planar because it contains a subgraph that is homeomorphic with $K_{3,3}$ as seen in Figure 19 below. Since we can find an imbedding of $C(\mathbb{F}_{11}, 2)$ on the torus, see Appendix A, $\gamma(C(\mathbb{F}_{11}, 2)) = 1$. The finite field of order 11 is planar since $\gamma(C(\mathbb{F}_{11}, 7)) = 0$. That is, $\gamma(\mathbb{F}_{11}) = 0$. 

35
To characterize the planar finite fields we first derive a genus bound for the prime order finite fields. We complete this task by counting the number of $i$-cycles for $1 \leq i \leq 4$. This will give us a bound for the number of possible $i$-sided regions for $1 \leq i \leq 4$. 

Figure 18. An Imbedding of $C(F_{11}, 7)$ on $S_0$. 

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
This in turn gives us a bound for the total number of regions, which allows us to produce a genus bound. Throughout this chapter we shall let $q = p'$ be a prime power and let $g$ be a generator for $F_q$. Let $D = C(F_q, g)$. Let $r$ be the number of regions in an embedding of $D$ and let $r$, equal the number of $i$-sided regions in that embedding. In Chapter II we showed that for all $q \neq 2$, $D$ has exactly one loop. For that reason we start by counting digons.

**Theorem 3.1** The graph $D = C(F_q, g)$ has $2t$ digons for $q \neq 2'$.

**Proof** To count the number of digons in $D$ we consider what these digons could look like. These digons might contain two multiplicative edges, two additive edges or may contain one additive and one multiplicative edge. We consider each case below.

**Case 1. The digon contains two multiplicative edges.** Here we have two vertices joined by two multiplicative edges. If $a$ is one of these vertices, then $ag^i$ is the other. This implies $ag^i = a$ (see Figure 20 below). Thus we
have $a(g^2-1) = 0$. This implies that either $a = 0$ or $g^2 = 1$. We know that $a \neq 0$ since $0g$ produces a loop in $D$, not a digon. If $g^2 = 1$, then $q = 3$. So for $q \neq 3$, we have no such digons in $D$. However, if $q = 3$, $D$ has 3 digons (see Figure 21).

![Figure 20. A Digon With Two Multiplicative Edges.](image)

![Figure 21. The Graph $C(F_v, 2)$.](image)

**Case 2. The digon contains two additive edges.** This case contains two subcases since these additive edges may come from the same additive generator or different additive generators.

**Subcase 2.1 The digon contains two additive edges with two distinct generators.** Suppose that our digon is formed by the additive generators $\alpha'$ and $\alpha''$. Then we have two possibilities for our digon as seen in Figure 22. below. The first tells us that $a + \alpha' = a + \alpha''$. Thus $\alpha' = \alpha''$. We know this is
impossible because these are distinct additive generators. The second configuration implies $a + \alpha' + \alpha' = a$. So $\alpha' + \alpha' = 0$. This is also impossible since the additive generators are linearly independent and so we have no such digons.

![Figure 22. Two Digons With Two Additive Edges and Two Distinct Generators.](image)

Subcase 2.2 The digon contains two additive edges with the same generator. In this case we have the configuration depicted in Figure 23. Thus $a + \alpha' + \alpha' = a$ implies $2\alpha' = 0$. This occurs precisely when $p = 2$. Thus when $q \neq 2^l$, we have no such digons.

![Figure 23. A Digon With Two Additive Edges and the Same Generator.](image)

Case 3. The digon contains exactly one additive and one multiplicative generator. As before, we consider what the possible digons could look like. We have the following two possibilities (see Figure 24 below). In the first case we may see that $ag = a + \alpha'$ implies that $a = \alpha'(g - 1)^i$. In the second
case we have \((a + a') g = a\). Thus \(a = \alpha' g (1 - g)^{-1}\). By solving for \(a\) uniquely we can count the number of such configurations. We note that the elements \(g^{-1}\) and \(1 - g\) are invertible if and only if \(q \neq 2\). So for \(q \neq 2\), we have \(t\) digons from the first configuration in the figure, one for each additive generator. We also have \(t\) digons from the second configuration, one from each additive generator. So this case yields \(2t\) digons in \(D\).

![Figure 24. Two Digons With One Additive and One Multiplicative Generator.](image)

Since this has exhausted all the possible cases we can conclude that when \(q \neq 2\), \(D\) has \(2t\) digons. Moreover, these digons consist of one multiplicative edge and one additive edge. □

**Corollary 3.2** If \(q = 2^t, t \neq 1\), \(D\) has \(t2^{t-1} + 2t\) digons.

**Proof** From the proof of Theorem 3.1 we know that \(D\) has \(2t\) digons which have one additive and one multiplicative edge. In subcase 2.2 of the proof we have a configuration that is only possible when \(p = 2\). In this case we may see that we have \(2^{t-1}\) choices for the vertex labeled \(a\) and \(t\) choices for the additive generator. Thus we have a total of \(t2^{t-1} + 2t\) digons. □
**Theorem 3.3** When \( q \neq 2, 3', \) or 4, there are \( 4t^2 \) 3-cycles in \( D \). For \( q = 2 \), there are no 3-cycles. For \( q = 3', t \geq 2 \), there are \( t3^{t-1} + 4t^2 \) 3-cycles in \( D \). When \( q = 4 \), \( D \) has thirteen 3-cycles.

**Proof** As in the proof of Theorem 3.1 we consider the different possible configurations of 3-cycles.

**Case 1. All the edges come from additive generators.**

**Subcase 1.1** All edges have the same additive generator. This subcase is depicted in Figure 25 below. Then \( a + 3\alpha' = a \) implies \( 3\alpha' = 0 \). This occurs if and only if \( q = 3' \). For \( q = 3' \), we have \( t3^{t-1} \) such 3-cycles.

\[
\begin{align*}
\text{Figure 25. The 3-cycle in Subcase 1.1.} \\
\end{align*}
\]

**Subcase 1.2** The edges are colored with two different additive generators. This case yields the situation in Figure 26 below. The first case tells us that \( a + \alpha' = a + 2\alpha' \). This means \( e_i = 2\alpha' \). The second implies \( 2\alpha' + \alpha' = 0 \). These are both impossible since these elements are linearly independent.
Subcase 1.3 The edges are colored with three distinct additive generators. Rather than looking at all possibilities with the directions on the edges we consider the undirected 3-cycle as shown below (Figure 27). This implies that these three additive generators are linearly dependent, which is a contradiction. Thus we have no such 3-cycles in $D$.

We may summarize case 1 by saying that there are 3-cycles in $D$ with only additive generators if and only if $q = 3'$. If $q = 3'$, we have $t3' - 1$ such 3-cycles.
Case 2. The 3-cycle contains two additive edges and one multiplicative edge. Here again we have subcases depending on whether the 3-cycle contains one or two distinct additive generators.

Subcase 2.1 One additive generator. If we have the same additive generator for both of our additive edges then we must have one of the two configurations depicted below (Figure 28). The first case tells us that $a = 2\alpha'(g-1)^{\prime}$ while the second tells us that $a = 2\alpha'g(1-g)^{\prime}$. We note that $g - 1$ and $1 - g$ are both invertible when $q \neq 2$. So when $q \neq 2$, we have $2t$ such 3-cycles in $D$.

![Figure 28. The 3-cycles in Subcase 2.1.](image)

Subcase 2.2 Two different additive generators. As in subcase 1.3 we shall draw the configuration without the directions on the edges. This may be seen in Figure 29. Then we have that either $ag = a \pm \alpha' \pm \alpha'^{\prime}g$. In either case we may solve each equation for $a$, namely, $a = (\pm \alpha' \pm \alpha'')(g - 1)^{\prime}$ and $a = (\pm \alpha' \pm \alpha')(1 - g)^{\prime}$ when $q \neq 2$. Then we have $\frac{t(t-1)}{2}$ ways
to choose the two additive generators and 8 ways to choose the directions on the edges. So when \( q \neq 2 \), we have \( 4t(t - 1) \) 3-cycles with two additive edges and one multiplicative edge.

\[
\begin{array}{c}
\bullet \ a \\
\bullet \ a' \ \\
\bullet \ a'' \\
\end{array}
\]

\( a \) \text{ is the vertex and } \{a', a''\} \text{ are the additive edges.}

Figure 29. The 3-cycle in Subcase 2.2.

Case 3. The 3-cycle contains one additive edge and two multiplicative edges. Again we have two possible configurations for the 3-cycle as in Figure 30. here we find that either \( a = a' (g^2 - 1)^{-1} \) or \( a = a' (1 - g^2)^{-1} \), respectively. We note that the elements \( g^2 - 1 \) and \( 1 - g^2 \) are invertible when \( q \neq 3 \). So when \( q \neq 3 \), we have 2t possibilities for 3-cycles.

Case 4. The 3-cycle contains no additive edges. This implies that \( g^3 = 1 \). Hence \( q = 4 \).

When we count all the possible 3-cycles in \( D \) we find that when \( q \neq 2, 3', \text{ or } 4 \), we have a total of \( 4t + 4t(t - 1) = 4t^2 \). For \( q = 2 \), we have no 3-cycles. For \( q = 3', \text{ } t \geq 2 \), we have \( t3'^{t-1} + 4t^2 \) 3-cycles. The \( 4t^2 \) comes from the count above. Recall in subcase 1.3 we had counted \( 3^{t-1} \) additive 3-cycles that
appear only in the graphs with \( q = 3' \). When \( q = 3 \), we have three 3-cycles in \( D \). Lastly, when \( q = 4 \), we may inspect the graph \( D \) as in Figure 16 and we note that there are 13 three-cycles. \( \Box \)

The previous result tells us that if \( t = 1 \), and \( p \geq 5 \), that is, if we are modeling a prime order finite field, then the graph contains four 3-cycles. As the last few results have indicated, in order to count \( i \)-cycles in \( D \) we look at the possible configurations, get equations in terms of the additive and multiplicative generators and then use these equations to eliminate some of the possibilities and to certify the uniqueness of others. Since we want these results to give us a genus bound for the prime order finite fields we shall count the number of 4-cycles in those graphs only. Since we may easily count the number of 4-cycles in the graphs when \( q = 2, 3, \) and 5, we omit these from the theorem below.
Theorem 3.4 Let \( p \geq 7 \) be a prime, let \( g \) generate \( \mathbb{F}_p^* \), and suppose \( D = C(\mathbb{F}_p, g) \). Then \( D \) contains exactly seven 4-cycles.

Proof Since we are assuming that \( p \geq 7 \), we claim that a 4-cycle in \( D \) cannot contain 4 additive or 4 multiplicative edges. If the 4-cycle contained 4 additive edges, this would imply that \( p = 4 \), which is a contradiction as \( p \) is prime. If the 4-cycle contains 4 multiplicative edges, then, necessarily, \( p = 5 \), yet we assumed \( p \geq 7 \). Thus, each of our possible configurations must contain at least one additive and one multiplicative edge. So we have the following cases.

Case 1. The 4-cycle contains three additive edges and one multiplicative edge. This yields the following two configurations seen in Figure 31 below. So we may solve for \( a \) and find that either \( a = 3(g - 1)^{1} \) or \( a = 3g(1 - g)^{1} \). This gives us two 4-cycles.

Case 2. The 4-cycle contains two additive and two multiplicative edges. In this case we have many possible configurations and so we consider the following subcases.

Subcase 2.1 The 4-cycle is as in Figure 32 below. Then we may solve for \( a \) and find \( a = -2g^2(g^2 - 1)^{1} \). So this subcase gives us one such 4-cycle.

Subcase 2.2 The 4-cycle is as in Figure 33 below. Here we have exactly one such 4-cycle since \( a = 3g(1 - g)^{1} \).
Subcase 2.3 The 4-cycle is as in Figure 34 below. Using this we can find that 
\[(a + 1)g = ag + 1,\] Thus we simplify and find that \[g = 1.\] Since \[p \neq 2,\] we know that there are no such 4-cycles.

Subcase 2.4 The 4-cycle is as in Figure 35 below. Here we have the equation 
\[(a + 1)g = ag - 1.\] Thus \[g = -1.\] Since \[p \neq 2,\] there are no such 4-cycles.
Subcase 2.5 The 4-cycle is as in Figure 36 below. Thus we have the equation $a = ((a + 1)g - 1)g$. Solving for $a$ we find $a = (g^2 - g)(1 - g)^{-1}$. So we have one such 4-cycle.

Subcase 2.6 The 4-cycles is as in Figures 37 and 38 below. In this subcase we get the equation $a = ((a + 1)g + 1)g$. If we solve for $a$ we have $a = g(1 - g)^{-1}$. However, we see below, this vertex $a$ is the same as the vertex $(a + 1)g$. 

Figure 33. The 4-cycle in Subcase 2.2.

Figure 34. The 4-cycle in Subcase 2.3.
Figure 35. The 4-cycle in Subcase 2.4.

We have already found $a = g(1 - g)^{-1}$. We wish to show that $a = (a + 1)g$. To do this we show $(1 - g)^{-1} = a + 1$. We may see that $a = g(1 - g)^{-1}$ implies that $a(1 - g) = g$. Thus $a - ag - g = 0$. Adding 1 to both sides and factoring we find $(a + 1)(1 - g) = 1$. So then $(1 - g)^{-1} = a + 1$. This tells us that this configuration actually represents a digon, not a 4-cycle. We also have Figure 38 below. We can show that this is not a 4-cycle in a similar manner.

Figure 36. The 4-cycle in Subcase 2.5.
Case 3. The 4-cycle contains one additive edge and three multiplicative edges. Thus we have the two configurations as in Figure 39. Again we may solve for $a$. We find $a = (g^3 - 1)^{-1}$ and $a = (1 - g^3)^{-1}$, respectively. We know that $g^3 \neq 1$ since $p \neq 4$. So this case yields another two 4-cycles.

We conclude that when $p \geq 7$, $D$ contains exactly seven 4-cycles. $\square$
As we have mentioned, we want a genus bound for the prime order finite fields. Thus it is convenient to summarize the previous results; this is done in Corollary 3.5. We are interested in characterizing those finite fields that yield planar graphs. We may easily see that the graphs $D$ are planar for $q = 2, 3,$ and $5$, we omit these from this result (see Figure 40).
Corollary 3.5 Let $p \geq 7$ be a prime, let $g$ generate $\mathbb{F}_p^*$, and suppose that $D = C(\mathbb{F}_p, g)$. Then $D$ contains precisely one loop, two digons, four 3-cycles and seven 4-cycles.

Theorem 3.6 Let $p \geq 7$ be a prime, let $g$ generate $\mathbb{F}_p^*$. Let us suppose $D = C(\mathbb{F}_p, g)$. If $D$ is imbedded in a surface such that $r_i$ is the number of $i$-sided regions in that imbedding, then $r_1 \leq 1$, $r_2 \leq 2$, $r_3 \leq 4$ and $r_4 \leq 7$.

Proof From Corollary 3.5 we know that $D$ contains exactly one loop, two digons, four 3-cycles and seven 4-cycles. This implies that the given imbedding of $D$ can have at most one 1-sided region, two 2-sided regions, four 3-sided regions and seven 4-sided regions. □

Theorem 3.7 Let $p$ be a prime, let $g$ generate $\mathbb{F}_p^*$, and let $D = C(\mathbb{F}_p, g)$. If $D$ is minimally imbedded on $S_k$, then

$$k \geq \frac{p-15}{10}.$$

Proof Suppose $D$ is minimally imbedded in $S_k$ with $r$ regions and let $r_i$ be the number of $i$-sided regions in that imbedding. Then

$$r = \sum_{i=1}^{r_1} 1 + \sum_{i=2}^{r_2} 2 + \sum_{i=3}^{r_3} 4 + \sum_{i=4}^{r_4} 7 = 14 + \sum_{i=5}^{r_4} r_i.$$

Since the most efficient imbedding of $D$ would have $r_1 = 1$, $r_2 = 2$, $r_3 = 4$ and $r_4 = 7$ along with $r_5 = r - 14$, we may see that
\[2(2p) = \sum_{i \geq 1} ir_i \geq 1(1) + 2(2) + 3(4) + 4(7) + 5(r - 14).\]

Solving for \( r \) we find that

\[r \leq \frac{4p + 25}{5}.\]

Euler's formula tells us that

\[k = 1 + \frac{1}{2}(p - r).\]

This along with the previous inequality gives us the desired result. \( \square \)

By finding bounds for the number of \( i \)-sided regions for \( i \) from 1 to 4 we were able to get a genus bound for the prime order finite fields. However we need not restrict ourselves to those finite fields with prime order. Using Theorems 3.1 and 3.3 we can also find genus bound for the remaining finite fields.

**Theorem 3.8** Let \( q = p' \) with \( q \neq 2', 3' \). If \( D = C(F_q, g) \) is minimally imbedded on \( S_t \) then

\[k \geq \frac{(2t - 2)p' - 4t^2 - 4t + 5}{8}.\]

**Proof** We know that \( D \) has order \( p' \) and size \( p'(t + 1) \). If \( D \) is minimally imbedded on \( S_t \) with \( r \) regions, then \( r = tp' + 2 - 2k \). We know that \( r \leq 1 \).
By Theorem 3.1 we have \( r_2 \leq 2t \) and by Theorem 3.3 we know \( r_3 \leq 4t^2 \). The most efficient imbedding of \( D \) on any surface would have \( r_1 = 1, r_2 = 2t \), and \( r_3 = 4t^2 \). So we assume that \( r_1 = 1, r_2 = 2t \), and \( r_3 = 4t^2 \). Then

\[
r = \sum_{i \geq 1} r_i = 1 + 2t + 4t^2 + \sum_{i \geq 1} r_i \text{ and } 2(t + 1)p' = \sum_{i \geq 1} ir_i = 1 + 4t + 12t^2 + \sum_{i \geq 1} ir_i.
\]

Thus

\[
\sum_{i \geq 1} r_i = tp' + 2 - 2k - 1 - 2t - 4t^2 \text{ and }
\sum_{i \geq 1} ir_i = 2(t + 1)p' - 1 - 4t - 12t^2.
\]

Together these imply

\[
2(t + 1)p' - 1 - 4t - 12t^2 = \sum_{i \geq 1} ir_i \geq 4\left(\sum_{i \geq 1} r_i\right) = 4\left(tp' + 1 - 2k - 2t - 4t^2\right).
\]

Simplifying these we get the inequality (3.1) above. \( \Box \)

**Theorem 3.9** Let \( q = 2^i \). If \( D = C(F, g) \) is minimally imbedded on \( S \), then

\[
k \geq \frac{(t - 2)2^{i} - 4t^2 - 2t + 5}{8}.
\]
Proof The proof of this is similar to the proof of Theorem 3.8 except that for $q = 2^r$ we have that $r_1 = 1$, $r_2 = t$, and $r_3 = 4t^2$. We note that we have $r_2 = t$ since we can replace each additive digon whose arcs are labeled with the same additive generator with a single edge. Recall that Corollary 3.2 gives us $t2^{r-1} + 2t$ digons. When we complete the replacement described above we only have $t$ digons left. We note that this replacement does not affect the genus of the graph. Routine algebra then gives the bound. □

Theorem 3.10 Let $q = 3^r$. If $D = C(F_q, g)$ is minimally imbedded on $S_k$ then

$$k \geq \frac{(5t - 6)3^{r-1} - 4t^2 - 4t + 5}{8}.$$  

Proof Again this proof is similar to the proof of Theorem 3.8. In this case we use $r_1 = 1$, $r_2 = 2t$, and $r_3 = t3^{r-1} + 4t^2$. □

3.2 The Characterization of the Planar Finite Fields

Before we give the characterization of the planar finite fields, we shall give some preliminary results, which shall help us in the proof of the characterization. We shall also take care of a few special cases. In particular, we shall show that the finite fields of order 8 and 13 are toroidal. First, recall that if $H$ is a subgraph of $G$ then $\gamma(H) \leq \gamma(G)$. Note that the additive generators in our generalized Cayley graphs create a
subgraph that is isomorphic to a cartesian product of cycles. In particular, if $q = p'$, then $D$ has a subgraph isomorphic to $(C_q)'$. Therefore, $\chi(C_q) \leq \chi(D)$.

We shall use this result frequently in the characterizations of the planar and toroidal finite fields.

Lemma 3.11 The finite field of order 8 is toroidal.

Proof For the finite field of order 8 we use the irreducible polynomial $f(x) = x^3 + x + 1$. To show that $\chi(F_8) = 1$, we first show that the genus is at least one by demonstrating that each graph $C(F_8, g)$ contains a subgraph that is homeomorphic with $K_{1,3}$. Thus we can see that these graphs are not planar by Kuratowski's Theorem which is given by theorem 1.4 in section 1.3. This may be seen in the figures below (Figures 41, 42, and 43). We have equality because we may find an imbedding on the torus for each graph (see Appendix A for the rotational imbedding schemes). □

![Figure 41. A Subgraph of $C(F_8, \alpha)$.](image-url)
**Lemma 3.12** The finite field of order 13 is toroidal.

**Proof** We know that $\chi(C(F_{13}, 2)) \geq 1$ and $\chi(C(F_{13}, 6)) \geq 1$ since each of these graphs contains a subgraph that is homeomorphic with $K_{3,3}$ (Figures 44 and 45). We have equality for $C(F_{13}, 6)$ because we may find an imbedding on the torus for this found in Appendix A. It can be shown that $C(F_{13}, 2)$ cannot be imbedded on the torus. □

![Figure 42. A Subgraph of $C(F_{3}, \alpha^2)$.](image1)

![Figure 43. A Subgraph of $C(F_{5}, \alpha^3)$.](image2)
Theorem 3.13 The finite field of order $q$ is planar if and only if $q = 2, 3, 4, 5, 7, \text{ or } 11$.

Proof First we shall characterize the planar finite fields with prime order.

Theorem 3.7 tells us that $\gamma(F_p) \leq 0$ if and only if $\frac{p - 15}{10} \leq 0$. Thus the only possible planar finite fields of prime order have $p \leq 15$, so $p = 2, 3, 5, 7, 11, \text{ or } 13$. We have already shown that the finite field of order $p$ is planar for
$p = 2, 3, 5,$ and $11$. In Figure 46 we see that the finite field of order 7 is planar. Lemma 3.12 tells us that the finite field of order 13 is toroidal.

![Figure 46. An Imbedding of $C(F_-, 3)$.](image)

Now we shall show that the only other planar finite field has order 4. We know that $F_4$ is planar by the imbedding given in Figure 16. So we now suppose $p = 2$ and suppose $t \geq 4$. Then let $q = 2^t$. Lemma 3.11 tells us that the finite field of order 8 is toroidal so that we may assume $t \geq 4$. Since the graph $Q_t$ is a subgraph of $C(F_-, g)$, we know that $\gamma(Q_t) \leq \gamma(C(F_-, g))$. We know that the genus of the $t$-cube is given by $1 + 2^{t^3}(t - 4)$, from Theorem 1.C. So we know that $\gamma(Q_t) = 1 + 2^{t^3}(t - 4)$. Thus for $t \geq 4$, we have $\gamma(Q_t) \geq 1$. Therefore $\gamma(C(F_-, g)) \geq 1$. Now let $p \geq 3$, $t \geq 2$ and let $q = p^t$. We have seen that $\gamma(C_p \times C_p) \leq \gamma(C(F_-, g))$. Since $p \geq 3$ implies $\gamma(C_p \times C_p) = 1$, we can see
\( \gamma(C(\mathbb{F}_{q}, g)) \geq 1. \) Since this covers all the possible cases, the only planar finite fields have orders 2, 3, 4, 5, 7, or 11. □
CHAPTER IV
THE TOROIDAL FINITE FIELDS

4.1 The Genus of $\mathbb{F}_{19}$ Is 2

Now that we have characterized those finite fields that are planar, we wish to characterize the toroidal finite fields. To do this we will first take care of a few special cases. In Theorem 3.7 we obtained a bound which allows us to list the possible toroidal finite fields of prime order. The finite fields with order 19 and 23 are on this list; however, neither of these finite fields is toroidal. After we have shown that both $\mathbb{F}_{19}$ and $\mathbb{F}_{23}$ are not toroidal we shall give the characterization. We shall find the following lemma useful in showing that $\mathbb{F}_{19}$ is not toroidal. We note that $\mathbb{F}_p$ is identified with $\mathbb{Z}_p$.

Lemma 4.1 If $K_{2,3}$ is a subgraph of $C(\mathbb{F}_p, g)$ for some prime $p$ and some multiplicative generator $g$, then in any imbedding of $C(\mathbb{F}_p, g)$ the number of possible 4-sided regions is at most five. If there are two copies of $K_{2,3}$ then the number of possible 4-sided regions is at most three.

Proof Theorem 3.6 showed us that the number of possible 4-sided regions is at most seven. Suppose $K_{2,3}$ is a subgraph of $C(\mathbb{F}_p, g)$. Since each vertex of degree two in this subgraph is incident with two more
edges in $C(F_p, g)$, only one of the three possible 4-sided regions from this subgraph can be a 4-sided region in an imbedding of $C(F_p, g)$.\□

**Theorem 4.2** The genus of $F_{19}$ is 2.

**Proof** In Theorem 3.7 we showed that if $D = C(F_p, g)$ is imbedded on $S_k$, then $k \geq \frac{p - 15}{10}$. This tells us that the finite field of order 19 is not planar.

Let us assume, to the contrary, that we can find an imbedding of $C(F_{19}, g)$ on the torus for some multiplicative generator $g$. The choices for $g$, up to inverses, are 2, 3, and 14. These graphs are shown in Appendix B. We shall first show that $g = 3$ and $g = 14$ lead to contradictions.

By Lemma 4.1 we see that for $g = 3$ and $g = 14$, $r_4 < 3$. This is because in each graph we have two copies of $K_{2,3}$ as seen below (Figures 47 and 48).

![Figure 47. Two Copies of $K_{2,3}$ in $C(F_{19}, 3)$.](image)

Without loss of generality, we may assume that if we do have an imbedding of $C(F_{19}, g)$ on $S_1$, then $r_1 = 1$ and $r_2 = 2$. Now let us examine
the "large" regions in this imbedding by looking at the possible regions containing the zero vertex. To do this we look at the cycles that contain the zero vertex. In particular, we look for the smallest such cycles. If we get a contradiction with the smallest possible cycles, then we would certainly get a contradiction with larger ones.

For $g = 3$, we note that the smallest cycles containing the zero vertex that could be regions in a single imbedding, not including the loop, are

$$C_1: 0, 1, 2, 6, 18, 0, \text{ and}$$

$$C_2: 0, 1, 13, 17, 18, 0.$$

If these cycles were actual regions, the loop at zero along with these cycles would yield a 5-sided and a 6-sided region. The next smallest cycles containing zero are

$$C_3: 0, 1, 2, 7, 6, 18, 0, \text{ and}$$

$$C_4: 0, 1, 13, 12, 17, 18, 0.$$
These would lead to a 6-sided and a 7-sided region. After these, the regions would have at least 8 sides.

For $g = 14$, the smallest cycles containing the zero vertex are

$$C_s: 0, 1, 2, 3, 4, 18, 0,$$

$$C_6: 0, 1, 15, 16, 17, 18, 0.$$  

These along with the loop at zero would produce a 6-sided and a 7-sided region. By examining the cycles we see the next smallest cycles would yield a 7-sided and an 8-sided region at zero.

For $g = 2$, we could have a 5 and a 9-sided region or a 6 and 8-sided region from the cycles

$$C_7: 0, 1, 10, 9, 18, 0,$$

$$C_8: 0, 1, 2, 4, 8, 16, 17, 18, 0.$$  

We could also have a 7-sided region and an 8-sided region from the cycles

$$C_9: 0, 1, 10, 11, 15, 17, 18, 0,$$

$$C_{10}: 0, 1, 2, 4, 8, 9, 18, 0.$$  

If $C(F_{19}, g)$ is imbedded on $S_1$, then we know that

$$\sum_{r_1} r_i = 19 \text{ and } \sum_{r_2} ir_i = 76.$$  

Since we are assuming that $r_1 = 1$ and $r_2 = 2$, these simplify to

$$(4.1) \quad \sum_{i \geq 3} r_i = 16 \text{ and }$$
We shall use these equations along with the information concerning the "large" regions to get the possible number of $i$-sided regions for $i \geq 3$. We consider cases based upon what $r_3$ could be. We know that any imbedding of $C(F_{19}, g)$ would have $r_3 \leq 4$.

If we use the inequalities $r_4 \leq 3$ and $r_3 \leq 2$ along with equations 4.1 and 4.2 above, we get a contradiction. Thus $r_3 = 3$ or $r_3 = 4$. First, suppose that $r_3 = 4$. Then equations (4.1) and (4.2) simplify to

$$\sum_{i \geq 4} r_i = 12 \quad \text{and} \quad \sum_{i \geq 4} r_i = 59.$$ 

Since $r_4 \leq 3$, when $g \neq 2$, we shall only check the cases $r_4 = 0, 1, 2,$ and 3. We will take care of the case where $g = 2$ later. Now we can check each possibility for $r_4$ to find the possible region distributions. If $r_4 = 0$, then $r_5 \geq 13$, which contradicts the fact that $\sum_{i \geq 4} r_i = 12$. If $r_4 = 1$, then some algebra tells us that $r_5 = 11$. If $r_4 = 2$, then $r_5 = 9$ and $r_6 = 1$. Lastly, if $r_4 = 3$, we have two possibilities. Either $r_5 = 7$ and $r_6 = 2$, or $r_5 = 8$ and $r_7 = 1$.

Next, suppose that $r_3 = 3$. Here we can use our equations again to find $r_4 = 3$ and $r_5 = 10$.

This information along with the possible regions at the zero vertex tells us immediately that we cannot have $C(F_{19}, 14)$ imbedded on $S_1$. This
is because we know that an imbedding of this graph must have two regions that have more than five sides at the zero vertex; they cannot be two 6-sided regions.

If $C(F_{19}, 3)$ were imbedded on $S_1$, then we must have either

$$r_3 = 4, \ r_4 = 3, \ r_5 = 7, \text{ and } r_6 = 2,$$

or

$$r_3 = 4, \ r_4 = 2, \ r_5 = 9, \text{ and } r_6 = 1.$$

So now we consider what the imbedding could look like. Since we have $r_3 = 4$ and a 5-sided and a 6-sided region at the zero vertex, we must have the following partial imbedding (Figure 49). This figure tells us that we must have $p_6 = (2, 18, 5, 7)$ and $p_{13} = (1, 14, 12, 17)$. We note that we may place the loop at zero in either of the regions at the zero vertex without changing the following argument.

Claim A. Neither of the two possible rotations at the vertex labeled 12 are possible.

Case A.1. $p_{12} = (17, 13, 11, 4)$. This tells us that $p_{16} = (10, 18, 17, 15)$. We know by our previous work that any additional region must have 6 or fewer sides. Thus the only way to finish the region 16-17-12-4 is by using the vertices 14 and 15 as in Figure 50. Then 5-6-18-16-10 is the start of a region with more than 6 sides. This is a contradiction as we know that each region must have 6 or fewer sides. Thus the rotation at 12 cannot be $p_{12} = (17, 13, 11, 4)$. 

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
Case A.2. \( p_{12} = (17, 13, 4, 11) \). From here we shall consider two subcases depending on the two possible rotations at the vertex labeled 16.

Subcase A.2.1. \( p_{16} = (18, 17, 15, 10) \). In this subcase the region containing 5-6-18-16-10 must be a region with 7 or more sides, a contradiction.

Figure 49. A Partial Imbedding of \( C(F_{19}, 3) \).
Subcase A.2.2. \( p_{16} = (18, 17, 10, 15) \). Here again we consider two subcases depending on the rotation of the vertex labeled 10.
Subcase A.2.2.1. \( \rho_{10} = (16, 11, 9) \). Here we have three regions which have six or more sides. The first starts with 7-8-9-10-16-15. The second begins 5-8-9-10-16-15. The third begins with 11-10-9-3. This is a contradiction as we know we can have at most two 6-sided regions and no regions with more than six sides.

Subcase A.2.2.2. \( \rho_{10} = (16, 9, 11) \). Then the region that begins with 9-10-16-17-12-11 must have seven or more sides.

Since this was our last case, we conclude that neither of the possible rotations at 12 are possible. Therefore, we must conclude that \( C(F_{19}, 3) \) cannot be imbedded on \( S_1 \). So we have taken care of the cases when \( g = 3 \) and 14. Lastly we show that \( C(F_{19}, 2) \) cannot be imbedded on \( S_1 \).

Suppose, to the contrary that we may find an imbedding on \( S_1 \). Our first claim is that if \( C(F_{19}, 2) \) is imbedded on \( S_1 \), then \( r_4 \neq 7 \). Suppose to the contrary that \( r_4 = 7 \). If this were the case then we are forced to have the following configuration of the 4-sided regions, up to mirror image (see Figure 51). The 4-sided regions are shaded. Then note that 14-13-7-14 and 12-6-5-12 cannot give us two of the possible 3-sided regions. Thus, \( r_3 \leq 2 \).

First suppose that \( r_3 = 0 \). Then \( r_4 = 7 \) implies \( \sum r_i = 9 \) and \( \sum ir_i = 43 \). This is a contradiction as this implies that

\[
43 = \sum_{i \geq 5} ir_i \geq 5\left( \sum_{i \geq 5} r_i \right) = 5(9) = 45.
\]
Figure 51. The 4-sided Regions in $C(F_{19}, 2)$. 
If \( r_3 = 1 \), then \( r_4 = 7 \) implies \( \sum_{i=5}^{n} r_i = 8 \) and \( \sum_{i=5}^{n} ir_i = 40 \). This tells us that we must have \( r_5 = 8 \) and \( r_i = 0 \) for \( i \geq 6 \). However we have seen that there is a region at the zero vertex that must have more than five sides. In fact we must have a region with eight or more sides. Thus \( r_3 \neq 1 \).

Since we know \( r_3 \neq 0 \) and \( r_3 \neq 1 \), we must have \( r_3 = 2 \). Thus, \( \sum_{i=5}^{n} r_i = 7 \) and \( \sum_{i=5}^{n} ir_i = 37 \). These equations tell us that \( 37 - 5r_5 \geq 6(7 - r_5) \). So we have \( r_5 \geq 5 \). We may also see that \( r_5 \leq 6 \) since

\[
37 = \sum_{i=5}^{n} ir_i \geq 5 \left( \sum_{i=5}^{n} r_i \right) = 5(7) = 35
\]
tells us that \( r_5 < 7 \). Now if \( r_5 = 5 \), then solving the above equations tells us that \( r_6 = 2 \) and \( r_i = 0 \) for \( i \geq 7 \). This is a contradiction as we know there is a region that has at least eight sides. If \( r_5 = 6 \), then we get \( r_7 = 1 \). Again this is a contradiction. Thus we have shown that \( r_4 \leq 6 \).

Using \( r_1 = 1, r_2 = 2 \) and our equations we can do some algebra to get the cases listed in Table 2. We note that in the case \( r_3 = 4 \), we have that \( r_4 \leq 5 \) by Figure 51 above. Our previous analysis concerning the regions at the zero vertex tells us that we have only two of the cases listed in the table that remain, namely the two bulleted below.

The only difference between these cases is the placement of the loop. Here we could have the loop as in Figure 52 or as in Figure 53, which give partial imbeddings of this graph.
Table 2

Possible Region Distributions for $C(F_{19}, 2) < S_1$

<table>
<thead>
<tr>
<th>$r_3 = 4$</th>
<th>$r_4 = 5$</th>
<th>$r_5 = 3$</th>
<th>$r_6 = 4$</th>
<th>$r_7 = 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$r_3 = 4$</td>
<td>$r_4 = 5$</td>
<td>$r_5 = 3$</td>
<td>$r_6 = 2$</td>
<td>$r_7 = 1$</td>
</tr>
<tr>
<td>$r_3 = 4$</td>
<td>$r_4 = 5$</td>
<td>$r_5 = 4$</td>
<td>$r_6 = 1$</td>
<td>$r_7 = 1$</td>
</tr>
<tr>
<td>$r_3 = 4$</td>
<td>$r_4 = 5$</td>
<td>$r_5 = 5$</td>
<td>$r_6 = 1$</td>
<td>$r_7 = 1$</td>
</tr>
<tr>
<td>$r_3 = 4$</td>
<td>$r_4 = 5$</td>
<td>$r_5 = 6$</td>
<td>$r_6 = 2$</td>
<td>$r_7 = 1$</td>
</tr>
<tr>
<td>$r_3 = 4$</td>
<td>$r_4 = 4$</td>
<td>$r_5 = 5$</td>
<td>$r_6 = 1$</td>
<td>$r_7 = 1$</td>
</tr>
<tr>
<td>$r_3 = 4$</td>
<td>$r_4 = 4$</td>
<td>$r_5 = 6$</td>
<td>$r_6 = 1$</td>
<td>$r_7 = 1$</td>
</tr>
<tr>
<td>$r_3 = 4$</td>
<td>$r_4 = 4$</td>
<td>$r_5 = 7$</td>
<td>$r_6 = 1$</td>
<td>$r_7 = 1$</td>
</tr>
<tr>
<td>$r_3 = 4$</td>
<td>$r_4 = 3$</td>
<td>$r_5 = 7$</td>
<td>$r_6 = 2$</td>
<td>$r_7 = 1$</td>
</tr>
<tr>
<td>$r_3 = 4$</td>
<td>$r_4 = 2$</td>
<td>$r_5 = 9$</td>
<td>$r_6 = 1$</td>
<td>$r_7 = 1$</td>
</tr>
<tr>
<td>$r_3 = 4$</td>
<td>$r_4 = 1$</td>
<td>$r_5 = 11$</td>
<td>$r_6 = 1$</td>
<td>$r_7 = 1$</td>
</tr>
<tr>
<td>$r_3 = 3$</td>
<td>$r_4 = 6$</td>
<td>$r_5 = 6$</td>
<td>$r_6 = 1$</td>
<td>$r_7 = 1$</td>
</tr>
<tr>
<td>$r_3 = 3$</td>
<td>$r_4 = 6$</td>
<td>$r_5 = 5$</td>
<td>$r_6 = 1$</td>
<td>$r_7 = 1$</td>
</tr>
<tr>
<td>$r_3 = 3$</td>
<td>$r_4 = 6$</td>
<td>$r_5 = 4$</td>
<td>$r_6 = 3$</td>
<td>$r_7 = 1$</td>
</tr>
<tr>
<td>$r_3 = 3$</td>
<td>$r_4 = 5$</td>
<td>$r_5 = 6$</td>
<td>$r_6 = 2$</td>
<td>$r_7 = 1$</td>
</tr>
<tr>
<td>$r_3 = 3$</td>
<td>$r_4 = 5$</td>
<td>$r_5 = 7$</td>
<td>$r_6 = 1$</td>
<td>$r_7 = 1$</td>
</tr>
<tr>
<td>$r_3 = 3$</td>
<td>$r_4 = 4$</td>
<td>$r_5 = 8$</td>
<td>$r_6 = 1$</td>
<td>$r_7 = 1$</td>
</tr>
<tr>
<td>$r_3 = 3$</td>
<td>$r_4 = 3$</td>
<td>$r_5 = 10$</td>
<td>$r_6 = 1$</td>
<td>$r_7 = 1$</td>
</tr>
<tr>
<td>$r_3 = 2$</td>
<td>$r_4 = 6$</td>
<td>$r_5 = 7$</td>
<td>$r_6 = 1$</td>
<td>$r_7 = 1$</td>
</tr>
<tr>
<td>$r_3 = 2$</td>
<td>$r_4 = 5$</td>
<td>$r_5 = 9$</td>
<td>$r_6 = 1$</td>
<td>$r_7 = 1$</td>
</tr>
</tbody>
</table>

Therefore, the proof of the first case, where $r_3 = 4$, $r_4 = 5$, $r_5 = 5$, $r_6 = 1$ and $r_8 = 1$, is exactly the same as second case, where $r_3 = 4$, $r_4 = 5$, $r_5 = 6$ and $r_9 = 1$. Since they are similar, we shall use the partial imbedding of $C(F_{19}, 2)$ in Figure 52 and assume $r_3 = 4$, $r_4 = 5$, $r_5 = 6$ and $r_9 = 1$.

Since $R_1$ is the only region with more than five sides, we know that $R_2$ is forced to be the 5-sided region as below, for otherwise we would have another region with more than five sides. Since we must have all four of the possible 3-sided regions we must also have the two 3-sided regions in
Figure 52 as well. This also tells us that 13-14-7-13 must be a 3-sided region.

So this gives us four cases for the possible rotations at 13.

Figure 52. A Partial Imbedding of $C(F_{19}, 2)$. 

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
Figure 53. Another Partial Imbedding of $C(\mathcal{F}_{19}, 2)$.

Case 1. $\rho_{13} = (14, 7, 12, 16)$. The arc $(7, 13)$ appears in 2 possible 4-sided regions and one possible 3-sided region. This and the rotation imply that
16-13-7-8-16 is not a 4-sided region in our imbedding as can be seen in Figure 54.

![Figure 54](image-url)

Figure 54. 16-13-7-8-16 Is Not a 4-sided Region.

If the 4-cycle 13-7-6-12-13 is not a 4-sided region as well, then $r_4 = 5$ tells us that all other possible 4-sided regions are actual regions. Thus we have the following regions in our imbedding (Figure 55). This would imply that $p_6 = (3, 5, 12)$. This is a contradiction as we know that 6 is adjacent to 7.

Thus we know that the 4-cycle 13-7-6-12-13 is a 4-sided region. This forces the configuration found in Figure 56. This in turn forces the 3-sided region containing 2, 3, 4 to be 4-3-2-4 as seen in the figure below. This contradicts Figure 52 where the region is given by 4-2-3-4. Thus the rotation at 13 cannot be $p_{13} = (14, 7, 12, 16)$.

Case 2. $p_{13} = (14, 7, 16, 12)$. Then 13-12-7-6-13 and 13-14-15-16-13 are not 4-sided regions in our imbedding. Then $r_4 = 5$ implies that the other
possible 4-sided regions must be present. This implies that we have the following regions depicted in Figure 57 below. This is a contradiction as this implies \( p_7 = (13, 14, 8) \), yet 7 is adjacent to 6.

![Figure 55. Some Regions Containing Vertex 6.](image)

**Case 3.** \( p_{13} = (7, 14, 12, 16) \). This implies that 13-12-7-6-13 and 13-14-15-16-13 are not 4-sided regions as in case 2. Since we must have five 4-sided regions, we have the following regions in our imbedding(Figure 58). This is a contradiction as 7 is adjacent to 6.

**Case 4.** \( p_{13} = (7, 14, 16, 12) \). This implies that 7-13-16-8-7 is not a 4-sided region. If 12 - 6 - 7 - 13 - 12 is not a 4-sided region, then we have the same figure and contradiction as case 1 (see Figure 54). Therefore 12-6-7-13-12 must be a 4-sided region. This gives us the following regions (Figure 59).
Figure 56. 13-7-6-12-13 and Other 4-sided Regions.

Figure 57. The Regions for Case 2.
Figure 58. The Regions for Case 3.

Figure 59. The Regions in Case 4.
Then, since $\rho_{16} = (13, 15, 17, 8)$, we may see that 11-12-13-16-8 is the start of a region that must have at least six sides. This is a contradiction and so there is no such imbedding.

Since this was our last case, we must conclude that $g = 2$ cannot give us an imbedding of $C(F_{19}, g)$ on the torus. Therefore we may see that the finite field of order 19 cannot be imbedded on the torus. However, this finite field does have generators that yield imbeddings on the double torus. The rotation schemes for the graphs with imbeddings on $S_2$ are given in Appendix C. □

4.2 The Genus of $F_{23}$ Is at Least 2

**Theorem 4.3** The finite field of order 23 has $\gamma(F_{23}) \geq 2$.

**Proof** In order to show $\gamma(F_{23}) \geq 2$ we shall first show $\gamma(F_{23}) \geq 1$ and then show $\gamma(F_{23}) \neq 1$.

We know that $C(F_{23}, g)$ cannot be imbedded on $S_9$ by our genus bound for the prime order finite fields. To show that $\gamma(F_{23}) \geq 2$, we assume, to the contrary, that we can find a $g$ such that $\gamma(C(F_{23}, g)) = 1$. Our choices for $g$, up to inverses, are 5, 7, 11, 15, and 17. These graphs are given in Appendix B. Again we use Euler's identity to get

$$\sum_{i \in I} r_i = 23 \text{ and } \sum_{i \in I} ir_i = 92.$$
As we mentioned earlier, an efficient imbedding of $C(F_{23}, g)$ on any surface would have $r_1 = 1$ and $r_2 = 2$. So if we get a contradiction with $r_1 = 1$ and $r_2 = 2$, we would certainly have one if $r_1 = 0$ and $r_2 = 0$ or 1. Therefore we assume that we have $r_1 = 1$ and $r_2 = 2$. Thus,

\[(4.3) \quad \sum_{i \geq 3} r_i = 20, \text{ and} \]

\[(4.4) \quad \sum_{i \geq 3} ir_i = 87. \]

We wish to use equations (4.3) and (4.4) to get bounds for $r_i$ when $i \geq 3$. Our first claim is that $r_3 = 4$. Equation (4.3) tells us that

$$20 - r_3 - r_4 = \sum_{i \geq 5} r_i.$$ 

Equation (4.4) tells us that

$$87 - 3r_3 - 4r_4 = \sum_{i \geq 5} ir_i.$$ 

Using these we find

$$87 - 3r_3 - 4r_4 = \sum_{i \geq 5} ir_i \geq 5\left(\sum_{i \geq 5} r_i\right) = 5(20 - r_3 - r_4).$$

This simplifies to $2r_3 + r_4 \geq 13$. We know that $r_4 \leq 7$. These two inequalities imply $r_3 \geq 3$. If $r_3 = 3$, then we must have $r_4 = 7$. We shall show that this is
impossible, that is, we shall show that \( r_4 \leq 6 \). This would imply that \( r_3 = 4 \), as claimed.

First, we must rule out \( g = 11 \), since in this case it is possible to have \( r_4 = 7 \). However, in this case, we note that \( r_3 \leq 2 \). We can’t have more than two of the possible triangles as actual regions in an imbedding since we must add the rest of the edges to the vertices in the figures below (see Figure 60). Since we know that \( r_3 \geq 3 \), this implies that \( C(F_{23}, 11) \) cannot be imbedded on the torus. So we shall assume that \( g \neq 11 \).

![Figure 60. The Triangles in \( C(F_{23}, 11) \).](image)

It turns out that we may examine the graphs \( C(F_{23}, g) \) for \( g = 5, 15, \) and 17 and show that \( r_4 \leq 5 \). For \( g = 5 \) and 17 we have two copies of \( K_{2,3} \). The situations for \( g = 5, 15, \) and 17 are depicted below (Figure 61). For \( g = 15 \) we have a similar situation which eliminates a 4-sided region. These diagrams eliminate one possible 4-gon. However, using the symmetry of these graphs we may eliminate another possible 4-gon. That is, if we
replace each vertex \( v \) above with \(-v\), we have a subgraph similar to the ones above. So in each of these cases we have \( r_4 \leq 5 \).

Now we consider the graph \( C(F_{2^r}, 7) \). If we have \( r_4 = 7 \), we cannot have all four of our possible 3-gons. In fact, in the following diagram, Figure 62, we may see that if \( r_4 = 7 \), then \( r_3 \leq 2 \), a contradiction, as \( r_3 \geq 3 \). This is because the two possible 3-sided regions with the vertices 10, 11, 8 and 12, 15, 13 cannot be actual 3-sided regions if \( r_4 = 7 \). So for this case \( r_4 \leq 6 \). Thus we have \( r_3 = 4 \).

Figure 62. The 3-gons and 4-gons in \( C(F_{2^r}, 7) \).
Then equations (4.3) and (4.4) simplify to

\[(4.5) \quad \sum_{i=2}^{4} r_i = 16 \text{ and} \]
\[(4.6) \quad \sum_{i=2}^{4} ir_i = 75. \]

So the inequality \(75 - 4r_4 - 5r_5 \geq 6 \left( \sum_{i=2}^{6} r_i \right) = 6(16 - r_4 - r_5)\) that we get from these equations tells us that \(2r_4 + r_5 \geq 21\). From equation (4.5) we find that \(r_4 + r_5 \leq 16\). Solving these two inequalities tells us that \(r_4 \geq 5\). This eliminates the case \(g = 7\) by Figure 62 above since \(r_3 = 4\) implies \(r_4 \leq 3\). For the other cases we have shown that \(r_4 \leq 5\). Thus, \(r_4 = 5\). Let us summarize what we have shown so far. We have eliminated the cases when \(g = 7\) and 11. We have also shown that if \(C(F_{23}, g)\) is imbedded on \(S\) with \(g = 5, 15\) or 17, then \(r_1 = 1, r_2 = 2, r_3 = 4,\) and \(r_4 = 5\). This implies

\[\sum_{i=2}^{4} r_i = 11 \text{ and } \sum_{i=2}^{4} ir_i = 55.\]

Now these equalities are satisfied if and only if \(r_5 = 11\) and \(r_i = 0\) for \(i \geq 6\). Thus all the other regions in this imbedding must have five sides.

We have been considering the 'small' regions in this imbedding. As in the proof of Theorem 4.2 for the finite field of nineteen, we consider the number of sides in the regions at the zero vertex. We know that the zero
vertex must be in a region that contains the three arcs \((22, 0), (0, 0)\) and \((0, 1)\). The next arc in this region could be an additive arc or a multiplicative arc. Suppose it is the additive arc \((1, 2)\). Since the arcs \((22, 2)\) and \((2, 22)\) are not present \((g \neq 11)\), this region must have more than five sides. If the next arc is a multiplicative arc, we note there is no path to vertex 22 that will yield a region with fewer than six sides. This tells us that there must be a region at the zero vertex with more than five sides. This is a contradiction as we have just shown all regions have fewer than six sides. Thus \(C(F_{23}, g)\) cannot be imbedded on the torus. Therefore we know that \(\chi(F_{23}) \geq 2\). □

4.3 The Characterization of the Toroidal Finite Fields

Before we give the characterization we take care of one more special case. We shall show that the finite field of order 16 is not toroidal and then give the characterization of the toroidal finite fields. At this time the genus of the finite field of order 16 is unknown although it is possible to show that the genus of \(F_{16}\) is at least 3.

Lemma 4.4 The finite field of order 16 is not toroidal.

Proof Let \(g\) be a generator for \(F_{16}\). Instead of considering the graph \(D = C(F_{16}, g)\), we will consider the graph \(D'\) where we have replaced each digon that consists of two additive arcs with a single edge. We note that \(\gamma(D) = \gamma(D')\). The graph \(D'\) has order 16, size 48 and is 6 regular. Suppose to
the contrary that we can imbed \( D' \) on \( S_1 \). Then Euler's formula tells us that the number of regions, \( r \), must equal 32. Thus,

\[
\sum_{i \geq 1} r_i = 32, \quad \text{and} \\
\sum_{i \geq 1} i r_i = 96.
\]

The most efficient imbedding of \( D' \) would have \( r_1 = 1, r_2 = 4, \) and \( r_3 = 16 \). We have \( r_1 = 1 \) because of the loop. We have 4 digons, not 16 as stated in Corollary 3.2, since we replaced the digons that arise from two additive arcs with a single edge. Similarly, we have 16 possible 3-cycles in \( D' \) as opposed to 64 as given in Theorem 3.4. Thus our equations above simplify to

\[
\sum_{i \geq 4} r_i = 11
\]

and

\[
\sum_{i \geq 4} i r_i = 39.
\]

Together we have

\[
39 = \sum_{i \geq 4} i r_i \geq 4 \left( \sum_{i \geq 4} r_i \right) = 4(11) = 44.
\]

This is clearly a contradiction and so the finite field of order 16 is not toroidal. \( \Box \)
Theorem 4.5  The finite field of order $q$ is toroidal if and only if $q = 8, 9, 13$ or 17.

Proof  Theorem 3.7 gave us a genus bound for the prime order finite fields. Thus the only possibilities for the toroidal finite fields of prime order have $p \leq 25$. We have already seen that when $p = 2, 3, 5, 7, \text{ and } 11, \gamma(F_p) = 0$. In Lemma 3.12 we showed $\gamma(F_{13}) = 1$. Theorem 3.13 has shown us that the finite field of order 17 is not planar. However, $\gamma(F_{17}) = 1$. The rotation scheme for $C(F_{17}, 14)$ imbedded on $S_1$ can be found in Appendix A. By Theorems 4.2 and 4.3 we know that the finite fields of orders 19 and 23 are not toroidal. Thus we have characterized the prime order finite fields that are toroidal.

Let $t \geq 3$ and let $q = 2^t$. We start with three since we know that the graph $C(F, \alpha + 1)$ is planar. In Lemma 3.11 we showed $\gamma(F_8) = 1$. In Lemma 4.4 we showed that the finite field of order 16 is not toroidal. The graph $Q_t$ is a subgraph of $C(F, g)$ and so $\gamma(Q_t) \leq \gamma(C(F, g))$. By Theorem 1.1.C we know that when $t \geq 5, \gamma(Q_t) \geq 2$. Therefore, in this case, the only toroidal finite field has order 8.

Suppose that $p \geq 3$ is a prime, $t = 2$ and let $q = p^2$. We know that this graph has order $p^2$ and size $3p^2$. Suppose that we can find an imbedding of $D = C(F, g)$ on $S_1$. We shall show that this is only possible when $p = 3$. Using Euler's identity we find that an imbedding of $D$ on $S_1$ would have $r = 2p^2$. From Theorems 3.2 and 3.3 we know that in any
imbedding of $D$, if $p \geq 5$, $r_1 \leq 1$, $r_2 \leq 4$, and $r_3 \leq 16$. Now the most efficient imbedding of $D$ would have $r_1 = 1$, $r_2 = 4$, and $r_3 = 16$. Then,

$$2p^2 - 21 = \sum_{i=4} r_i \quad \text{and} \quad 6p^2 - 57 = \sum_{i=4} ir_i.$$ 

Even if the remaining regions had four sides each we have

$$6p^2 - 57 = \sum_{i=4} ir_i = 4\left(\sum_{i=4} r_i\right) = 4\left(2p^2 - 21\right).$$

Thus $27 \geq 2p^2 \geq 50$, a contradiction. Hence only the case $p = 3$ remains. We know that when $p = 2$, we have a planar finite field. In the proof of Theorem 3.13 we showed that the finite field of order 9 is not planar. It is toroidal since we can find a multiplicative generator that yields a toroidal graph as we have seen in Chapter II (Figure 16).

Now let $p \geq 3$ be a prime, let $t \geq 3$ and let $q = p^t$. In this case, the generalized Cayley graph $C(F_q, g)$ contains a subgraph that is homeomorphic with $C_3 \times C_3 \times C_3$. Since $\gamma(C_3 \times C_3 \times C_3) = 7$, see [3], and $\gamma(C_3 \times C_3 \times C_3) \leq \gamma(C(F_q, g))$, we know that these finite fields are not toroidal. Thus the toroidal finite fields have orders 8, 9, 13, and 17. □

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
CHAPTER V

OTHER GENUS RESULTS

5.1 Asymptotic Results

We know that the process of constructing these generalized Cayley graphs gives us a cartesian product of cycles, a loop at the zero vertex and what we could call a near hamiltonian cycle. That is, if \( q = p' \) the graph \( C(F_{q'}, g) \) can be decomposed into \( (C_p)^{'} \), \( C_{q^{'}-1} \) and a loop. So one may ask, is it possible to say something about the genus of \( C(F_{q'}, g) \) if we know something about the genus of \( (C_p)^{'} \)? When \( p = 2 \), we know the genus of \( (C_p)^{'} \). In general, the genus of \( (C_p)^{'} \) is unknown. However there are asymptotic results when \( p \) is odd[11]. In this section we give asymptotic results for the genus of \( C(F_{q'}, g) \), using this result.

First, we focus our attention to the case when \( p = 2 \). Suppose \( D = C(F_{q'}, g) \). Here the additive generators have order two. Suppose \( \alpha' \) is one such additive generator. Here we replace the two arcs \( (a + \alpha', a) \) and \( (a, a + \alpha') \) with a single undirected edge(see Figure 63). Thus the additive structure of \( D \) is isomorphic to the \( t \)-cube, \( Q_t \).
Theorem 5.1 Let $t \geq 2$, $q = 2^t$, and suppose $D = C(F_q, g)$. Then

$$\gamma(D) = \gamma(Q_t) = 1 + 2^{t-3}(t - 4).$$

Proof. As we have just noted, the additive structure of $D$ is isomorphic to $Q_t$. This tells us that $\gamma(Q_t) \leq \gamma(D)$. However, to get an imbedding of $D$, we may simply add handles to an imbedding of $Q_t$. That is, we may add handles for each multiplicative edge. Of course, we need not add a handle for the loop at zero, nor do we need to add a handle for the $t$ digons that consist of one multiplicative and one additive edge (see Corollary 3.2). We note that this is actually $t$, not $2t$, since we replaced each additive digon with a single edge. This tells us that $\gamma(D) \leq \gamma(Q_t) + 2^t - t - 1$. So we have that

$$\gamma(Q_t) \leq \gamma(D) \leq \gamma(Q_t) + 2^t - t - 1,$$

or rather,

$$1 + 2^{t-3}(t - 4) \leq \gamma(D) \leq 2^{t-3}(t+4) - t.$$
This implies

$$1 \leq \frac{\gamma(D)}{1 + 2^{r-1}(t - 4)} \leq 1 + \frac{2^r - t - 1}{1 + 2^{r-3}(t - 4)}.$$ 

Since \(\frac{2^r - t - 1}{2^{r-3}(t - 4) + 1} \to 0\) as \(t \to \infty\), we have that \(\gamma(D) = 1 + 2^r(t - 4)\), which is equal to \(\gamma(Q_0)\). □

Now we direct our attention to the case where \(p\) is an odd prime. We shall derive an asymptotic result for the finite field of order \(p^r\). We know that, for \(p \geq 5\),

$$1 + \left(\frac{p^2 - 2}{4}\right)p^r \leq \gamma(C_p)^r \leq \left(\frac{p^2 - 2}{4}\right)p^r + \frac{p^2}{4} - \frac{p^2 - 1}{2p - 2} - \frac{p^2}{4} + \frac{p}{4} + 1$$

as shown in \([11]\). We shall use this to prove the following result.

**Theorem 5.2** Let \(p\) be an odd prime and let \(q = p^r\). Let \(D = C(\mathbb{F}_q, g)\). Then,

$$\gamma(D) = \frac{p^{r+1}}{4}.$$ 

**Proof** The subgraph of \(D\) containing all of its additive edges forms a graph that is isomorphic to \((C_p)^r\), the cartesian product of \(p\) cycles of length \(p\). This tells us that \(\gamma(C_p)^r \leq \gamma(D)\). We may find an upper bound for the genus of \(D\) by taking an imbedding of \((C_p)^r\) and adding handles for the multiplicative edges. It is not necessary to add a handle for the loop at
zero, nor do we need to add a handle for the $2p$ digons which consist of one multiplicative and one additive edge (see Theorem 3.1). This tells us that $\gamma(D) \leq \gamma(C_p)^p + p^p - 2p - 1$. Together we have $\gamma(C_p)^p \leq \gamma(D) \leq \gamma(C_p)^p + p^p - 2p - 1$. So our genus bounds for $(C_p)^p$ from above tell us

$$(5.1) \quad 1 + \frac{p - 2}{4} p^p \leq \gamma(D)$$

and

$$(5.2) \quad \gamma(D) \leq \left(\frac{p - 2}{4}\right) p^p + \frac{p^p - 2}{4} + \frac{p^p - 1}{2p - 2} + \frac{p^2}{4} + \frac{p}{4} + 1 + p^p - 2p - 1.$$ 

If we divide both sides of the inequality found in (5.1) by $\frac{p^{p+1}}{4}$, we have

$$\frac{4}{p^{p+1}} + \frac{p - 2}{p} \leq \frac{\gamma(D)}{\frac{p^{p+1}}{4}}.$$ 

Similarly, we may use (5.2) to see that

$$\frac{\gamma(D)}{\frac{p^{p+1}}{4}} \leq \frac{p - 2}{p} + \frac{1}{p - 2} + \frac{2(p^{p-2} - 1)}{(p - 1)p^{p+1}} - \frac{1}{p^{p-1}} + \frac{1}{p} + \frac{4}{p} - \frac{8}{p^p}.$$ 

Then as $p \to \infty$, we have that
This tells us that as \( p \to \infty \), \( \gamma(D) = \frac{p^{p+1}}{4} \). \( \square \)

Corollary 5.3 \( \gamma(\mathbb{F}_{p^t}) = \frac{p^{p+1}}{4} \).

5.2 The Maximum Genus of a Finite Field

As we have seen, determining the genus of a finite field is quite complex. However, finding the maximum genus of a finite field is relatively easy. Recall that the maximum genus of a graph is the maximum genus among all surfaces in which that graph can be 2-cell imbedded. As it turns out, the maximum genus of the graph \( C(\mathbb{F}_q, g) \) is independent of \( g \). Suppose \( g \) and \( h \) generate \( \mathbb{F}_q^* \). Then \( \gamma_M(C(\mathbb{F}_q, g)) = \gamma_M(C(\mathbb{F}_q, h)) \). We will show this in the proof of Theorem 5.4.

Theorem 5.4 Let \( p \) be a prime, let \( t \) be a positive integer and let \( q = p^t \). Suppose that \( g \) generates \( \mathbb{F}_q^* \) and let \( D = C(\mathbb{F}_q, g) \). Then \( D \) is upper imbeddable and

\[
\gamma_M(D) = \left\lfloor \frac{tp^t + 1}{2} \right\rfloor.
\]
Proof Theorem 1.6 tells us that in order to show that $D$ is upper imbeddable, it suffices to show that $D$ has a splitting tree. We note that the multiplicative edges in $D$ form a cycle of length $p' - 1$. In fact, this cycle contains all the vertices except the zero vertex. Let $T$ be the tree formed by taking all but one multiplicative edge along with the edge from zero to one. Then it is clear that $T$ is a spanning tree. We have seen that the additive edges of $D$ form a cartesian product of $t$ $p$-cycles. Thus removing the additive edge from zero to one in this cartesian product leaves a connected graph. Thus, $D - E(T)$ is connected. This tells us that $T$ is in fact a splitting tree. Thus, Theorem 1.6 implies that $D$ is upper imbeddable. Then by Theorem 1.6, we know that

$$\gamma_M(D) = \left\lceil \frac{tp' + 1}{2} \right\rceil.$$ 

We note that this splitting tree is independent of the multiplicative generator. Therefore the maximum genus is independent of the multiplicative generator as well. □

We define the maximum genus of a finite field $\mathbb{F}_q$ to be the maximum genus of $C(\mathbb{F}_{q'} g)$ for any multiplicative generator $g$. So as an immediate corollary to Theorem 5.4 we have the following result.

**Corollary 5.5** $\gamma_M(\mathbb{F}_{q'}) = \left\lceil \frac{tp' + 1}{2} \right\rceil$. 

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
5.3 Finite Number of Finite Fields of a Given Genus

In Chapters III and IV we saw that there is a finite number of finite fields that are planar and toroidal respectively. Let us define the function \( f \) as \( f(n) = |\{ q \mid \gamma(F_q) = n\}| \). Then \( f(0) = 6 \) and \( f(1) = 4 \) by Theorems 3.13 and 4.5.

In Chapter I we noted the theorem by Maschke which shows that there is an infinite number of planar finite groups. There is an infinite number of toroidal finite groups as well [12]. However, for each \( n \geq 2 \), there are only finitely many groups of genus \( n \) [15]. A natural question to ask is whether or not there is always a finite number of finite fields for a given genus. That is, is it true that \( f(n) < \infty \) for all \( n \geq 0 \)? The answer is yes and we prove this below.

**Theorem 5.6** For each \( n \geq 0 \), \( f(n) < \infty \).

**Proof** By Theorem 3.7 we know that the finite field of order \( p \) satisfies

\[
\gamma(F_p) \geq \frac{p^2 - 15}{10}.
\]

So for a fixed genus \( n \) we have only finitely many \( p \) that satisfy the above inequality.

Now let us consider the finite fields of order \( p^2 \). We need not consider the cases \( p = 2 \) and 3 for we know that \( f(0) \) and \( f(1) \) are finite. So let \( p \geq 5 \). By using Theorem 3.8 we get the bound...
\[ \gamma(F_{p^t}) \geq \frac{2p^2 - 15}{10}. \]

Again, for a fixed genus \( n \) we have only finitely many \( p \) that satisfy the above inequality.

Next let us consider the finite field of order \( q = 2^t \), where \( t \geq 3 \). Then we know \( \gamma(F_q) \geq \gamma(Q_t) = 1 + 2^{t-3}(t-4) \). Thus we have finitely many \( t \) which satisfy this inequality for a fixed genus \( n \).

Lastly we consider the finite fields of order \( q = p^t \) where \( p \geq 3 \) and \( t \geq 3 \). Theorem 3.8 gives us a bound for the genus if \( q \neq 2^t \) or \( 3^t \). We wish to include \( 3^t \) and so we modify the proof of Theorem 3.8 to get another bound. To do this we use the bounds for both \( r_1 \) and \( r_2 \); we will not use the bound for \( r_3 \). We note that this theorem excludes the case \( q = 3^t \) when we count the number of possible 3-sided regions. By simply using the bounds for \( r_1 \) and \( r_2 \) we may get a bound which would include the case \( q = 3^t \). So using \( r_1 = 1 \) and \( r_2 = 2t \) we get the bound

\[ \gamma(F_{p^t}) \geq \frac{(t-2)(p^t-2)}{6} \geq \frac{p^3 - 2}{6}. \]

For a fixed genus \( n \), we have finitely many \( p \) which satisfy the inequality

\[ \gamma(F_{p^t}) \geq \frac{p^3 - 2}{6}. \]

Also for each such \( p \) we have finitely many \( t \) which satisfy the inequality

\[ \gamma(F_{p^t}) \geq \frac{(t-2)(p^t-2)}{6}. \]
Therefore, for a fixed $n$ we have finitely many $p'$ which satisfy each of the above inequalities. This tells us that there are finitely many finite fields of a given genus. Thus, for each $n \geq 0$, $f(n) < \infty$. □
CHAPTER VI

CONCLUSIONS

6.1 Conclusions and Open Problems

In Chapter II we calculated various parameters. We still do not know the chromatic number for most generalized cayley graphs for finite fields. Corollary 2.4 tells us that the chromatic number for the graphs that model the prime order finite fields is either 3 or 4. It would be interesting to see how many prime order finite fields have chromatic number 3 and how many have chromatic number 4, if there are any at all. In Theorem 2.5 we found the edge chromatic number for a large class of finite fields; the edge chromatic number for the other finite fields is not yet known. Also in Chapter II we defined and found various automorphism groups. There are many such automorphism groups left to investigate. There is another automorphism group, not mentioned in Chapter II, that could be studied. This would be the automorphism group where we respect directions yet ignore colors.

In Chapter V we showed that $f(n)$ is always finite. In fact, Theorems 3.13 and 4.5 have shown us $f(0) = 6$ and $f(1) = 4$. By using our genus bounds we can show that $1 \leq f(2) \leq 4$. We know that the finite field
of orders 19 has genus 2. The other possibilities for those finite fields $\mathbb{F}_q$ with $\gamma(\mathbb{F}_q) = 2$ are $q = 23, 29$ and 31. As we mentioned in Chapter IV, it is possible to show that $\gamma(\mathbb{F}_{16}) \neq 2$. So the finite fields of genus 2 have prime orders. There are various questions one could ask about the function $f$. First, does $f$ attain a maximum? If $f$ does attain a maximum, where does it occur? In particular, does $f$ attain a maximum at 0? Also, is there an $n$ such that $f(n) = 0$? That is, is there a number $n$ such that there are no finite fields of genus $n$? If there are $n$ such that $f(n) = 0$, how many are there? Are there an infinite or finite number of such $n$?

In Chapter V we found the maximum genus for each finite field and we also obtained some asymptotic results. These asymptotic results were for two classes of finite fields, namely, those of order $2^i$ and order $t^i$. It would be interesting to find asymptotic results for other classes of finite fields, such as those of order $3^i$ and order $5^i$.

Theorem 3.7 gave us bounds for the number of $i$-sided regions, $1 \leq i \leq 4$, for the prime order finite fields. In turn, this gave us a genus bound for those finite fields. Using this we were able to characterize the planar and toroidal finite fields. By counting the number of closed walks of length 5 in these graphs we could improve our genus bound. As we have just mentioned above the finite fields of order 29 and 31 might have genus 2. Perhaps the improved genus bound could show us that these finite fields do not have imbeddings on the double torus.
Throughout this dissertation we have been imbedding these graphs on orientable surfaces. We denote the nonorientable surface of genus $h$ by $N_h$ ($h \geq 1$). The nonorientable genus of a graph $G$, denoted by $\gamma(G)$, is defined to be the minimum $h$ such that $G$ can be imbedded in the nonorientable surface $N_h$. One may define the nonorientable genus of a finite field $\mathbb{F}$ to be

$$\hat{\gamma}(\mathbb{F}) = \min \{ \hat{\gamma}(C(\mathbb{F}, g)) \}$$

where the minimum is taken over all $g$ that generate $\mathbb{F}^*$. Thus we can ask which finite fields have nonorientable genus $h$ for $h \geq 1$? To help answer this question we can follow the strategy we used in the orientable case. That is, we may use Corollary 3.5 along with the nonorientable form of Euler's identity. This form tells us if $G$ is a connected graph of order $n$ and size $m$ that is 2-cell imbedded on $N_h$ with $r$ regions, then $n - m + r = 2 - h$.

We also have various questions if we modify how we define these generalized Cayley graphs. Recall we use one element to generate the multiplicative edges in our graphs. One can also examine the graphs where we use more than one element to generate the set of multiplicative edges, or use an element that does not necessarily give us a cycle of length $q - 1$. For example, we used the element 3 to generate the multiplicative edges for the finite field of order 7. Suppose we use the element 2 instead.
In this case the multiplicative edges would consist of a loop at 0 and two disjoint 3-cycles, as opposed to a loop and a single 6-cycle. We could then define the genus of a finite field to be \( \gamma(F) = \min \{ \gamma(C(F, \Delta)) \} \) where the minimum is taken over all \( \Delta \), where \( 0, 1 \in \Delta \) such that \( \Delta \) is a set of elements that we use to model the multiplicative structure of the finite field. With this definition we could ask all the questions that we answered for our original definition of a generalized Cayley graph.
Appendix A

Rotational Imbedding Schemes for $F_8$, $F_{11}$, $F_{13}$ and $F_{17}$
A Rotation Scheme for an Imbedding of $C(F_g, \alpha)$ on $S_1$.

$p_0 : (0, 0, 1, \alpha^2, \alpha)$
$p_1 : (0, \alpha, \alpha + 1, \alpha^2 + 1, \alpha^2 + \alpha)$
$p_2 : (0, \alpha^2, \alpha^2 + \alpha, \alpha + 1, 1)$
$p_{\alpha_1} : (1, \alpha, \alpha^2, \alpha^2 + \alpha, \alpha^2 + \alpha + 1)$
$p_{\alpha_2} : (0, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha + 1)$
$p_{\alpha_3} : (1, 1, \alpha^2 + \alpha + 1, \alpha^2 + \alpha + 1, \alpha^2)$
$p_{\alpha_4} : (\alpha, \alpha^2, \alpha^2 + \alpha + 1, \alpha^2 + \alpha + 1, \alpha + 1)$
$p_{\alpha_5} : (\alpha + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1, \alpha^2 + 1)$

A Rotation Scheme for an Imbedding of $C(F_g, \alpha^2)$ on $S_1$.

$p_0 : (0, 0, 1, \alpha^2, \alpha)$
$p_1 : (0, \alpha + 1, \alpha^2 + \alpha + 1, \alpha^2 + \alpha)$
$p_2 : (0, \alpha^2 + \alpha, \alpha + 1, 1, \alpha^2 + \alpha)$
$p_{\alpha_1} : (1, \alpha, \alpha^2 + \alpha + 1, \alpha^2 + \alpha + 1)$
$p_{\alpha_2} : (0, 1, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha)$
$p_{\alpha_3} : (1, \alpha^2 + \alpha + 1, \alpha^2 + \alpha + 1, \alpha^2 + \alpha + 1)$
$p_{\alpha_4} : (\alpha, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha + 1, \alpha + 1)$
$p_{\alpha_5} : (\alpha + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1, \alpha^2 + 1)$

A Rotation Scheme for an Imbedding of $C(F_g, \alpha^3)$ on $S_1$.

$p_0 : (0, 0, 1, \alpha^2, \alpha)$
$p_1 : (0, \alpha + 1, \alpha + 1, \alpha^2 + 1, \alpha^2 + \alpha)$
$p_2 : (0, \alpha^2 + \alpha, \alpha^2 + \alpha, \alpha + 1, \alpha + 1)$
$p_{\alpha_1} : (1, 1, \alpha, \alpha^2 + \alpha + 1, \alpha^2 + \alpha + 1)$
$p_{\alpha_2} : (0, \alpha^2 + 1, \alpha^2 + 1, \alpha^2 + \alpha + 1, \alpha^2 + \alpha)$
$p_{\alpha_3} : (1, \alpha + 1, \alpha^2 + \alpha + 1, \alpha^2 + \alpha)$
$p_{\alpha_4} : (1, \alpha^2, \alpha^2 + \alpha + 1, \alpha, \alpha)$
$p_{\alpha_5} : (\alpha + 1, \alpha, \alpha^2 + \alpha, \alpha^2, \alpha^2 + 1)$
A Rotation Scheme for an Imbedding of $C(\mathbb{F}_{11}, 2)$ on $S_1$.

$\rho_0$: (0, 0, 1, 10)
$\rho_1$: (0, 6, 2, 2)
$\rho_2$: (1, 3, 9, 12)
$\rho_3$: (2, 4, 5, 7)
$\rho_4$: (3, 11, 5, 5)
$\rho_5$: (3, 4, 4, 6)
$\rho_6$: (1, 7, 5, 10)
$\rho_7$: (3, 6, 12, 8)
$\rho_8$: (7, 10, 9, 9)
$\rho_9$: (2, 8, 8, 10)
$\rho_{10}$: (6, 9, 8, 11)
$\rho_{11}$: (1, 10, 12, 4)
$\rho_{12}$: (0, 2, 11, 7)

A Rotation Scheme for an Imbedding of $C(\mathbb{F}_{13}, 6)$ on $S_1$.

$\rho_0$: (0, 0, 1, 12)
$\rho_1$: (0, 6, 11, 2)
$\rho_2$: (1, 3, 9, 12)
$\rho_3$: (2, 4, 5, 7)
$\rho_4$: (3, 11, 5, 5)
$\rho_5$: (3, 4, 4, 6)
$\rho_6$: (1, 7, 5, 10)
$\rho_7$: (3, 6, 12, 8)
$\rho_8$: (7, 10, 9, 9)
$\rho_9$: (2, 8, 8, 10)
$\rho_{10}$: (6, 9, 8, 11)
$\rho_{11}$: (1, 10, 12, 4)
$\rho_{12}$: (0, 2, 11, 7)
A Rotation Scheme for an Imbedding of $C(F_{17}, 14)$ on $S_1$.

$\rho_0: (0, 0, 1, 16)$
$\rho_1: (0, 14, 11, 2)$
$\rho_2: (1, 11, 5, 3)$
$\rho_3: (2, 4, 8, 16)$
$\rho_4: (3, 5, 5, 10)$
$\rho_5: (2, 6, 4, 4)$
$\rho_6: (5, 15, 16, 7)$
$\rho_7: (6, 8, 9, 13)$
$\rho_8: (3, 10, 9, 7)$
$\rho_9: (7, 8, 10, 14)$
$\rho_{10}: (4, 11, 9, 8)$
$\rho_{11}: (1, 10, 12, 2)$
$\rho_{12}: (11, 13, 13, 15)$
$\rho_{13}: (7, 14, 12, 12)$
$\rho_{14}: (1, 15, 13, 9)$
$\rho_{15}: (6, 12, 14, 16)$
$\rho_{16}: (0, 3, 6, 15)$
Appendix B

The Graphs $C(\mathbb{F}_{19}, g)$ and $C(\mathbb{F}_{23}, g)$
$C(F_{19}, 2)$
$C(F_{19}, 3)$
$C(F_{19}, 14)$
$C(\mathbb{F}_{23}, 5)$
$C(\mathbb{F}_{23}, 7)$
$C(F_{23}, 11)$
$C(\mathbb{F}_{25}, 15)$
$C(\mathbb{F}_{23}, 17)$
Appendix C

Rotational Embedding Schemes for $F_{19}$
A Rotation Scheme for an Imbedding of $C(F_{19}, 3)$ on $S_2$.

$\rho_0$: (0, 0, 1, 18)  
$\rho_1$: (0, 13, 3, 2)  
$\rho_2$: (1, 3, 7, 6)  
$\rho_3$: (1, 4, 9, 2)  
$\rho_4$: (3, 14, 12, 5)  
$\rho_5$: (4, 15, 6, 8)  
$\rho_6$: (2, 7, 5, 18)  
$\rho_7$: (2, 15, 8, 6)  
$\rho_8$: (5, 7, 9, 9)  
$\rho_9$: (3, 8, 8, 10)  
$\rho_{10}$: (9, 11, 11, 16)  
$\rho_{11}$: (10, 10, 14, 12)  
$\rho_{12}$: (4, 11, 13, 17)  
$\rho_{13}$: (1, 17, 12, 14)  
$\rho_{14}$: (4, 13, 11, 15)  
$\rho_{15}$: (5, 16, 14, 7)  
$\rho_{16}$: (10, 15, 17, 18)  
$\rho_{17}$: (12, 13, 18, 16)  
$\rho_{18}$: (0, 6, 16, 17)
A Rotation Scheme for an Imbedding of $C(F_{19}, 2^1)$ on $S_2$.

$\rho_0$: (0, 0, 1, 18)
$\rho_1$: (0, 2, 2, 10)
$\rho_2$: (1, 1, 4, 3)
$\rho_3$: (2, 4, 6, 11)
$\rho_4$: (2, 8, 5, 3)
$\rho_5$: (4, 10, 12, 6)
$\rho_6$: (3, 5, 12, 7)
$\rho_7$: (6, 13, 14, 8)
$\rho_8$: (4, 16, 7, 9)
$\rho_9$: (8, 14, 18, 10)
$\rho_{10}$: (1, 11, 5, 9)
$\rho_{11}$: (3, 15, 12, 10)
$\rho_{12}$: (5, 11, 13, 6)
$\rho_{13}$: (7, 12, 16, 14)
$\rho_{14}$: (7, 13, 15, 9)
$\rho_{15}$: (11, 14, 16, 17)
$\rho_{16}$: (8, 17, 15, 13)
$\rho_{17}$: (15, 16, 18, 18)
$\rho_{18}$: (0, 9, 17, 17)
A Rotation Scheme for an Imbedding of $C(F_{19}, 14)$ on $S_2$.

$\rho_0$: (0, 0, 1, 18)
$\rho_1$: (0, 2, 14, 15)
$\rho_2$: (1, 3, 9, 11)
$\rho_3$: (2, 4, 4, 7)
$\rho_4$: (3, 3, 18, 5)
$\rho_5$: (4, 18, 13, 6)
$\rho_6$: (5, 14, 8, 7)
$\rho_7$: (3, 6, 8, 10)
$\rho_8$: (6, 9, 17, 7)
$\rho_9$: (2, 10, 8, 12)
$\rho_{10}$: (7, 11, 17, 9)
$\rho_{11}$: (2, 12, 13, 10)
$\rho_{12}$: (9, 16, 13, 11)
$\rho_{13}$: (5, 11, 12, 14)
$\rho_{14}$: (1, 6, 13, 15)
$\rho_{15}$: (1, 14, 16, 16)
$\rho_{16}$: (12, 17, 15, 15)
$\rho_{17}$: (8, 10, 18, 16)
$\rho_{18}$: (0, 17, 5, 4)
REFERENCES


