School of Mathematics and Statistics

GRAPHS WITH PRESCRIBED
ADJACENCY PROPERTIES

WATCHARAPHONG ANANCHUEN

This thesis is presented as part of the requirements for the award of
Degree of Doctor of Philosophy
of
Curtin University of Technology

December 1993
DEDICATION

To my beloved mother,

in the memory of my father

and

to my wife Nawarat, for her interest and encouragement.
CERTIFICATION

I certify that the work presented in this thesis is my own work and that all references are duly acknowledged. This thesis has not been submitted previously, in whole or in part, in respect of any academic award at Curtin University of Technology or elsewhere.

Watcharaphong Ananchuen

December 1993
SUMMARY

A graph $G$ is said to have property $P(m,n,k)$ if for any set of $m + n$ distinct vertices there are at least $k$ other vertices, each of which is adjacent to the first $m$ vertices but not adjacent to any of the latter $n$ vertices. The class of graphs having property $P(m,n,k)$ is denoted by $\mathcal{G}(m,n,k)$. The problem that arises is that of characterizing the class $\mathcal{G}(m,n,k)$. One particularly interesting problem that arises concerns the function

$$p(m,n,k) = \min\{\nu(G) : G \in \mathcal{G}(m,n,k)\}.$$

In Chapter 2, we establish some important properties of graphs in the class $\mathcal{G}(m,n,k)$ and a lower bound on $p(m,n,k)$. In particular, we prove that

$$p(n,n,k) \geq 4^{n-1}[2(n + k) + \frac{1}{2}(3 + (-1)^{n+k+1}) + \frac{1}{3}] - \frac{1}{3}.$$

One of the results in Chapter 2 is that almost all graphs have property $P(m,n,k)$. However, few members of $\mathcal{G}(m,n,k)$ have been exhibited. In Chapter 3, we construct classes of graphs having property $P(1,n,k)$. These classes include the cubes, "generalized" Petersen graphs and "generalized" Hoffman-Singleton graphs.

An important graph in the study of the class $\mathcal{G}(m,n,k)$ is the Paley graph $G_q$, defined as follows. Let $q = 1(\text{mod } 4)$ be a prime power. The vertices of $G_q$ are the elements of the finite field $\mathbb{F}_q$. Two vertices $a$ and $b$ are joined by an edge if and only if
their difference is a quadratic residue, that is $a - b = y^2$ for
some $y \in \mathbb{F}_q$. In chapter 4, we prove that for a prime $p \equiv 1(\text{mod} 4)$, all sufficiently large Paley graphs $G_p$ satisfy property $P(m,n,k)$. This is established by making use of results from prime
number theory.

In Chapter 5, we establish, by making use of results from
finite fields, the adjacency properties of Paley graphs of order
$q = p^d$, with $p$ a prime. In particular, we show that for a prime
power $q \equiv 1(\text{mod} 4)$,

- $G_q \in \mathcal{S}(1,n,k) \cap \mathcal{S}(n,1,k)$, for every
  
  $$q > ((n - 2)2^n + 2)\sqrt{q} + (n + 2k - 1)2^n - 2n - 1;$$

- $G_q \in \mathcal{S}(n,n,k)$, for every
  
  $$q > ((2n - 3)2^{2n-1} + 2)\sqrt{q} + (n + 2k - 1)2^{2n-1} - 2n^2 - 1;$$

and

- $G_q \in \mathcal{S}(m,n,k)$, for every
  
  $$q > ((t - 3)2^{t-1} + 2)\sqrt{q} + (t + 2k - 1)2^{t-1} - 1,$$

where $m + n \leq t$.

For directed graphs, there is an analogue of the above
adjacency property concerning tournaments. A tournament $T_q$ of
order $q$ is said to have property $Q(n,k)$ if every subset of $n$
vertices of $T_q$ is dominated (if there is an arc directed from a
vertex $u$ to a vertex $v$, we say that $u$ dominates $v$ and that $v$ is
dominated by $u$) by at least $k$ other vertices.

Let $q = 3(\text{mod} 4)$ is a prime power. The Paley tournament $D_q$
is defined as follows. The vertices of $D_q$ are the elements of the
finite field $\mathbb{F}_q$. Vertex $a$ is joined to vertex $b$ by an arc if and
only if $a - b$ is a quadratic residue in $\mathbb{F}_q$. In Chapter 6, we
prove that the Paley tournament $D_q$ has property $Q(n,k)$ whenever

$$q > \{(n - 3)2^{n-1} + 2\sqrt{q} + k2^n - 1\}.$$

A graph $G$ is said to have property $P^*(m,n,k)$ if for any set

of $m + n$ distinct vertices of $G$ there are exactly $k$ other

vertices, each of which is adjacent to the first $m$ vertices of the

set but not adjacent to any of the latter $n$ vertices. The class

of graphs having property $P^*(m,n,k)$ is denoted by $\mathcal{P}^*(m,n,k)$. The

class $\mathcal{P}^*(m,n,k)$ has been studied when one of $m$ or $n$ is zero. In

Chapter 7, we show that, for $m = n = 1$, graphs with this property

are the strongly regular graphs with parameters $\left(\frac{(k + t)^2}{t} + 1, k + t, t - 1, t\right)$ for some positive integer $t$. For $m \geq 1$, $n \geq 1$, and

$m + n \geq 3$, we show that, there is no graph having property

$P^*(m,n,k)$, for any positive integer $k$.

The first Chapter of this thesis provides the motivation, terminology, general concepts and the problems concerning the

adjacency properties of graphs. In Chapter 8, we present some

open problems.
ACKNOWLEDGEMENTS

I am grateful to Prof. Lou Caccetta, my thesis supervisor, for the invaluable guidance considerately offered during the period of my study. His suggestions and careful reading have been of great value to me in the preparation and completion of this thesis. I would like to express my thanks to Sue Woods for her valuable help. Special thanks to Mr. Peter Caccetta for his assistance with the computational work. Also thanks to my fellow graduate students for their friendships and encouragement during the period of my study.

I am grateful to Curtin University of Technology for providing me a Curtin Overseas Student Scholarship (COSS). My deep appreciation goes to Sukhothai Thammathirat Open University for allowing me to study here. I also like to thank Sukhothai Thammathirat Open University and Prof. Lou Caccetta for their kind financial support given during the period of my study.

Finally, I wish to thank the School of Mathematics and Statistics for providing me with the necessary facilities, and all the staff in the School for their assistance.
6. **PALEY TOURNAMENTS**
   6.1 Preliminaries  120
   6.2 Results  124
   6.3 Property R(n,k)  135
   6.4 Paley Digraphs  136

7. **STRONG ADJACENCY PROPERTY**  138
   7.1 Preliminaries  139
   7.2 The Class $S^*(1,1,k)$  141
   7.3 The Class $S^*(m,n,k)$, $m \geq 1$, $n \geq 1$ and $m + n \geq 3$  151
   7.4 Property $P^*(n,k)$  153

8. **SOME OPEN PROBLEMS**  156

**REFERENCES**  162
CHAPTER 1
INTRODUCTION

Over its 250 year history, graph theory has enjoyed considerable success in problem solving and has developed into an elegant and rapidly growing branch of mathematics. In particular, it has undergone a period of spectacular growth over the past twenty years or so. This is well reflected by the number of books and the numerous research papers that have been published in this area. A major reason for this rapid growth is its applicability to a wide range of problems arising in science, engineering, computer science, modern business and many more. Our objective in this thesis is to study some theoretical aspects of graph theory which have some applications in the area of network design and analysis. For a detailed discussion on graph theory applications we refer to the expository papers of Caccetta (1989) and Caccetta and Vijayan (1987).

The very simple structure of a graph, as a collection of points called vertices together with a set of lines called edges such that each edge is identified with a pair of vertices, makes it suitable for modeling a wide variety of situations. For instance, graphs can be conveniently used to represent many complex networks consisting of components, some of which interact. For example: communication networks for the transmission of information; transportation networks for the movement of commodities; data communication networks capable of supporting
large scale on-line applications and powerful multiprocessor systems for solving complex problems such as radar signal processing. In the graph model of such systems, the vertices represent the components and the edges (or arcs where orientation is a factor) represent the interaction between components.

A fundamental network design problem [see Caccetta (1989)] is to construct a network that satisfies certain requirements and that is optimal according to some criterion such as cost, throughput, reliability, delay time or traffic density. In the graph model, the requirements of the network (such as efficiency and reliability) can be expressed in terms of restrictions on the values of certain graph parameters such as connectivity, edge-connectivity, diameter and independence number.

In this thesis, we focus on networks whose requirements translate into adjacency restrictions on the graph representing the network. The particular adjacency properties that we consider are defined in Section 1.2. This section also contains an overview of the thesis. In Section 1.1, we introduce some basic graph theory notation and terminology.

1.1 Notation and Terminology

As there is considerable variation in the graph theory notation and terminology used in the literature, we present, in this section, the basic notation and terminology that we use throughout this thesis. We use standard set theoretic notation. For the most part, our graph theoretic notation and terminology follows that of Bondy and Murty (1976). We now give, for completeness, a more formal presentation of the concepts used in this thesis.
The cardinality of a set \( X \) is denoted by \( |X| \). Given a set \( X \), we are usually interested in subsets of \( X \) having some specified property. Suppose \( S \subseteq X \) has property \( P \). \( S \) is said to be maximal with respect to \( P \) if there is no other set \( S' \subseteq X \) such that \( S' \) has property \( P \) and \( S \) is a proper subset of \( S' \). If \( |S| \geq |S'| \) for any other set \( S' \subseteq X \) that has property \( P \), then \( S \) is said to be maximum with respect to property \( P \). The terms minimal and minimum are analogously defined.

A graph \( G \) is an ordered triple \((V(G), E(G), \psi_G)\) consisting of a non-empty set \( V(G) \) of vertices and a set \( E(G) \), disjoint from \( V(G) \), of edges and an incidence function \( \psi_G \) that associates with each edge of \( G \) an unordered pair of (not necessarily distinct) vertices of \( G \). If \( u \) and \( v \) are vertices of the graph \( G \) identified with an edge \( e \), that is \( \psi_G(e) = uv \), then \( e \) is said to join \( u \) and \( v \), and we write \( e = uv \). We also say that \( u \) and \( v \) are adjacent, and the edge \( e \) is incident with \( u \); vertices \( u \) and \( v \) are called the ends of \( e \).

If for a graph \( G \) both \( V(G) \) and \( E(G) \) are finite sets, then we say that \( G \) is finite. The number of vertices of a graph \( G \) is usually called the order of \( G \) and is denoted by \( v(G) \). Similarly, the number of edges of \( G \), denoted by \( e(G) \), is called the size of \( G \). Thus \( v(G) = |V(G)| \) and \( e(G) = |E(G)| \). A loop is an edge of a graph joining a vertex to itself. Two or more edges joining the same pair of vertices are called multiple edges. A graph with no loops and no multiple edges is called a simple graph. The trivial graph is a simple graph having exactly one vertex. For our purposes, graphs are finite and simple.

To any graph \( G \) there corresponds a \( v \times v \) matrix called the adjacency matrix of \( G \). Let us denote the vertices of \( G \) by \( v_1, v_2, \ldots, v_v \). Then the adjacency matrix of \( G \) is the matrix \( A(G) = \)
$[a_{ij}]$, where $a_{ij}$ is the number of edges joining $v_i$ and $v_j$.

For disjoint subsets $A$ and $B$ of $V(G)$ we find it very convenient to use the following special notation in our work. We denote by $N(A/B)$ the set of vertices of $G$ not in $A \cup B$ which are adjacent to each vertex of $A$ and not adjacent to any vertex of $B$. When $A = \{a_1, a_2, \ldots, a_m\}$ and $B = \{b_1, b_2, \ldots, b_n\}$ we sometimes write, for convenience, $N(A/B)$ as $N(a_1, a_2, \ldots, a_m/b_1, b_2, \ldots, b_n)$. Further, we extend our notation so that for $X \subseteq V(G)$, $N(X/-)$ denotes the set of vertices of $G - X$ which are adjacent to every vertex of $X$ and $N(-/X)$ denotes the set of vertices of $G - X$ which are non-adjacent to any vertex of $X$. We call $N(X/-)$ the neighbour set of $X$ in $G$ and $N(-/X)$ the non-neighbour set of $X$ in $G$. Note that $X$ can be a single element. So if $X = \{x\}$, then $N(x/-)$ is the neighbour set of $x$ in $G$ and $N(-/x)$ is the non-neighbour set of $x$ in $G$. Where appropriate, lower case letters will denote the cardinality of the set defined by the corresponding upper case letters. Thus, for example, $n(a/b) = |N(a/b)|$.

The degree of a vertex $u$ in a graph $G$, denoted by $d_G(u)$, is $n(u/-)$, the number of edges of $G$ incident to $u$. It is very well-known that for any graph $G$,

$$\sum_{u \in V(G)} d_G(u) = 2e(G).$$

The minimum and maximum degrees of a graph $G$ are denoted by $\delta(G)$ and $\Delta(G)$, respectively. If $\delta(G) = \Delta(G) = r$, then $G$ is called an $r$-regular graph. In view of the above equation, an $r$-regular graph on $n$ vertices exists only if $r$ or $n$ is even. Further, it has $\frac{1}{2}r n$ edges.
Regular graphs are a special class of graphs. There are many other special classes of graphs. The empty graph is the graph with no edges. A complete graph is one with every pair of vertices adjacent. The complete graph on \( n \) vertices is denoted by \( K_n \). Note that \( K_n \) is an \((n - 1)\)-regular graph with \( e(K_n) = \frac{1}{2}n(n - 1) \). \( K_1 \) is, of course, the trivial graph. A graph \( G \) is bipartite if \( V(G) \) can be partitioned into two subsets \( X \) and \( Y \) such that each edge joins a vertex in \( X \) to some vertex in \( Y \). A complete bipartite graph is a bipartite graph with bipartitioning sets \( X \) and \( Y \) in which each vertex in \( X \) is joined to each vertex in \( Y \); such a graph is denoted by \( K_{m,n} \) when \( |X| = m \) and \( |Y| = n \).

An \( r \)-regular graph \( G \) of order \( n \) is called strongly regular with parameters \((\nu,r,\lambda,\mu)\), if \( G \) has the property that any two adjacent vertices have exactly \( \lambda \) common neighbours and any two non-adjacent vertices have exactly \( \mu \) common neighbours. A strongly regular graph with parameters \((4t + 1,2t,t - 1,t)\), where \( t \) is a positive integer, is called a pseudo-cyclic (PC) graph.

We call two graphs \( H \) and \( G \) isomorphic (written \( H \cong G \)) if there exists a one to one correspondence between their vertex sets that preserves adjacency.

A graph \( H = (V(H),E(H),\psi_H) \) is a subgraph of \( G = (V(G),E(G),\psi_G) \) if \( V(H) \subseteq V(G) \), \( E(H) \subseteq E(G) \) and \( \psi_H \) is the restriction of \( \psi_G \) to \( E(H) \). Further, if \( H \neq G \), we call \( H \) a proper subgraph of \( G \) and if \( V(H) = V(G) \), we call \( H \) a spanning subgraph of \( G \). Suppose that \( V' \) is a non-empty subset of \( V(G) \), the subgraph of \( G \) induced by \( V' \), denoted by \( G[V'] \), is a graph with vertex set \( V' \) and \( E(G[V']) = \{uv \in E(G) : u, v \in V'\} \). The subgraph \( G[E'] \) of \( G \) induced by \( E' \subseteq E(G) \) is similarly defined. Let \( S \subseteq V(G) \). Then \( G - S \) is the subgraph obtained from \( G \) by deleting the vertices of
S together with their incident edges. When \( S = \{v\} \), we write \( G - v \) instead of \( G - \{v\} \). The spanning subgraph of \( G \) obtained by deleting the edges in \( R \subseteq E(G) \) is denoted by \( G - R \). Similarly, if \( R = \{e\} \), we write \( G - e \) instead of \( G - \{e\} \).

The complement \( \overline{G} \) of a graph \( G \) is the graph with vertex set \( V(G) \), two vertices being adjacent in \( \overline{G} \) if and only if they are not adjacent in \( G \). When \( H \) is a subgraph of \( G \), the complement \( \overline{H}(G) \) of \( H \) in \( G \) is the subgraph \( G - E(H) \).

A matching in \( G \) is a one-regular subgraph of \( G \). A one-regular spanning subgraph is called a perfect matching.

A subset \( S \) of \( V(G) \) is called an independent set of \( G \) if no two vertices of \( S \) are adjacent in \( G \). A clique of a simple graph \( G \) is a subset \( S \) of \( V \) such that \( G[S] \) is complete. Clearly, \( S \) is a clique of \( G \) if and only if \( S \) is an independent set in \( \overline{G} \), and so the two concepts are complementary.

Given any positive integers \( k \) and \( \ell \), the Ramsey number is the smallest integer \( r(k, \ell) \) such that every graph on \( r(k, \ell) \) vertices contains either a clique of \( k \) vertices or an independent set of \( \ell \) vertices.

Let \( G_1 \) and \( G_2 \) be graphs. The union \( G_1 \cup G_2 \) of \( G_1 \) and \( G_2 \) is a graph with vertex set \( V(G_1) \cup V(G_2) \) and edge set \( E(G_1) \cup E(G_2) \). The graphs \( G_1 \) and \( G_2 \) are disjoint if \( V(G_1) \cap V(G_2) = \emptyset \); \( G_1 \) and \( G_2 \) are edge disjoint if \( E(G_1) \cap E(G_2) = \emptyset \). If \( G_1 \) and \( G_2 \) are disjoint, we sometimes denote their union by \( G_1 \cup G_2 \). The intersection \( G_1 \cap G_2 \) of \( G_1 \) and \( G_2 \) is defined similarly, but in this case \( G_1 \) and \( G_2 \) must have at least one vertex in common. The join \( G \vee H \) of disjoint graphs \( G \) and \( H \) is the graph obtained from \( G + H \) by joining each vertex of \( G \) to each vertex of \( H \).
A walk in a graph \( G \) is a finite, non-empty alternating sequence \( W = v_0, e_1, v_1, e_2, \ldots, e_n, v_n \) of vertices and edges, such that, for \( 1 \leq i \leq n \), the ends of edge \( e_i \) are \( v_{i-1} \) and \( v_i \). \( W \) is said to be a walk from \( v_0 \) (the origin) to \( v_n \) (the terminus), or simply a \((v_0, v_n)\)-walk. Further, the length of \( W \) is the number of edges in \( W \). In our case, since all graphs are simple, we denote the walk \( W = v_0, v_1, v_2, \ldots, v_n \). A closed walk is a walk whose origin and terminus are the same. A path is a walk with distinct vertices.

A cycle \( C \) is a closed walk \( v_1, v_2, \ldots, v_n, v_1 \), where \( n \geq 3 \) and \( v_1, v_2, \ldots, v_n \) are distinct vertices. A cycle of length \( n \) is called an \( n \)-cycle and denoted by \( C_n \). A triangle is a 3-cycle. A graph is triangle-free if it contains no triangles. The girth of a graph \( G \) is the length of a shortest cycle in \( G \); if \( G \) has no cycles we define the girth of \( G \) to be infinite. An \( r \)-regular graph of girth \( g \) with the least possible number of vertices is called an \((r,g)\)-cage.

Two vertices \( u \) and \( v \) of \( G \) are connected if there is a \((u,v)\)-path in \( G \). If every pair of vertices of \( G \) are connected, then we say \( G \) is connected; otherwise, \( G \) is disconnected.

Throughout this thesis \( G \) denotes a graph. Further, when no confusion arises we sometimes omit the letter \( G \) from graph theoretic symbols. Thus, for example, we may write \( \nu, \varepsilon, \delta \) and \( \Delta \) instead of \( \nu(G), \varepsilon(G), \delta(G) \) and \( \Delta(G) \), respectively.

If we think of the edge between two vertices as an ordered pair, a natural direction from the first vertex to the second vertex can be associated with the edge. Such an edge will be called an arc (to maintain the historical terminology), and a graph in which each edge has such a direction will be called a directed graph or digraph. Formally, a digraph \( D \) is an ordered
triple \((V(D), A(D), \psi_D)\) consisting of a non-empty set \(V(D)\) of vertices, a set \(A(D)\), disjoint from \(V(D)\), of arcs and an incidence function \(\psi_D\) that associates with each arc of \(D\) an ordered pair of (not necessarily distinct) vertices of \(D\). If \(a\) is an arc and \(u\) and \(v\) are vertices such that \(\psi_D(a) = (u, v)\), then \(a\) is said to join \(u\) to \(v\); \(u\) is the tail of \(a\), and \(v\) is its head. A digraph \(D'\) is a subdigraph of \(D\) if \(V(D') \subseteq V(D)\), \(A(D') \subseteq A(D)\) and \(\psi_D\) is the restriction of \(\psi_D\) to \(A(D')\). The terminology and notation for subdigraphs is similar to that used for subgraphs.

To any digraph \(D\) there corresponds a \(v \times v\) matrix called the adjacency matrix of \(D\). Let us denote the vertices of \(D\) by \(v_1, v_2, \ldots, v_v\). Then the adjacency matrix of \(D\) is the matrix \(M(D) = [m_{ij}]\) where \(m_{ij}\) is the number of arcs of \(D\) with tail \(v_i\) and head \(v_j\).

With each digraph \(D\) we can associate a graph \(G\) on the same vertex set and corresponding to each arc of \(D\) there is an edge of \(G\) with the same ends. This graph is the underlying graph of \(D\). Conversely, given any graph \(G\), we can obtain a digraph from \(G\) by specifying a direction for each edge of \(G\). Such a digraph is called an orientation of \(G\).

For digraphs, the number of arcs directed away from a vertex \(u\) is called the outdegree of \(u\), denoted by \(d_D^+(u)\), and the number of arcs directed to a vertex \(u\) is the indegree, denoted by \(d_D^-(u)\), of \(u\). We denote the minimum and maximum indegree and outdegree in \(D\) by \(\delta^-(D)\), \(\Delta^-(D)\), \(\delta^+(D)\) and \(\Delta^+(D)\), respectively. In a digraph, we define the degree of a vertex \(u\) to be \(d_D^-(u) + d_D^+(u)\). A digraph is strict if it has no loops and no two arcs with the same ends have the same orientation. Also, as with undirected graphs, we shall drop the letter \(D\) from our notation whenever possible; thus we write \(A\) for \(A(D)\), \(d^+(u)\) for \(d_D^+(u)\), \(\delta^-\) for \(\delta^-(D)\).
and so on.

An orientation of a complete graph is called a tournament. If there exists an arc directed away from a vertex \( u \) to a vertex \( v \), we say that \( u \) dominates \( v \) and that \( v \) is dominated by \( u \).

1.2  Review and Summary of Thesis

The major focus of this thesis is the study of graphs having a prescribed adjacency property. More specifically, a graph \( G \) is said to have property \( P(m,n,k) \) if for any set of \( m + n \) distinct vertices there are at least \( k \) other vertices, each of which is adjacent to the first \( m \) vertices but not adjacent to any of the latter \( n \) vertices. The class of graphs having property \( P(m,n,k) \) is denoted by \( \mathcal{Y}(m,n,k) \). The cycle \( C_v \) of length \( v \) is a member of \( \mathcal{Y}(1,1,1) \) for every \( v \geq 5 \). The well-known Petersen graph is a member of \( \mathcal{Y}(1,2,1) \) and also of \( \mathcal{Y}(1,1,2) \), see Figure 1.2.1.

![Figure 1.2.1: The cycle of length 5 and the Petersen graph.](image)

Despite these relatively simple examples, few members of \( \mathcal{Y}(m,n,k) \) have been found. The problem that arises [see Caccetta (1989), Problem 3.12] is that of characterizing the class \( \mathcal{Y}(m,n,k) \). In Chapter 2, we establish some basic properties of graphs in the class \( \mathcal{Y}(m,n,k) \). Two particularly interesting
problems that arise concern the functions

\[ p(m,n,k) = \min \{ \nu(G) : G \in \mathcal{G}(m,n,k) \} \]

and

\[ q(l, (m,n,k)) = \min \{ c(G) : \nu(G) = l, G \in \mathcal{G}(m,n,k) \}. \]

The only result concerning the latter function is due to Erdös and Moser (1970) who determined \( q(l, (m,0,1)) \). Exoo (1981) established the following bound on \( p(n,n,1) \):

**Theorem 1.2.1:** (Exoo). For all \( n \geq 1 \)

\[
p(n,n,1) \geq 4^{n-1} \left\{ 2n + \frac{1}{2} \left[ 7 + (-1)^n \right] \right\} + \frac{1}{3} 4^{n-1}. \]

\[ \square \]

In Chapter 2, we extend this result and obtain bounds for \( p(n,n,k) \) and \( p(m,n,k) \). In particular, we prove:

- \( p(n,n,k) \geq 4^{n-1} \left[ 2(n + k) + \frac{1}{2} \left( 3 + (-1)^{n+k+1} \right) + \frac{1}{3} \right] - \frac{1}{3} \); and

- \( p(m,n,k) \geq 4^{t-1} \left[ 2(t + k') + \frac{1}{2} \left( 3 + (-1)^{n+k'+1} \right) + \frac{1}{3} \right] - \frac{1}{3}, \)

where \( t = \min\{m,n\} \) and \( k' = k + |m - n| \).

For a property \( P \), we denote the class of graphs having property \( P \) by \( \mathcal{G}_P \). Let \( \mathcal{G}_\nu \) be the family of all graphs with \( \nu \) vertices. We say that almost all graphs have property \( P \) if the ratio of the number of graphs of order \( \nu \) having property \( P \) to the total number of graphs of order \( \nu \) approaches unity as \( \nu \to \infty \), that is
\[
\lim_{\nu \to \infty} \frac{|\mathcal{G}_\nu \cap \mathcal{G}_P|}{|\mathcal{G}_\nu|} = 1.
\]

Blass and Harary (1979) established, using probabilistic methods, that almost all graphs have property \(P(n,n,1)\). Note that this result was proved earlier, using symbolic logic, by Fagin (1976). From this it is not too difficult to show that almost all graphs have property \(P(m,n,k)\); we do this in Chapter 2. Despite this result, few graphs have been constructed which exhibit the property \(P(m,n,k)\). In Chapter 3, we construct classes of graphs having property \(P(1,n,k)\). These classes include the cubes, "generalized" Petersen graphs and "generalized" Hoffman-Singleton graphs.

Exoo and Harary (1980) studied the class \(\mathcal{G}(1,n,1)\) and established a number of important properties including the connection with cages. They established that for \(n \leq 6\) the smallest order graphs of this class are the \((n + 1,5)\)-cages. In particular, they proved:

**Theorem 1.2.2:** (Exoo and Harary). The smallest graph in \(\mathcal{G}(1,2,1)\) is the Petersen graph which has order 10 and is the \((3,5)\)-cage. Every other graph in \(\mathcal{G}(1,2,1)\) has at least 12 vertices.  

**Theorem 1.2.3:** (Exoo and Harary). Robertson's graph (see Figure 1.2.2), the \((4,5)\)-cage, is the smallest graph in \(\mathcal{G}(1,3,1)\).
In Chapter 3, we construct all graphs in the class $\mathcal{S}(1,2,1)$ with 12 vertices and establish that $\mathcal{S}(1,2,1) \neq \emptyset$ for every order $n$, $n \geq 10$, except $n = 11$.

Exoo (1981) proved the following result.

Lemma 1.2.4: (Exoo). If $G$ has girth at least 5 and $\delta \geq n + k$, then $G \in \mathcal{S}(1,n,k)$.

Exoo and Harary (1980) conjectured that if $G \in \mathcal{S}(1,n,1)$ and $G$ has girth at most 4, then $\nu(G) \geq n^2 + 3n + 2$. For $n \leq 6$, they proved this conjecture by considering each value of $n$ separately. Caccetta and Vijayan (1986) established, by non-elementary counting methods, the conjecture for all graphs for which

$$\min\{d_G(u) : u \in V(G) \text{ and } d_G(u) > n + 1\} \leq \frac{1}{2}(3n + 2).$$
Exoo and Hamada (1980) proved that $31 \leq p(2,2,1) \leq 61$. Exoo (1981) and Caccetta, Vijayan and Wallis (1984) proved that $p(2,2,1) = 34$. Moreover, Caccetta, Vijayan and Wallis (1984) proved that, if $G \in \mathcal{G}(2,2,1)$, then $\delta(G) \geq 15$. Further, Exoo (1981) observed a connection with the Ramsey numbers and conjectured that

$$p(2,2,1) = r(5,5) - 1.$$ 

Caccetta, Vijayan and Wallis (1984) established the following result.

**Theorem 1.2.5:** (Caccetta, Vijayan and Wallis). Let $G \in \mathcal{G}(2,2,1)$ and

$$t = \min \{n(u/v)\}, \quad u, v \in G$$

Then $\nu(G) \geq 4t + 1$ with equality possible only if $G$ is a PC-graph with parameters $(4t + 1, 2t, t - 1, t)$.

In Chapter 2, we extend this result to the class $\mathcal{G}(2,2,k)$ for any positive integer $k$. In particular, we prove that:

- For $G \in \mathcal{G}(2,2,k)$

$$\nu(G) \geq \begin{cases} 34, & \text{if } k = 1, \\ 8k + 25, & \text{if } k \geq 3 \text{ and } k \text{ is odd}, \\ 8k + 21, & \text{otherwise}, \end{cases}$$

with equality possible only if $G$ is a PC-graph with parameters $(4t_0 + 1, 2t_0, t_0 - 1, t_0)$, where

$$t_0 = \min \{n(u/v)\}, \quad u, v \in G$$
Exoo and Harary (1983) studied the smallest graphs of girth 3 and 4 with the property P(1,2,1) and P(1,3,1). In particular, they constructed smallest graphs in the class $\mathcal{G}(1,2,1)$ with girth 3 and 4, and a smallest graph in the class $\mathcal{G}(1,3,1)$ with girth 3. Their graphs are shown in the figures 1.2.3 and 1.2.4.

Figure 1.2.3: Smallest graphs in $\mathcal{G}(1,2,1)$ having girth 3 and girth 4, respectively.

Figure 1.2.4: A smallest graph in $\mathcal{G}(1,3,1)$ having girth 3.
An important graph in the study of the class $\mathcal{S}(m,n,k)$ is the so-called **Paley graph** $G_q$ defined as follows [see Paley (1933)]. Let $q \equiv 1(\text{mod } 4)$ be a prime power. The vertices of $G_q$ are the elements of the finite field (Galois field) $\mathbb{F}_q$. Two vertices $a$ and $b$ are joined by an edge if and only if their difference is a quadratic residue, that is $a - b = y^2$ for some $y \in \mathbb{F}_q$.

Exoo (1981) established that $G_{17} \in \mathcal{S}(1,2,1) \cap \mathcal{S}(2,1,1)$. Moreover, for a prime $p \equiv 1(\text{mod } 4)$, Blass, Exoo and Harary (1981) proved that:

**Theorem 1.2.6:** (Blass, Exoo and Harary). If $p \equiv 1(\text{mod } 4)$ is a prime and $p > n^2 2^{4n}$, then $G_p \in \mathcal{S}(n,n,1)$.

Caccetta, Vijayan and Wallis (1984) established that $G_p \notin \mathcal{S}(2,2,1)$ for $p < 61$ and $G_p \in \mathcal{S}(2,2,1)$ for $61 \leq p \leq 173$. They conjectured that $G_p \in \mathcal{S}(2,2,1)$ for every $p \geq 61$. It is proved in Chapter 4, that for a prime $p \equiv 1(\text{mod } 4)$,

- $G_p \in \mathcal{S}(1,2,k) \cap \mathcal{S}(2,1,k)$, for every $p > (1 + 2\sqrt{2k})^2$;
- $G_p \in \mathcal{S}(1,n,k) \cap \mathcal{S}(n,1,k)$, for every $p > \{(n - 2)2^n + 2\sqrt{p} + (n + 2k - 1)2^n - 2n - 1$;
- $G_p \in \mathcal{S}(2,2,k)$, for every $p > (5 + 2\sqrt{4k + 6})^2$;

and

- $G_p \in \mathcal{S}(n,n,k)$, for every $p > \{(2n - 3)2^{2n-1} + 2\sqrt{p} + (n + 2k - 1)2^{2n-1} - 2n^2 - 1$.  

15
These results are established by making use of results from prime number theory.

In Chapter 5, we improve the above results by exploiting the structure of finite fields. In particular, we prove that for a prime power \( q = 1 \pmod{4} \),

- \( G_q \in \mathcal{G}(1,n,k) \cap \mathcal{G}(n,1,k) \), for every
  \[ q > \{(n - 2)2^n + 2\sqrt{q} + (n + 2k - 1)2^n - 2n - 1; \]

- \( G_q \in \mathcal{G}(n,n,k) \), for every
  \[ q > \{(2n - 3)2^{2n-1} + 2\sqrt{q} + (n + 2k - 1)2^{2n-1} - 2n^2 - 1; \]

and

- \( G_q \in \mathcal{G}(m,n,k) \), for every
  \[ q > \{(t - 3)2^{t-1} + 2\sqrt{q} + (t + 2k - 1)2^{t-1} - 1, \]

where \( t = m + n \).

We also present computational results which establish the smallest Paley graphs in \( \mathcal{G}(2,2,k) \) for small \( k \).

Several variations of the adjacency property have been studied. Caccetta, Erdős and Vijayan (1985) considered the following property. A graph \( G \) is said to have property \( P(n) \) if for any two sets \( A \) and \( B \) of vertices of \( G \) with \( A \cap B = \emptyset \) and \( |A \cup B| = n \), there is a vertex \( u \notin A \cup B \) which is joined to every vertex of \( A \) but not joined to any vertex of \( B \). The cycle \( C_\nu \) of length \( \nu \) has property \( P(1) \) for every \( \nu \geq 4 \). This property has also been considered by Bollobás (1985) and Caccetta, Erdős and Vijayan (1985). Moreover, given an integer \( \nu \), Caccetta, Erdős and Vijayan (1985) considered the problem of determining the largest integer \( f(\nu) \) for which there exists a graph on \( \nu \) vertices having property \( P(f(\nu)) \). They established the following result, using probabilistic methods:
Theorem 1.2.7: (Caccetta, Erdős and Vijayan). For \( \nu \) sufficiently large

\[
\frac{\log \nu - (2 + o(1)) \log \log \nu}{\log 2} < f(\nu) < \frac{\log \nu}{\log 2}.
\]

\[\blacksquare\]

In the same paper, a class of graphs having property P(2) was given.

Bollobás (1985) showed that if \( n \geq 2 \) and \( q \equiv 1(\text{mod } 4) \) is a prime power with

\[
q > ((n - 2)2^{n-1} + 1)\sqrt{q} + n2^{n-1},
\]

then \( G \) has property P(n). In Chapter 5, we improve this bound slightly to:

\[
q > ((n - 3)2^{n-1} + 2)\sqrt{q} + ((n + 1)2^{n-1} - 1).
\]

We can generalize property P(n) as follows. A graph \( G \) is said to have property P(n,k) if for any two sets A and B of vertices of \( G \) with \( A \cap B = \emptyset \) and \( |A \cup B| = n \), there are at least \( k \) vertices not in \( A \cup B \) which are joined to every vertex of \( A \) but not joined to any vertex of \( B \). In Chapter 5, we prove that for a prime power \( q \equiv 1(\text{mod } 4) \), \( G \) has property P(n,k), for every

\[
q > ((n - 3)2^{n-1} + 2)\sqrt{q} + (n + 2k - 1)2^{n-1} - 1.
\]

Another variation of the adjacency property is with respect to the Friendship theorem. Let \( G \) be a graph with the property that for any two vertices in the graph there is a unique vertex adjacent to both of them. The Friendship Theorem states that in such a graph there must be a vertex which is adjacent to all other
vertices. Graphs satisfying this property are called friendship graphs. By virtue of the Friendship Theorem, a friendship graph is either a triangle or a union of triangles having precisely one vertex in common. This was first proved by Erdős, Rényi and Sós (1966), and later alternative proofs were given by Wilf (1971) and Longyear and Parsons (1972).

Friendship graphs can be generalized in several ways. These generalizations are typically concerned with specifying either the number of paths between any two vertices or the size of the common neighbour set of any \(m\)-subset of vertices. For more details, we refer the interested reader to Bondy (1985), Delorme and Hahn (1984) and the articles cited therein. One particularly interesting problem is that of determining the graphs with the property that any two vertices are connected by a unique path of length \(k\), where \(k \geq 1\). Obviously, for \(k = 1\) these graphs are complete graphs; for \(k = 2\) these graphs are friendship graphs, described by Erdős, Rényi and Sós (1966). Kotzig (1983) conjectured that there are no such graphs for \(k \geq 3\). Kotzig has verified his conjecture for \(k \leq 9\). Kostochka (1988) established the conjecture for \(3 \leq k \leq 20\). He also remarked that by developing the idea of Erdős, Rényi and Sós (1966) it can be shown that there are no such graphs for \(3 \leq k \leq 30\).

Since almost all graphs have the property \(P(m,n,k)\), it is of interest to ask what happens if the conditions are varied. For example, what happens if there are exactly \(k\) other vertices, each of which is adjacent to the first \(m\) vertices of the set but not adjacent to any of the latter \(n\) vertices. This problem was mentioned by Alspach, Chen and Heinrich (1991). We consider this question in Chapter 7.
More specifically, a graph $G$ is said to have property $P^*(m,n,k)$ if for any set of $m + n$ distinct vertices of $G$ there are exactly $k$ other vertices, each of which is adjacent to the first $m$ vertices of the set but not adjacent to any of the latter $n$ vertices. The class of graphs having property $P^*(m,n,k)$ is denoted by $\mathcal{G}^*(m,n,k)$. The case $n = 0$ is, of course, a generalization of the property of the Friendship Theorem. The cycle $C_5$ of length 5 is a member of $\mathcal{G}^*(1,1,1)$. The well-known Petersen graph is a member of $\mathcal{G}^*(1,1,2)$. In Chapter 7, we show that, for $m = n = 1$, graphs with this property are the so-called strongly regular graphs with parameters $\left(\frac{(k + t)^2}{t} + 1, k + t, t - 1, t\right)$ for some positive integer $t$. In particular, we show the existence of such graphs. For $m \geq 1$, $n \geq 1$, and $m + n \geq 3$, we show that, there is no graph having property $P^*(m,n,k)$, for any positive integer $k$.

Alspach, Chen and Heinrich (1991) characterized the class of triangle-free graphs with a certain adjacency property. To be more precise, let $m$ and $n$ be positive integers. They characterized all graphs $G$ which have the following property:

(1) $G$ is triangle-free;

(2) $V(G)$ contains two disjoint subsets $M$ and $N$ where $M$ is an independent set of cardinality $m$ and $N$ is a set of cardinality $n$; and

(3) for any such pair $(M,N)$ of subsets of $V(G)$, there is a unique vertex in $G$ which is joined to every vertex of $M$ but not joined to any vertex of $N$.

Heinrich (1990) determined all graphs $G$ of order at least $m + 1$, $m \geq 3$, with the property that for any $m$-subset $S$ of $V(G)$
there is a unique vertex \( u, u \notin S \), which has exactly two neighbours in \( S \). Such graphs have exactly \( m + 1 \) vertices and consist of a family of vertex-disjoint union of cycles. When \( m = 2 \) it is clear that graphs with this property are the so-called friendship graphs.

A graph \( G \) is said to have property \( P^*(n,k) \) if for any two sets \( A \) and \( B \) of vertices of \( G \) with \( A \cap B = \emptyset \) and \( |A \cup B| = n \), there are exactly \( k \) vertices not in \( A \cup B \) which are joined to every vertex of \( A \) but not joined to any vertex of \( B \). We consider this property in Chapter 7. In particular, we prove that:

- (a) for \( n > 1 \), \( \mathcal{G}^*(n,k) = \emptyset \); and
- (b) for \( n = 1 \), \( G \in \mathcal{G}^*(1,k) \) if and only if \( G \) is a \( k \)-regular graph on \( 2k + 1 \) vertices.

We note that the property \( P(m,n,1) \) with \( m, n \leq t \) for positive integer \( t \) and property \( P(n,1) \) have been considered in the case of random graphs by Bollobás (1985).

It is natural to ask whether analogous adjacency properties could be obtained for directed graphs. Consider a round robin tournament \( T_q \) on \( q \) players \( 1, 2, \ldots, q \) in which there are no draws. It is very well-known that such a tournament can be represented by a directed graph in which the vertices represent the players. If Player 1 defeats Player 2, then the graph contains the arc \( (1, 2) \), and we say that vertex 1 dominates vertex 2. Further, we say a set of vertices \( A \) dominates a set of vertices \( B \) if every vertex of \( A \) dominates every vertex of \( B \). For convenience we refer to the graph of the tournament as \( T_q \).

A tournament \( T_q \) is said to have property \( Q(n,k) \) if every subset of \( n \) vertices of \( T_q \) is dominated by at least \( k \) other
vertices. An interesting problem is that of determining the smallest integer $f(n,k)$ for which there exists a tournament $T_q$ of order $q$ having property $Q(n,k)$ whenever $q \geq f(n,k)$. This problem was posed to Erdős in 1962 by Schütte for the particular case $k = 1$.

Using the probabilistic method, Erdős (1963) proved that for sufficiently large $n$

$$2^{n-1} - 1 \leq f(n,1) \leq n^2 2^n (\log 2 + \epsilon)$$

for any $\epsilon > 0$. E. Szekeres and G. Szekeres (1965) improved the lower bound to

$$f(n,1) \geq (n + 2)2^{n-1} - 1.$$ 

Graham and Spencer (1971) defined the following class of tournaments. Let $p \equiv 3 \pmod{4}$ be a prime. The directed graph $D_p$ is defined as follows. The vertices of $D_p$ are $0, 1, \ldots, p - 1$ and $D_p$ contains the arc $(i,j)$ if and only if $i - j$ is a quadratic residue modulo $p$. The graph $D_p$ is sometimes referred to as the Paley tournament [see Paley (1933)]. Graham and Spencer (1971) proved, using results from number theory, that $D_p$ has property $Q(n,1)$ whenever $p > n^2 2^{n-2}$. Further, they observed that $D_7$ and $D_{19}$ are the smallest Paley tournaments having property $Q(2,1)$ and $Q(3,1)$, respectively. They noted that $D_{67}$ may be the smallest Paley tournament having property $Q(4,1)$. This is indeed the case and is a consequence of our work in Chapter 6 [see Ananchuen and Caccetta (1993)].

Bollobás (1985) extended the results of Graham and Spencer to prime powers. More specifically, if $q \equiv 3 \pmod{4}$ is a prime power, the Paley tournament $D_q$ is defined as follows. The
vertices of $D_q$ are the elements of the finite field $F_q$. Vertex $a$ joins to vertex $b$ by an arc if and only if $a - b$ is a quadratic residue in $F_q$. Bollobás noted that $D_q$ has property $Q(n,1)$ whenever

$$q > ((n - 2)2^{n-1} + 1)\sqrt{q} + n2^{n-1}.$$ 

In Chapter 6, we improve this bound to

$$q > ((n - 3)2^{n-1} + 2)\sqrt{q} + 2^n - 1.$$ 

In addition, we establish that $D_q$ has property $Q(n,k)$ whenever,

$$q > ((n - 3)2^{n-1} + 2)\sqrt{q} + k2^n - 1.$$ 

We can generalize the property $Q(n,k)$ as follows. We say that a tournament $T_q$ of order $q$ has property $Q(m,n,k)$ if for any set of $m + n$ distinct vertices of $T_q$ there exist at least $k$ other vertices each of which dominates the first $m$ vertices and is dominated by each of the latter $n$ vertices. We consider this property for the case of Paley tournaments in Section 6.2. In addition, we establish that all sufficiently large Paley tournaments satisfy property $Q(m,n,k)$.

A number of the results we present in this thesis have been published in Ananchuen and Caccetta (1992, 1993(a), 1993(b), 1993(c)) or have been submitted for publication in Ananchuen and Caccetta (1993(d) and 1993(e)).

We conclude this thesis with a discussion on some open problems.
CHAPTER 2

PROPERTIES OF THE CLASS $\mathcal{G}(m,n,k)$

In this chapter, we present some important properties of graphs in the class $\mathcal{G}(m,n,k)$.

Recall that a graph $G$ is said to have property $P(m,n,k)$ if for any set of $m + n$ distinct vertices there are at least $k$ other vertices, each of which is adjacent to the first $m$ vertices but not adjacent to the latter $n$ vertices. The class of graphs having property $P(m,n,k)$ is denoted by $\mathcal{G}(m,n,k)$. We have mentioned in Section 1.2 that, the cycle $C_\nu$ of length $\nu$ is a member of $\mathcal{G}(1,1,1)$. The well-known Petersen graph is a member of $\mathcal{G}(1,2,1) \cap \mathcal{G}(1,1,2)$. Observe that if $G \in \mathcal{G}(m,n,k)$, then $\tilde{G} \in \mathcal{G}(n,m,k)$.

A number of basic but important properties concerning the class $\mathcal{G}(m,n,k)$ are established in Section 2.1. We study the class $\mathcal{G}(n,n,k)$ in Section 2.2. In particular, we prove that if $G \in \mathcal{G}(2,2,k)$, then

$$\nu(G) \geq \begin{cases} 34, & \text{if } k = 1, \\ 8k + 25, & \text{if } k \geq 3 \text{ and } k \text{ is odd}, \\ 8k + 21, & \text{otherwise} \end{cases}$$

with equality possible only if $G$ is a PC-graph with certain prescribed parameters. More generally, we prove that:

$$p(n,n,k) \geq 4^{n-1} \left[ 2(n + k) + \frac{1}{2}(3 + (-1)^{n+k+1}) \right] + \frac{1}{3} - \frac{1}{3}.$$

A consequence of our work is a lower bound on $p(m,n,k)$. 

23
2.1 Basic Lemmas

In the following lemmas we establish a number of properties of the class \( \mathcal{S}(m,n,k) \). We often make use of the following simple fact. If \( G \in \mathcal{S}(m,n,k) \), then \( n(X) \geq k \) for any disjoint sets of vertices \( X \) and \( Y \) of \( G \) with \( |X| \leq m \) and \( |Y| \leq n \).

Lemma 2.1.1: If \( G \in \mathcal{S}(m,n,k) \), then \( \delta(G) \geq m + n + k - 1 \).

Proof: Suppose to the contrary that \( d_G(u) = d \leq m + n + k - 2 \).
Let \( v_1, v_2, \ldots, v_d \) denote the neighbours of \( u \). Observe that
\[
d - (m + n - 1) \leq k - 1 \quad \text{and hence,}
\]
\[
n(u, v_1, \ldots, v_m^{-1}, v_{m+1}, \ldots, v_{m+n-1}) \leq k - 1,
\]
a contradiction. This proves the lemma. \( \Box \)

Lemma 2.1.2: Let \( \{u_1, u_2, \ldots, u_m, v_1, v_2, \ldots, v_n\} \) be a set of \( m + n \) vertices in a graph \( G \in \mathcal{S}(m,n,k) \). Then

(a) \( n(u_1, u_2, \ldots, u_t/-) \geq m + n + k - t \), for \( t \leq m \),

and

(b) \( n(u_1, u_2, \ldots, u_m/v_1, v_2, \ldots, v_t) \geq n + k - \ell \), for \( \ell \leq n \).

Proof: We prove only (a) as the proof of (b) is similar. Suppose to the contrary that
\[
n(u_1, u_2, \ldots, u_t/-) = d \leq m + n + k - t - 1.
\]
Let \( x_1, x_2, \ldots, x_d \) denote the vertices of \( N(u_1, u_2, \ldots, u_t/-) \). We have
\[ n(u_1, u_2, \ldots, u_t, x_1, x_2, \ldots, x_{m-t}/x_{m-t+1}, x_{m-t+2}, \ldots, x_{m-t+n}) \]
\[ \leq d - (m + n - t) \leq k - 1, \]

a contradiction. This proves (a). \hfill \Box

An immediate corollary of Lemma 2.1.2(b) is the following.

Corollary 2.1.3: For \(1 \leq j \leq n\), \(\mathcal{G}(m, n, k) \subseteq \mathcal{G}(m, n - j, k + j)\). \hfill \Box

Corollary 2.1.3 is very useful in our work, especially in Chapter 3.

Remark 2.1.1: Blass and Harary (1979) proved that almost all graphs have property \(P(n, n, 1)\). From this, Corollary 2.1.3 and the fact that \(\mathcal{G}(r, s, t) \subseteq \mathcal{G}(m, n, k)\) for every \(r \geq m\), \(s \geq n\) and \(t \geq k\), we can establish that almost all graphs have property \(P(m, n, k)\).

Remark 2.1.2: From Corollary 2.1.3, we know that \(\mathcal{G}(1, n, k) \subseteq \mathcal{G}(1, n - j, k + j)\) for \(1 \leq j \leq n\). But \(\mathcal{G}(1, n, k)\) is not a subclass of \(\mathcal{G}(1, n + 1, k - 1)\) for \(1 \leq i < k\). This implies that for \(n + k = n' + k'\), \(\mathcal{G}(1, n, k)\) is not necessarily equal to \(\mathcal{G}(1, n', k')\). The following graph illustrates this.
Observe that $G \in \mathcal{Y}(1,1,2)$ but $G \notin \mathcal{Y}(1,2,1)$, since $N(v_0 \vee v_2 \vee v_7) = \phi$. Note that $G$ is the PC-graph with parameters $(9,4,1,2)$.

The next few lemmas establish some properties of graphs in the class $\mathcal{Y}(m,n,k)$ in terms of vertex degrees.

**Lemma 2.1.4:** Let $G_0$ be a graph in $\mathcal{Y}(m,n,k)$ having minimum order. Then for any $G \in \mathcal{Y}(m,n+1,k)$

$$\nu(G) \geq \nu(G_0) + \Delta(G) + 1.$$ 

**Proof:** Let $w$ be any vertex of $G$. Clearly,

$$G_w = G - w - N(w/-) \in \mathcal{Y}(m,n,k)$$

and hence,

$$\nu(G_w) = \nu(G) - 1 - d_G(w)$$

$$\geq \nu(G_0).$$

This proves the lemma. \qed
The above result was proved by Exoo and Harary (1980) for the case $k = 1$.

Observe that for $m \geq 2$ every vertex of a graph $G \in \mathcal{G}(m,n,k)$ is contained in a triangle. In fact, every edge of $G$ is in at least $m + n + k - 2$ triangles (by Lemma 2.1.2(a)). For $m = 1$, we have the following result.

**Lemma 2.1.5:** Let $G \in \mathcal{G}(1,n,k)$. If $d_G(u) = n + k$, then $u$ is on no cycle of length less than 5.

**Proof:** Let $v_1, v_2, \ldots, v_{n+k}$ be the neighbours of $u$. Suppose $C$ is the smallest cycle of $G$ containing $u$. We may suppose without any loss of generality that $v_1, v_2 \in C$. If $C$ has length 3, then $v_1 v_2 \in E(G)$. Since $d_G(u) = n + k$, we have

$$n(u/v_2, v_3, \ldots, v_{n+1}) \leq k - 1.$$ 

This contradicts the fact that $G \in \mathcal{G}(1,n,k)$. So $C$ cannot have length 3. Suppose it has length 4 and let $u, v_1, v_2$ and $w$ be the vertices of $C$. Then since $d_G(u) = n + k$, we have

$$n(u/w, v_3, v_4, v_{n+1}) \leq k - 1,$$

again a contradiction. This completes the proof. \[\Box\]

The above result was proved by Exoo and Harary (1980) for the case $k = 1$.

From Remark 2.1.2 we known that $\mathcal{G}(1,n,k)$ is not a subclass of $\mathcal{G}(1,n+1,k-i)$ for $1 \leq i < k$, but when $G$ has girth at least 5 or is $(n + k)$-regular, we have the following results.
Lemma 2.1.6: Let \( G \in \mathcal{G}(1,n,k) \). If \( G \) has girth at least 5, then \( G \in \mathcal{G}(1,n + \ell,k - \ell) \) for \( 1 \leq \ell \leq k - 1 \).

Proof: Let \( u,v_1,v_2,\ldots,v_{n+\ell} \) be any \( n + \ell + 1 \) vertices of \( G \). Let

\[ N(u, v_1, v_2, \ldots, v_{n+\ell}) = \{x_1, x_2, \ldots, x_d\}. \]

Then \( d \geq k \). Since \( G \) has girth at least 5, we have for each \( i \), \( v_i \in N(x_j/-) \cup \{x_j\} \) for at most one \( j \). Consequently, \( n(u, v_1, v_2, \ldots, v_{n+\ell}) \geq k - \ell \) and hence, \( G \in \mathcal{G}(1,n + \ell,k - \ell) \) as required. \( \Box \)

As a corollary we have:

Corollary 2.1.7: If \( G \in \mathcal{G}(1,n,k) \) is \((n+k)\)-regular, then \( G \in \mathcal{G}(1,n + \ell,k - \ell) \) for \( 1 \leq \ell \leq k - 1 \).

Lemma 2.1.8: Let \( G \in \mathcal{G}(1,n,k) \) be a graph with girth at least 5. If \( G \) is not an \((n+k)\)-regular graph of girth 5, then \( \nu(G) \geq (n+k)^2 + (n+k) \).

Proof: If \( G \) is \((n+k)\)-regular, then by the hypothesis of the lemma \( G \) has girth at least 6. Thus the result follows at once from a theorem in Biggs (1974, p 154), which states that if an \( r \)-regular graph \( G \) has odd girth \( g \), then

\[ \nu(G) \geq 1 + r + r(r-1) + \ldots + r(r-1)^{\frac{1}{2}(g-3)} \]

and if \( G \) has even girth \( g \), then

\[ \nu(G) \geq 1 + r + r(r-1) + \ldots + r(r-1)^{\frac{1}{2}(g-2)} + (r-1)^{\frac{1}{2}(g-1)} \]

28
If $G$ is not $(n + k)$-regular, then, by Lemma 2.1.1, $G$ contains a vertex $u$ of degree $d \geq (n + k) + 1$. If $v_1, v_2, \ldots, v_d$ are the neighbours of $u$, then, by Lemma 2.1.2(b), $n(v_i/u) \geq (n + k) - 1$, $1 \leq i \leq d$. Since $G$ has girth at least 5,

$$\nu(G) \geq 1 + d + \sum_{i=1}^{d} n(v_i/u)$$

$$= 1 + (n + k + 1) + (n + k + 1)(n + k - 1)$$

$$> (n + k)^2 + (n + k)$$

as required. \hfill \Box

Remark 2.1.3: For the case $k = 1$, Exoo and Harary (1980) conjectured that if $G \in \mathcal{G}(1,n,1)$ and $G$ has girth at most 4, then $\nu(G) \geq n^2 + 3n + 2$. For $n \leq 6$, they proved this conjecture by considering each value of $n$ separately. Further, they established that the $(n + 1,5)$-cage is a smallest order graph in the class $\mathcal{G}(1,n,1)$ for $n \leq 6$. Caccetta and Vijayan (1986) established, by nonelementary counting methods, the conjecture for all graphs for which

$$\min\{d_G(u) : u \in V(G) \text{ and } d_G(u) > n + 1\} \leq \frac{1}{2}(3n + 2).$$

Observe that if $G$ is a known $(n + k,5)$-cage, then $\nu(G) \leq (n + k)^2 + (n + k)$.

2.2 The Class $\mathcal{G}(n,n,k)$

In this section, we establish some fundamental properties of graphs in the class $\mathcal{G}(n,n,k)$. In addition, we conclude this section by establishing a lower bound on the order of a graph having property $P(m,n,k)$.
Lemma 2.2.1: Let \( \{u_1, u_2, \ldots, u_n, v_1, v_2, \ldots, v_n\} \) be a set of \( 2n \) vertices in a graph \( G \in \mathcal{G}(n,n,k) \). Then

(a) \( n(u_1, u_2, \ldots, u_n) \geq 2n + k - 1 \),

and

(b) \( n(u_1, u_2, \ldots, u_n / v_1, v_2, \ldots, v_\ell) \geq n + k \), for \( \ell < n \).

Proof: (a) Let \( N(u_1, u_2, \ldots, u_n) = \{x_1, x_2, \ldots, x_d\} \). Then by Lemma 2.1.2(a), \( d \geq n + k \). Consequently, there exists

\[ w \in N(x_1, x_2, \ldots, x_n / u_1, u_2, \ldots, u_n) . \]

If \( d < 2n \), then \( N(u_1, u_2, \ldots, u_n / w, x_{n+1}, x_{n+2}, \ldots, x_d) = \emptyset \), a contradiction. Hence, \( d \geq 2n \). Since \( G \in \mathcal{G}(n,n,k) \),

\[ n(u_1, u_2, \ldots, u_n / w, x_{n+1}, x_{n+2}, \ldots, x_{2n-1}) \geq k \].

Then \( d - n = (n-1) \geq k \) and so \( d \geq 2n + k - 1 \) as required.

(b) Let \( N(u_1, u_2, \ldots, u_n / v_1, v_2, \ldots, v_\ell) = \{x_1, x_2, \ldots, x_d\} \). If \( d \leq n \), then there exists

\[ w \in N(x_1, x_2, \ldots, x_d / u_1, u_2, \ldots, u_n) . \]

Hence, \( N(u_1, u_2, \ldots, u_n / w, v_1, v_2, \ldots, v_\ell) = \emptyset \), a contradiction so \( d > n \). Let \( w' \in N(x_1, x_2, \ldots, x_n / u_1, u_2, \ldots, u_n) \). Since \( G \in \mathcal{G}(n,n,k) \),

\[ n(u_1, u_2, \ldots, u_n / w', v_1, v_2, \ldots, v_\ell) \geq k \].

Hence, \( d - n \geq k \) and so \( d \geq n + k \) as required. \( \square \)

Lemma 2.2.2: Let \( G \in \mathcal{G}(n,n,k) \) and \( \{u_1, u_2, \ldots, u_{n-1}, v_1, v_2, \ldots, v_{n-1}\} \) a set of \( 2n - 2 \) vertices of \( G \). Then the subgraph

\[ H = G[N(u_1, u_2, \ldots, u_{n-1} / v_1, v_2, \ldots, v_{n-1})] \]

has \( \delta(H) \geq n + k \).
Proof: Suppose to the contrary that $d_H(x) = d \leq n + k + 1$. Let $y_1, y_2, \ldots, y_d$ be the neighbours of $x$ in $H$. Suppose $d < n$. Since $G \in \mathcal{G}(n, n, k)$, there exists $w \in N(y_1, y_2, \ldots, y_d, u_1, u_2, \ldots, u_{n-1})$ and a $y \in N(u_1, u_2, \ldots, u_{n-1}, x, v_1, v_2, \ldots, v_{n-1}, w)$. Thus $y \in V(H)$ and, since $y$ is adjacent to $x$, $y = y_i$ for some $i$. Hence, $y$ is adjacent to $w$, a contradiction. Now consider a vertex $z \in N(y_1, y_2, \ldots, y_n, u_1, u_2, \ldots, u_{n-1}, x)$; such a $z$ exists since $G \in \mathcal{G}(n, n, k)$. Clearly $n(u_1, u_2, \ldots, u_{n-1}, x, v_1, v_2, \ldots, v_{n-1}, z) \leq k - 1$, a contradiction. This proves that $\delta(H) \geq n + k$. \hfill $\Box$

Our next two lemmas are essentially a generalization of Lemma 1 in Caccetta, Vijayan and Wallis (1984).

Lemma 2.2.3: Let $G \in \mathcal{G}(2, 2, k)$. Then

(a) \[ n(u, v/x) \geq k + 2 \text{ and } n(x/u, v) \geq k + 2, \] for any $u, v, x \in V(G)$,

(b) \[ n(u, v/-) \geq k + 4, \] for any $u, v \in V(G)$.

Proof: (a) $n(u, v/x) \geq k + 2$ by Lemma 2.2.1(b). Further, by applying Lemma 2.2.1(b) to $\overline{G}$, we obtain $n(x/u, v) \geq k + 2$. This proves (a).

(b) Let $x, y \in N(u, v/-)$ and let $w \in N(x, y/u, v)$. We have

\[ n(u, v/-) = n(u, v, w/-) + n(u, v/w) \]
\[ \geq 2 + (k + 2); \text{ since } n(u, v/w) \geq k + 2 \]
\[ = k + 4, \]

proving (b). \hfill $\Box$
Lemma 2.2.4: Let $G \in \mathcal{Y}(2,2,k)$. Then

$$n(x/y) \geq \begin{cases} 
2k + 6, & \text{if } k \text{ is odd}, \\
2k + 5, & \text{otherwise}.
\end{cases}$$

Proof: Let $z \in N(x/y)$. Then

$$n(x/y) = 1 + n(x,z/y) + n(x/y,z)$$

$$\geq 1 + (k + 2) + (k + 2) \quad \text{[by Lemma 2.2.1(b)]}$$

$$= 2k + 5,$$

with equality possible only if $n(x,z/y) = n(x/y,z) = k + 2$ for every $z \in N(x/y)$. So $n(x/y) = 2k + 5$ only if the subgraph $H = G[N(x/y)]$ induced by the vertices of $N(x/y)$ is $(k + 2)$-regular. But if $k$ is odd, then $k + 2$ and $2k + 5$ are odd, which is impossible, since in any graph the number of vertices of odd degree is even. So we have

$$n(x/y) \geq \begin{cases} 
2k + 6, & \text{if } k \text{ is odd}, \\
2k + 5, & \text{otherwise}.
\end{cases}$$

This proves the lemma. \qed

Recall that an $r$-regular graph of order $\nu$ is called strongly regular with parameters $(\nu,r,\lambda,\mu)$ if $G$ has the property that any two adjacent vertices have exactly $\lambda$ common neighbours and any two non-adjacent vertices have exactly $\mu$ common neighbours. A strongly regular graph with parameters $(4t + 1,2t,t - 1,t)$, where $t$ is a positive integer, is called a pseudo-cyclic (PC) graph. Observe that the 5-cycle $C_5$ is a PC-graph with parameters $(5,2,0,1)$. The well-known Petersen graph is a strongly regular...
graph with parameters \((10,3,0,1)\) but it is not a PC-graph. Note that the complement of a PC-graph is again a PC-graph with the same parameters as the original graph.

The following discussion is from Caccetta, Vijayan and Wallis (1984).

The adjacency matrix \(A\) of a PC-graph with parameters \((4t+1, 2t, t-1, t)\) satisfies:

\[
\begin{align*}
A^2 + A &= t(J + I), \\
AJ &= 2tJ
\end{align*}
\]

where \(J\) is the all one matrix, and \(I\) is the identity matrix. Note that the dimension of the matrices are implied by the context in which they are used.

Further, the matrix

\[
M = \begin{bmatrix}
0 & e^T \\
e & B
\end{bmatrix}
\]

(2.2.2)

where \(e^T = [1 \ 1 \ \ldots \ 1]_{1 \times 4t+1}\) and \(B = 2A - J + I\), satisfies the orthogonality condition

\[MM^T = (4t + 1)I.\]

Note that the matrix \(B\) is symmetric, has zeros on the diagonal and \(\pm 1\) elsewhere (\(+1\) if the corresponding entry in \(A\) is 1, \(-1\) if the corresponding non-diagonal entry in \(A\) is 0). A conference matrix of order \(n\) is a square matrix \(C\) with zeros on the diagonal and \(\pm 1\) elsewhere satisfying the orthogonality condition

\[CC^T = (n - 1)I.\]

If, in addition, \(C\) is symmetric, then its order \(n = 2(\text{mod } 4)\).
Thus the matrix $M$ given in (2.2.2) is a symmetric conference matrix of order $4t + 2$.

The adjacency matrix $A$ of a PC-graph can, as shown above, be uniquely extended to a symmetric conference matrix. Conversely, a PC-graph can be obtained from a symmetric conference matrix $C$ by normalizing it to contain ones in the $i^{th}$ row and column except $c_{ii} = 0$ and by deleting this row and column from $C$. The resulting matrix $B$ yields a $(0, 1)$-matrix $A = \frac{1}{2}(B + J - I)$ satisfying (2.2.1). Note that by choosing different rows for normalization we may obtain different non-isomorphic PC-graphs.

The following result [see Wallis, Street and Wallis (1972), p 294] gives a necessary condition for the existence of PC-graphs.

**Lemma 2.2.5:** A necessary condition for the existence of a PC-graph of order $\nu = 4t + 1$, $t > 0$ is that $\nu$ is the sum of squares of two integers.

The next few lemmas establish the adjacency property of strongly regular graphs.

**Lemma 2.2.6:** Let $G$ be a strongly regular graph with parameters $(\nu, r, \lambda, \mu)$. Then $G \in \mathcal{Y}(1,1,t)$ if and only if $r \geq t + \max(\lambda + 1, \mu)$.

**Proof:** Suppose $G \in \mathcal{Y}(1,1,t)$. Let $u$ and $v$ be any vertices of $G$. Then $n(u, v/-) = \lambda$ or $\mu$. Since $n(u/v) \geq t$ and $n(u/-) = r$, $r - t \geq \max(\lambda + 1, \mu)$ as required.

Conversely, suppose $r \geq t + \max(\lambda + 1, \mu)$. Let $u$ and $v$ be any vertices of $G$. Then $n(u, v/-) = \lambda$ or $\mu$. Since $r \geq
\[ t + \max(\lambda + 1, \mu), \ n(u/v) \geq t. \text{ Hence, } G \in \mathcal{G}(1,1,t). \]

An immediate corollary of Lemma 2.2.6 is the following.

Corollary 2.2.7: If \( G \) is a PC-graph with parameters \((4t + 1, 2t, t - 1, t)\), then \( G \in \mathcal{G}(1,1,s) \) for every \( s \leq t \).

The following result concerns the smallest (order) graph in the class \( \mathcal{G}(1,1,t) \).

Lemma 2.2.8: If \( G \in \mathcal{G}(1,1,t) \), then \( \nu(G) \geq 4t + 1 \). Furthermore, \( \nu(G) = 4t + 1 \) if and only if there exists a PC-graph with parameters \((4t + 1, 2t, t - 1, t)\).

Proof: Consider a vertex \( x \) of \( G \). Since \( G \in \mathcal{G}(1,1,t) \),

\[ n(u/x) \geq t, \quad \text{for any } u \in N(x/-), \quad (2.2.3) \]

and

\[ n(x/w) \geq t, \quad \text{for any } w \in N(-/x). \quad (2.2.4) \]

Therefore,

\[ \sum_{u \in N(x/-)} n(u/x) + \sum_{w \in N(-/x)} n(x/w) \geq t(\nu - 1). \]

Now, in the left hand side of the above equation, the first sum counts the edges between the sets \( N(x/-) \) and \( N(-/x) \) whilst the second sum counts the non-edges between the sets \( N(x/-) \) and \( N(-/x) \). Therefore,

\[ \sum_{u \in N(x/-)} n(u/x) + \sum_{w \in N(-/x)} n(x/w) = n(x/-)n(-/x). \]
and so
\[ n(x/-)n(-/x) = n(x/-)(\nu - n(x/-) - 1) \]
\[ \geq t(\nu - 1). \]

Consequently,
\[ \nu \geq \frac{n(x/-)^2 + n(x/-) - t}{n(x/-) - t} \]
\[ = 1 + \frac{n(x/-)^2}{n(x/-) - t} \]
\[ \geq 1 + 4t. \quad (2.2.5) \]

For equality to hold in (2.2.5), we must have for every \( x \in V(G) \) equality in (2.2.3) and (2.2.4) and also \( n(x/-) = 2t \). Thus \( n(x,u/-) = t - 1 \) for all \( u \in N(x/-) \) and \( n(x,w/-) = t \) for all \( w \in N(-/x) \). Therefore, \( \nu = 4t + 1 \) only if \( G \) is a PC-graph with parameters \((4t + 1, 2t, t - 1, t)\).

The converse follows immediately from Corollary 2.2.7. \( \square \)

The above result was proved, using a different method, by Exoo (1981).

For \( G \in \mathcal{G}(2,2,k) \), let
\[ t_0 = \min_{u,v \in V(G)} \{n(u/v)\}. \]

Lemma 2.2.4 implies that
\[ t_0 \geq \begin{cases} 2k + 6, & \text{if } k \text{ is odd}, \\ 2k + 5, & \text{otherwise}. \end{cases} \]

Thus we have the following corollary to Lemma 2.2.4:
Corollary 2.2.9: $l(2,2,k) \leq l(1,1,t_0)$.

Caccetta, Vijayan and Wallis (1984) proved that if $G \in l(2,2,1)$, then $\nu(G) \geq 34$. We now extend this result.

Theorem 2.2.10: Let $G \in l(2,2,k)$. Then

$$\nu(G) = \begin{cases} 
34, & \text{if } k = 1, \\
8k + 25, & \text{if } k \geq 3 \text{ and } k \text{ is odd}, \\
8k + 21, & \text{otherwise}; 
\end{cases}$$

with equality possible only if $G$ is a PC-graph with parameters $(4t_0 + 1, 2t_0, t_0 - 1, t_0)$.

Proof: Consider a vertex $x$ of $G$. Since

$$n(u/x) \geq t_0, \quad \text{for any } u \in N(x/-), \quad (2.2.6)$$

and

$$n(x/w) \geq t_0, \quad \text{for any } w \in N(-/x), \quad (2.2.7)$$

we have

$$\sum_{u \in N(x/-)} n(u/x) + \sum_{w \in N(-/x)} n(x/w) \geq t_0(\nu - 1).$$

Since

$$\sum_{u \in N(x/-)} n(u/x) + \sum_{w \in N(-/x)} n(x/w) = n(x/-)n(-/x),$$

$$n(x/-)n(-/x) = n(x/-)(\nu - n(x/-) - 1) \geq t_0(\nu - 1).$$

Consequently,
\[ \nu \geq \frac{n(x/-)^2 + n(x/-) - t_0}{n(x/-) - t_0} \]
\[ = 1 + \frac{n(x/-)^2}{n(x/-) - t_0} \]
\[ \geq 1 + 4t_0 \]
\[ \geq \begin{cases} 
8k + 25, & \text{if } k \text{ is odd,} \\
8k + 21, & \text{otherwise.} 
\end{cases} \quad (2.2.8) \]

For equality to hold in (2.2.8), we must have for every \( x \in V(G) \) equality in (2.2.6) and (2.2.7) and also \( n(x/-) = 2t_0 \). Thus \( n(x,w/-) = t_0 - 1 \) for all \( u \in N(x/-) \) and \( n(x,w/-) = t_0 \) for all \( w \in N(-/x) \). Consequently, \( \nu = 4t_0 + 1 \) only if \( G \) is a PC-graph with parameters \((4t_0 + 1, 2t_0, t_0 - 1, t_0)\).

For \( k = 1 \), \( \nu(G) = 33 \) only if there exist a PC-graph with parameters \((33, 16, 7, 8)\). But from Lemma 2.2.5 we know that no such graph exists. Therefore,
\[ \nu(G) \geq \begin{cases} 
34, & \text{if } k = 1, \\
8k + 25, & \text{if } k \geq 3 \text{ and } k \text{ is odd}, \\
8k + 21, & \text{otherwise} 
\end{cases} \]

For the class \( \mathcal{Y}(n,n,k) \) we have the following theorem.

**Theorem 2.2.11:** If \( G \in \mathcal{Y}(n,n,k) \), then
\[ \nu(G) \geq 4^{n-1} \left[ 2(n + k) + \frac{1}{2} (3 + (-1)^{n+k+1}) + \frac{1}{3} \right] - \frac{1}{3}. \quad (2.2.9) \]
Proof: Let $G \in \mathcal{G}(n,n,k)$. For $1 \leq i \leq n$ define

$$\mathcal{Y}_i = \{A : A \subseteq V(G) \text{ and } |A| = i\}.$$ 

Clearly for disjoint sets $A$ and $B$ in $\mathcal{Y}_i$, $N(A \cap B) \neq \phi$. Thus the subgraph $H = G[N(A \cap B)]$ has vertices; in fact $\nu(H) \geq k$. For $1 \leq i \leq n$, let

$$h_i^* = \min\{n(A \cap B) : A \cap B = \phi, A, B \in \mathcal{Y}_i\}.$$ 

Suppose that $h_i^* = n(A \cap B)$ and let

$$H_i^* = G[N(A \cap B)].$$ 

Observe that $G \in \mathcal{G}(1,1,h_i^*)$. We show that $H_i^* \in \mathcal{G}(1,1,h_{i+1}^*)$ for each $1 \leq i \leq n - 2$.

Consider the graph $H_i^* = G[N(A \cap B)]$. Then for any $a, b \in V(H_i^*)$, the number $n^*(a/b)$ of vertices of $H_i^*$ joined to $a$ but not joined to $b$ satisfies

$$n^*(a/b) = n(A \cup \{a\}/B \cup \{b\}) \geq h_{i+1}^*.$$

Thus, as $a$ and $b$ are arbitrary, $H_i^* \in \mathcal{G}(1,1,h_i^*)$. Now, by Lemma 2.2.8,

$$h_i^* \geq 4h_{i+1}^* + 1, \quad 1 \leq i \leq n - 2.$$ 

Consequently, since $G \in \mathcal{G}(1,1,h_1^*)$, we have

$$\nu(G) \geq 4h_1^* + 1 \geq 4(4h_2^* + 1) + 1 \geq 4(4(4h_3^* + 1) + 1) + 1 \geq \ldots \geq 4^{n-1}h_{n-1}^* + \frac{4^{n-1} - 1}{3} \text{.}$$

(2.2.10)

We next prove that
\[ h_{n-1}^* \geq 2(n + k) + \frac{1}{2}[3 + (-1)^{n+k+1}] \]  \hspace{1cm} (2.2.11)

By Lemma 2.2.2, \( \delta(H_{n-1}^*) \geq n + k \). Further, since \( \mathcal{G} \in \mathcal{F}(n,n,k) \) we also have \( \delta(H_{n-1}^*) \geq n + k \). Consequently, \( h_{n-1}^* \geq 2(n + k) + 1 \), proving (2.2.11) when \( n + k \) is even. When \( n + k \) is odd, then at least one of \( H_{n-1}^* \) or \( H_{n-1}^* \) contains a vertex of degree at least \( n + k + 1 \) and thus (2.2.11) also holds. Now (2.2.10) and (2.2.11) together yield (2.2.9). This completes the proof of the theorem. \( \Box \)

The above result was proved by Exoo (1981) for the case \( k = 1 \).

The following corollary of Theorem 2.2.11 establishes a lower bound on the order of a graph having property \( P(m,n,k) \) for any \( m, n \) and \( k \).

**Corollary 2.2.12:** Let \( t = \min(m,n) \) and \( k' = k + |m - n| \). Then

\[ p(m,n,k) \geq 4^{t-1} \left[ 2(t + k') + \frac{1}{2}(3 + (-1)^{t+k'+1}) + \frac{1}{3} \right] - \frac{1}{3}. \]

**Proof:** Since \( G \in \mathcal{F}(m,n,k) \) implies that \( \mathcal{G} \in \mathcal{F}(n,m,k) \), we have \( p(m,n,k) = p(n,m,k) \). Hence,

\[ p(m,n,k) = p(t,t + |m - n|,k) \]

\[ \geq p(t,t,k') \hspace{1cm} \text{[by Corollary 2.1.3]} \]

\[ \geq 4^{t-1} \left[ 2(t + k') + \frac{1}{2}(3 + (-1)^{t+k'+1}) + \frac{1}{3} \right] - \frac{1}{3} \]

as required. \( \Box \)
Remark 2.2.1: A consequence of the proof of the Theorem 2.2.11 is that \( \mathcal{G}(n,n,k) \leq \mathcal{G}(n-1,n-1,h_{n-1}) \). For the particular case \( n = 2, k = 1 \), we have \( \mathcal{G}(2,2,1) \leq \mathcal{G}(1,1,8) \). Thus by Lemma 2.2.8, \( p(2,2,1) \geq 33 \) with equality possible only if there exists a strongly regular graph with parameters \((33,16,7,8)\). But from Lemma 2.2.5 we known that no such graph exists. Hence, \( p(2,2,1) \geq 34 \), as we proved in Theorem 2.2.10. To date, the smallest known graph in the class \( \mathcal{G}(2,2,1) \) is the Paley graph on 61 vertices; this graph is showed in the Figure 5.2.2 in Chapter 5.

Remark 2.2.2: Since \( G \in \mathcal{G}(m,n,k) \) implies \( \tilde{G} \in \mathcal{G}(n,m,k) \), we have \( p(m,n,k) = p(n,m,k) \). But the class \( \mathcal{G}(m,n,k) \) is not necessary equal to the class \( \mathcal{G}(n,m,k) \). For example \( \mathcal{G}(1,2,1) \neq \mathcal{G}(2,1,1) \), since the Petersen graph \( P \) belongs to the class \( \mathcal{G}(1,2,1) \) but not in the class \( \mathcal{G}(2,1,1) \).
CHAPTER 3

SOME CONSTRUCTIONS

In the previous chapter, we noted (Remark 2.1.1) that almost all graphs have property $P(m,n,k)$. Despite this result few members of $\mathcal{F}(m,n,k)$ have been constructed. In this chapter, we construct classes of graphs having property $P(1,n,k)$. These classes include: the cubes; "generalized" Exoo-Harary graphs; "generalized" Petersen graphs; and "generalized" Hoffman-Singleton graphs. These graphs are described in sections 3.1 and 3.2. In the final section of this chapter we establish that $\mathcal{F}(1,2,1) \neq \emptyset$ for every order $n$, $n \geq 10$, except $n = 11$.

3.1 The Class $\mathcal{F}(1,n,k)$, $n + k \leq 4$

In this section, we construct classes of graphs satisfying property $P(1,n,k)$, $n + k \leq 4$.

We noted in the introduction that Exoo and Harary (1983) determined the smallest graphs of girth 3 and 4 in the class $\mathcal{F}(1,n,1)$ for some $n$. In particular, they proved that the graphs displayed in figures 3.1.1 and 3.1.2 are smallest graphs of girth 3 in the classes $\mathcal{F}(1,2,1)$ and $\mathcal{F}(1,3,1)$, respectively.
We now generalize these graphs. Let $C = u_0 u_1 \ldots u_{m-1} u_0$ be a cycle of length $m$, $m \geq 5$ and $\bar{C}$ the complement of $C$. For $s$ a positive integer, define the graph $E(m,s)$ as follows. Take $\bar{C}$ and $s$ copies $C_0, C_1, \ldots, C_{s-1}$ of $C$. Join vertex $u_i$ of $C_j$, $0 \leq i \leq m-1$, $0 \leq j \leq s-1$, to vertex $u_{i'}$ of $\bar{C}$. $E(m,s)$ is the resulting graph.

Observe that $E(5,1)$ is the Petersen graph and the graph of Figure 3.1.1 is $E(6,1)$. Figure 3.1.2 displays $E(6,2)$, $E(7,1)$, $E(8,2)$ and $E(8,3)$. 

43
It is easy to see that $E(m,s)$ is a graph on $(s + 1)m$ vertices having minimum degree $3$ and maximum degree $m + s - 3$. The adjacency properties of $E(m,s)$ are given in the following result.

Theorem 3.1.1: For any positive integers $m \geq 5$ and $s$, $E(m,s) \in \mathcal{H}(1,n,k)$, for $n + k \leq 3$.

Proof: In view of Corollary 2.1.3 it is sufficient to show that $E(m,s) \in \mathcal{H}(1,2,1)$. Let $u$ be any vertex of $E(m,s)$. If $u \in C_j$ for some $j$, then $u$ does not belong to any cycle of length less than 5.
Since $d_G(u) = 3$, for any other vertices $v$ and $w$, $N(u/v/w) \neq \emptyset$.

If, on the other hand, $u \in \bar{C}$ then there are at least three other vertices $x$, $y$ and $z$ of $E(m,s)$ such that $N(u/-) \subseteq N(x/-) \cup N(y/-) \cup N(z/-)$. Hence, for any distinct pair of vertices $v$ and $w$ of $E(m,s) - u$, $N(u/v/w) \neq \emptyset$. Therefore, $E(m,s) \in \mathcal{F}(1,2,1)$ as required.

We next generalize the graph displayed in Figure 3.1.2. Let $m = 2r \geq 6$ and $2 \leq s \leq r$. Define the graph $E^s(2r,s)$ from the graph $E(2r,s)$ by adding $r$ isolated vertices labelled $0,1,2,\ldots, r - 1$ and the $2rs$ edges:

$$\{(1,u_{i+j}),(1,u_{i+j+r}) : u_{i+j}, u_{i+j+r} \in C, 0 \leq i \leq r - 1, 0 \leq j \leq s - 1\};$$

all subscripts are read modulo $2r$. Note that the graph in Figure 3.1.2 is just $E^s(6,2)$. Figure 3.1.4 displays the graph $E^s(8,3)$ and $E^s(10,2)$; note that for convenience edges from the 4 and 5 "isolated" vertices are not shown, however we adopt the convention that each of these vertices is joined to the vertices of $E(8,3)$ and $E(10,2)$ having the same letter label, respectively.
It is easy to see that $E^s(2r,s)$ is a graph on $(2s + 3)r$ vertices having minimum degree 4 and maximum degree $2r + s - 3$. The adjacency properties of $E^s(2r,s)$ are given in the following result.

Theorem 3.1.2: For $r \geq 3$ and $2 \leq s \leq r$, $E^s(2r,s) \in \Psi(1,n,k)$, for $n + k \leq 4$.

Proof: In view of Corollary 2.1.3 it is sufficient to show that $E^s(2r,s) \in \Psi(1,3,1)$. Let $u$ be any vertex of $E^s(2r,s)$. If $u$ is an isolated vertex or $u \in C_j$ for some $j$, then $u$ does not belong to any cycle of length less than 5. Since $d_G(u) = 4$, for any other distinct vertices $x$, $v$ and $w$, $N(u/x,v,w) \neq \phi$. If, on the other hand, $u \in \overline{C}$, then there are at least four other vertices $y_1$, $y_2$, $y_3$, and $y_4$ of $E^s(2r,s)$ such that $N(u/-) \subseteq \bigcup_{i=1}^{4} N(y_i/-)$. Hence, for any distinct vertices $x$, $v$ and $w$ of $E^s(2r,s) - u$, $N(u/x,v,w) \neq \phi$. Therefore, $E^s(2r,s) \in \Psi(1,3,1)$ as required.
We noted in the introduction that the Petersen graph is in the class $\mathcal{G}(1,2,1) \cap \mathcal{G}(1,1,2)$. We now generalize this graph to get another class of graphs in $\mathcal{G}(1,n,k)$, $n + k \leq 4$.

Let $m$ and $t$ be integers, $m \geq 5$ and $m \neq 6$, satisfying

$$1 < t < m - 1, \quad m \neq 2t. \quad (3.1.1)$$

Define the graph $I(m,t)$ as follows. The vertices of $I(m,t)$ are $v_0, v_1, \ldots, v_{m-1}$ and the edges are

$$\{(v_i, v_{i+t}) : 0 \leq i \leq m - 1\};$$

all subscripts are read modulo $m$. Noting that $I(m,t) \cong I(m,m-t)$, we can replace (3.1.1) with

$$1 < t < \frac{1}{2}m. \quad (3.1.2)$$

We use the normal convention of denoting the greatest common divisor of integers $a$ and $b$ by $\gcd(a,b)$. Observe that $I(m,t)$ is 2-regular and thus the union of cycles. In fact, it consists of exactly $\gcd(m,t)$ cycles each of length $m/\gcd(m,t)$. Furthermore, for each $m$ we can choose at least one value $t_0$ of $t$ such that $m/\gcd(m,t_0) \geq 5$.

Define the graph $G(m,t_0,s)$ as follows. Start with the graph $I(m,t_0)$ and $s$ copies $C_0, C_1, \ldots, C_{s-1}$ of the $m$-cycle $C = u_0 u_1 \ldots u_{m-1} u_0$. Add the $ms$ edges:

$$\{(v_i, u_j) : v_i \in I(m,t_0), u_j \in C_j, 0 \leq i \leq m - 1, 0 \leq j \leq s - 1\}.$$

Note that $G(5,2,1)$ is the Petersen graph. The graphs $G(7,3,3), G(8,3,2), G(9,2,3)$ and $G(10,4,2)$ are displayed in Figure 3.1.5.
Observe that the graph $G(m,t_0,s)$ has $(s + 1)m$ vertices, girth at least 5, minimum degree 3 and maximum degree $s + 2$. Therefore, by Lemma 1.2.4 and Corollary 2.1.3 we have:

**Theorem 3.1.3**: $G(m,t_0,s) \in \mathcal{Y}(1,n,k)$, for $n + k \leq 3$. □

**Remark 3.1.1**: When $I(m,t_0) \not= I(m,t'_0)$, $t_0 \not= t'_0$ it is possible for $G(m,t'_0,s) \not= G(m,t'_0,s)$. For example, $I(11,2) \not= I(11,3)$ but $G(11,2,1) \not= G(11,3,1)$ as they have difference girths (5 and 6, respectively).
For \( r \geq 4, 2 \leq s \leq r \), we construct the graph \( G^*(2r,t_0,s) \), from \( G(2r,t_0,s) \) as follows. Add \( r \) isolated vertices labelled \( 0,1,2,\ldots,r-1 \) to \( G(2r,t_0,s) \) and the \( 2rs \) edges:

\[
\{(i,u_{i+j}), (i,u_{i+j+r}) : u_{i+j}, u_{i+j+r} \in C_j, 0 \leq i \leq r-1, 0 \leq j \leq s-1\};
\]

all subscripts are read modulo \( 2r \). Figure 3.1.6 displays the graph \( G^*(8,3,2) \); note that for convenience edges from the 4 and 5 "isolated" vertices are not shown. However, we adopt the earlier convention that each of these vertices is joined to the vertices of \( G(8,3,2) \) and \( G(10,2,2) \) having the same letter label, respectively.
It is easy to see that $G^*(2r, t_0, s)$ is a graph on $(2s + 3)r$ vertices having minimum degree 4 and maximum degree $2s$. Thus the graph $G^*(2r, t_0, 2)$ is 4-regular. The adjacency properties of $G^*(2r, t_0, s)$ are given in the following result.

**Theorem 3.1.4:** For $r \geq 4$ and $2 \leq s \leq r$, $G^*(2r, t_0, s) \subseteq \mathcal{Y}(1, n, k)$, for $n + k \leq 4$.

**Proof:** In view of Lemma 1.2.4 and Corollary 2.1.3, we need only show that $G^*(2r, t_0, s)$ has girth 5. From the construction of the graph $G^*(2r, t_0, s)$ it is sufficient to show that this graph contains no 4-cycle. Since $G(2r, t_0, s)$ has girth at least 5, without any loss of generality we can assume that $G^*(2r, t_0, s)$ contains a cycle of length 4 as shown in Figure 3.1.7 below, for some $g$, $h$, $i$ and $j$. 
Since vertex 1 is adjacent to vertices $u_{1+j}$ and $u_{1+j+r}$ of $C_j$ and adjacent to $u_{1+h}$ and $u_{1+h+r}$ of $C_h$, we have $j = h$ or $h = r$, a contradiction. This proves the theorem.

3.2 The Class $\mathcal{P}(1,n,k)$

In this section, we show that the $t$-cube is in the class $\mathcal{P}(1,n,k)$, for $2n + k \leq t$. Further, we construct, for any $n$ and $k$, a class of graphs with property $\mathcal{P}(1,n,k)$. We begin with the cube.

The $t$-cube, $Q_t$, is defined as follows: the vertices of $Q_t$ are the $2^t$ symbols $(e_1, e_2, \ldots, e_t)$ where $e_i = 0$ or $1$, $i = 1, 2, \ldots, t$ and two vertices are adjacent if and only if their symbols differ in exactly one coordinate. Then from the definition of a cube we know that $Q_t$ is a $t$-regular graph on $2^t$ vertices. Figure 3.2.1 displays the cubes $Q_2$ and $Q_3$. 

![Diagram of Q2 and Q3](image-url)
Exoo and Harary (1983) proved that \( Q_{2n+1} \in \mathcal{G}(1,n,1) \). A more general result is:

**Theorem 3.2.1:** \( Q_t \in \mathcal{G}(1,n,k) \), for any \( 2n + k \leq t \).

**Proof:** Let \( x \) be a vertex of \( Q_t \) and \( u_1, u_2, \ldots, u_t \) the neighbours of \( x \). From the definition of a cube we know that \( Q_t \) contains no triangle and no other vertex of \( Q_t \) except \( x \) is adjacent to more than two of the \( u_i \)'s, \( i = 1, 2, \ldots, t \). Since \( 2n + k \leq t \), for any set \( A \) of \( n \) vertices of \( Q_t - x \) there are at least \( k \) other vertices, each of which is adjacent to \( x \) but not adjacent to any vertex of \( A \) as required.

\( \square \)

**Remark 3.2.1:** For any \( n \) and \( k \), there exists a \( t \) such that \( Q_t \in \mathcal{G}(1,n,k) \). Note, however, that for \( m \geq 2 \), \( Q_t \notin \mathcal{G}(m,n,k) \) for any \( t \) since every \( G \in \mathcal{G}(m,n,k) \) contains a triangle.

Our next class of graphs comes from generalizing the Hoffman-Singleton graphs.

Let \( p \geq 5 \) be a prime number and \( t \) an integer satisfying \( 1 < t < \frac{1}{2}p \). For \( m = p \) the graph \( I(m,t) \) defined in Section 2 is just a cycle of length \( p \). For \( 1 \leq r, s \leq p \) we define the graph \( H^r_s(p,t) \) as follows. Take \( r \) copies \( I_0, I_1, \ldots, I_{r-1} \) of \( I(p,t) \) and \( s \) copies \( C_0, C_1, \ldots, C_{s-1} \) of the \( p \)-cycle \( C = u_0 u_1 \ldots u_{p-1} u_0 \). Add the prs edges:

\[
\{(v_i, u_{i+jk}) : v_i \in I_j, u_{i+jk} \in C_k, \ 0 \leq i \leq p-1, \\
0 \leq j \leq r-1, \ 0 \leq k \leq s-1\}.
\]

Note that for the particular case \( p = 5, t = 2 \) we have (see
Wong (1982)): the Petersen graph $H_1^1(5,2)$; the Wegner graph $H_3^3(5,2)$; the O'Keefe-Wong graph $H_4^4(5,2)$ and the Hoffman-Singleton graph $H_5^5(5,2)$. Figure 3.2.2 displays $H_7^7(7,3)$; we show only the edges for vertex $v_3$ of $I_j$.

![Diagram](image)

Figure 3.2.2: $H_7^7(7,3)$

Note that we can replace the graphs $I_j$ for all $j$ by the graph $I(7,2)$ in Figure 3.2.3.

![Diagram](image)

Figure 3.2.3: $I(7,2)$

Observe that the graph $H_r^r(p,t)$ has $(r + s)p$ vertices, minimum degree $\delta = 2 + \min(r,s)$ and maximum degree $\Delta = 2 + \max(r,s)$. Of course, $H_r^r(p,t)$ is $(r + 2)$-regular. The adjacency properties of $H_r^r(p,t)$ are given in the following theorem.
Theorem 3.2.2: \( H^r_s(p, t) \in \mathcal{S}(1, n, k) \), for \( n + k \leq 2 + \min(r, s) \).

Proof: In view of Lemma 1.2.4 and Corollary 2.1.3, we need only show that \( H^r_s(p, t) \) has girth at least 5. From the construction of \( H^r_s(p, t) \) it is sufficient to show that the graph contains no 4-cycle. So suppose \( v_i u_k v_j u_l v_i \) is a 4-cycle in \( H^r_s(p, t) \). Without any loss of generality assume that \( v_i \in I_a \), \( v_j \in I_b \), \( u_l \in C_c \) and \( u_k \in C_d \). Then

\[
\begin{align*}
l &\equiv i + ac \equiv j + bc \pmod{p}, \\
k &\equiv i + ad \equiv j + bd \pmod{p}.
\end{align*}
\]

Therefore,

\[
ac - ad \equiv bc - bd \pmod{p},
\]

and hence,

\[
a \equiv b \pmod{p}.
\]

Now, since \( a, b < p \) and \( p \) is a prime, this is impossible. This completes the proof of the theorem.

\[\square\]

Remark 3.2.2: For any \( n, k \) there always exists a \( H^r_s(p, t) \in \mathcal{S}(1, n, k) \).

Remark 3.2.3: For \( t \neq t' \), the graphs \( H^r_s(p, t) \) and \( H^r_s(p, t') \) need not be isomorphic. For example, \( H^1_1(11, 2) \neq H^1_1(11, 3) \).

Remark 3.2.4: \( E(5, s) \not\cong G(5, 2, s) \cong H^1_1(5, 2) \) and \( H^1_s(p, t) \not\cong G(p, t, s) \).

Remark 3.2.5: The girth of \( H^r_s(p, t) \) is at least 5. Choosing \( t = 2 \) will always result in a graph having girth 5. Regular graphs of girth 5 have been constructed by Murty (1979) and by O'Keefe and Wong (1984). Our construction gives another class of such graphs.
Remark 3.2.6: For the case $m, n \geq 2$, the problem of constructing graphs with the property $P(m,n,k)$ seems difficult. In particular, in Section 5.2, we proved that all sufficiently large Paley graphs satisfy property $P(m,n,k)$ for any $m$, $n$ and $k$. In Section 5.4, we give, without proof, further examples of classes of graphs in $\mathcal{Y}(2,2,k)$ for small $k$. Such graphs are called "generalized" Paley graphs. To date the only published examples of such graphs are the Paley graphs.

3.3 The Class $\mathcal{Y}(1,2,1)$

In this section, we construct a graph $G \in \mathcal{Y}(1,2,1)$ on $n$ vertices for every integer $n$, $n \geq 10$, except $n = 11$.

Exoo and Harary (1980, 1983) proved that the smallest graph in $\mathcal{Y}(1,2,1)$ is the Petersen graph of order 10. Further, every other graph in $\mathcal{Y}(1,2,1)$ has at least 12 vertices. They exhibited two graphs of order 12 in the class $\mathcal{Y}(1,2,1)$. We prove that the only graphs on 12 vertices in $\mathcal{Y}(1,2,1)$ are the 3 graphs $G_1$, $G_2$ and $G_3$ displayed in Figure 3.3.1 below; $G_1$ and $G_3$ are two Exoo-Harary graphs.

![Figure 3.3.1](image-url)
We begin with the following lemma.

Lemma 3.3.1: If $G$ is a 3-regular graph of girth 5 and $\nu(G) = 12$, then $G \cong G_1$ or $G_2$.

Proof: Let $u \in V(G)$ and label the vertices of $G - u$ as shown in Figure 3.3.2 below. Observe that for $i = 1$ and 2, $|N(v_i/-) \cap N(x/-)| \leq 1$ for $x = a, b, c$. We consider two cases according to whether or not $v_1$ and $v_2$ are adjacent.

![Figure 3.3.2](image)

Case (i): $v_1v_2 \notin E(G)$. If $v_1$ and $v_2$ have no common neighbour, then we may assume without loss of generality that $v_1$ is adjacent to $a_1, b_1$ and $c_1$, $i = 1, 2$. In this case it is easily seen that $G \cong G_1$.

So suppose $N(v_1/-) \cap N(v_2/-) \neq \emptyset$. Then $|N(v_1/-) \cap N(v_2/-)| = 1$, as otherwise $G$ would have girth 4. Without loss of generality, assume that $N(v_1/-) = \{a_1, b_1, c_1\}$ and $N(v_2/-) = \{a_1, b_2, c_2\}$. Now it is easy to see that $G \cong G_2$.

Case (ii): $v_1v_2 \in E(G)$. Then $N(v_1/-) \cap N(v_2/-) = \emptyset$. Without loss of generality let $N(v_1/-) = \{v_2, a_1, b_1\}$. If $N(v_2/-) \cap N(c/-) = \emptyset$ then $N(v_2/-) = \{v_1, a_2, b_2\}$ and $G \cong G_2$. If $v_2$ is joined to $c_1$ or $c_2$ (it can only be joined to one of these), then $v_2$ is joined
to $a_2$ or $b_2$. In either case it is easy to deduce $G \cong G_1$. This proves the lemma.

In our next theorem we make use of the following two results of Exoo and Harary (1984).

Lemma 3.3.2: Let $G \in \mathcal{G}(1,2,1)$ be a graph of girth 3. If $\nu(G) = 12$, then $G \cong G_3$.

Lemma 3.3.3: Let $G \in \mathcal{G}(1,2,1)$ be a graph of girth 4. Then $\nu(G) \geq 14$.

Theorem 3.3.4: Let $G \in \mathcal{G}(1,2,1)$ be a graph on 12 vertices. Then $G \cong G_1$, $G_2$ or $G_3$.

Proof: Suppose to the contrary that $G \in \mathcal{G}(1,2,1)$ is a graph on 12 vertices not isomorphic to $G_1$, $G_2$ or $G_3$. Then by lemmas 3.3.1 to 3.3.3, $G$ has girth at least 5 and cannot be 3-regular.

Observe that for any vertex $u$ of $G$, $G[N(\sim u)] \in \mathcal{G}(1,1,1)$. Therefore, since the smallest member of $\mathcal{G}(1,1,1)$ has 5 vertices we conclude that $3 \leq d_0(u) \leq 6$. So $4 \leq \Delta(G) \leq 6$. Since $G$ has girth at least 5, $\Delta(G) \geq 4$ implies that $\nu(G) \geq 13$, a contradiction.

For $m \geq 9$ we modify the graph $G(m,t_0,1)$ defined in Section 3.2 as follows. Add a new vertex $x$ and the edges $xu_0, xu_j$ and $xu_6$. Call the resulting graph $\hat{G}(m,t_0,1)$. Figure 3.3.3 displays the graph $\hat{G}(9,2,1)$.
Figure 3.3.3: $\hat{G}(9,2,1)$

Observe that $\hat{G}(m,t_0,1)$ has $2m + 1$ vertices, girth 5, minimum degree 3 and maximum degree 4. Consequently, by Lemma 1.2.4 $\hat{G}(m,t_0,1) \in \mathcal{G}(1,2,1)$.

Theorem 3.3.5: Let $G \in \mathcal{G}(1,2,1)$ be a graph on $n$ vertices. Then $G$ exists for $n = 10$ and every $n \geq 12$. Moreover, no $G$ exists for $n \leq 9$ and $n = 11$.

Proof: That no graph $G$ exists for $n \leq 9$ and $n = 11$ was established in Theorem 1.2.2. The graph $\hat{G}(m,t_0,1)$, $m = 9$, defined above together with Theorem 3.1.3 establishes the existence of $G$ for $n = 14, 15, 16$ and for $n \geq 18$. We have already exhibited graphs for $n = 10$ and 12. So all that remains are $n = 13$ and 17. The graph displayed in Figure 3.3.4 will do for $n = 13$. For $n = 17$ we take the Paley graph $G_{17}$ defined in the introduction. This completes the proof of the theorem. $\Box$
Remark 3.3.1: For \( m \geq 9 \) we can obtain another class of graphs having the property \( P(1,2,1) \) by applying the above procedure to the graph \( E(m,1) \) defined in Section 3.1. That is, add a new vertex \( x \) and the edges \( xu_0, xu_3 \) and \( xu_6 \).
CHAPTER 4
PALEY GRAPHS OF PRIME ORDER

Recall that for a prime \( p \equiv 1 \pmod{4} \), the Paley graph \( G_p \) of order \( p \) is the graph with:
\[
V(G_p) = \{0, 1, \ldots, p - 1\} \quad \text{and} \quad E(G_p) = \{(i, j) : i - j \equiv y^2 \pmod{p} \text{ for some } y \in V(G_p)\}.
\]

In this chapter, we study the adjacency properties of the Paley graph \( G_p \). In particular, we prove, in sections 4.2 and 4.3, that for prime \( p \equiv 1 \pmod{4} \),

- \( G_p \in \mathcal{G}(1,2,k) \cap \mathcal{G}(2,1,k) \), for every \( p > (1 + 2\sqrt{2k})^2 \);

- \( G_p \in \mathcal{G}(1,n,k) \cap \mathcal{G}(n,1,k) \), for every \( p > \{(n - 2)2^n + 2\sqrt{p} + (n + 2k - 1)2^n - 2n - 1\} \);

- \( G_p \in \mathcal{G}(2,2,k) \), for every \( p > (5 + 2\sqrt{4k + 6})^2 \);

and

- \( G_p \in \mathcal{G}(n,n,k) \) for every \( p > \{(2n - 3)2^{2n-1} + 2\sqrt{p} + (n + 2k - 1)2^{2n-1} - 2n^2 - 1\} \).

We also present computational results which establish the smallest Paley graph of prime order in \( \mathcal{G}(2,2,k) \) for small \( k \).

In Section 4.1, we present some basic terminology and results from number theory that we make use of in our work. In
addition, we establish an important result (Theorem 4.1.2) which plays a crucial role in the proofs of our main theorems in sections 4.2 and 4.3.

4.1 Preliminaries

In this section, we present some results on number theory which we make use of in establishing the main results of this chapter. We begin with some basic number theoretic facts.

For odd prime \( p \) the Legendre symbol \( \left( \frac{a}{p} \right) \) is defined as:

\[
\left( \frac{a}{p} \right) = \begin{cases} 
1, & \text{if } a \text{ is a quadratic residue modulo } p, \\
0, & \text{if } p | a, \\
-1, & \text{otherwise}.
\end{cases}
\]

It is well-known [see Andrews (1971)] that

\[
\left( \frac{a}{p} \right) = \left( \frac{b}{p} \right), \quad \text{if } a \equiv b \pmod{p}, \quad \text{(4.1.1)}
\]

\[
\left( \frac{ab}{p} \right) = \left( \frac{a}{p} \right) \left( \frac{b}{p} \right), \quad \text{(4.1.2)}
\]

and

\[
\sum_{x=0}^{p-1} \left( \frac{x}{p} \right) = 0. \quad \text{(4.1.3)}
\]

It follows from (4.1.3) that

\[
\sum_{x=0}^{p-1} \left( \frac{x-a}{p} \right) = 0. \quad \text{(4.1.4)}
\]
The set of integers \( \{x_1, x_2, \ldots, x_t\} \) is called a complete residue system modulo \( m \) if

1. \( x_i \equiv x_j \pmod{m} \) whenever \( i \neq j \);
2. for each integer \( n \) there corresponds an \( x_i \) such that \( n \equiv x_i \pmod{m} \).

The set of integers \( \{x_1, x_2, \ldots, x_t\} \) is called a reduced residue system modulo \( m \) if

1. \( \gcd(x_i, m) = 1 \) for each \( i \);
2. \( x_i \equiv x_j \pmod{m} \) whenever \( i \neq j \); and
3. for each integer \( n \) relatively prime to \( m \) there corresponds an \( x_i \) such that \( n \equiv x_i \pmod{m} \).

For example, for a positive integer \( m \), the set \( \{0, 1, 2, \ldots, m - 1\} \) is a complete residue system modulo \( m \) and for a prime \( p \), the set \( \{1, 2, \ldots, p - 1\} \) is a reduced residue system modulo \( p \) [see Andrews (1971)].

In our next two theorems we make use of the following standard terminology. For a prime \( p \), we write "\( \sum \)" whenever the summation is taken over a complete residue system modulo \( p \) and "\( \sum \)" whenever the summation is taken over a reduced residue system modulo \( p \). More specifically, if \( \{x_1, x_2, \ldots, x_p\} \) is any complete residue system modulo \( p \) and \( C_j = C_{x_j} \), whenever \( j \equiv x_i \pmod{p} \), then

\[
\sum_{j=0}^{p-1} C_j = \sum_{i=1}^{p} C_{x_i} = \sum_{x \pmod{p}} C_x.
\]
The following theorem, due to Burgess (1957), is very useful in our work.

Theorem 4.1.1: (Burgess) Let $p$ be an odd prime and let $a_1, a_2, \ldots, a_s$ be distinct residues modulo $p$. Then

$$\sum_{x \equiv a_1 \mod{p}} \left( \frac{(x - a_1)(x - a_2) \ldots (x - a_s)}{p} \right) \leq (s - 1)^{1/p}.$$

Our next theorem is crucial to our work in establishing a lower bound on $p$ for $G_p \in \mathcal{S}(m,n,k)$.

Theorem 4.1.2: Let $p$ be an odd prime and let $a_1, a_2, \ldots, a_s$ be distinct residues modulo $p$. Then for even $s$

$$\sum_{x=0}^{p-1} \left( \frac{(x - a_1)(x - a_2) \ldots (x - a_s)}{p} \right)$$

$$= -1 \pm \sum_{y \equiv b_1 \mod{p}} \left( \frac{(y + b_1)(y + b_2) \ldots (y + b_{s-1})}{p} \right)$$

for some set $\{b_1, b_2, \ldots, b_{s-1}\}$ of distinct residues modulo $p$.

Proof: We write

$$\sum_{x=0}^{p-1} \left( \frac{(x - a_1)(x - a_2) \ldots (x - a_s)}{p} \right)$$
\[\sum_{x \equiv a_i \pmod{p}} \left( \frac{(x - a_1)(x - a_2) \cdots (x - a_s)}{p} \right)\]

\[= \sum_{x \equiv a_i \pmod{p}} \left( \frac{x(x + a_1 - a_2)(x + a_1 - a_3) \cdots (x + a_1 - a_s)}{p} \right).\]

(4.1.5)

Note that the latter equality is valid, since \(x\) and hence \(x \equiv a_i \pmod{p}\) assume all values in a complete residue system modulo \(p\). Now since \(a_1, a_2, \ldots, a_s\) are distinct residues modulo \(p\), then \(\lambda_1 = a_1 - a_{i+1} \equiv 0 \pmod{p}\) for \(1 \leq i \leq s - 1\).

If \(x \equiv 0 \pmod{p}\), then there exists an \(y\) such that \(xy \equiv 1 \pmod{p}\). Furthermore, \(\left(\frac{y}{p}\right)^s = 1\), since \(s\) is even. If \(x \equiv 0 \pmod{p}\), then \(\left(\frac{x}{p}\right) = 0\). Thus we can write (4.1.5) as:

\[\sum_{x \equiv \lambda \pmod{p} \setminus 0} \frac{x(x + \lambda_1)(x + \lambda_2) \cdots (x + \lambda_{s-1})}{p}\]

\[= \sum_{x \equiv \lambda \pmod{p} \setminus 0} \left(\frac{y^s}{p}\right) \left(\frac{x(x + \lambda_1)(x + \lambda_2) \cdots (x + \lambda_{s-1})}{p}\right)\]

\[= \sum_{x \equiv \lambda \pmod{p} \setminus 0} \frac{xy(xy + \lambda_1y)(xy + \lambda_2y) \cdots (xy + \lambda_{s-1}y)}{p}\]

\[= \sum_{x \equiv \lambda \pmod{p} \setminus 0} \frac{(1 + \lambda_1y)(1 + \lambda_2y) \cdots (1 + \lambda_{s-1}y)}{p}.\]
Since, for each $i$, $\lambda_i \equiv 0 \pmod{p}$ there exists $\lambda'_i$, such that $\lambda_i\lambda'_i = 1$. Furthermore,

$$\left( \frac{\lambda_1\lambda' \lambda_2 \lambda' \ldots \lambda_{s-1} \lambda'_{s-1}}{p} \right) = 1.$$ 

Now using the same idea as above we can write:

$$\sum_{\substack{x \equiv (\mod p) \\ x \neq 0 \equiv (\mod p)}} \left( \frac{(1 + \lambda_1 y)(1 + \lambda_2 y) \ldots (1 + \lambda_{s-1} y)}{p} \right)$$

$$= \sum_{\substack{x \equiv (\mod p) \\ x \neq 0 \equiv (\mod p)}} \left( \frac{(\lambda_1 \lambda_2 \ldots \lambda_{s-1})(\lambda_1 + y)(\lambda_2 + y) \ldots (\lambda_{s-1} + y)}{p} \right).$$ 

(4.1.6)

Let $\lambda = \lambda_1 \lambda_2 \ldots \lambda_{s-1}$ and $\lambda' = \lambda'_1 \lambda'_2 \ldots \lambda'_{s-1}$. Since $\lambda_i \equiv 0 \pmod{p}$ for each $i$, we have $\lambda \equiv 0 \pmod{p}$ and so $\left( \frac{\lambda}{p} \right) = \pm 1$. As $x$ assumes all values in a reduced residue system modulo $p$, so does $y$. Hence, we can write (4.1.6) as:

$$\sum_{\substack{y \equiv (\mod p) \\ y \neq 0 \equiv (\mod p)}} \left( \frac{\lambda}{p} \right) \left( \frac{(y + \lambda')(y + \lambda') \ldots (y + \lambda'_{s-1})}{p} \right)$$

$$= \sum_{\substack{y \equiv (\mod p)}} \left( \frac{\lambda}{p} \right) \left( \frac{(y + \lambda')(y + \lambda') \ldots (y + \lambda'_{s-1})}{p} \right) - \left( \frac{\lambda}{p} \right) \left( \frac{\lambda'}{p} \right)$$

$$= \left( \frac{\lambda}{p} \right) \sum_{\substack{y \equiv (\mod p)}} \left( \frac{(y + \lambda')(y + \lambda') \ldots (y + \lambda'_{s-1})}{p} \right) - 1$$

65
\[ -1 \pm \sum_{y \pmod{p}} \left( \frac{(y + \lambda_1')(y + \lambda_2') \ldots (y + \lambda_{s-1}')}{p} \right) \]

This completes the proof of the theorem.

Using (4.1.4) and Theorem 4.1.1 we have the following corollaries to Theorem 4.1.2.

Corollary 4.1.3: If \( p \) is an odd prime, then for \( a \neq b \pmod{p} \)

\[
\sum_{x=0}^{p-1} \left( \frac{(x - a)(x - b)}{p} \right) = -1.
\]

Corollary 4.1.4: Let \( p \) be an odd prime and let \( a_1, a_2, \ldots, a_s \) be distinct residues modulo \( p \). Then for even \( s \)

\[
\left| \sum_{x=0}^{p-1} \left( \frac{(x - a_1)(x - a_2) \ldots (x - a_s)}{p} \right) \right| \leq 1 + (s - 2)\sqrt{p}.
\]

4.2 \( \mathcal{F}(1,n,k) \)

In this section, we prove that \( G_p \in \mathcal{F}(1,n,k) \cap \mathcal{F}(n,1,k) \) for sufficiently large \( p \). We begin by exhibiting some small Paley graphs. Clearly \( G_5 \in \mathcal{F}(1,1,1) \). It is not too difficult to establish that \( G_{13} \in \mathcal{F}(1,1,3) \). Figure 4.2.1 displays the Paley graphs \( G_5 \) and \( G_{13} \).
It is well-known (see, for example, Bollobás (1985)) that the Paley graph $G_p$ is self-complementary and is a PC-graph with parameters $(4t + 1, 2t, t - 1, t)$, when $q = 4t + 1$ is a prime. In this section, we shall establish that every Paley graph of prime order

$$p > ((n - 2)2^n + 2)^{\sqrt{p}} + (n + 2k - 1)2^n - 2n - 1$$

belongs to the class $\mathcal{F}(1, n, k)$. This will be accomplished by the application of theorems 4.1.1 and 4.1.2. To illustrate the method we begin with the simple case when $n = 1$. In fact, this result is a special case of Corollary 2.2.7 that was proved using the theory of strongly regular graphs.

Observe that if $a, b \in V(G)$, then

$$\left(\frac{a - b}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is adjacent to } b, \\ 0, & \text{if } a = b, \\ -1, & \text{otherwise.} \end{cases}$$
Further, since \( p \equiv 1(\text{mod } 4) \), then \(-1\) is a quadratic residue modulo \( p \). Consequently,

\[
\left( \frac{a - b}{p} \right) = \left( \frac{b - a}{p} \right).
\]

**Lemma 4.2.1:** Let \( p = 4t + 1 \) be a prime. Then \( G_p \in \mathcal{G}(1,1,k) \) for every \( k \leq t \).

**Proof:** Let \( a \) and \( b \) be any two distinct vertices of \( G_p \). Then \( n(a/b) \equiv k \) if and only if

\[
f = \sum_{x=0}^{p-1} \left( 1 + \left( \frac{x - a}{p} \right) \right) \left( 1 - \left( \frac{x - b}{p} \right) \right) \geq 4k.
\]

We now show that \( f \equiv 4k \) for \( t \equiv k \). We can write

\[
g = \sum_{x=0}^{p-1} \left( 1 + \left( \frac{x - a}{p} \right) \right) \left( 1 - \left( \frac{x - b}{p} \right) \right)
\]

\[
= \sum_{x=0}^{p-1} 1 + \sum_{x=0}^{p-1} \left( \frac{x - a}{p} \right) - \sum_{x=0}^{p-1} \left( \frac{x - b}{p} \right) - \sum_{x=0}^{p-1} \left( \frac{x - a}{p} \right) \left( \frac{x - b}{p} \right)
\]

\[
= p - \sum_{x=0}^{p-1} \left( \frac{x - a}{p} \right) \left( \frac{x - b}{p} \right) \quad \text{[by (4.1.4)]}
\]

\[
= p + 1. \quad \text{[by Corollary 4.1.3]}
\]

Now

\[
g - f = \left( 1 - \left( \frac{a - b}{p} \right) \right) + \left( 1 + \left( \frac{b - a}{p} \right) \right) = 2.
\]
Hence,
\[ f = g - 2 = p - 1 = 4t \equiv 4k \]
for \( t \geq k \) as required. \( \Box \)

Remark 4.2.1: When \( t < k \) the above proof yields \( f < 4k \) and hence, \( G_p \in \mathcal{Y}(1,1,k) \).

We noted in the introduction that Exoo and Harary (1980) proved that the Petersen graph is the smallest member of \( \mathcal{Y}(1,2,1) \). Exoo (1981) proved that if \( G \in \mathcal{Y}(1,2,1) \cap \mathcal{Y}(2,1,1) \), then \( \nu(G) \geq 17 \) and furthermore \( G_{17} \in \mathcal{Y}(1,2,1) \cap \mathcal{Y}(2,1,1) \). Figure 4.2.2 displays the Paley graph \( G_{17} \).

![Diagram of Paley Graph G_{17}](image)

*Figure 4.2.2*

Our next result concerns the classes \( \mathcal{Y}(1,2,k) \) and \( \mathcal{Y}(2,1,k) \).

Lemma 4.2.2: Let \( p \equiv 1(\text{mod } 4) \) be a prime and \( k \) a positive integer. If \( p > (1 + 2\sqrt{k})^2 \), then \( G_p \in \mathcal{Y}(1,2,k) \cap \mathcal{Y}(2,1,k) \).
Proof: Since \( G_p \) is a self-complementary graph, it is sufficient to prove that \( G_p \in \mathcal{S}(1,2,k) \). Let \( S = \{a,b,c\} \) be any set of distinct vertices of \( G_p \). Then \( n(a/b,c) \geq k \) if and only if

\[
f = \sum_{x=0}^{p-1} \left( 1 + \left( \frac{x-a}{p} \right) \right) \left( 1 - \left( \frac{x-b}{p} \right) \right) \left( 1 - \left( \frac{x-c}{p} \right) \right)
\]

\[\geq 8k.\]

To show that \( f \geq 8k \), it is clearly sufficient to establish that \( f > 8(k - 1) \).

We can write

\[
g = \sum_{x=0}^{p-1} \left( 1 + \left( \frac{x-a}{p} \right) \right) \left( 1 - \left( \frac{x-b}{p} \right) \right) \left( 1 - \left( \frac{x-c}{p} \right) \right)
\]

\[
= \sum_{x=0}^{p-1} \left( 1 + \sum_{x=0}^{p-1} \left( \frac{x-a}{p} \right) - \left( \frac{x-b}{p} \right) - \left( \frac{x-c}{p} \right) \right)
\]

\[
- \sum_{x=0}^{p-1} \left( \frac{x-a}{p} \right) \left( \frac{x-b}{p} \right) + \left( \frac{x-a}{p} \right) \left( \frac{x-c}{p} \right)
\]

\[
- \left( \frac{x-b}{p} \right) \left( \frac{x-c}{p} \right)
\]

\[
= p + 1 + \sum_{x=0}^{p-1} \left( \frac{x-a}{p} \right) \left( \frac{x-b}{p} \right) \left( \frac{x-c}{p} \right).
\]

[by (4.1.4) and Corollary 4.1.3]

Thus
\[ |g - p - 1| = \left| \sum_{x=0}^{p-1} \left( \frac{x-a}{p} \right) \left( \frac{x-b}{p} \right) \left( \frac{x-c}{p} \right) \right| \leq 2\sqrt{p}. \]  

(by Theorem 4.1.1) \hfill (4.2.1)

Hence,

\[
g - f = \left[ 1 - \left( \frac{a-b}{p} \right) \right] \left[ 1 - \left( \frac{a-c}{p} \right) \right] + \left[ 1 + \left( \frac{b-a}{p} \right) \right] \left[ 1 - \left( \frac{b-c}{p} \right) \right] + \left[ 1 + \left( \frac{c-a}{p} \right) \right] \left[ 1 - \left( \frac{c-b}{p} \right) \right] \leq 8,
\]

since either \(ab \in E(G_p)\) or \(ab \notin E(G_p)\). Consequently,

\[
f \geq g - 8 \geq p + 1 - 2\sqrt{p} - 8.
\]

Hence, \(f > 8(k - 1)\) for \(p > (1 + 2\sqrt{2k})^2\) as required. As \(S\) is arbitrary this completes the proof.

\[\Box\]

Remark 4.2.2: We have verified, by a computer, that if \(p \equiv 1(\text{mod 4})\) is a prime number less than or equal to 1009 and \(k\) is a positive integer with \(p \leq (1 + 2\sqrt{2k})^2\), then \(G_p \notin \mathcal{Y}(1,2,k) \land \mathcal{Y}(2,1,k)\); details of this computational work are given in a more general setting in Section 5.2. We conjecture that this is true for all \(p\). We can choose \(a, b\) and \(c\) in the proof of Lemma 4.2.2 so that \(ab, ac \in E(G_p)\) and \(bc \notin E(G_p)\). Then \(g - f = 8\) and hence,
\[ f = g - 8 \leq p + 2\sqrt{p} + 1 - 8. \]  
(by (4.2.1))

Consequently, \( f < 8k \) for \( p < (-1 + 2\sqrt{2}(k + 1))^2 \). So the problem is to look at \((-1 + 2\sqrt{2}(k + 1))^2 \leq p \leq (1 + 2\sqrt{2})^2 \).

We now extend the above arguments to the classes \( \mathcal{S}(1,n,k) \) and \( \mathcal{S}(n,1,k) \) and prove the main result of this section.

**Theorem 4.2.3:** Let \( p \equiv 1(\text{mod } 4) \) be a prime and \( k \) a positive integer. If

\[ p > (2n^2 + 2)\sqrt{p} + (n + 2k - 1)2^n - 2n - 1, \quad (4.2.2) \]

then \( G_p \in \mathcal{S}(1,n,k) \cap \mathcal{S}(n,1,k) \).

**Proof:** Since \( G_p \) is a self-complementary graph, it is sufficient to prove that \( G_p \in \mathcal{S}(1,n,k) \). Let \( a \) be a vertex of \( G_p \) and \( B = \{b_1, b_2, \ldots, b_n\} \) any set of \( n \) distinct vertices of \( G_p \). Then \( n(a/b_1, b_2, \ldots, b_n) = k \) if and only if

\[
f = \sum_{x=0}^{p-1} \left\{ \left( 1 + \left( \frac{x - a}{p} \right) \right)^n \prod_{l=1}^{n} \left( 1 - \left( \frac{x - b_l}{p} \right) \right) \right\} \equiv k 2^{n+1}.
\]

To show that \( f \equiv k 2^{n+1} \), it is clearly sufficient to establish that \( f > (k - 1)2^{n+1} \). Now

\[
g = \sum_{x=0}^{p-1} \left\{ \left( 1 + \left( \frac{x - a}{p} \right) \right)^n \prod_{l=1}^{n} \left( 1 - \left( \frac{x - b_l}{p} \right) \right) \right\}
\]
\[
\begin{align*}
&= \sum_{x=0}^{p-1} 1 + \sum_{x=0}^{p-1} \left\{ \left( \frac{x - a}{p} \right) - \sum_{i=1}^{n} \left( \frac{x - b_i}{p} \right) \right\} + \sum_{x=0}^{p-1} \left[ \sum_{i=1}^{n-1} \sum_{j=1+1}^{n} \left( \frac{x - b_i}{p} \right) \left( \frac{x - b_j}{p} \right) - \sum_{i=1}^{n} \left( \frac{x - a}{p} \right) \left( \frac{x - b_i}{p} \right) \right] \\
&\quad + \ldots + \sum_{x=0}^{p-1} \prod_{i=1}^{n} \left( \frac{x - a}{p} \right) \left( \frac{x - b_i}{p} \right).
\end{align*}
\]

Observe that the first term in the above expression is equal to \( p \) and from (4.1.4) the second term is 0. Using Corollary 4.1.3 the third term of the above expression is equal to \( n - \left( \begin{array}{c} n \\ 2 \end{array} \right) = \frac{1}{2}(3n - n^2) \). Hence,

\[
|g - p - \frac{1}{2}(3n - n^2)|
\]

\[
\begin{align*}
&\leq \left| \sum_{x=0}^{p-1} \sum_{i=1}^{n-1} \sum_{j=1+1}^{n} \sum_{k=j+1}^{n+1} \left( \frac{x - c_i}{p} \right) \left( \frac{x - c_j}{p} \right) \left( \frac{x - c_k}{p} \right) \right| \\
&\quad + \left| \sum_{x=0}^{p-1} \sum_{i=1}^{n-2} \sum_{j=1+1}^{n} \sum_{k=j+1}^{n+1} \sum_{\ell=k+1}^{n+1} \left( \frac{x - c_i}{p} \right) \left( \frac{x - c_j}{p} \right) \left( \frac{x - c_k}{p} \right) \left( \frac{x - c_{\ell}}{p} \right) \right| \\
&\quad + \ldots + \left| \sum_{x=0}^{p-1} \prod_{i=1}^{n+1} \left( \frac{x - c_i}{p} \right) \right|.
\end{align*}
\]

(4.2.3)

where \( \{c_1, c_2, \ldots, c_{n+1}\} = \{a\} \cup B \). Now Theorem 4.1.1 and Corollary 4.1.4 together imply
\[
\left| p \sum_{x=0}^{p-1} \prod_{1 < i_1 < i_2 < \ldots < i_s} \left( \frac{x - c_{i_1}}{p} \right) \left( \frac{x - c_{i_2}}{p} \right) \ldots \left( \frac{x - c_{i_s}}{p} \right) \right|
\]

\[
\sum_{s} \begin{cases} 
\binom{n + 1}{s} (s - 1)\sqrt{p}, & \text{if } s \text{ is odd}, \\
\binom{n + 1}{s} \{1 + (s - 2)\sqrt{p}\}, & \text{otherwise.}
\end{cases}
\tag{4.2.4}
\]

Making use of (4.2.4) we get, from (4.2.3),

\[
|g - p + \frac{1}{2}(3n - n^2)|
\]

\[
\leq \sum_{t=3}^{n+1} \binom{n + 1}{t} (t - 1)\sqrt{p} + \sum_{t=4}^{n+1} \binom{n + 1}{t} \{1 + (t - 2)\sqrt{p}\}
\]

\[
= \left[ \sum_{t=3}^{n+1} \binom{n + 1}{t} t - \sum_{t=3}^{n+1} \binom{n + 1}{t} - \sum_{t=4}^{n+1} \binom{n + 1}{t} \right] \sqrt{p}
\]

\[
+ \sum_{t=4}^{n+1} \binom{n + 1}{t}
\]

\[
= (n - 2)2^n + 2\sqrt{p} + 2^n - \frac{1}{2}(n^2 + n) - 1.
\]

Hence,

\[
g = p + \frac{1}{2}(3n - n^2) - (n - 2)2^n + 2\sqrt{p} - (2^n - \frac{1}{2}(n^2 + n) - 1)
\]

\[
= p - (n - 2)2^n + 2\sqrt{p} - (2^n - 2n - 1).
\]

Now
\[ g - f = \sum_{x \in (a) \cup B} \left\{ \left( 1 + \left( \frac{x - a}{p} \right) \right)^n \prod_{i=1}^{n} \left( 1 - \left( \frac{x - b_i}{p} \right) \right) \right\}. \]  

(4.2.5)

If \( g - f \neq 0 \), then for some \( y \) the product

\[ \left( 1 + \left( \frac{y - a}{p} \right) \right)^n \prod_{i=1}^{n} \left( 1 - \left( \frac{y - b_i}{p} \right) \right) \neq 0. \]  

(4.2.6)

If \( y = a \), then for (4.2.6) to hold we must have \( \left( \frac{a - b_i}{p} \right) = -1 \) for all \( i \). Hence, the term in (4.2.5) with \( x = b_i \) contributes zero to the sum. Therefore, \( g - f = 2^n \), since each factor is 2 and one factor is 1. If \( y = b_j \) for some \( j \), then for (4.2.6) to hold we must have \( \left( \frac{b_j - a}{p} \right) = 1 \). Hence, the term in (4.2.5) with \( x = a \) contributes zero to the sum. Consequently, we can write (4.2.5) as:

\[ g - f = \sum_{x \in B} \left\{ \left( 1 + \left( \frac{x - a}{p} \right) \right)^n \prod_{i=1}^{n} \left( 1 - \left( \frac{x - b_i}{p} \right) \right) \right\} \leq n2^n, \]

since

\[ \left( 1 + \left( \frac{x - a}{p} \right) \right)^n \prod_{i=1}^{n} \left( 1 - \left( \frac{x - b_i}{p} \right) \right) \leq 2^n \]

for each \( x \); note that each factor is at most 2 and at least one factor is 1. Then we conclude that

\[ g - f \leq n2^n. \]

So

\[ f \geq g - n2^n \]

75
\[ p - (2^n - 2n - 1) - ((n - 2)2^n + 2)\sqrt{p} - n2^n \]
\[ = p - ((n - 2)2^n + 2)\sqrt{p} - ((n + 1)2^n - 2n - 1). \]

So, if (4.2.2) holds, then \( f > (k - 1)2^{n+1} \) as required. Since \( S \) is arbitrary, this completes the proof of the theorem. \( \square \)

For the particular case \( n = 3 \) we have:

Corollary 4.2.4: Let \( p \equiv 1(\text{mod} \ 4) \) be a prime and \( k \) a positive integer. If \( p > (5 + \sqrt{16k + 34})^2 \), then \( G_p \in \mathcal{G}(1,3,k) \cap \mathcal{G}(3,1,k). \)

4.3 \( \mathcal{G}(n,n,k) \)

We now turn our attention to the class \( \mathcal{G}(n,n,k) \). To illustrate the method we begin with the simple case when \( n = 2 \). This class has been studied for \( k = 1 \) by Blass, Exoo and Harary (1981) and for \( n = 2, k = 1 \) by Caccetta, Vijayan and Wallis (1984).

Theorem 4.3.1: Let \( p \equiv 1(\text{mod} \ 4) \) be a prime and \( k \) a positive integer. If \( p > (5 + 2\sqrt{4k + 6})^2 \), then \( G_p \in \mathcal{G}(2,2,k) \).

Proof: The method of proof is similar to that of Lemma 4.2.2. Here we take \( S = \{a,b,c,d\} \) to be any set of four distinct vertices of \( G_p \) and observe that \( n(a,b/c,d) \geq k \) if and only if

\[
\begin{align*}
\sum_{x \in S} \left[ \left( 1 + \left( \frac{x - a}{p} \right) \right) \left( 1 + \left( \frac{x - b}{p} \right) \right) \right] \\
\left( 1 - \left( \frac{x - c}{p} \right) \right) \left( 1 - \left( \frac{x - d}{p} \right) \right)
\end{align*}
\]

76
\[ g \geq 16k. \]

To show that \( g \geq 16k \), it is clearly sufficient to establish that \( f > 16(k - 1) \).

Simple algebra together with (4.1.4) and Corollary 4.1.3 yield:

\[
g = \sum_{x=0}^{p-1} \left\{ \left[ 1 + \left( \frac{x-a}{p} \right) \right] \left[ 1 + \left( \frac{x-b}{p} \right) \right] \right. \\
\left. \left[ 1 - \left( \frac{x-c}{p} \right) \right] \left[ 1 - \left( \frac{x-d}{p} \right) \right] \right\} \\
= p + 2 + \sum_{x=0}^{p-1} \left\{ \left( \frac{x-a}{p} \right) \left( \frac{x-c}{p} \right) \left( \frac{x-d}{p} \right) \\
+ \left( \frac{x-b}{p} \right) \left( \frac{x-c}{p} \right) \left( \frac{x-d}{p} \right) - \left( \frac{x-a}{p} \right) \left( \frac{x-b}{p} \right) \left( \frac{x-c}{p} \right) \right. \\
- \left. \left( \frac{x-a}{p} \right) \left( \frac{x-b}{p} \right) \left( \frac{x-d}{p} \right) \right\} \\
+ \sum_{x=0}^{p-1} \left\{ \left( \frac{x-a}{p} \right) \left( \frac{x-b}{p} \right) \left( \frac{x-c}{p} \right) \left( \frac{x-d}{p} \right) \right\}. \\
\]

Now by Theorem 4.1.1 and Corollary 4.1.4 we have

\[ |g - (p + 2)| \leq 10\sqrt{p} + 1, \]

and hence,

\[ g \geq p + 1 - 10\sqrt{p}. \]

Now
\[ g - f = \left\{ \begin{array}{c} 1 + \left( \frac{a - b}{p} \right) \left\{\right. \left. 1 - \left( \frac{a - c}{p} \right) \left( 1 - \left( \frac{a - d}{p} \right) \right) \right. \\
+ \left( \frac{d - a}{p} \right) \left( 1 + \left( \frac{d - b}{p} \right) \left( 1 - \left( \frac{d - c}{p} \right) \right) \right) \\
+ \left( \frac{c - a}{p} \right) \left( 1 + \left( \frac{c - b}{p} \right) \left( 1 - \left( \frac{c - d}{p} \right) \right) \right) \\
+ \left( \frac{b - a}{p} \right) \left( 1 - \left( \frac{b - c}{p} \right) \left( 1 - \left( \frac{b - d}{p} \right) \right) \right) \end{array} \right. \]

Observing that at least one of the first two terms and at least one of the last two terms on the right hand side of the above expression is zero, we conclude that \( g - f \leq 16 \). Consequently,

\[
f \geq g - 16 \geq p + 1 - 10\sqrt{p} - 16.
\]

Hence, \( f > 16(k - 1) \) for \( p > (5 + 2\sqrt{6k + 6})^2 \) as required. Since \( S \) is arbitrary, this completes the proof.

Remark 4.3.1: Blass, Exoo and Harary (1981) proved that \( G_p \in \mathcal{F}(n,n,1) \) for \( p \equiv 1(\text{mod } 4) \) and \( p > n^{2.4n} \). For the particular case \( n = 2 \), this result asserts that \( G_p \in \mathcal{F}(2,2,1) \) for prime \( p \geq 1033 \). When \( k = 1 \), Theorem 4.7 asserts that \( G_p \in \mathcal{F}(2,2,1) \) for all prime \( p \geq 137 \). We have verified, using a computer, that \( G_p \in \mathcal{F}(2,2,1) \) only for prime \( p \geq 61 \). Thus Theorem 4.7 is not sharp. However, computer analysis shows that the bound on \( p \) given in Theorem 4.3.1 is fairly close to best possible. Table 4.3.1 gives the maximum \( k \) for which \( G_p \in \mathcal{F}(2,2,k) \); we give only some of the computational results.
<table>
<thead>
<tr>
<th>Maximum k</th>
<th>Order p</th>
<th>Maximum k</th>
<th>Order p</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$\leq 53$</td>
<td>24</td>
<td>593</td>
</tr>
<tr>
<td>1</td>
<td>61, 73</td>
<td>25</td>
<td>601, 617</td>
</tr>
<tr>
<td>2</td>
<td>89, 97, 101, 109</td>
<td>26</td>
<td>613</td>
</tr>
<tr>
<td></td>
<td>113</td>
<td>27</td>
<td>641, 653</td>
</tr>
<tr>
<td>3</td>
<td>137</td>
<td>28</td>
<td>673</td>
</tr>
<tr>
<td>4</td>
<td>149, 157, 173</td>
<td>29</td>
<td>677</td>
</tr>
<tr>
<td>5</td>
<td>181</td>
<td>30</td>
<td>701</td>
</tr>
<tr>
<td>6</td>
<td>193, 197, 233</td>
<td>31</td>
<td>709</td>
</tr>
<tr>
<td>7</td>
<td>229</td>
<td>32</td>
<td>733, 769</td>
</tr>
<tr>
<td>8</td>
<td>241, 257</td>
<td>33</td>
<td>773</td>
</tr>
<tr>
<td>9</td>
<td>269, 277, 281</td>
<td>34</td>
<td>757, 761</td>
</tr>
<tr>
<td>10</td>
<td>293, 313, 317</td>
<td>35</td>
<td>809</td>
</tr>
<tr>
<td>11</td>
<td>337</td>
<td>36</td>
<td>797, 821</td>
</tr>
<tr>
<td>12</td>
<td>349, 353</td>
<td>37</td>
<td>829</td>
</tr>
<tr>
<td>14</td>
<td>373</td>
<td>38</td>
<td>857, 877</td>
</tr>
<tr>
<td>15</td>
<td>389, 397, 401</td>
<td>39</td>
<td>853</td>
</tr>
<tr>
<td>16</td>
<td>409, 421, 433</td>
<td>42</td>
<td>937</td>
</tr>
<tr>
<td>17</td>
<td>449</td>
<td>43</td>
<td>929, 953</td>
</tr>
<tr>
<td>18</td>
<td>457, 461</td>
<td>44</td>
<td>941, 961</td>
</tr>
<tr>
<td>20</td>
<td>521</td>
<td>45</td>
<td>977</td>
</tr>
<tr>
<td>21</td>
<td>509</td>
<td>46</td>
<td>997</td>
</tr>
<tr>
<td>22</td>
<td>541, 557, 569</td>
<td>47</td>
<td>1009</td>
</tr>
<tr>
<td>23</td>
<td>577</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 4.3.1: Maximum $k$ for which $G_p \in \mathcal{S}(2, 2, k)$.  

79
Our next result concerns the class $\mathcal{U}(n,n,k)$.

**Theorem 4.3.2:** Let $p \equiv 1 \pmod{4}$ be a prime and $k$ a positive integer. If

$$p > (2n - 3)2^{2n-1} + 2)\sqrt{p} + (n + 2k - 1)2^{n-1} - 2n^2 - 1,$$

(4.3.1)

then $G_p \in \mathcal{U}(n,n,k)$.

**Proof:** Let $S = \{a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n\}$ be any set of $2n$ distinct vertices of $G_p$. Then $n(a_1, a_2, \ldots, a_n/b_1, b_2, \ldots, b_n) \geq k$ if any only if

$$f = \sum_{x=0}^{p-1} \prod_{i=1}^{n} \left\{ \left( 1 + \left( \frac{x - a_i}{p} \right) \right) \left( 1 - \left( \frac{x - b_i}{p} \right) \right) \right\} \geq k2^{2n}.$$

To show that $f \geq k2^{2n}$, it is clearly sufficient to establish that $f > (k - 1)2^{2n}$.

Now

$$g = \sum_{x=0}^{p-1} \prod_{i=1}^{n} \left\{ \left( 1 + \left( \frac{x - a_i}{p} \right) \right) \left( 1 - \left( \frac{x - b_i}{p} \right) \right) \right\}$$

$$= \sum_{x=0}^{p-1} 1 + \sum_{x=0}^{p-1} \sum_{i=1}^{n} \left\{ \left( \frac{x - a_i}{p} \right) - \left( \frac{x - b_i}{p} \right) \right\}$$

$$+ \sum_{x=0}^{p-1} \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} \left( \frac{x - a_i}{p} \right) \left( \frac{x - a_j}{p} \right) + \sum_{i=1}^{n} \sum_{j=1}^{n} \left( \frac{x - a_i}{p} \right) \left( \frac{x - a_j}{p} \right).$$

80
\[
\left( \frac{x-a_1}{p} \right) \left( \frac{x-b_1}{p} \right) + \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} \left( \frac{x-b_1}{p} \right) \left( \frac{x-b_j}{p} \right) \\
+ \ldots + \sum_{x=0}^{p-1} \prod_{i=1}^{n} \left\{ \left( \frac{x-a_1}{p} \right) \left( \frac{x-b_i}{p} \right) \right\}.
\]

Observe that the first term in the above expression is equal to \( p \) and from (4.1.4) the second term is 0.

Using Corollary 4.1.3 the third term of the above expression is equal to \( n^2 - \binom{n}{2} - \binom{n}{2} = n \). Hence,

\[|g - p - n|\]

\[= \left| \sum_{x=0}^{p-1} \sum_{i=1}^{2n-2} \sum_{j=i+1}^{2n-1} \sum_{k=j+1}^{2n} \left( \frac{x-c_1}{p} \right) \left( \frac{x-c_j}{p} \right) \left( \frac{x-c_k}{p} \right) \right|\]

\[+ \left| \sum_{x=0}^{p-1} \sum_{i=1}^{2n-3} \sum_{j=i+1}^{2n-2} \sum_{k=j+1}^{2n-1} \sum_{\ell=k+1}^{2n} \left( \frac{x-c_1}{p} \right) \left( \frac{x-c_j}{p} \right) \left( \frac{x-c_k}{p} \right) \left( \frac{x-c_\ell}{p} \right) \right| + \ldots + \left| \sum_{x=0}^{p-1} \prod_{i=1}^{2n} \left( \frac{x-c_i}{p} \right) \right|.
\]

(4.3.2)

where \( \{c_1, c_2, \ldots, c_{2n}\} = S \). Now Theorem 4.1.1 and Corollary 4.1.4 together imply that

\[\left| \sum_{x=0}^{p-1} \sum_{1 < i_2 < \ldots < i_s} \left\{ \left( \frac{x-c_{i_1}}{p} \right) \left( \frac{x-c_{i_2}}{p} \right) \ldots \left( \frac{x-c_{i_s}}{p} \right) \right\} \right|
\]
\[ |g - p - n| \leq \sum_{t=1}^{n-1} \left[ \binom{2n}{2t+1} 2t\sqrt{p} \right] + \left[ \binom{2n}{2t+2} \left( 1 + 2t\sqrt{p} \right) \right] \]

\[ = \sum_{t=1}^{n-1} \left[ \binom{2n}{2t+1} - \sum_{t=1}^{n-1} \left[ \binom{2n}{2t+1} + 2 \binom{2n}{2t+2} \right] \right] \sqrt{p} \]

\[ + \sum_{t=1}^{n-1} \binom{2n}{2t+2} \]

\[ = (2n - 3)2^{2n-1} + 2 \sqrt{p} + 2^{2n-1} - 2n^2 + n - 1. \]

Hence,

\[ g \geq p + n - 2^{2n-1} + 2n^2 - n + 1 - (2n - 3)2^{2n-1} + 2 \sqrt{p} \]

\[ = p - 2^{2n-1} + 2n^2 + 1 - (2n - 3)2^{2n-1} + 2 \sqrt{p}. \quad (4.3.4) \]

Now

\[ g - f = \sum_{x \in S} \frac{\prod_{i=1}^{n} \left( 1 + \left( \frac{x - a_i}{p} \right) \right) \left( 1 - \left( \frac{x - b_i}{p} \right) \right)}{1 - \left( \frac{y - a_i}{p} \right) \left( 1 - \left( \frac{y - b_i}{p} \right) \right)} \]

\[ = 0. \quad (4.3.5) \]

If \( g - f \neq 0 \), then for some \( y \) the product

\[ \prod_{i=1}^{n} \left( 1 + \left( \frac{y - a_i}{p} \right) \right) \left( 1 - \left( \frac{y - b_i}{p} \right) \right) \neq 0. \quad (4.3.6) \]
Without any loss of generality suppose \( y = a_k \). For (4.3.6) to hold we must have \( \left( \frac{a_k - b_1}{p} \right) = -1 \) for all \( l \). Hence, the term in (4.3.5) with \( x = b_1 \) contributes zero to the sum. Then we can write (4.3.5) as:

\[
g - f = \sum_{x=a_1}^{a_n} \prod_{l=1}^{n} \left( 1 + \left( \frac{x - a_1}{p} \right) \right) \left( 1 - \left( \frac{x - b_1}{p} \right) \right)
\]

\[\leq n 2^{2n-1},\]

since

\[
\prod_{l=1}^{n} \left( 1 + \left( \frac{x - a_1}{p} \right) \right) \left( 1 - \left( \frac{x - b_1}{p} \right) \right) \leq 2^{2n-1}
\]

for each \( x \); note that each factor is at most 2 and at least one factor is 1. Hence,

\[
f \geq g - n 2^{2n-1}
\]

\[\geq p - (n + 1)2^{2n-1} + 2n^2 + 1 - \{(2n - 3)2^{2n-1} + 2\} \sqrt{p}.
\]

[using (4.3.4)]

So, if (4.3.1) holds, then \( f > (k - 1)2^n \) as required. Since \( S \) is arbitrary, this completes the proof of the theorem.

\[\square\]

For the particular case \( k = 1 \) we have:

**Corollary 4.3.3:** Let \( p \equiv 1(\text{mod } 4) \) be a prime. If \( p > ((2n - 3)2^{2n-1} + 4)^2 \), then \( G_p \in \mathcal{S}(n,n,1) \).

\[\square\]
Corollary 4.3.4: Let $p = 1 \pmod{4}$ be a prime. If $n \geq 4$ and $p > ((2n - 3)2^{2n-1} + 3)^2$, then $G_p \in \mathcal{F}(n,n,1)$. 

Remark 4.3.2: Note that the bound given in Corollary 4.3.3 is better than the bound of $p > n2^{4n}$ obtained by Exoo and Harary (1980).
CHAPTER 5

PALEY GRAPHS OF ORDER $q = p^d$, $p$ PRIME

Recall that for a prime power $q \equiv 1(\text{mod } 4)$, the Paley graph $G_q$ of order $q$ is the graph whose vertices are elements of the finite field $\mathbb{F}_q$, two vertices are adjacent if and only if their difference is a quadratic residue. In Chapter 4, we established the adjacency properties of Paley graphs of prime order. These results were obtained by making use of results from prime number theory. In this chapter, we establish, by making use of results from finite fields, the adjacency properties of Paley graphs of order $q = p^d$, with $p$ a prime. In particular, in Section 5.2, we prove that for a prime power $q \equiv 1(\text{mod } 4)$;

- $G_q \in \mathcal{S}(1,n,k) \cap \mathcal{S}(n,1,k)$, for every
  
  $$q > ((n - 2)2^n + 2)\sqrt{q} + (n + 2k - 1)2^n - 2n - 1;$$

- $G_q \in \mathcal{S}(n,n,k)$, for every
  
  $$q > ((2n - 3)2^{2n-1} + 2)\sqrt{q} + (n + 2k - 1)2^{2n-1} - 2n^2 - 1;$$

and

- $G_q \in \mathcal{S}(m,n,k)$, for every
  
  $$q > ((t - 3)2^{t-1} + 2)\sqrt{q} + (t + 2k - 1)2^{t-1} - 1,$$

where $m + n \leq t$. This means that, for any $m$, $n$ and $k$, all sufficiently large Paley graphs satisfy property $P(m,n,k)$.
Our results give us better bounds than the results established in Chapter 4 because we pick up the prime powers. For example, Lemma 4.2.2 shows that $G_p \in \mathcal{G}(1,2,4) \cap \mathcal{G}(2,1,4)$ for every $p \geq 53$ but in this chapter we show that $G_q \in \mathcal{G}(1,2,4) \cap \mathcal{G}(2,1,4)$ for every $q \geq 49$.

We also present computational results which establish the smallest Paley graphs in $\mathcal{G}(1,2,k) \cap \mathcal{G}(2,1,k)$, $\mathcal{G}(1,3,k) \cap \mathcal{G}(3,1,k)$ and $\mathcal{G}(2,2,k)$ for small $k$.

Recall that a graph $G$ is said to have property $P(n,k)$ if for any two sets $A$ and $B$ of vertices of $G$ with $A \cap B = \emptyset$ and $|A \cup B| = n$, there are at least $k$ other vertices not in $A \cup B$ which are joined to every vertex of $A$ but not joined to any vertex of $B$. In Section 5.3, we prove that $G_q$ has property $P(n,k)$ if

$$q > \{(n - 3)2^{n-1} + 2\sqrt{q} + (n + 2k - 1)2^{n-1} - 1\}.$$

Section 5.1 contains some basic terminology and results on finite fields that we make use of in our work. In addition, we establish two important results concerning a quadratic (residue) character defined on the finite field. These results play a crucial role in the proofs of our main theorems in sections 5.2 and 5.3.

In Section 5.4, we give another example of a class of graphs satisfying property $P(m,n,k)$. We refer to this class as "generalized" Paley graphs. We also present computational results which establish the smallest "generalized" Paley graphs in $\mathcal{G}(2,2,k)$ for small $k$. 
5.1 Finite Fields

In this section, we present some results on finite fields which we make use of in establishing the main results of this chapter. We begin with some basic notation and terminology.

Let \( F_q \) be the finite field (Galois field) of order \( q \) where \( q \) is a prime power and let \( F_q[x] \) be a polynomial ring over \( F_q \). A character \( \chi \) on \( F_q^* \), the multiplicative group of the non-zero elements of \( F_q \), is a map from \( F_q^* \) to the multiplicative group of complex numbers with \( |\chi(x)| = 1 \) for all \( x \) and with

\[
\chi(xy) = \chi(x)\chi(y)
\]

for any \( x, y \in F_q^* \), so that the values of \( \chi \) are the \((q - 1)^{th}\) roots of unity. Since \( \chi(1) = \chi(1)\chi(1) \), we have \( \chi(1) = 1 \).

Among the characters of \( F_q^* \), we have the principal character \( \chi_0 \) defined by \( \chi_0(x) = 1 \) for all \( x \in F_q^* \); all other characters of \( F_q^* \) are called non-principal. A character \( \chi \) is of order \( d \) if \( \chi^d = e \) and \( d \) is the smallest positive integer with this property.

It will be convenient to extend the definition of a non-principal character \( \chi \) to the whole \( F_q \) by putting \( \chi(0) = 0 \).

If \( \chi \) is a non-principal character on \( F_q^* \), it is well-known [see Lidl and Niederreiter (1983)] that

\[
\sum_{x \in F_q} \chi(x) = 0. \tag{5.1.1}
\]

It follows that, for \( a \in F_q \)

\[
\sum_{x \in F_q} \chi(x - a) = 0. \tag{5.1.2}
\]
The following theorem is very useful in our work. The proof is based on Weil's Theorem proving the Riemann hypothesis for (algebraic) curves over finite fields [see Schmidt (1976)].

**Theorem 5.1.1:** Let $\chi$ be a non-principal character on $\mathbb{F}_q$ of order $d > 1$. If $a_1, a_2, \ldots, a_s$ are distinct elements of $\mathbb{F}_q$, then

$$\left| \sum_{x \in \mathbb{F}_q} \chi((x - a_1)(x - a_2) \ldots (x - a_s)) \right| \leq (s - 1)\sqrt{q}.$$  \hfill \Box

Let $q$ be a power of an odd prime. We define a quadratic (residue) character $\eta$ on $\mathbb{F}_q$ by

$$\eta(a) = a^{\frac{q-1}{2}}, \text{ for all } a \in \mathbb{F}_q.$$  

Equivalently, $\eta$ is 1 on squares, 0 at 0 and -1 otherwise. Therefore, $\eta$ is a non-principal character of order 2.

If $q = p$ is an odd prime, then for $a \in \mathbb{F}_p$ we have $\eta(a) = \left( \frac{a}{p} \right)$, the Legendre symbol defined in Section 4.1 as:

$$\left( \frac{a}{p} \right) = \begin{cases} 
1, & \text{if } a \text{ is a quadratic residue modulo } p, \\
0, & \text{if } p|a, \\
-1, & \text{otherwise}.
\end{cases}$$

Our next two results are crucial to our work in establishing a lower bound on $q$ for $q \in \mathcal{B}(m,n,k)$.

**Theorem 5.1.2:** Let $\eta$ be a quadratic character on $\mathbb{F}_q$. If $a_1, a_2, \ldots, a_s$ are distinct elements of $\mathbb{F}_q$ and $s$ is even, then
$$\sum_{x \in \mathbb{F}_q} \eta((x - a_1)(x - a_2) \ldots (x - a_s))$$

$$= -1 \pm \sum_{x \in \mathbb{F}_q} \eta((x + b_1)(x + b_2) \ldots (x + b_{s-1}))$$

for some distinct elements $b_1, b_2, \ldots, b_{s-1}$ of $\mathbb{F}_q$.

Proof: We write

$$\sum_{x \in \mathbb{F}_q} \eta((x - a_1)(x - a_2) \ldots (x - a_s))$$

$$= \sum_{x \in \mathbb{F}_q} \eta(x(x + a_1 - a_2)(x + a_1 - a_3) \ldots (x + a_1 - a_s)).$$

(5.1.3)

Note that the equality (5.1.3) is valid, since $x$ and $x + a_1$ assume all values in $\mathbb{F}_q$. Now since $a_1, a_2, \ldots, a_s$ are distinct, then $c_i = a_i - a_{i+1} \neq 0$ for $1 \leq i \leq s - 1$.

If $x \neq 0$, then there exists an $x^{-1}$ such that $xx^{-1} = 1$.

Furthermore, $\eta((x^{-1})^s) = 1$, since $s$ is even. If $x = 0$, then $\eta(x) = 0$. Thus we can write (5.1.3) as:

$$\sum_{x \in \mathbb{F}_q^*} \eta(x(x + c_1)(x + c_2) \ldots (x + c_{s-1}))$$

$$= \sum_{x \in \mathbb{F}_q^*} \eta((x^{-1})^s)\eta(x(x + c_1)(x + c_2) \ldots (x + c_{s-1}))$$

$$= \sum_{x \in \mathbb{F}_q^*} \eta(xx^{-1}(xx^{-1} + c_1x^{-1})(xx^{-1} + c_2x^{-1}) \ldots (xx^{-1} + c_{s-1}x^{-1}))$$

89
Using (5.1.2) and Theorem 5.1.1 we have the following corollaries to Theorem 5.1.2.

Corollary 5.1.3: If \( \eta \) is a quadratic character on \( \mathbb{F}_q \), then for \( a, b \in \mathbb{F}_q \) with \( a \neq b \)

\[
\sum_{x \in \mathbb{F}_q} \eta((x - a)(x - b)) = -1.
\]

Corollary 5.1.4: Let \( \eta \) be a quadratic character on \( \mathbb{F}_q \). If \( a_1, a_2, \ldots, a_s \) are distinct elements of \( \mathbb{F}_q \), then for even \( s \)

\[
\left| \sum_{x \in \mathbb{F}_q} \eta((x - a_1)(x - a_2) \ldots (x - a_s)) \right| \leq 1 + (s - 2)\sqrt{q}.
\]

Theorem 5.1.5: Let \( \eta \) be a quadratic character on \( \mathbb{F}_q \) and let \( A \) and \( B \) be disjoint subsets of \( \mathbb{F}_q \). Put

\[
g = \sum_{x \in \mathbb{F}_q} \prod_{a \in A} (1 + \eta(x - a)) \prod_{b \in B} (1 - \eta(x - b)).
\]

As usual, an empty product is defined to be 1. Then

(a) \( g \geq q - \{(n - 2)2^n + 2\sqrt{q} - \{2 - 2n - 1\}, \)

where \( |B| = n \) and \( |A| = 1 \).

(b) \( g \geq q - \{(t - 3)2^{t-1} + 2\sqrt{q} - \{2 - 1\}, \)

where \( t = |A \cup B| \).

(c) \( g \geq q - \{(2n - 3)2^{2n-1} + 2\sqrt{q} - \{2^{2n-1} - 2n^2 - 1\}, \)

where \( n = |A| = |B| \).
Proof: (a) Let $A = \{a\}$ and $B = \{b_1, b_2, \ldots, b_n\}$. Expanding $g$ we see that

$$g = \sum_{x \in \mathbb{F}_q} (1 + \eta(x - a)) \prod_{i=1}^{n} (1 - \eta(x - b_i))$$

$$= \sum_{x \in \mathbb{F}_q} 1 + \sum_{x \in \mathbb{F}_q} \left\{ \eta(x - a) - \sum_{i=1}^{n} \eta(x - b_i) \right\}$$

$$+ \sum_{x \in \mathbb{F}_q} \left\{ \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} \eta((x - b_i)(x - b_j)) - \sum_{i=1}^{n} \eta((x - a)(x - b_i)) \right\}$$

$$+ \ldots + \sum_{x \in \mathbb{F}_q} \prod_{i=1}^{n} \eta((x - a)(x - b_i)).$$

Observe that the first term in the above expansion is equal to $q$ and from (5.1.2) the second term is 0. Using Corollary 5.1.3 the third term of the above expansion is equal to $n - \left( \begin{array}{c} n \\ 2 \end{array} \right) = \frac{1}{2}(3n - n^2)$. Hence,

$$|g - q - \frac{1}{2}(3n - n^2)|$$

$$\leq \left| \sum_{x \in \mathbb{F}_q} \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} \sum_{k=j+1}^{n+1} \eta((x - c_i)(x - c_j)(x - c_k)) \right|$$

$$+ \left| \sum_{x \in \mathbb{F}_q} \sum_{i=1}^{n-2} \sum_{j=i+1}^{n-1} \sum_{k=j+1}^{n} \sum_{\ell=k+1}^{n+1} \eta((x - c_i)(x - c_j)(x - c_k)(x - c_\ell)) \right|$$
\[(x - c_k)(x - c_l)) + \ldots + \left| \sum_{x \in \mathbb{F}_q} \prod_{i=1}^{n+1} \eta(x - c_i) \right|,\]

where \(\{c_1, c_2, \ldots, c_{n+1}\} = A \cup B.\)

Now Theorem 5.1.1 and Corollary 5.1.4 together imply that

\[\left| \sum_{x \in \mathbb{F}_q} \sum_{1 < l_1 < \cdots < l_s} \eta((x - c_{l_1})(x - c_{l_2}) \ldots (x - c_{l_s})) \right| \leq \begin{cases} \binom{n+1}{s}(s-1)\sqrt{q}, & \text{if } s \text{ is odd}, \\ \binom{n+1}{s}(1 + (s - 2)\sqrt{q}), & \text{if } s \text{ is even}. \end{cases} \]

Making use of (5.1.6) we get, from (5.1.5),

\[|g - q - \frac{1}{2}(3n - n^2)| \leq \sum_{s=3}^{n+1} \binom{n+1}{s}(s-1)\sqrt{q} + \sum_{s=4}^{n+1} \binom{n+1}{s}(1 + (s - 2)\sqrt{q}) \]

\[= \sum_{s=3}^{n+1} \binom{n+1}{s} - \sum_{s=3}^{n+1} \binom{n+1}{s} - \sum_{s=4}^{n+1} \binom{n+1}{s}\sqrt{q} + \sum_{s=4}^{n+1} \binom{n+1}{s} \]

\[= \{(n - 2)2^n + 2\sqrt{q} + 2^n - \frac{1}{2}(n^2 + n) - 1. \]
Hence,

\[ g \geq q + \frac{1}{2}(3n - n^2) - \{(n - 2)2^n + 2\sqrt{q} - \{2^n - \frac{1}{2}(n^2 + n) - 1\} \]

\[ = q - \{(n - 2)2^n + 2\sqrt{q} - \{2^n - 2n - 1\} \}, \]

proving (a).

(b) Let \( A \cup B = \{c_1, c_2, \ldots, c_t\} \). Expanding \( g \) and noting that \( q = \sum_{x \in F_q} 1 \), we can write:

\[
|g - q| \leq \left\| \sum_{x \in F_q} \sum_{i=1}^t \eta(x - c_i) \right\| + \left| \sum_{x \in F_q} \sum_{1 \leq i_1 < i_2} \eta((x - c_{i_1})(x - c_{i_2})) \right| + \ldots + \left| \sum_{x \in F_q} \sum_{1 \leq i_1 < i_2 < \ldots < i_s} \eta((x - c_{i_1})(x - c_{i_2}) \ldots (x - c_{i_s})) \right| + \ldots + \left| \sum_{x \in F_q} \eta((x - c_1)(x - c_2) \ldots (x - c_t)) \right|.
\]

(5.1.8)

Observe that from (5.1.2) the first term in the above expansion is 0. Now Theorem 5.1.1 and Corollary 5.1.4 together with a little algebra, [note (5.1.6)], yield:

\[
|g - q| \leq \sum_{s=1}^t \left\{ \begin{array}{c} t \end{array} \right\} (s - 1)\sqrt{q} + \sum_{s=2}^t \left\{ \begin{array}{c} t \end{array} \right\} \{1 + (s - 2)\sqrt{q}\} \]

s odd

s even
\[
\begin{align*}
= \left\{ \sum_{s=3}^{t} \binom{t}{s} s - \sum_{s=3}^{t} \binom{t}{s} \right\} \sqrt{q} + \sum_{s=2}^{t} \binom{t}{s} \\
= \{(t - 3)2^{t-1} + 2\sqrt{q} + (2^{t-1} - 1).
\end{align*}
\]

Therefore,
\[
g \geq q - \{(t - 3)2^{t-1} + 2\sqrt{q} - (2^{t-1} - 1),
\]
proving (b).

(c) Let \(A = \{a_1, a_2, \ldots, a_n\}\) and \(B = \{b_1, b_2, \ldots, b_n\}\). Now expanding \(g\) we see that
\[
g = \sum_{x \in \mathbb{F}_q} 1 \sum_{x \in \mathbb{F}_q} \sum_{i=1}^{n} \{\eta(x - a_i) - \eta(x - b_i)\} + \sum_{x \in \mathbb{F}_q} \sum_{i=1}^{n-1} \sum_{j=1+1}^{n} \eta((x - a_i)(x - a_j)) - \sum_{i=1}^{n} \sum_{j=1+1}^{n} \eta((x - a_i)(x - b_j)) + \cdots + \sum_{x \in \mathbb{F}_q} \prod_{i=1}^{n} \eta((x - a_i)(x - b_i)).
\]

Observe that the first term in the above expansion is equal to \(q\) and from (5.1.2) the second term is 0. Using Corollary 5.1.3 the third term of the above expansion is equal to
\[
n^2 - \binom{n}{2} - \binom{n}{2} = n.
\]
Hence,
\[ |g - q - n| \]

\[
\begin{array}{cccc}
2n-2 & 2n-1 & 2n \\
\sum & \sum & \sum & \sum \\
x \in \mathbb{F}_q & j = j + 1 & k = k + 1
\end{array} \eta((x - c_i)(x - c_j)(x - c_k))
\]

\[
+ \left| \begin{array}{cccc}
2n-3 & 2n-2 & 2n-1 & 2n \\
\sum & \sum & \sum & \sum \\
x \in \mathbb{F}_q & j = j + 1 & k = k + 1 & \ell = \ell + 1
\end{array} \right| \eta((x - c_i)(x - c_j)(x - c_k))(x - c_{\ell})
\]

\[
+ \ldots + \left| \begin{array}{cc}
2n & \prod_{i = 1}^{\ell} \eta(x - c_i)
\end{array} \right|
\]

\quad (5.1.9)

where \( \{c_1, c_2, \ldots, c_{2n}\} = A \cup B \). Now Theorem 5.1.1 and Corollary 5.1.4 together with a little algebra, [note (5.1.6)], yield:

\[ |g - q - n| \leq \sum_{s = 3}^{2n-1} \left( \begin{array}{c} 2n \\ s \end{array} \right) (s - 1) \sqrt{q} + \sum_{s = 4}^{2n} \left( \begin{array}{c} 2n \\ s \end{array} \right) \left( 1 + (s - 2) \sqrt{q} \right) \]

\[ = \left\{ \sum_{s = 3}^{2n} \left( \begin{array}{c} 2n \\ s \end{array} \right) s - \sum_{s = 3}^{2n} \left( \begin{array}{c} 2n \\ s \end{array} \right) - \sum_{s = 4}^{2n} \left( \begin{array}{c} 2n \\ s \end{array} \right) \right\} \sqrt{q} + \sum_{s = 4}^{2n} \left( \begin{array}{c} 2n \\ s \end{array} \right) \]

\[ = \left\{ (2n - 3)2^{2n-1} + 2 \right\} \sqrt{q} + \left\{ 2^{2n-1} - 2n^2 + n - 1 \right\}. \]

Hence,

\[ g \geq q + n - \left\{ (2n - 3)2^{2n-1} + 2 \right\} \sqrt{q} - \left\{ 2^{2n-1} - 2n^2 + n - 1 \right\} \]
\[ q = \{(2n - 3)2^{2n-1} + 2\sqrt{q} - (2^{2n-1} - 2n^2 - 1), \]

proving (c). \( \square \)

5.2 Adjacency Properties of Paley Graphs

In this section, we establish, by making use of results from finite fields, the adjacency properties of Paley graphs of order \( q = p^d \) with \( p \) a prime. Throughout this section \( q \equiv 1 \pmod{4} \) is a prime power and \( G_q \) is the Paley graph of order \( q \).

Since \( q \equiv 1 \pmod{4} \), then \(-1\) is a square in \( \mathbb{F}_q \). Consequently, \( \eta(a) = \eta(-a) \) for all \( a \in \mathbb{F}_q \). Figures 4.2.1 and 4.2.2 display the Paley graphs of order 5, 13 and 17 with \( F_5 = \mathbb{Z}_5 \), \( F_{13} = \mathbb{Z}_{13} \) and \( F_{17} = \mathbb{Z}_{17} \), respectively. Figure 5.2.1 below displays the Paley graphs of order 9 and 25 with

\[ F_9 = \mathbb{Z}_3[x]/(x^2+1) \]

\[ = \{0,1,2,x,x+1,x+2,2x,2x+1,2x+2\} \]

and

\[ F_{25} = \mathbb{Z}_5[x]/(x^2+3) \]

\[ = \{0,1,2,3,4,x,x+1,x+2,x+3,x+4,2x,2x+1,2x+2,2x+3,3x,3x+1,3x+2,3x+3,3x+4,4,4x,4x+1,4x+2,4x+3,4x+4,4x+5\} \]

respectively.
$G_9$

$G_{25}$

Figure 5.2.1
It is well-known that the Paley graph $G_q$ is a PC-graph. In fact, $G_q$ is a self-complementary and strongly regular graph with parameters $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$ [see Bollobás (1985)]. So, if $q = 4t + 1$ for some positive integer $t$, then $G_q$ is a strongly regular graph with parameters $(4t + 1, 2t, t - 1, t)$. Consequently, by the Corollary 2.2.7, $G_q \in \mathfrak{F}(1,1,k)$ for every $k \leq t$. In fact, by Lemma 2.2.8, if $q = 4t + 1$ is a prime power, then $G_q$ is the smallest (order) Paley graph in $\mathfrak{F}(1,1,t)$.

As noted in Chapter 4, Exoo and Harary (1980) proved that the Petersen graph is the smallest member of $\mathfrak{F}(1,2,1)$. Exoo (1981) proved that if $G \in \mathfrak{F}(1,2,1) \cap \mathfrak{F}(2,1,1)$, then $\nu(G) \geq 17$ and furthermore, $G_{17} \in \mathfrak{F}(1,2,1) \cap \mathfrak{F}(2,1,1)$. Our next result concerns the classes $\mathfrak{F}(1,n,k)$ and $\mathfrak{F}(n,1,k)$ for any $n \geq 0$ and $k \geq 1$. Computational results show that the given bound on $q$ is best possible for $n = 1$ (all $k$) and for $n = 2$ (most $k$) and fairly close to best possible for $n = 3$. Before stating our result we observe that if $a$ and $b$ are any vertices of $G_q$, then

$$
\eta(a - b) = \begin{cases} 
1, & \text{if } a \text{ is adjacent to } b, \\
0, & \text{if } a = b, \\
-1, & \text{otherwise.}
\end{cases}
$$

Theorem 5.2.1: Let $q \equiv 1(\text{mod } 4)$ be a prime power and $k$ a positive integer. If

$$
q > (n - 2)2^n + 2\sqrt{q} + (n + 2k - 1)2^n - 2n - 1, \quad (5.2.1)
$$

then $G_q \in \mathfrak{F}(1,n,k) \cap \mathfrak{F}(n,1,k)$. 

99
Proof: Since \( G_q \) is a self-complementary graph, it is sufficient to prove that \( G_q \in \mathcal{G}(1,n,k) \). Let \( a \) be a vertex of \( G_q \) and \( B = \{b_1, b_2, \ldots, b_n\} \) be any set of distinct vertices of \( G_q \) so that \( a \notin B \). Then \( n(a/b_1, b_2, \ldots, b_n) \geq k \) if and only if

\[
f = \sum_{\substack{x \in F_q \setminus (a) \cup B \atop x \neq a}} \left(1 + \eta(x - a)\right) \prod_{i=1}^{n} \left(1 - \eta(x - b_i)\right) \geq k2^{n+2}.
\]

To show that \( f \geq k2^{n+1} \), it is clearly sufficient to establish that \( f > (k - 1)2^{n+1} \). Let

\[
g = \sum_{x \in F_q} \left(1 + \eta(x - a)\right) \prod_{i=1}^{n} \left(1 - \eta(x - b_i)\right)
\]

Now by Theorem 5.1.5(a) we have

\[
g = q - ((n - 2)2^n + 2)\sqrt{q} - \{2^n - 2n - 1\}
\]

Consider

\[
g - f = \sum_{x \in (a) \cup B} \left(1 + \eta(x - a)\right) \prod_{i=1}^{n} \left(1 - \eta(x - b_i)\right). \tag{5.2.2}
\]

If \( g - f \neq 0 \), then for some \( y \) the product

\[
\prod_{i=1}^{n} \left(1 + \eta(y - a)\right) \prod_{i=1}^{n} \left(1 - \eta(y - b_i)\right) \neq 0. \tag{5.2.3}
\]

If \( y = a \), then for (5.2.3) to hold we must have \( \eta(a - b_i) = -1 \) for all \( i \). Hence, the term in (5.2.2) with \( x = b_i \) contributes zero to the sum. Therefore, \( g - f = 2^n \), since each factor is 2 and one factor is 1. If \( y = b_j \) for some \( j \), then for (5.2.3) to hold we must have \( \eta(b_j - a) = 1 \). Hence, the term in (5.2.2) with \( x = a \)
contributes zero to the sum. Thus we can write (5.2.2) as:

\[ g - f = \sum_{x \in B} \{1 + \eta(x - a)\} \prod_{i=1}^{n} \{1 - \eta(x - b_i)\} \leq n2^n, \]

since

\[ \{1 + \eta(x - a)\} \prod_{i=1}^{n} \{1 - \eta(x - b_i)\} \leq 2^n, \]

for each x. Note that, each factor is at most 2 and at least one factor is 1. Then we conclude that

\[ g - f \leq n2^n. \]

So

\[ f = g - n2^n \]

\[ \geq \sqrt{q} - \{(n - 2)2^n + 2\sqrt{q} - \{2^n - 2n - 1\} - n2^n \}
= q - \{(n - 2)2^n + 2\sqrt{q} - \{(n + 1)2^n - 2n - 1\}. \]

Now if inequality (5.2.1) holds, then \( f > (k - 1)2^{n+1} \) as required. Since a and B are arbitrary, this completes the proof. \( \Box \)

As corollaries of Theorem 5.2.1 we have:

Corollary 5.2.2: Let \( q \equiv 1(\text{mod}\ 4) \) be a prime power and k a positive integer. Then \( G_q \in \mathbb{Y}(1,1,k) \) for every \( q \geq 4k + 1. \)

Proof: Inequality (5.2.1) shows that q satisfying

\[ q > 4k - 3. \]

Since \( q \equiv 1(\text{mod}\ 4), \) \( q \geq 4k + 1. \)

\( \Box \)
Corollary 5.2.3: Let \( q \equiv 1 \pmod{4} \) be a prime power and \( k \) a positive integer. If \( q > (1 + 2\sqrt{2k})^2 \), then \( G_q \in \mathcal{S}(1,2,k) \cap \mathcal{S}(2,1,k) \). □

Corollary 5.2.4: Let \( q \equiv 1 \pmod{4} \) be a prime power and \( k \) a positive integer. If \( q > (5 + \sqrt{16k + 34})^2 \), then \( G_q \in \mathcal{S}(1,3,k) \cap \mathcal{S}(3,1,k) \). □

Remark 5.2.1: From Lemma 2.2.8 and Corollary 5.2.2 it follows that Theorem 5.2.1 is best possible for \( n = 1 \).

Remark 5.2.2: We have verified, by a computer, that if \( q \equiv 1 \pmod{4} \) is a prime power less than or equal to 1009 and \( k \) is a positive integer with \( q < (1 + 2\sqrt{2k})^2 \), then \( G_q \notin \mathcal{S}(1,2,k) \cap \mathcal{S}(2,1,k) \). We conjecture that this is true for all \( q \). In fact, the computer analysis shows that the bound on \( q \) given in Corollary 5.2.3 is the best possible when \( q \) is a prime number less than or equal to 1009.

Consider Theorem 5.2.1 with \( n = 2 \) and \( q \equiv 1 \pmod{4} \) is a prime power. Let \( A = \{a\} \) and \( B = \{b_1, b_2\} \) which \( ab_1, ab_2 \in E(G_q) \) and \( b_1b_2 \notin E(G_q) \). Then \( g - f = 8 \), since

\[
\begin{align*}
g - f &= (1 - \eta(a - b_1))(1 - \eta(a - b_2)) \\
      &+ (1 + \eta(b_1 - a))(1 - \eta(b_1 - b_2)) \\
      &+ (1 + \eta(b_2 - a))(1 - \eta(b_2 - b_1)).
\end{align*}
\]

From inequality (5.1.7) we have

\[
|g - q - 1| \leq 2\sqrt{q}.
\]

Therefore, \( g \leq q + 2\sqrt{q} + 1 \), and hence, \( f \leq q + 2\sqrt{q} - 7 \). Consequently, \( f < 8k \) for \( q < (-1 + 2\sqrt{2(k + 1)})^2 \). We expect that
this is true for \( q < (1 + 2\sqrt{k})^2 \). So the problem is to look at \((-1 + 2\sqrt{k + 1})^2 \leq q \leq (1 + 2\sqrt{k})^2\).

Table 5.2.1 gives the maximum \( k \) for which \( G_q \in \mathcal{Y}(1,2,k) \cap \mathcal{Y}(2,1,k) \); we give only some of the computational results.

Remark 5.2.3: When \( k = 2 \), Corollary 5.2.4 above asserts that \( G_q \in \mathcal{Y}(1,3,1) \cap \mathcal{Y}(3,1,1) \) for a prime power \( q \geq 149 \). We have verified, by a computer, that \( G_q \in \mathcal{Y}(1,3,1) \cap \mathcal{Y}(3,1,1) \) only for \( q \) a prime power of order at least 89. Thus Corollary 5.2.4 is not sharp. However, computer analysis shows that the bound on \( q \) given in Corollary 5.2.4 is fairly close to best possible.

Table 5.2.2 gives the maximum \( k \) for which \( G_q \in \mathcal{Y}(1,3,k) \cap \mathcal{Y}(3,1,k) \); we give only some of the computational results.

All our computational work has been carried out on a SUN SPARC II work station. Further, in the case of prime powers we utilized the MAPLE software package to create the graphs.
<table>
<thead>
<tr>
<th>Maximum k</th>
<th>Order q</th>
<th>Maximum k</th>
<th>Order q</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>≤ 13</td>
<td>51</td>
<td>457</td>
</tr>
<tr>
<td>1</td>
<td>17</td>
<td>52</td>
<td>461</td>
</tr>
<tr>
<td>2</td>
<td>25, 29</td>
<td>58</td>
<td>509</td>
</tr>
<tr>
<td>3</td>
<td>37, 41</td>
<td>59</td>
<td>521</td>
</tr>
<tr>
<td>4</td>
<td>49, 53</td>
<td>60</td>
<td>529</td>
</tr>
<tr>
<td>5</td>
<td>61</td>
<td>61</td>
<td>541</td>
</tr>
<tr>
<td>7</td>
<td>73</td>
<td>63</td>
<td>557</td>
</tr>
<tr>
<td>8</td>
<td>81, 89</td>
<td>65</td>
<td>569</td>
</tr>
<tr>
<td>9</td>
<td>97</td>
<td>66</td>
<td>577</td>
</tr>
<tr>
<td>10</td>
<td>101</td>
<td>68</td>
<td>593</td>
</tr>
<tr>
<td>11</td>
<td>109, 113</td>
<td>69</td>
<td>601</td>
</tr>
<tr>
<td>12</td>
<td>121, 125</td>
<td>70</td>
<td>613</td>
</tr>
<tr>
<td>14</td>
<td>137</td>
<td>71</td>
<td>617</td>
</tr>
<tr>
<td>15</td>
<td>149</td>
<td>72</td>
<td>625</td>
</tr>
<tr>
<td>16</td>
<td>157</td>
<td>73</td>
<td>641</td>
</tr>
<tr>
<td>18</td>
<td>169, 173</td>
<td>75</td>
<td>653</td>
</tr>
<tr>
<td>19</td>
<td>181</td>
<td>76</td>
<td>661</td>
</tr>
<tr>
<td>20</td>
<td>193</td>
<td>77</td>
<td>673</td>
</tr>
<tr>
<td>21</td>
<td>197</td>
<td>78</td>
<td>677</td>
</tr>
<tr>
<td>24</td>
<td>229</td>
<td>81</td>
<td>701</td>
</tr>
<tr>
<td>25</td>
<td>233</td>
<td>82</td>
<td>709</td>
</tr>
<tr>
<td>26</td>
<td>241</td>
<td>84</td>
<td>729, 733</td>
</tr>
<tr>
<td>28</td>
<td>257</td>
<td>87</td>
<td>757</td>
</tr>
<tr>
<td>29</td>
<td>269</td>
<td>88</td>
<td>761</td>
</tr>
<tr>
<td>30</td>
<td>277</td>
<td>89</td>
<td>769, 773</td>
</tr>
<tr>
<td>31</td>
<td>181</td>
<td>92</td>
<td>797</td>
</tr>
<tr>
<td>32</td>
<td>289, 293</td>
<td>94</td>
<td>809</td>
</tr>
<tr>
<td>34</td>
<td>313</td>
<td>95</td>
<td>821</td>
</tr>
<tr>
<td>35</td>
<td>317</td>
<td>96</td>
<td>829</td>
</tr>
<tr>
<td>37</td>
<td>337</td>
<td>98</td>
<td>841</td>
</tr>
<tr>
<td>39</td>
<td>349, 353</td>
<td>99</td>
<td>853, 857</td>
</tr>
<tr>
<td>40</td>
<td>361</td>
<td>102</td>
<td>877, 881</td>
</tr>
<tr>
<td>41</td>
<td>373</td>
<td>108</td>
<td>929</td>
</tr>
<tr>
<td>43</td>
<td>389</td>
<td>109</td>
<td>937</td>
</tr>
<tr>
<td>44</td>
<td>397</td>
<td>110</td>
<td>941</td>
</tr>
<tr>
<td>45</td>
<td>401</td>
<td>111</td>
<td>953</td>
</tr>
<tr>
<td>46</td>
<td>409</td>
<td>112</td>
<td>961</td>
</tr>
<tr>
<td>47</td>
<td>421</td>
<td>114</td>
<td>977</td>
</tr>
<tr>
<td>49</td>
<td>433</td>
<td>116</td>
<td>997</td>
</tr>
<tr>
<td>50</td>
<td>449</td>
<td>118</td>
<td>1009</td>
</tr>
</tbody>
</table>

Table 5.2.1: Maximum k for which $G_q \in S(1,2,k) \cap S(2,1,k)$.  

104
<table>
<thead>
<tr>
<th>Maximum $k$</th>
<th>Order $q$</th>
<th>Maximum $k$</th>
<th>Order $q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$\leq 73$</td>
<td>22</td>
<td>$541, 557, 569$</td>
</tr>
<tr>
<td>2</td>
<td>$89, 97, 101,$</td>
<td>23</td>
<td>577</td>
</tr>
<tr>
<td></td>
<td>$109, 113, 121,$</td>
<td>24</td>
<td>625</td>
</tr>
<tr>
<td></td>
<td>125</td>
<td>25</td>
<td>$593, 601, 617$</td>
</tr>
<tr>
<td>3</td>
<td>137</td>
<td>26</td>
<td>613</td>
</tr>
<tr>
<td>4</td>
<td>$149, 157, 173,$</td>
<td>27</td>
<td>$641, 653, 661$</td>
</tr>
<tr>
<td></td>
<td>169</td>
<td>28</td>
<td>673</td>
</tr>
<tr>
<td>5</td>
<td>181, 197</td>
<td>29</td>
<td>677</td>
</tr>
<tr>
<td>6</td>
<td>$193, 229, 233$</td>
<td>30</td>
<td>$701, 709$</td>
</tr>
<tr>
<td>8</td>
<td>$241, 257, 269$</td>
<td>32</td>
<td>$729, 733, 769$</td>
</tr>
<tr>
<td>9</td>
<td>$277, 281$</td>
<td>33</td>
<td>$757, 773$</td>
</tr>
<tr>
<td>10</td>
<td>$289, 293, 313,$</td>
<td>34</td>
<td>761</td>
</tr>
<tr>
<td></td>
<td>317</td>
<td>36</td>
<td>$797, 809, 821,$</td>
</tr>
<tr>
<td>12</td>
<td>$337, 349, 353$</td>
<td>38</td>
<td>841</td>
</tr>
<tr>
<td></td>
<td>361</td>
<td>39</td>
<td>$829, 853, 857$</td>
</tr>
<tr>
<td>14</td>
<td>$373, 389$</td>
<td>40</td>
<td>877, 881</td>
</tr>
<tr>
<td>15</td>
<td>401</td>
<td>42</td>
<td>$929, 937$</td>
</tr>
<tr>
<td>16</td>
<td>$409, 421, 433$</td>
<td>43</td>
<td>953</td>
</tr>
<tr>
<td>17</td>
<td>449</td>
<td>44</td>
<td>$941, 961$</td>
</tr>
<tr>
<td>18</td>
<td>$457, 461$</td>
<td>45</td>
<td>977</td>
</tr>
<tr>
<td>20</td>
<td>$521, 529$</td>
<td>46</td>
<td>$997, 1009$</td>
</tr>
<tr>
<td>21</td>
<td>509</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 5.2.2: Maximum $k$ for which $G_q \in \mathcal{G}(1,3,k) \cap \mathcal{G}(3,1,k)$. 
For the class $Y(m,n,k)$ we have the following result.

**Theorem 5.2.5:** Let $q \equiv 1 \pmod{4}$ be a prime power and $k$ a positive integer. If

$$q > \{(t-3)2^{t-1} + 2\sqrt{q} + (t+2k-1)2^{t-1} - 1, \quad (5.2.4)$$

then $G_q \in Y(m,n,k)$ for all $m, n$ with $m + n \leq t$.

**Proof:** It clearly suffices to establish the result for $m + n = t$.

Let $A$ and $B$ be disjoint subsets of $V(G_q)$ with $|A| = m$ and $|B| = n$.

Then $n(A \cup B) \geq k$ if and only if

$$f = \sum_{x \in F_q} \prod_{a \in A} \{1 + \eta(x-a)\} \prod_{b \in B} \{1 - \eta(x-b)\} > (k-1)2^t.$$

Let

$$g = \sum_{x \in F_q} \prod_{a \in A} \{1 + \eta(x-a)\} \prod_{b \in B} \{1 - \eta(x-b)\}.$$

Now by Theorem 5.1.5(b) we have

$$g \geq q - \{(t-3)2^{t-1} + 2\sqrt{q} - \{2^{t-1} - 1\}.$$

Consider

$$g - f = \sum_{x \in A \cup B} \prod_{a \in A} \{1 + \eta(x-a)\} \prod_{b \in B} \{1 - \eta(x-b)\}$$

$$\leq t2^{t-1},$$

since each factor is at most 2 and one factor is 1, so each of
these terms is at most $2^{t-1}$. Therefore,

$$f \geq g - t2^{t-1}$$

$$\geq q - \{(t - 3)2^{t-1} + 2\sqrt{q} - \{(t + 1)2^{t-1} - 1\}.$$

Now if (5.2.4) holds, then $f > (k - 1)2^t$ as required. Since $A$ and $B$ are arbitrary, this completes the proof. \hfill \Box

For the case $m = n$ we have the following sharper result.

**Theorem 5.2.6:** Let $q \equiv 1 \pmod{4}$ be a prime power and $k$ a positive integer. If

$$q > \{(2n - 3)2^{2n-1} + 2\sqrt{q} + (n + 2k - 1)2^{2n-1} - 2n^2 - 1,$$

(5.2.5)

then $G_q \in \mathcal{Y}(n, n, k)$.

**Proof:** Let $A$ and $B$ be disjoint subsets of $V(G_q)$ so that $|A| = |B| = n$. Then $n(A//B) \geq k$ if and only if

$$f = \sum_{x \in F_q} \prod_{a \in A} (1 + \eta(x - a)) \prod_{b \in B} (1 - \eta(x - b)) > (k - 1)2^{2n}.$$  

Let

$$g = \sum_{x \in F_q} \prod_{a \in A} (1 + \eta(x - a)) \prod_{b \in B} (1 - \eta(x - b)).$$

Now Theorem 5.1.5(c) implies

$$g \geq q - \{(2n - 3)2^{2n-1} + 2\sqrt{q} - \{2^{2n-1} - 2n^2 - 1\}.$$
Consider
\[ g - f = \sum_{x \in A \cup B} \prod_{i=1}^{n} (1 + \eta(x - a_i))(1 - \eta(x - b_i)). \] (5.2.6)

where \( A = \{a_1, a_2, \ldots, a_n\} \) and \( B = \{b_1, b_2, \ldots, b_n\} \).

If \( g - f \neq 0 \), then for some \( y \) the product
\[ \prod_{i=1}^{n} (1 + \eta(y - a_i))(1 - \eta(y - b_i)) \neq 0. \] (5.2.7)

Without any loss of generality, suppose \( y = a_j \) for some \( j \). Then for (5.2.7) to hold, we must have \( \eta(a_j - b_i) = -1 \) for all \( i \). Hence, the term in (5.2.6) with \( x = b_i \) contributes zero to the sum. Thus we can write (5.2.6) as:
\[ g - f = \sum_{x \in A} \prod_{i=1}^{n} (1 + \eta(x - a_i))(1 - \eta(x - b_i)) \leq n 2^{2n-1}, \]

since
\[ \prod_{i=1}^{n} (1 + \eta(x - a_i))(1 - \eta(x - b_i)) \leq 2^{2n-1}, \]

for each \( x \). Note that each factor is at most 2 and at least one factor is 1. Hence,
\[ f \geq g - n 2^{2n-1} \geq q - ((2n - 3)2^{2n-1} + 2)\sqrt{q} - ((n + 1)2^{2n-1} - 2n^2 - 1). \]

Now if (5.2.5) holds, then \( f > (k - 1)2^n \) as required. Since \( A \) and \( B \) are arbitrary, this completes the proof of the theorem. \( \square \)
For the particular cases \( k = 1 \) and \( n = 2 \), we have the following corollaries of Theorem 5.2.6:

**Corollary 5.2.7:** If \( q \equiv 1 \pmod{4} \) is a prime power with \( q > ((2n - 3)2^{2n-1} + 4)^2 \), then \( G_q \in \mathcal{F}(n,n,1) \).

**Corollary 5.2.8:** If \( q \equiv 1 \pmod{4} \) is a prime power with \( q > (5 + 2\sqrt{4k + 6})^2 \), then \( G_q \in \mathcal{F}(2,2,k) \).

**Corollary 5.2.9:** If \( q \equiv 1 \pmod{4} \) is a prime power, \( n \geq 4 \) and \( q > ((2n - 3)2^{2n-1} + 3)^2 \), then \( G_q \in \mathcal{F}(n,n,1) \).

**Remark 5.2.4:** As we noted in Chapter 4; Blass, Harary and Exoo (1981) proved that \( G_p \in \mathcal{F}(n,n,1) \) for a prime \( p \equiv 1 \pmod{4} \) and \( p > n^22^{4n} \). For the particular case \( n = 2 \) that result asserts that \( G_p \in \mathcal{F}(2,2,1) \) for prime \( p \geq 1033 \). When \( k = 1 \) Corollary 5.2.8 above asserts that \( G_q \in \mathcal{F}(2,2,1) \) for all prime powers \( q \geq 137 \). We have verified, using a computer, that \( G_q \in \mathcal{F}(2,2,1) \) only for \( q \) a prime power of order at least 61. Thus Corollary 5.2.8 is not sharp. However, computer analysis shows that the bound on \( q \) given in Corollary 5.2.8 is fairly close to best possible.

Table 5.2.3 gives the maximum \( k \) for which \( G_q \in \mathcal{F}(2,2,k) \); we give only some of the computational results. Note that this table extends the results in Table 4.3.1 to include prime power.
<table>
<thead>
<tr>
<th>Maximum k</th>
<th>Order q</th>
<th>Maximum k</th>
<th>Order q</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>≤ 53</td>
<td>23</td>
<td>577</td>
</tr>
<tr>
<td>1</td>
<td>61, 73, 125</td>
<td>24</td>
<td>593</td>
</tr>
<tr>
<td>2</td>
<td>81, 89, 97, 101, 109, 113, 121</td>
<td>25</td>
<td>601, 617</td>
</tr>
<tr>
<td>3</td>
<td>137</td>
<td>26</td>
<td>613</td>
</tr>
<tr>
<td>4</td>
<td>149, 157, 169, 173</td>
<td>27</td>
<td>625, 641, 653</td>
</tr>
<tr>
<td>5</td>
<td>181</td>
<td>28</td>
<td>661</td>
</tr>
<tr>
<td>6</td>
<td>193, 197, 233</td>
<td>29</td>
<td>673</td>
</tr>
<tr>
<td>7</td>
<td>229</td>
<td>30</td>
<td>677</td>
</tr>
<tr>
<td>8</td>
<td>241, 257</td>
<td>31</td>
<td>701</td>
</tr>
<tr>
<td>9</td>
<td>269, 277, 281</td>
<td>32</td>
<td>709</td>
</tr>
<tr>
<td>10</td>
<td>289, 293, 313, 317</td>
<td>33</td>
<td>733, 769</td>
</tr>
<tr>
<td>11</td>
<td>337</td>
<td>34</td>
<td>729, 773</td>
</tr>
<tr>
<td>12</td>
<td>349, 353, 361</td>
<td>35</td>
<td>757, 761</td>
</tr>
<tr>
<td>14</td>
<td>373</td>
<td>36</td>
<td>809</td>
</tr>
<tr>
<td>15</td>
<td>389, 397, 401</td>
<td>37</td>
<td>797, 821</td>
</tr>
<tr>
<td>16</td>
<td>409, 421, 433</td>
<td>38</td>
<td>829</td>
</tr>
<tr>
<td>17</td>
<td>449</td>
<td>39</td>
<td>841, 857, 877</td>
</tr>
<tr>
<td>18</td>
<td>457, 461</td>
<td>40</td>
<td>853, 881</td>
</tr>
<tr>
<td>20</td>
<td>521, 529</td>
<td>41</td>
<td>937</td>
</tr>
<tr>
<td>21</td>
<td>509</td>
<td>42</td>
<td>929, 953</td>
</tr>
<tr>
<td>22</td>
<td>541, 557, 569</td>
<td>43</td>
<td>941, 961</td>
</tr>
<tr>
<td></td>
<td></td>
<td>44</td>
<td>977</td>
</tr>
<tr>
<td></td>
<td></td>
<td>45</td>
<td>997</td>
</tr>
<tr>
<td></td>
<td></td>
<td>46</td>
<td>1009</td>
</tr>
</tbody>
</table>

Table 5.2.3: Maximum k for which $G_q \in \mathcal{Y}(2, 2, k)$. 
Remark 5.2.5: Table 5.2.3 shows that the Paley graph of order 61 is the smallest Paley graph in the class $\mathcal{P}(2,2,1)$. In fact, to date the smallest graph in $\mathcal{P}(2,2,1)$ constructed is the Paley graph on 61 vertices. Figure 5.2.2 below displays the Paley graph of order 61. We show only all the edges for vertex 0, the remaining edges are obtained by rotation.

Figure 5.2.2
5.3 Property $P(n,k)$

Recall that a graph $G$ is said to have property $P(n)$ if for any two sets $A$ and $B$ of vertices of $G$ with $A \cap B = \emptyset$ and $|A \cup B| = n$, there is a vertex $u \in A \cup B$ which is joined to every vertex of $A$ and not joined to any vertex of $B$. The cycle $C_v$ of length $v$ has property $P(1)$ for every $v \geq 4$. The Paley graph $G_q$ of order $9$, see Figure 5.2.1, has property $P(2)$. Observe that if $G$ has property $P(n)$, then $\tilde{G}$ also has property $P(n)$. This property has been studied by Bollobás (1985) and Caccetta, Erdős and Vijayan (1985). Moreover, given an integer $v$, Caccetta, Erdős and Vijayan (1985) considered the problem of determining the largest integer $f(v)$ for which there exists a graph on $v$ vertices having property $P(f(v))$. They established, using probabilistic methods, that

$$\log v - \frac{(2 + o(1)) \log \log v}{\log 2} < f(v) < \frac{\log v}{\log 2}.$$ 

In the same paper, a class of graphs having property $P(2)$ was given.

Bollobás (1985) showed that if $n \geq 2$ and $q \equiv 1(\text{mod } 4)$ is a prime power with

$$q > \left((n - 2)2^{n-1} + 1\right)\sqrt{q} + n2^{n-1},$$

then $G_q$ has property $P(n)$. In this section, we improve this bound slightly to:

$$q > \left((n - 3)2^{n-1} + 2\right)\sqrt{q} + (n + 1)2^{n-1} - 1.$$ 

Note that if a graph $G$ has property $P(n)$, then $G$ also has property $P(s,t,1)$ where $s + t \leq n$ for all $s \geq 0$, $t \geq 0$. In fact, $P(2n)$ implies $P(n,n,1)$, which implies $P(n)$, which implies $P(m)$ for
all $1 \leq m \leq n$.

**Theorem 5.3.1:** Let $q \equiv 1 (\text{mod} 4)$ be a prime power. If

$$q > ((n - 3)2^{n-1} + 2)\sqrt{q} + ((n + 1)2^{n-1} - 1), \quad (5.3.1)$$

then $G_q$ has property $P(n)$. In particular, for $n \geq 3$, $G_q$ has property $P(n)$ whenever $q > ((n - 3)2^{n-1} + 5)^2$.

**Proof:** Let $A$ and $B$ be disjoint subsets of $V(G_q)$ with $|A \cup B| = n$. Then $n(A/B) \geq 1$ if and only if

$$f = \sum_{x \in F} \prod_{a \in A} (1 + \eta(x - a)) \prod_{b \in B} (1 - \eta(x - b)) > 0.$$ 

Now using the method of proof of Theorem 5.2.5 we get $f > 0$ when

$$q > ((n - 3)2^{n-1} + 2)\sqrt{q} + ((n + 1)2^{n-1} - 1).$$

Hence, the result. It is easily checked that for $n \geq 3$, $q > ((n - 3)2^{n-1} + 5)^2$ implies $f > 0$. \[ \Box \]

Observe that for $n = 1, 2$ and 3, (5.3.1) yields $q \geq 5$, $q \geq 9$ and $q \geq 29$, respectively. In fact, $G_5$, $G_9$ and $G_{29}$ are the smallest members of $G_q$ having property $P(1)$, $P(2)$ and $P(3)$, respectively. This is clearly so for the case of $G_5$ and also $G_9$ [as $G_5$ does not have property $P(2)$]. The case of $G_{29}$ is established as follows.

Since, as noted in the previous section, $G_q \in S(1,2,1)$ only if $q \geq 17$, we need only look at $q = 17$ and 25. Making use of the methodology of Frucht (1970) we can denote $G_{17}$ by $I_{17}(1,2,4,8)$, which means that $V(G_{17}) = \{0,1,\ldots,16\}$ and vertex 1 is adjacent
to the vertices: \( 1 \pm 1, 1 \pm 2, 1 \pm 4 \) and \( 1 \pm 8 \pmod{17} \) [see also Figure 4.2.2]. Since \( N(0,1,2/-) = \phi \), \( G_{17} \) does not have property \( P(3) \). Consider now \( q = 25 \). We can denote \( G_{25} \) by \( \mathbb{Z}_5[x]/(x^2 + 3) \langle 1.2, x + 1, x + 4, 2x + 2, 2x + 3 \rangle \) which means that \( V(G_{25}) = \{ a_0 + a_1 x : a_1 \in \mathbb{Z}_5 \} \) and vertex \( y \) is adjacent to the vertices: \( y \pm 1, y \pm 2, y \pm (x + 1), y \pm (x + 4), y \pm (2x + 2) \) and \( y \pm (2x + 3) \pmod{x^2 + 3} \) [see also Figure 5.2.1]. Now since \( N(0,2,x + 1/-) = \phi \), \( G_{25} \) does not have property \( P(3) \). Therefore, \( G_{29} \) is the smallest member of \( G_q \) having property \( P(3) \). Thus Theorem 5.3.1 is sharp for \( n = 1, 2 \) and \( 3 \).

Recall that, we can generalize property \( P(n) \) as follows. A graph \( G \) is said to have property \( P(n,k) \) if for any two sets \( A \) and \( B \) of vertices of \( G \) with \( A \cap B = \phi \) and \( |A \cup B| = n \), there are at least \( k \) vertices not in \( A \cup B \) which are joined to every vertex of \( A \) and not joined to any vertex of \( B \). Observe that \( P(n,k) \) implies \( P(n - 1,k - 1) \) for any \( 1 \leq k \). Using the method of proof of theorems 5.2.5 and 5.3.1 we can establish the following result.

**Theorem 5.3.2:** Let \( q \equiv 1(\text{mod} \ 4) \) be a prime power and \( k \) a positive integer. If

\[
q > \left( (n - 3)^2 + 2 \sqrt{q} + (n + 2k - 1)^2 \right) - 1,
\]

then \( G_q \) has property \( P(n,k) \).

### 5.4 "Generalized" Paley Graphs

In previous sections quadratic residues played an important role in constructing Paley graphs. By using higher order residues on finite fields we can generate other classes of graphs. More
specifically, let \( q \equiv 1 \pmod{3} \). Define the graph \( G^{(3)}_q \) as follows. The vertices of \( G^{(3)}_q \) are the elements of the finite field \( F_q \). Two vertices \( a \) and \( b \) are adjacent if and only if \( a - b = y^3 \) for some \( y \in F_q \). Since \( q \equiv 1 \pmod{3} \), \(-1\) is a cubic in \( F_q \). Consequently, \( G^{(3)}_q \) is well-defined. Figure 5.4.1 below displays the graph \( G^{(3)}_{13} \). Note that the graph is 4-regular and is different to the Paley graph \( G_{13} \) which is 6-regular.

![Graph G^{(3)}_{13}](image)

Figure 5.4.1

What can we say about the adjacency properties of \( G^{(3)}_{13} \)? Table 5.4.1 presents computational results which establish the smallest graph \( G^{(3)}_q \) in \( S(2,2,k) \) for small \( k \). We give only some of the computational results.
<table>
<thead>
<tr>
<th>Maximum k</th>
<th>Order q</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>≤ 139 and 163</td>
</tr>
<tr>
<td>1</td>
<td>151, 157, 223</td>
</tr>
<tr>
<td>2</td>
<td>169, 181, 193, 199, 229</td>
</tr>
<tr>
<td>3</td>
<td>211, 241, 271, 361</td>
</tr>
<tr>
<td>4</td>
<td>256, 277, 289, 313</td>
</tr>
<tr>
<td>5</td>
<td>283, 307, 331</td>
</tr>
<tr>
<td>6</td>
<td>337, 343, 349, 373, 379</td>
</tr>
<tr>
<td>7</td>
<td>367, 397, 409</td>
</tr>
<tr>
<td>8</td>
<td>433, 439, 463, 523</td>
</tr>
<tr>
<td>9</td>
<td>421, 457, 487, 529</td>
</tr>
<tr>
<td>11</td>
<td>499</td>
</tr>
<tr>
<td>12</td>
<td>547, 571, 577</td>
</tr>
<tr>
<td>13</td>
<td>541, 607</td>
</tr>
<tr>
<td>14</td>
<td>601, 613, 619, 631, 634</td>
</tr>
<tr>
<td>15</td>
<td>661</td>
</tr>
<tr>
<td>16</td>
<td>673, 625</td>
</tr>
<tr>
<td>17</td>
<td>691, 709, 769</td>
</tr>
<tr>
<td>18</td>
<td>727, 733, 757</td>
</tr>
<tr>
<td>19</td>
<td>751</td>
</tr>
<tr>
<td>20</td>
<td>739, 787, 811, 829</td>
</tr>
<tr>
<td>22</td>
<td>823</td>
</tr>
<tr>
<td>23</td>
<td>859, 883</td>
</tr>
<tr>
<td>24</td>
<td>853, 877, 907</td>
</tr>
<tr>
<td>25</td>
<td>919, 937</td>
</tr>
<tr>
<td>27</td>
<td>967, 991</td>
</tr>
<tr>
<td>28</td>
<td>997, 1009</td>
</tr>
</tbody>
</table>

Table 5.4.1: Maximum k for which $G_q^{(3)} \in \mathcal{G}(2,2,k)$.
Remark 5.4.1: For $q \equiv 1 \pmod{3}$ a prime power, there is a character $\chi$ of order 3. The values of $\chi$ are in the set $\{1, \omega, \omega^2\}$ where $\omega = e^{\frac{2\pi i}{3}}$, and $\chi(-1) = 1$. Consequently, $\chi(-a) = \chi(a)$ for any $a \in \mathbb{F}_q$. Observe that $\chi^2$ is also a character of order 3.

Now we turn our attention to quadruple residues. Let $q = 1 \pmod{8}$. Define the graph $G^{(4)}_q$ as follows. The vertices of $G^{(4)}_q$ are the elements of the finite field $\mathbb{F}_q$. Two vertices $a$ and $b$ are adjacent if and only if $a - b = y^4$ for some $y \in \mathbb{F}_q$. Since $q = 1 \pmod{8}$, $-1$ is a quadruple in $\mathbb{F}_q$. Consequently, $G^{(4)}_q$ is well-defined. Figure 5.4.2 below shows the graph $G^{(4)}_{17}$. Note that the graph is 4-regular and is different to the Paley graph $G_{17}$, which is 8-regular.

![Figure 5.4.2](image-url)
What can we say about the adjacency properties of $G^{(4)}_{13}$?

Table 5.4.2 presents computational results which establish the smallest graph $G^{(4)}_q$ in $\mathcal{G}(2,2,k)$ for small $k$. We give only some of the computational results.

<table>
<thead>
<tr>
<th>Maximum k</th>
<th>Order $q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$\leq 313$</td>
</tr>
<tr>
<td>1</td>
<td>353</td>
</tr>
<tr>
<td>2</td>
<td>337, 361, 457</td>
</tr>
<tr>
<td>3</td>
<td>625</td>
</tr>
<tr>
<td>4</td>
<td>401, 409, 433, 449, 521, 529</td>
</tr>
<tr>
<td>5</td>
<td>577</td>
</tr>
<tr>
<td>6</td>
<td>569, 593, 617, 641, 673</td>
</tr>
<tr>
<td>7</td>
<td>601</td>
</tr>
<tr>
<td>8</td>
<td>761, 769</td>
</tr>
<tr>
<td>9</td>
<td>729</td>
</tr>
<tr>
<td>10</td>
<td>809, 841, 857, 881, 961</td>
</tr>
<tr>
<td>12</td>
<td>929, 937</td>
</tr>
<tr>
<td>13</td>
<td>977</td>
</tr>
<tr>
<td>14</td>
<td>953, 1009</td>
</tr>
</tbody>
</table>

Table 5.4.2: Maximum k for which $G^{(4)}_q \in \mathcal{G}(2,2,k)$.  

118
Remark 5.4.2: (1) For $q = 1 \pmod{8}$ a prime power, there is a character $\chi$ of order 4. The values of $\chi$ are in the set $\{1, -1, i, -i\}$ where $i = \sqrt{-1}$, and $\chi(-1) = 1$. Consequently, $\chi(-a) = \chi(a)$ for any $a \in \mathbb{F}_q$. Observe that $\chi^3$ is also a character of order 4 and $\chi^2$ is a character of order 2 or the quadratic character.

In general, we can choose $q$ and $d$ such that $q$ is a prime power and

$$d > 1 \text{ odd or } \frac{(q - 1)}{d} \text{ even.}$$

Define the "generalized" Paley graph, $G_{q}^{(d)}$ as follows. The vertices of $G_{q}^{(d)}$ are the element of the finite field $\mathbb{F}_q$. Two vertices $a$ and $b$ are adjacent if and only if $a - b = y^d$ for some $y \in \mathbb{F}_q$. Since $q$ is a prime power and $d > 1$ is odd or $\frac{(q - 1)}{d}$ is even, $-1 = y^d$ for some $y \in \mathbb{F}_q$. Consequently, $G_{q}^{(d)}$ is well-defined. Clearly $G_{q}^{(2)}$ is the Paley graph.

Remark 5.4.3: For $q$ a prime power and $d > 1$ odd or $\frac{(q - 1)}{d}$ even, there is a character $\chi$ of order $d$. The values of $\chi$ are the $d^{th}$ roots of unity and $\chi(-1) = 1$. Consequently, $\chi(-a) = \chi(a)$ for any $a \in \mathbb{F}_q$.

Remark 5.4.4: We conjecture that for any $m$, $n$ and $k$, all sufficiently large "generalized" Paley graphs satisfy property $P(m,n,k)$. 

119
CHAPTER 6
PALEY TOURNAMENTS

In this chapter, our graphs are directed. For our purposes, all digraphs are finite and strict. Consider a round robin tournament $T_q$ on $q$ players $1,2,\ldots,q$ in which there are no draws. It is very well-known that such a tournament can be represented by a directed graph in which the vertices represent the players. If Player $i$ defeats Player $j$, then the graph contains the arc $(i,j)$, and we say that vertex $i$ dominates vertex $j$. Further, we say a set of vertices $A$ dominates a set of vertices $B$ if every vertex of $A$ dominates every vertex of $B$. For convenience we refer to the graph of the tournament as $T_q$.

6.1 Preliminaries

Recall that a tournament $T_q$ is said to have property $Q(n,k)$ if every subset of $n$ vertices of $T_q$ is dominated by at least $k$ other vertices. For example, the tournament $T_7$ in the Figure 6.1.1 has property $Q(2,1)$. 

120
An interesting problem is that of determining the smallest integer \( f(n,k) \) such that there exists a tournament \( T_q \) of order \( q \) which has property \( Q(n,k) \) whenever \( q \geq f(n,k) \). This problem was posed to Erdös in 1962 by Schütte for the particular case \( k = 1 \).

Using the probabilistic method, Erdös (1963) proved that for sufficiently large \( n \)

\[
2^{n+1} - 1 \leq f(n,1) \leq n^2 2^n (\log 2 + \varepsilon) \quad (6.1.1)
\]

for any \( \varepsilon > 0 \). E. Szekeres and G. Szekeres (1965) improved the lower bound to

\[
f(n,1) \geq (n + 2)2^{n-1} - 1. \quad (6.1.2)
\]

As noted in the introduction Graham and Spencer (1971) defined the following class of tournaments. Let \( p = 3 \text{mod} 4 \) be a prime. The directed graph \( D_p \) is defined as follows. The vertices of \( D_p \) are \( 0,1,\ldots,p-1 \) and \( D_p \) contains the arc \((i,j)\) if and only if \( 1 - j \) is a quadratic residue modulo \( p \). The graph \( D_p \) is sometimes referred to as the Paley tournament. Figure 6.1.1 displays the Paley tournament of order 7 whilst Figure 6.1.2 displays the Paley tournament of order 11. It is not too difficult to establish that \( D_{11} \) has property \( Q(2,2) \).
Graham and Spencer (1981) proved, using results from number theory, that $D_p$ has property $Q(n,1)$ whenever $p > n^2 2^{2n-2}$. Further, they observed that $D_7$ and $D_{19}$ are the smallest Paley tournaments having property $Q(2,1)$ and $Q(3,1)$, respectively. They noted that $D_{67}$ may be the smallest Paley tournament having property $Q(4,1)$. This is indeed the case and is a consequence of our work. Figure 6.1.3 displays the Paley tournament of order 19. We show only all the arcs of vertex 0, the remaining arcs are obtained by rotation; for completeness we give the adjacency matrix of $D_{19}$. 

Figure 6.1.2
$D_{19}$

Figure 6.1.3

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>13</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>14</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>16</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

The adjacency matrix of $D_{19}$
Bollobás (1985) extended the results of Graham and Spencer to prime powers. More specifically, if \( q \equiv 3 \text{ (mod 4)} \) is a prime power, the Paley tournament \( D_q \) is defined as follows. The vertices of \( D_q \) are the elements of the finite field \( \mathbb{F}_q \). Vertex \( a \) joins to vertex \( b \) by an arc if and only if \( a - b \) is a quadratic residue in \( \mathbb{F}_q \). Bollobás noted that \( D_q \) has property \( Q(n,1) \) whenever

\[
q > \{(n - 2)2^{n-1} + 1\sqrt{q} + n2^{n-1}.
\]

In Section 6.3, we improve this bound to

\[
q > \{(n - 3)2^{n-1} + 2\sqrt{q} + 2^n - 1.
\]

In addition, we establish a lower bound on \( q \) so that \( D_q \) has property \( Q(n,k) \).

Let \( \eta \) be the quadratic (residue) character, defined in Chapter 5, of the finite field \( \mathbb{F}_q \). Observe that if \( a \) and \( b \) are vertices of \( D_q \), \( q \equiv 3 \text{ (mod 4)} \) a prime power, then

\[
\eta(a - b) = \begin{cases} 
1, & \text{if } a \text{ dominates } b, \\
0, & \text{if } a = b, \\
-1, & \text{otherwise}.
\end{cases}
\]

Further, \( \eta(-a) = -\eta(a) \) for any \( a \in \mathbb{F}_q \) since \( q \equiv 3 \text{ (mod 4)} \).

6.2 Results

In this section, we prove that for a prime power \( q \equiv 3 \text{ (mod 4)} \), all sufficiently large Paley tournaments \( D_q \) satisfy properties \( Q(n,k) \) and \( Q(m,n,k) \).

Our first result concerns Paley tournaments having property \( Q(n,k) \).
Theorem 6.2.1: Let $q \equiv 3 \pmod{4}$ be a prime power and $k$ a positive integer. If

$$q > \{(n - 3)2^{n-1} + 2\sqrt{2} + k2^n - 1, \quad (6.2.1)$$

then $D_q$ has property $Q(n,k)$.

Proof: Let $A$ be any subset of $n$ vertices of $D_q$. Then there are at least $k$ other vertices each of which dominates $A$ if and only if

$$h = \sum_{x \in F_q} \prod_{a \in A, x \notin A} \{1 + \eta(x - a)\} > (k - 1)2^n.$$

Let

$$g = \sum_{x \in F_q} \prod_{a \in A} \{1 + \eta(x - a)\}.$$

Lemma 5.1.5(b) with $B$ empty, yields

$$g \geq q - \{(n - 3)2^{n-1} + 2\sqrt{q} - \{2^{n-1} - 1\}.$$

Now

$$g - h = \sum_{x \in A} \prod_{i=1}^{n} \{1 + \eta(x - a_i)\}$$

where $A = \{a_1, a_2, \ldots, a_n\}$. If $g - h \neq 0$, then for some $a_k$ the product

$$\prod_{i=1}^{n} \{1 + \eta(a_k - a_i)\} \neq 0. \quad (6.2.2)$$

For (6.2.2) to hold we must have $\eta(a_k - a_i) \neq -1$ for all $i$. This
means that for \( i \neq k \), \( \eta(a_k - a_i) = 1 \). Hence, \( a_k \) dominates all other vertices in \( A \). Therefore, \( a_k \) is unique and \( g - h = 2^{n-1} \).

Then since \( g - h \) could be 0 we conclude that

\[
g - h \leq 2^{n-1}.
\]

So

\[
h \geq g - 2^{n-1} \geq q - ((n - 3)2^{n-1} + 2)\sqrt{q} - (2^n - 1).
\]

Now if inequality (6.2.1) holds, then \( h > (k - 1)2^n \) as required.

Since \( A \) is arbitrary, this completes the proof. \( \Box \)

Some immediate corollaries of Theorem 6.2.1 are the following.

**Corollary 6.2.2:** If \( q = 4t + 3 \) is a prime power, then \( D_q \) has property \( Q(2,k) \) for every \( t \geq k \). \( \Box \)

**Corollary 6.2.3:** If \( q = 3(\text{mod} \ 4) \) is a prime power and \( q > (1 + 2\sqrt{2k})^2 \), then \( D_q \) has property \( Q(3,k) \). \( \Box \)

**Corollary 6.2.4:** If \( q = 3(\text{mod} \ 4) \) is a prime power and \( q > (5 + 2\sqrt{4k + 6})^2 \), then \( D_q \) has property \( Q(4,k) \). \( \Box \)

**Corollary 6.2.5:** If \( q = 3(\text{mod} \ 4) \) is a prime power, \( n \geq 5 \) and \( q > ((n - 3)2^{n-1} + 3)^2 \), then \( D_q \) has property \( Q(n,1) \). \( \Box \)
Remark 6.2.1: Consider Theorem 6.2.1 with $n = 2$, $q = 4t + 3$ a prime power and let $A = \{a_1, a_2\}$. Then there are at least $k$ other vertices each of which dominates $A$ if and only if $h \geq 4k$.

Expanding the $g$ in the proof of Theorem 6.2.1, we get

$$g = \sum_{x \in \mathbb{F}_q} (1 + \eta(x - a_1))(1 + \eta(x - a_2))$$

$$= \sum_{x \in \mathbb{F}_q} 1 + \sum_{x \in \mathbb{F}_q} \{\eta(x - a_1) + \eta(x - a_2)\}$$

$$+ \sum_{x \in \mathbb{F}_q} \eta((x - a_1)(x - a_2))$$

$$= q - 1. \quad \text{[by (5.1.2) and Corollary 5.1.3]}$$

Consider

$$g - h = \{1 + \eta(a_1 - a_2)\}{1 + \eta(a_2 - a_1)} = 2.$$ 

Now if $t < k$, then $h < 4k$. Thus $D_q$ does not have property $Q(2,k)$. Therefore, the bound on $q$ given in Corollary 6.2.2 is the best possible.

Remark 6.2.2: We have verified, using a computer, that if $q \equiv 3 \pmod{4}$ is a prime power less than or equal to 1031 and $k$ is a positive integer with $q \leq (1 + 2\sqrt{2k})^2$, then $D_q$ does not have property $Q(3,k)$. We conjecture that this is true for any $q$ and $k$. Thus the bound on $q$ given in Corollary 6.2.3 is the best possible. Consider Theorem 6.2.1 with $n = 3$ and $q \equiv 3 \pmod{4}$ a prime power. Let $A = \{a_1, a_2, a_3\}$ so that $a_1$ dominates $a_2$ and $a_3$. Then $g - h = 4$, since

$$g - h = \{1 + \eta(a_1 - a_2)\}{1 + \eta(a_1 - a_3)}$$
+ \{1 + \eta(a_2 - a_1)\} \{1 + \eta(a_2 - a_3)\}
+ \{1 + \eta(a_3 - a_1)\} \{1 + \eta(a_3 - a_2)\}.

Expanding the \( g \) in the proof of Theorem 6.2.1, we get

\[
g = \sum_{x \in F_q} 1 + \sum_{x \in F_q} \eta(x - a_1) + \eta(x - a_2) + \eta(x - a_3) \\
+ \sum_{x \in F_q} \left\{ \eta((x - a_1)(x - a_2)) + \eta((x - a_1)(x - a_3)) \\
+ \eta((x - a_2)(x - a_3)) \right\} + \sum_{x \in F_q} \eta((x - a_1)(x - a_2)(x - a_3))
\]

\[= q - 3 + \sum_{x \in F_q} \eta((x - a_1)(x - a_2)(x - a_3)).\]  

[by (5.1.2) and Corollary 5.1.3]

Thus

\[
|g - q + 3| = \left| \sum_{x \in F_q} \eta((x - a_1)(x - a_2)(x - a_3)) \right| \\
\leq 2\sqrt{q}. \quad [\text{by Theorem 5.1.1}]
\]

Hence, \( g \leq q + 2\sqrt{q} - 3 \). Consequently, \( h < 8k \) for \( q < (-1 + 2\sqrt{2}(k + 1))^2 \). Thus \( D_q \) does not have property \( Q(3, k) \) for \( q < (-1 + 2\sqrt{2}(k + 1))^2 \). We expect that this is true for all \( q \leq (1 + 2\sqrt{2}k)^2 \). So the problem is to look at \( (-1 + 2\sqrt{2}(k + 1))^2 \leq q \leq (1 + 2\sqrt{2}k)^2 \).

Table 6.2.1 gives the maximum \( k \) for which \( D_q \) has property \( Q(3, k) \); we give only some of the computational results.
<table>
<thead>
<tr>
<th>Maximum k</th>
<th>Order q</th>
<th>Maximum k</th>
<th>Order q</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>≤ 11</td>
<td>55</td>
<td>487, 491</td>
</tr>
<tr>
<td>1</td>
<td>19, 23</td>
<td>56</td>
<td>499</td>
</tr>
<tr>
<td>2</td>
<td>27, 31</td>
<td>57</td>
<td>503</td>
</tr>
<tr>
<td>3</td>
<td>43</td>
<td>59</td>
<td>523</td>
</tr>
<tr>
<td>4</td>
<td>47</td>
<td>62</td>
<td>547</td>
</tr>
<tr>
<td>5</td>
<td>59</td>
<td>64</td>
<td>563</td>
</tr>
<tr>
<td>6</td>
<td>67, 71</td>
<td>65</td>
<td>571</td>
</tr>
<tr>
<td>7</td>
<td>79</td>
<td>67</td>
<td>587</td>
</tr>
<tr>
<td>8</td>
<td>83</td>
<td>68</td>
<td>599</td>
</tr>
<tr>
<td>10</td>
<td>103, 107</td>
<td>69</td>
<td>607</td>
</tr>
<tr>
<td>13</td>
<td>127, 131</td>
<td>71</td>
<td>619</td>
</tr>
<tr>
<td>14</td>
<td>139</td>
<td>72</td>
<td>631</td>
</tr>
<tr>
<td>15</td>
<td>151</td>
<td>74</td>
<td>643, 647</td>
</tr>
<tr>
<td>17</td>
<td>163, 167</td>
<td>76</td>
<td>659</td>
</tr>
<tr>
<td>19</td>
<td>179</td>
<td>78</td>
<td>683</td>
</tr>
<tr>
<td>20</td>
<td>191</td>
<td>79</td>
<td>691</td>
</tr>
<tr>
<td>21</td>
<td>199</td>
<td>83</td>
<td>719</td>
</tr>
<tr>
<td>22</td>
<td>211</td>
<td>84</td>
<td>727</td>
</tr>
<tr>
<td>24</td>
<td>223, 227</td>
<td>85</td>
<td>739</td>
</tr>
<tr>
<td>26</td>
<td>239, 243</td>
<td>86</td>
<td>743</td>
</tr>
<tr>
<td>27</td>
<td>251</td>
<td>87</td>
<td>751</td>
</tr>
<tr>
<td>28</td>
<td>263</td>
<td>91</td>
<td>787</td>
</tr>
<tr>
<td>29</td>
<td>271</td>
<td>94</td>
<td>811</td>
</tr>
<tr>
<td>31</td>
<td>283</td>
<td>95</td>
<td>823</td>
</tr>
<tr>
<td>32</td>
<td>307, 311</td>
<td>96</td>
<td>827</td>
</tr>
<tr>
<td>36</td>
<td>331</td>
<td>97</td>
<td>839</td>
</tr>
<tr>
<td>38</td>
<td>343, 347</td>
<td>100</td>
<td>859, 863</td>
</tr>
<tr>
<td>40</td>
<td>359</td>
<td>103</td>
<td>883</td>
</tr>
<tr>
<td>41</td>
<td>367</td>
<td>105</td>
<td>907</td>
</tr>
<tr>
<td>42</td>
<td>379</td>
<td>106</td>
<td>911</td>
</tr>
<tr>
<td>43</td>
<td>383</td>
<td>107</td>
<td>919</td>
</tr>
<tr>
<td>47</td>
<td>419</td>
<td>110</td>
<td>947</td>
</tr>
<tr>
<td>48</td>
<td>431</td>
<td>113</td>
<td>967, 971</td>
</tr>
<tr>
<td>49</td>
<td>439</td>
<td>115</td>
<td>983</td>
</tr>
<tr>
<td>50</td>
<td>443</td>
<td>116</td>
<td>991</td>
</tr>
<tr>
<td>52</td>
<td>463</td>
<td>119</td>
<td>1019</td>
</tr>
<tr>
<td>53</td>
<td>467</td>
<td>120</td>
<td>1031</td>
</tr>
</tbody>
</table>

Table 6.2.1: Maximum k for which $D_q$ has property $Q(3,k)$. 
Remark 6.2.3: We have verified, using a computer, that \( D_{67} \) is the smallest Paley tournament having property \( Q(4,1) \). Thus the bound in Corollary 6.2.3 is not sharp. However, our computer analysis reveals that \( D_{103} \) does not have property \( Q(4,1) \) whilst, \( D_{107} \) and \( D_{127} \) do and thus the bound of 131 given in Corollary 6.2.4 is fairly close to best possible.

Table 6.2.2 gives the maximum \( k \) for which \( D_q \) has property \( Q(4,k) \); we give only some of the computational results.
<table>
<thead>
<tr>
<th>Maximum k</th>
<th>Order q</th>
<th>Maximum k</th>
<th>Order q</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>≤ 59 and 103</td>
<td>22</td>
<td>563</td>
</tr>
<tr>
<td>1</td>
<td>67, 71, 79, 83</td>
<td>23</td>
<td>547, 571</td>
</tr>
<tr>
<td>2</td>
<td>107, 131</td>
<td>24</td>
<td>587</td>
</tr>
<tr>
<td>3</td>
<td>127</td>
<td>25</td>
<td>607</td>
</tr>
<tr>
<td>4</td>
<td>139, 151, 163</td>
<td>26</td>
<td>599, 619, 631, 647</td>
</tr>
<tr>
<td>5</td>
<td>167, 179, 199</td>
<td></td>
<td>647</td>
</tr>
<tr>
<td>6</td>
<td>191, 211</td>
<td>28</td>
<td>643, 659</td>
</tr>
<tr>
<td>7</td>
<td>223, 227</td>
<td>29</td>
<td>683</td>
</tr>
<tr>
<td>8</td>
<td>239, 243, 251, 263, 283</td>
<td>30</td>
<td>691, 727</td>
</tr>
<tr>
<td>9</td>
<td>271</td>
<td>33</td>
<td>743</td>
</tr>
<tr>
<td>10</td>
<td>311</td>
<td>34</td>
<td>751, 787</td>
</tr>
<tr>
<td>11</td>
<td>307</td>
<td>36</td>
<td>811, 839</td>
</tr>
<tr>
<td>12</td>
<td>331, 343</td>
<td>37</td>
<td>823</td>
</tr>
<tr>
<td>13</td>
<td>347, 359</td>
<td>38</td>
<td>827</td>
</tr>
<tr>
<td>14</td>
<td>367, 379</td>
<td>39</td>
<td>859, 863</td>
</tr>
<tr>
<td>15</td>
<td>383, 431</td>
<td>40</td>
<td>883</td>
</tr>
<tr>
<td>16</td>
<td>419</td>
<td>41</td>
<td>907, 911</td>
</tr>
<tr>
<td>17</td>
<td>439</td>
<td>43</td>
<td>919, 947, 967</td>
</tr>
<tr>
<td>18</td>
<td>443, 463, 467</td>
<td>45</td>
<td>971, 983, 1019</td>
</tr>
<tr>
<td>19</td>
<td>479, 487</td>
<td>46</td>
<td>991</td>
</tr>
<tr>
<td>20</td>
<td>491, 499, 503</td>
<td>47</td>
<td>1031</td>
</tr>
<tr>
<td>21</td>
<td>523</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 6.2.2: Maximum k for which $D_q$ has property $Q(4,k)$.  

131
Recall that we can generalize the property $Q(n,k)$ as follows. We say a tournament $T_q$ of order $q$ has property $Q(m,n,k)$ if for any set of $m + n$ distinct vertices of $T_q$ there exist at least $k$ other vertices each of which dominates the first $m$ vertices and is dominated by each of the latter $n$ vertices. The Paley tournament $D_7$ (see Figure 6.1.1) has property $Q(1,1,1)$. It is not too difficult to establish that the Paley tournament $D_{11}$ (see Figure 6.1.2) has property $Q(1,1,2)$. In general, we have the following result.

Theorem 6.2.6: Let $q = 3 \mod 4$ be a prime power and $k$ a positive integer. If

$$q > \{(t - 3)2^{t-1} + 2\sqrt{q} + (t + 2k - 1)2^{t-1} - 1, \quad (6.2.3)$$

then $D_q$ has property $Q(m,n,k)$, where $m + n = t$.

Proof: It clearly suffices to establish the result for $m + n = t$. Let $A$ and $B$ be disjoint subsets of vertices of $D_q$ with $|A| = m$ and $|B| = n$. Then there are at least $k$ other vertices, each of which dominates every vertex of $A$ but is dominated by every vertex of $B$ if any only if

$$h = \sum_{x \in F_q, x \notin A \cup B} \prod_{a \in A} \{1 + \eta(x - a)\} \prod_{b \in B} \{1 - \eta(x - b)\} > (k - 1)2^t.$$

Let

$$g = \sum_{x \in F_q} \prod_{a \in A} \{1 + \eta(x - a)\} \prod_{b \in B} \{1 - \eta(x - b)\}.$$
Using Lemma 5.1.5(b) we have

\[ g \geq q - \{(t - 3)^{t-1} + 2\sqrt{q} - (2^{t-1} - 1). \]

Now

\[ g - h = \sum_{x \in A \cup B} \prod_{a \in A} (1 + \eta(x - a)) \prod_{b \in B} (1 - \eta(x - b)). \]

\[ \leq t2^{t-1}, \]

since, in each product, each factor is at most 2 and one factor is 1, so each term is at most 2^{t-1}. Therefore,

\[ h \geq g - t2^{t-1}. \]

\[ \geq q - \{(t - 3)2^{t-1} + 2\sqrt{q} - (t + 1)2^{t-1} - 1. \]

Now if inequality (6.2.3) holds, then \( h > (k - 1)2^t \) as required.

Since \( A \) and \( B \) are arbitrary, this completes the proof. \( \Box \)

For \( m = n \), we have the following sharper result.

**Theorem 6.2.7:** Let \( q \equiv 3(\text{mod } 4) \) be a prime power and \( k \) a positive integer. If

\[ q > \{(2n - 3)2^{2n-1} + 2\sqrt{q} + (n + 2k)2^{2n-1} - 2n^2 - 1, \]

then \( D_q \) has property \( Q(n,n,k) \).

**Proof:** Let \( A \) and \( B \) be disjoint subsets of vertices of \( D_q \) with \( |A| = |B| = n \). Then there are at least \( k \) other vertices each of which dominates \( A \) and is dominated by \( B \) if and only if
\[ h = \sum_{x \in F_q} \prod_{a \in A} (1 + \eta(x - a))^k \prod_{b \in B} (1 - \eta(x - b)) \geq (k - 1)2^{kn}. \]

Let
\[ g = \sum_{x \in F_q} \prod_{a \in A} (1 + \eta(x - a))^k \prod_{b \in B} (1 - \eta(x - b)). \]

Using Lemma 5.1.5(c) we have
\[ g = q - ((2^{n-1})2^{2n-1} + 2)\sqrt{q} - (2^{2n-1} - 2^{n-1} - 1). \]

Consider
\[ g - h = \sum_{x \in A \cup B} \prod_{i=1}^{n} (1 + \eta(x - a_i))(1 - \eta(x - b_i)) \tag{6.2.5} \]

where \( A = \{ a_1, a_2, \ldots, a_n \} \) and \( B = \{ b_1, b_2, \ldots, b_n \} \).

If \( g - h \neq 0 \), then for some \( x \) the product
\[ \prod_{i=1}^{n} (1 + \eta(x - a_i))(1 - \eta(x - b_i)) \neq 0. \tag{6.2.6} \]

Without any loss of generality suppose \( x = a_k \). For (6.2.6) to hold we must have \( \eta(a_k - a_i) = -1 \) and \( \eta(a_k - b_i) \neq 1 \) for all \( i \).

This means that \( \eta(a_k - a_i) = 1 \) for \( i \neq k \) and \( \eta(a_k - b_i) = -1 \) for all \( i \). Hence, the term in (6.2.5) with \( x = a_i \) for \( i \neq k \) contributes zero to the sum. Then we can write (6.2.5) as:
\[ g - h = \sum_{x \in \{ a_k \} \cup B} \prod_{i=1}^{n} (1 + \eta(x - a_i))(1 - \eta(x - b_i)) \leq (n + 1)2^{2n-1}, \]
since, in each product, each factor is at most 2 and at least one factor is 1. Hence,

\[ h \geq g - (n + 1)2^{2n-1} \]

\[ \geq q - ((2n - 3)2^{2n-1} + 2)\sqrt{q} - ((n + 2)2^{2n-1} - 2n^2 - 1). \]

Now if inequality (6.2.4) holds, then \( h > (k - 1)2^n \) as required. Since \( A \) and \( B \) are arbitrary, this completes the proof of the theorem. \( \Box \)

6.3 Property \( R(n,k) \)

A tournament \( T_q \) is said to have property \( R(n,k) \) if for any sets \( A \) and \( B \) of vertices of \( T_q \) with \( A \cap B = \emptyset \) and \( |A \cup B| = n \), there are at least \( k \) vertices not in \( A \cup B \) each of which dominates every vertex of \( A \) but is dominated by every vertex of \( B \). The Paley tournament \( D_7 \) (see Figure 6.1.1) has property \( R(2,1) \). It is not too difficult to establish that the Paley tournament \( D_{11} \) (see Figure 6.1.2) has property \( R(2,2) \). Note that if a tournament \( T_q \) has property \( R(n,k) \), then \( T_q \) has property \( Q(n,k) \) and also has property \( Q(s,t,k) \) for any \( s \) and \( t \) with \( s + t \leq n \).

Using the method of proof of the Theorem 6.2.6, we can establish the following result.

Theorem 6.3.1: Let \( q \equiv 3(\text{mod } 4) \) be a prime power and \( k \) a positive integer. If

\[ q > ((n - 3)2^{n-1} + 2)\sqrt{q} + (n + 2k - 1)2^{n-1} - 1, \]

then \( D_q \) has property \( R(n,k) \). \( \Box \)
6.4 Paley Digraphs

Our discussion on directed graphs has so far focussed on tournaments. It is natural to extend the properties $Q(n,k)$ and $Q(m,n,k)$ to general digraphs. We now consider this.

In previous sections quadratic residues played an important role in constructing Paley tournaments. By using higher order residues on finite fields we can generate other classes of digraphs. More specifically, let $q \equiv 5 \pmod{8}$ be a prime power. Define a digraph $D^{(4)}_q$ as follows. The vertices of $D^{(4)}_q$ are the elements of the finite field $\mathbb{F}_q$. Vertex $a$ joins to vertex $b$ by an arc if and only if $a - b$ is a quadruple in $\mathbb{F}_q$. Since $q \equiv 5 \pmod{8}$ is prime power, there is a character $\chi$ of order 4 and $\chi(-1) = -1$. Consequently, $\chi(-a) = -\chi(a)$ for any $a \in \mathbb{F}_q$. Therefore, $D^{(4)}_q$ is well-defined. However, $D^{(4)}_q$ is not a tournament. Figure 6.4.1 below displays the digraph $D^{(4)}_{13}$.

![Figure 6.4.1](image_url)
Remark 6.4.1: For \( q = 5(\text{mod} \ 8) \) a prime power, there is a character \( \chi \) of order 4. The values of \( \chi \) are in the set \( \{1, -1, 1, -1\} \) where \( i = \sqrt{-1} \). Observe that \( \chi^3 \) is also a character of order 4 but \( \chi^2 \) is a character of order 2 or a quadratic character.

Remark 6.4.2: We expect that for sufficiently large \( q \), the digraph \( D^{(4)}_q \) has the properties \( Q(n,k) \) and \( Q(m,n,k) \) for any \( m, n \) and \( k \).

In general, let \( q \) be a prime power and \( d \) satisfy

\[
d > 1 \text{ even and } \frac{q - 1}{d} \text{ odd. (6.4.1)}
\]

Given \( Y^{(d)} = \{ y^d : y \in F_q^* \} \) and define the Paley digraph \( D^{(d)}_q \) as follows. The vertices of \( D^{(d)}_q \) are the elements of the finite field \( F_q \). Vertex \( a \) joins to vertex \( b \) by an arc if and only if \( a - b \in Y^{(d)} \). Since \( d \) satisfies condition (6.4.1), there is a character \( \chi \) of order \( d \) and \( \chi(-1) = -1 \). Consequently, \( \chi(-a) = -\chi(a) \) for any \( a \in F_q \). Therefore, \( D^{(d)}_q \) is well-defined. Clearly for \( q = 3(\text{mod} \ 4) \) a prime power \( D^{(2)}_q \) is the Paley tournament.

Remark 6.4.3: (1) For \( q \) a prime power and \( d \) satisfying condition (6.4.1), there is a character \( \chi \) of order \( d \) of the finite field \( F_q \). The values of \( \chi \) are the \( d^{\text{th}} \) roots of unity.

(2) For any given \( m, n \) and \( k \), we expect that all sufficiently large Paley digraphs \( D^{(d)}_q \) satisfy the properties \( Q(n,k) \) and \( Q(m,n,k) \).
CHAPTER 7

STRONG ADJACENCY PROPERTY

Recall that a graph $G$ is said to have property $P^*(m,n,k)$ if for any set of $m + n$ distinct vertices of $G$ there are exactly $k$ other vertices, each of which is adjacent to the first $m$ vertices of the set but not adjacent to any of the latter $n$ vertices. The class of graphs having property $P^*(m,n,k)$ is denoted by $\mathcal{G}^*(m,n,k)$. The case $n = 0$ is, of course, a generalization of the property in the Friendship Theorem. A necessary and sufficient condition for $G \in \mathcal{G}^*(2,0,k)$ was proved by Bose and Shrikhande (1970), [see Theorem 7.1.2]. For $m = 3$, $\mathcal{G}^*(n,m,k) = \{K_{m+k}\}$, [see Theorem 7.1.3]. Observe that if $G \in \mathcal{G}^*(m,n,k)$, then $\overline{G} \in \mathcal{G}^*(n,m,k)$. The cycle $C_5$ of length 5 is a member of $\mathcal{G}^*(1,1,1)$. The well-known Petersen graph is a member of $\mathcal{G}^*(1,1,2)$. Also, if $G$ has property $P^*(m,n,k)$ then it has property $P(m,n,k)$.

In Section 7.2, we show that, for $m = n = 1$, graphs with the property $P^*(1,1,k)$ are the so-called strongly regular graphs with parameters $\left(\frac{(k + t)^2}{t} + 1, k + t, t - 1, t\right)$ for some positive integer $t$. In particular, we show the existence of such graphs. In Section 7.3, we show that for $m \geq 1$, $n \geq 1$ and $m + n \geq 3$, there is no graph having property $P^*(m,n,k)$, for any positive integer $k$.

Our proof of the above mentioned results make use of some results on strongly regular graphs. We state these in Section 7.1.
Recall that a graph $G$ is said to have property $P^*(n,k)$ if for any two sets $A$ and $B$ of vertices of $G$ with $A \cap B = \emptyset$ and $|A \cup B| = n$, there are exactly $k$ vertices not in $A \cup B$ which are joined to every vertex of $A$ but not joined to any vertex of $B$. The class of graphs having property $P^*(n,k)$ is denoted by $\mathcal{S}^*(n,k)$. For any positive integers $n$ and $k$, we prove, in Section 7.4, that

- (a) for $n > 1$, $\mathcal{S}^*(n,k) = \emptyset$; and
- (b) for $n = 1$, $G \in \mathcal{S}^*(1,k)$ if and only if $G$ is a $k$-regular graph on $2k + 1$ vertices.

7.1 Preliminaries

The class $\mathcal{S}^*(m,n,k)$ has been studied when one of $m$ or $n$ is zero. Trivially, the only members of $\mathcal{S}^*(1,0,k)$ and $\mathcal{S}^*(0,1,k)$ are the $k$-regular and the $(\nu - k - 1)$-regular graphs, respectively. Erdős, Rényi and Sós (1966) proved that a graph $G \in \mathcal{S}^*(2,0,1)$ if and only if $G$ consists of $\frac{1}{2}(\nu-1)$ triangles joined at one common vertex [that is, $G \cong K_1 \lor (\frac{\nu-1}{2} K_2)$]. This result is the well-known Friendship Theorem. For other values of $m$, $n$ and $k$ there is a connection with the class of the so-called strongly regular graphs, first introduced by Bose (1963).

Recall that, an $r$-regular graph of order $\nu$ is called strongly regular with parameters $(\nu, r, \lambda, \mu)$ if $G$ has the property that any two adjacent vertices have exactly $\lambda$ common neighbours and any two non-adjacent vertices have exactly $\mu$ common neighbours. The following well-known result [see Hughes and Piper (1988), pp 119-124 and Cameron and van Lint (1991), p 37] provides a necessary condition for a graph to be strongly regular.
Theorem 7.1.1: Let $G$ be a strongly regular graph with parameters $(\nu, r, \lambda, \mu)$. Then the following holds.

(i) $r(r - \lambda - 1) = \mu(\nu - r - 1)$.

(ii) $\tilde{G}$ is a strongly regular graph with parameters $(\nu, \nu - r - 1, \nu - 2r + \mu - 2, \nu - 2r + \lambda)$.

(iii) The adjacency matrix $A$ of $G$ has three distinct real eigenvalues $r, s_1$ and $s_2$, which $s_1$ and $s_2$ are the zeros of the polynomial $f(x) = x^2 - (\lambda - \mu)x - (r - \mu)$, and both are integral unless $G$ has parameters $(4\mu + 1, 2\mu, \mu - 1, \mu)$.

(iv) The eigenvalues $r, s_1$ and $s_2$ have multiplicities $1, m_1$, and $m_2$, respectively, which satisfy $m_1 + m_2 = \nu - 1$, $s_1 m_1 + s_2 m_2 = -r$ and

$$m_1, m_2 = \frac{1}{2} \left( (\nu - 1) \pm \frac{(\nu - 1)(\mu - \lambda) - 2r}{\sqrt{(\mu - \lambda)^2 + 4(r - \mu)}} \right)$$

and these must clearly be nonnegative integers.

Bose and Shrikhande (1970) proved the following result.

Theorem 7.1.2: For $k \geq 2$, $G \in \mathcal{G}^*(2,0,k)$ if and only if $G$ is a strongly regular graph with parameters $(\frac{r(r - 1)}{k} + 1, r, k, k)$ for some positive integer $r$ and there exists a positive integer $s$, such that $r = k + s^2$ and $s$ divides $k$.

Some constructions of graphs in the class $\mathcal{G}^*(2,0,k)$ are also given in the above-mentioned paper. The only other known result is the following due to Carstens and Kruse (1977) and Sudolsky'
Theorem 7.1.3: For \( n \geq 3 \) and \( k \geq 1 \), \( \mathcal{G}^*(n,0,k) = \{K_{m+k}\} \)

7.2 The Class \( \mathcal{G}^*(1,1,k) \)

In this section, we establish that the members of \( \mathcal{G}^*(1,1,k) \) are strongly regular graphs with parameters \( \left( \frac{(k + t)^2}{t} + 1, k + t, t - 1, t \right) \). Further, we present some constructions to demonstrate the existence of graphs in this class. We make use of a particular strongly regular graph, the so-called pseudo-cyclic (PC) graph, with parameters \( (4k + 1, 2k, k - 1, k) \) where \( k \) is a positive integer. We note that, the complement of a PC-graph is again a PC-graph with the same parameters as the original graph. Observe that, the simplest PC-graph is the 5-cycle which gives rise to the parameters \( (5,2,0,1) \).

We now present our main result of this section.

Theorem 7.2.1: \( G \in \mathcal{G}^*(1,1,k) \) if and only if \( G \) is a strongly regular graph with parameters \( \left( \frac{(k + t)^2}{t} + 1, k + t, t - 1, t \right) \) for some positive integer \( t \).

Proof: Let \( G \in \mathcal{G}^*(1,1,k) \) and \( u, v \) any two adjacent vertices of \( G \). Then \( n(u/v) = n(v/u) = k \), and so \( \delta(G) \geq k + 1 \). Consequently, any pair of non-adjacent vertices have at least one common neighbour. Hence, \( G \) is connected. Now suppose that \( n(u,v/-) = t - 1 \) for some positive integer \( t \). Then \( n(u/-) = k + t = n(v/-) \). Hence, \( G \) is \( (k + t) \)-regular. Therefore, for any two non-adjacent vertices \( u, w \) of \( G \), \( n(u,w/-) = t \). Consider a vertex \( x \) of \( G \), we
have

\[ n(u/x) = k, \quad \text{for any } u \in N(x/-) \]

and

\[ n(x/v) = k, \quad \text{for any } v \in N(-/x). \]

Thus

\[ \sum_{u \in N(x/-)} n(u/x) + \sum_{v \in N(-/x)} n(x/v) = k(v - 1). \]

Now, in the left hand side of the above equation, the first sum counts the edges between the sets \( N(x/-) \) and \( N(-/x) \) whilst the second sum counts the non-edges between the sets \( N(x/-) \) and \( N(-/x) \). Therefore,

\[ \sum_{u \in N(x/-)} n(u/x) + \sum_{v \in N(-/x)} n(x/v) = n(x/-)n(-/x), \]

and so

\[ k(v - 1) = n(x/-)n(-/x) = n(x/-)(v - n(x/-) - 1). \]

Consequently,

\[ \nu = 1 + \frac{n(x/-)^2}{n(x/-) - k} \]

\[ = 1 + \frac{(k + t)^2}{t}, \quad \text{(7.2.1)} \]

since \( n(x/-) = k + t \). Therefore, \( G \) is a strongly regular graph with the required parameters.

The converse follows directly from the definition of strongly regular graphs. This completes the proof of the theorem.  

\[ \Box \]
Lemma 7.2.2: For a fixed k, there are only finitely many graphs in the class $S^*(1,1,k)$.

Proof: It follows from the parameters of strongly regular graphs in the class $S^*(1,1,k)$. □

We now present a number of corollaries to Theorem 7.2.1.

Corollary 7.2.3: Let $G \in S^*(1,1,k)$. Then $\nu(G) \geq 4k + 1$, with equality possible if and only if $G$ is a PC-graph with parameters $(4k + 1,2k,k - 1,k)$.

Proof: The right hand side of equation (7.2.1) achieves its minimum value of $4k + 1$ when $k = t$. Hence, $\nu(G) \geq 4k + 1$. Further, if $k \neq t$ then $\nu(G) > 4k + 1$, thus establishing the corollary. □

Corollary 7.2.4: Let $G \in S^*(1,1,k)$ be a non PC-graph. Then $k = l(l - 1)$ for some integer $l > 1$.

Proof: This corollary is easily established by the application of Theorem 7.1.1(iii). □

Observe that if $k$ is a prime number or 1, the right hand side of equation (7.2.1) is integral only if $t = 1$, $k$ or $k^2$. For these cases the graphs in the class $S^*(1,1,k)$ are strongly regular graphs with parameters $((k + 1)^2 + 1,k + 1,0,1)$, $(4k + 1,2k,k - 1,k)$ and $((k + 1)^2 + 1,k(k + 1),k^2 - 1,k^2)$, respectively. Strongly regular graphs with parameters $((k + 1)^2 + 1,k + 1,0,1)$
exist if and only if strongly regular graphs with parameters 
\(((k + 1)^2 + 1, k(k + 1), k^2 - 1, k^2)\) exist [by Theorem 7.1.1(ii)].
If \(G\) is a strongly regular graph with \(\lambda = 0\) and \(\mu = 1\), then \(G\) has
girth 5. So a strongly regular graph with parameters
\(((k + 1)^2 + 1, k + 1, 0, 1)\) is a Moore graph. Further, from a result
of Hoffman and Singleton [see Biggs (1974), Chapter 23], it follows
that strongly regular graphs with parameters
\(((k + 1)^2 + 1, k + 1, 0, 1)\) exist only if \(k + 1 = 2, 3, 7\) or
(possibly) 57. Only three strongly regular graphs with \(\mu = 1\) are
known [see Brouwer, Cohen and Neumaier (1989), p 39]: the cycle of
length 5 with parameters \((5, 2, 0, 1)\); the Petersen graph with
parameters \((10, 3, 0, 1)\); and the Hoffman-Singleton graph with
parameters \((50, 7, 0, 1)\). The existence of a strongly regular graph
with parameters \((3250, 57, 0, 1)\) remains an open question. Using
this fact, the following corollaries to Theorem 7.2.1 are directly
obtained.

**Corollary 7.2.5:** \(\mathcal{S}^*(1, 1, 1) = \{C_5\}.\)

**Corollary 7.2.6:** \(G \in \mathcal{S}^*(1, 1, 2)\) if and only if \(G\) is the Petersen
graph, or the complement of the Petersen graph or a PC-graph with
parameters \((9, 4, 1, 2)\).

**Corollary 7.2.7:** If \(k\) is an odd prime, then \(\mathcal{S}^*(1, 1, k) = \{G | G\) is a
PC-graph with parameters \((4k + 1, 2k, k - 1, k)\}.

Figure 7.2.1 shows the PC-graph with parameters \((9, 4, 1, 2)\).
Remark 7.2.1. Cameron and Van Lint (1991) [see pp 136-137] constructed a class of strongly regular graphs with parameters \((243, 22, 1, 2)\) from ternary Golay code. These graphs along with their complements are members of \(S^\ast(1, 1, 20)\).

Remark 7.2.2. A strongly regular graph with parameters \(\left(\frac{(k + 2)^2 - 1}{2}, k + 2, 1, 2\right)\) exists only if \(k + 2 = 2, 4, 14, 22, 112\) or 994 [see Cameron and van Lint (1991), p 138]. For \(k + 2 = 2\) or 4 the graph is a triangle or a PC-graph of order 9 respectively; an example with \(k + 2 = 22\) is that mentioned in Remark 7.2.1. For \(k + 2 = 14\), the strongly regular graph with parameters \((99, 14, 1, 2)\) does not exist [see Makhnév (1988)]. The other cases are undecided.

Remark 7.2.3. The Hoffman-Singleton graph, \(H_{50}\), with parameters \((50, 7, 0, 1)\) and its complement are members of \(S^\ast(1, 1, 6)\). By using theorems 7.1.1 and 7.2.1, Remark 7.2.2 and results from the book of Weisfeller (1976), sections T and U; we get \(S^\ast(1, 1, 6) = \{H_{50}, \bar{H}_{50}\}\), PC-graph with parameters \((25, 12, 5, 6)\), strongly regular graphs with parameters \((26, 10, 3, 4)\) and \((26, 15, 8, 9)\), since there
are no strongly regular graphs with parameters (28,9,2,3), (28,18,11,12) [by Theorem 7.1.1(iv) and (ii)], (33,8,1,2) and (33,24,17,18) [by Remark 7.2.2 and Theorem 7.1.1(ii)].

Remark 7.2.4. The well-known Paley graphs [see Paley (1933)] provide further examples of graphs in the class $\mathcal{G}^*(1,1,k)$. Let $q = 4k + 1$ be a prime power. As already mentioned in this thesis, the Paley graph $G_q$ of order $q$ is strongly regular with parameters $(4k + 1, 2k, k - 1, k)$. Thus $G_q \in \mathcal{G}^*(1,1,k)$. Note that the graphs in Figure 7.2.1 is the Paley graph of order 9.

Remark 7.2.5. There are other known members of $\mathcal{G}^*(1,1,k)$ that are not PC-graphs. One construction is through partial geometries [Bose (1963)]. The graph of a partial geometry is obtained by taking the vertices of the graph to correspond to the points of the partial geometry, and taking two vertices to be adjacent if and only if they are incident with the same line of the geometry. A partial geometry with parameters $(\ell, \alpha, t)$ [each point is incident to $\ell$ lines, no two points are incident to more than one line, each line is incident to $\alpha$ points and if a point $P$ is not incident to a line $L$, then there are $t$ lines through $P$ intersecting $L$ ] gives rise to a strongly regular graph with parameters

$$\frac{\alpha[(\ell - 1)(\alpha - 1) + t]}{t}, \ell(\alpha - 1), \ell t - 1, \ell t$$

provided $\alpha = \ell + t$.

These graphs along with their complements are members of $\mathcal{G}^*(1,1,\ell(\ell - 1))$ for some integer $\ell > 1$. 

146
Remark 7.2.6. There exist graphs which can be obtained from symmetric conference matrix (defined in Section 2.2) and are not PC-graphs [see Cameron and van Lint (1991), pp 39-40]. Such graphs are strongly regular with parameters \((4s^2 + 4s + 2, s(2s + 1), s^2 - 1, s^2)\) which exist whenever \(2s + 1\) is a prime power. Thus these graphs along with their complements are members of \(\mathcal{G}^*(1,1,s(s + 1))\) for some integer \(s \geq 1\).

Remark 7.2.7. In the following table we list all of the possible parameters of strongly regular graphs in the class \(\mathcal{G}^*(1,1,k)\) with \(\nu \leq 100\), except their complements as we know that, a strongly regular graph \(G\) exists if and only if a strongly regular graph \(\bar{G}\) exists and \(G \in \mathcal{G}^*(1,1,k)\) if and only if \(\bar{G} \in \mathcal{G}^*(1,1,k)\).
<table>
<thead>
<tr>
<th>$\nu$</th>
<th>$r$</th>
<th>$\lambda$</th>
<th>$\mu$</th>
<th>Realizable</th>
<th>$\Psi^*(1,1,k)$</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>yes</td>
<td>$\Psi^*(1,1,1)$</td>
<td>PC-graph</td>
</tr>
<tr>
<td>9</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>yes</td>
<td>$\Psi^*(1,1,2)$</td>
<td>PC-graph</td>
</tr>
<tr>
<td>10</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>yes</td>
<td>$\Psi^*(1,1,2)$</td>
<td>Petersen graph</td>
</tr>
<tr>
<td>13</td>
<td>6</td>
<td>2</td>
<td>3</td>
<td>yes</td>
<td>$\Psi^*(1,1,3)$</td>
<td>PC-graph</td>
</tr>
<tr>
<td>17</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>no</td>
<td>$\Psi^*(1,1,4)$</td>
<td>$\lambda = 0 \land \mu = 1$</td>
</tr>
<tr>
<td>17</td>
<td>8</td>
<td>3</td>
<td>4</td>
<td>yes</td>
<td>$\Psi^*(1,1,6)$</td>
<td>PC-graph</td>
</tr>
<tr>
<td>19</td>
<td>6</td>
<td>1</td>
<td>2</td>
<td>no</td>
<td></td>
<td>Remark 7.2.2</td>
</tr>
<tr>
<td>21</td>
<td>10</td>
<td>4</td>
<td>5</td>
<td>no</td>
<td></td>
<td>Lemma 2.2.5</td>
</tr>
<tr>
<td>25</td>
<td>12</td>
<td>5</td>
<td>6</td>
<td>yes</td>
<td>$\Psi^*(1,1,6)$</td>
<td>PC-graph</td>
</tr>
<tr>
<td>26</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>no</td>
<td>$\Psi^*(1,1,6)$</td>
<td>$\lambda = 0 \land \mu = 1$</td>
</tr>
<tr>
<td>26</td>
<td>10</td>
<td>3</td>
<td>4</td>
<td>yes</td>
<td>$\Psi^*(1,1,6)$</td>
<td>Remark 7.2.3</td>
</tr>
<tr>
<td>28</td>
<td>9</td>
<td>2</td>
<td>3</td>
<td>no</td>
<td></td>
<td>Theorem 7.1.1(iv)</td>
</tr>
<tr>
<td>29</td>
<td>14</td>
<td>6</td>
<td>7</td>
<td>yes</td>
<td>$\Psi^*(1,1,7)$</td>
<td>PC-graph</td>
</tr>
<tr>
<td>33</td>
<td>8</td>
<td>1</td>
<td>2</td>
<td>no</td>
<td></td>
<td>Remark 7.2.2</td>
</tr>
<tr>
<td>33</td>
<td>16</td>
<td>7</td>
<td>8</td>
<td>no</td>
<td></td>
<td>Lemma 2.2.5</td>
</tr>
<tr>
<td>37</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>no</td>
<td>$\Psi^*(1,1,9)$</td>
<td>PC-graph</td>
</tr>
<tr>
<td>37</td>
<td>12</td>
<td>3</td>
<td>4</td>
<td>no</td>
<td></td>
<td>Theorem 7.1.1(iii)</td>
</tr>
<tr>
<td>41</td>
<td>20</td>
<td>9</td>
<td>10</td>
<td>yes</td>
<td>$\Psi^*(1,1,9)$</td>
<td>PC-graph</td>
</tr>
<tr>
<td>45</td>
<td>22</td>
<td>10</td>
<td>11</td>
<td>yes</td>
<td>$\Psi^*(1,1,10)$</td>
<td>PC-graph</td>
</tr>
<tr>
<td>46</td>
<td>15</td>
<td>4</td>
<td>5</td>
<td>no</td>
<td></td>
<td>Mathon (1978)</td>
</tr>
<tr>
<td>49</td>
<td>12</td>
<td>2</td>
<td>3</td>
<td>no</td>
<td></td>
<td>Theorem 7.1.1(iii)</td>
</tr>
<tr>
<td>49</td>
<td>24</td>
<td>11</td>
<td>12</td>
<td>yes</td>
<td>$\Psi^*(1,1,12)$</td>
<td>PC-graph</td>
</tr>
<tr>
<td>50</td>
<td>7</td>
<td>0</td>
<td>1</td>
<td>yes</td>
<td>$\Psi^*(1,1,6)$</td>
<td>Hoffman-Singleton graph</td>
</tr>
<tr>
<td>50</td>
<td>14</td>
<td>3</td>
<td>4</td>
<td>no</td>
<td>$\Psi^*(1,1,12)$</td>
<td>Theorem 7.1.1(iii)</td>
</tr>
<tr>
<td>50</td>
<td>21</td>
<td>8</td>
<td>9</td>
<td>yes</td>
<td>$\Psi^*(1,1,12)$</td>
<td>Remark 7.2.6</td>
</tr>
<tr>
<td>51</td>
<td>10</td>
<td>1</td>
<td>2</td>
<td>no</td>
<td></td>
<td>Remark 7.2.2</td>
</tr>
<tr>
<td>51</td>
<td>20</td>
<td>7</td>
<td>8</td>
<td>no</td>
<td></td>
<td>Theorem 7.1.1(iv)</td>
</tr>
<tr>
<td>53</td>
<td>26</td>
<td>12</td>
<td>13</td>
<td>yes</td>
<td>$\Psi^*(1,1,13)$</td>
<td>PC-graph</td>
</tr>
<tr>
<td>55</td>
<td>18</td>
<td>5</td>
<td>6</td>
<td>no</td>
<td></td>
<td>Theorem 7.1.1(iv)</td>
</tr>
<tr>
<td>57</td>
<td>28</td>
<td>13</td>
<td>14</td>
<td>no</td>
<td></td>
<td>Lemma 2.2.5</td>
</tr>
</tbody>
</table>

148
<table>
<thead>
<tr>
<th>ν</th>
<th>r</th>
<th>λ</th>
<th>μ</th>
<th>Realizable</th>
<th>$\mathcal{G}^*(1,1,k)$</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>61</td>
<td>30</td>
<td>14</td>
<td>15</td>
<td>yes</td>
<td>$\mathcal{G}^*(1,1,15)$</td>
<td>PC-graph</td>
</tr>
<tr>
<td>64</td>
<td>21</td>
<td>6</td>
<td>7</td>
<td>no</td>
<td>$\mathcal{G}^*(1,1,15)$</td>
<td>Theorem 7.1.1(iii)</td>
</tr>
<tr>
<td>65</td>
<td>8</td>
<td>0</td>
<td>1</td>
<td>no</td>
<td>$\mathcal{G}^*(1,1,15)$</td>
<td>$\lambda = 0 &amp; \mu = 1$</td>
</tr>
<tr>
<td>65</td>
<td>16</td>
<td>3</td>
<td>4</td>
<td>no</td>
<td>$\mathcal{G}^*(1,1,15)$</td>
<td>Theorem 7.1.1(iii)</td>
</tr>
<tr>
<td>65</td>
<td>24</td>
<td>8</td>
<td>9</td>
<td>no</td>
<td>$\mathcal{G}^*(1,1,15)$</td>
<td>Theorem 7.1.1(iii)</td>
</tr>
<tr>
<td>65</td>
<td>32</td>
<td>15</td>
<td>16</td>
<td>?</td>
<td>$\mathcal{G}^*(1,1,15)$</td>
<td></td>
</tr>
<tr>
<td>69</td>
<td>34</td>
<td>16</td>
<td>17</td>
<td>no</td>
<td>$\mathcal{G}^*(1,1,15)$</td>
<td>Remark 7.2.2</td>
</tr>
<tr>
<td>73</td>
<td>12</td>
<td>1</td>
<td>2</td>
<td>no</td>
<td>$\mathcal{G}^*(1,1,15)$</td>
<td></td>
</tr>
<tr>
<td>73</td>
<td>24</td>
<td>7</td>
<td>8</td>
<td>no</td>
<td>$\mathcal{G}^*(1,1,15)$</td>
<td>Theorem 7.1.1(iii)</td>
</tr>
<tr>
<td>73</td>
<td>36</td>
<td>17</td>
<td>18</td>
<td>yes</td>
<td>$\mathcal{G}^*(1,1,15)$</td>
<td>Theorem 7.1.1(iii)</td>
</tr>
<tr>
<td>76</td>
<td>15</td>
<td>2</td>
<td>3</td>
<td>no</td>
<td>$\mathcal{G}^*(1,1,15)$</td>
<td></td>
</tr>
<tr>
<td>76</td>
<td>30</td>
<td>11</td>
<td>12</td>
<td>no</td>
<td>$\mathcal{G}^*(1,1,15)$</td>
<td>Theorem 7.1.1(iii)</td>
</tr>
<tr>
<td>77</td>
<td>38</td>
<td>18</td>
<td>19</td>
<td>no</td>
<td>$\mathcal{G}^*(1,1,15)$</td>
<td>Lemma 2.2.5</td>
</tr>
<tr>
<td>81</td>
<td>20</td>
<td>4</td>
<td>5</td>
<td>no</td>
<td>$\mathcal{G}^*(1,1,15)$</td>
<td>Theorem 7.1.1(iii)</td>
</tr>
<tr>
<td>81</td>
<td>40</td>
<td>19</td>
<td>20</td>
<td>yes</td>
<td>$\mathcal{G}^*(1,1,15)$</td>
<td></td>
</tr>
<tr>
<td>82</td>
<td>9</td>
<td>0</td>
<td>1</td>
<td>no</td>
<td>$\mathcal{G}^*(1,1,15)$</td>
<td>$\lambda = 0 &amp; \mu = 1$</td>
</tr>
<tr>
<td>82</td>
<td>18</td>
<td>3</td>
<td>4</td>
<td>no</td>
<td>$\mathcal{G}^*(1,1,15)$</td>
<td>Theorem 7.1.1(iii)</td>
</tr>
<tr>
<td>82</td>
<td>27</td>
<td>8</td>
<td>9</td>
<td>no</td>
<td>$\mathcal{G}^*(1,1,15)$</td>
<td>Theorem 7.1.1(iii)</td>
</tr>
<tr>
<td>82</td>
<td>36</td>
<td>15</td>
<td>16</td>
<td>yes</td>
<td>$\mathcal{G}^*(1,1,15)$</td>
<td>Remark 7.2.6</td>
</tr>
<tr>
<td>85</td>
<td>42</td>
<td>20</td>
<td>21</td>
<td>?</td>
<td>$\mathcal{G}^*(1,1,15)$</td>
<td></td>
</tr>
<tr>
<td>89</td>
<td>44</td>
<td>21</td>
<td>22</td>
<td>yes</td>
<td>$\mathcal{G}^*(1,1,15)$</td>
<td>PC-graph</td>
</tr>
<tr>
<td>91</td>
<td>30</td>
<td>9</td>
<td>10</td>
<td>no</td>
<td>$\mathcal{G}^*(1,1,15)$</td>
<td>Theorem 7.1.1(iv)</td>
</tr>
<tr>
<td>93</td>
<td>46</td>
<td>22</td>
<td>23</td>
<td>no</td>
<td>$\mathcal{G}^*(1,1,15)$</td>
<td>Lemma 2.2.5</td>
</tr>
<tr>
<td>97</td>
<td>48</td>
<td>23</td>
<td>24</td>
<td>yes</td>
<td>$\mathcal{G}^*(1,1,15)$</td>
<td>PC-graph</td>
</tr>
<tr>
<td>97</td>
<td>24</td>
<td>5</td>
<td>6</td>
<td>no</td>
<td>$\mathcal{G}^*(1,1,15)$</td>
<td>Theorem 7.1.1(iii)</td>
</tr>
<tr>
<td>99</td>
<td>14</td>
<td>1</td>
<td>2</td>
<td>no</td>
<td>$\mathcal{G}^*(1,1,15)$</td>
<td>Makhnëv (1988)</td>
</tr>
<tr>
<td>99</td>
<td>28</td>
<td>7</td>
<td>8</td>
<td>no</td>
<td>$\mathcal{G}^*(1,1,15)$</td>
<td>Theorem 7.1.1(iv)</td>
</tr>
<tr>
<td>100</td>
<td>33</td>
<td>10</td>
<td>11</td>
<td>no</td>
<td>$\mathcal{G}^*(1,1,15)$</td>
<td>Theorem 7.1.1(iv)</td>
</tr>
</tbody>
</table>

Table 7.2.1: Possible parameter sets with $\nu \leq 100$.  

149
Remark 7.2.8: Table 7.2.1 and the existence of strongly regular graphs with \( \lambda = 0 \) and \( \mu = 1 \) yield: \( \Psi^*(1,1,5) = \Psi^*(1,1,8) = \Psi^*(1,1,14) = \Psi^*(1,1,17) = \Psi^*(1,1,19) = \phi \).

Remark 7.2.9: There is only one PC-graph of order 5, 9, 13 and 17 and there are 15 non-isomorphic PC-graphs of order 25. Further, there are 10 non-isomorphic strongly regular graphs with parameters \((26,10,3,4)\) [see Weisfeiler (1976), sections T and U]. There are 1504 non-isomorphic PC-graph of order 45 [see Mathon (1978)]. Figures 4.2.1, 4.2.2 and 5.2.1 display PC-graphs of order 5, 9, 13, 17 and 25. Figure 7.2.1 displays a strongly regular graph with parameters \((26,10,3,4)\).

Remark 7.2.10: The existence of strongly regular graphs with parameters \((65,32,15,16)\) and \((85,42,20,21)\) are undecided; the \((65,32,15,16)\) is the smallest (order) undecided case.

Figure 7.2.2: A strongly regular graph with parameters \((26,10,3,4)\).
7.3 The Class $\mathcal{S}^\ast(m,n,k)$, $m \geq 1$, $n \geq 1$ and $m + n \geq 3$

In this section, we establish that there is no graph having property $\mathcal{S}^\ast(m,n,k)$ for $m \geq 1$, $n \geq 1$, $m + n \geq 3$ and $k \geq 1$. We begin with the following simple lemma.

Lemma 7.3.1: Let $G \in \mathcal{S}^\ast(m,n,k)$ and let $w$ be any vertex of $G$. Then for $m \geq 1$, $n \geq 1$ and $k \geq 1$, $G[N(w/-)] \in \mathcal{S}^\ast(m - 1,n,k)$ and $G[N(-/w)] \in \mathcal{S}^\ast(m,n - 1,k)$. □

Lemma 7.3.2: If $\mathcal{S}^\ast(2,1,k) = \phi$, then $\mathcal{S}^\ast(m,n,k) = \phi$ for any $m \geq 1$, $n \geq 1$ and $m + n \geq 3$.

Proof: Suppose to the contrary that $\mathcal{S}^\ast(m,n,k) \neq \phi$, and let $m_0 + n_0$ be the smallest value of $m + n \geq 3$ for which $\mathcal{S}^\ast(m,n,k) \neq \phi$. Then since $\mathcal{S}^\ast(1,2,k) = \phi$ when $\mathcal{S}^\ast(2,1,k) = \phi$, we must have $m_0 + n_0 \geq 4$. Let $G \in \mathcal{S}^\ast(m_0,n_0,k)$ and $w$ any vertex of $G$. By Lemma 7.3.1, $G[N(w/-)] \in \mathcal{S}^\ast(m_0 - 1,n_0,k)$ and $G[N(-/w)] \in \mathcal{S}^\ast(m_0,n_0 - 1,k)$. Since $m_0 + n_0 \geq 4$ one of $m_0$ or $n_0$ is at least 2 and so, by our assumption, at least one of $\mathcal{S}^\ast(m_0,n_0 - 1,k)$ or $\mathcal{S}^\ast(m_0 - 1,n_0,k)$ is empty. As $w$ is arbitrary this implies that $G$ is either the complete graph or its complement, which is impossible. Therefore, $\mathcal{S}^\ast(m,n,k) = \phi$. This proves the lemma. □

We now present our main result of this section.

Theorem 7.3.3: For $m \geq 1$, $n \geq 1$, $m + n \geq 3$ and $k \geq 1$, $\mathcal{S}^\ast(m,n,k) = \phi$.  

151
Proof: In view of Lemma 7.3.2, we need only show that $S^*(2,1,k) = \phi$. Suppose to the contrary that $S^*(2,1,k) \neq \phi$. Let $G \in S^*(2,1,k)$ and let $w$ be any vertex of $G$. Observe that $G$ cannot be a complete graph and its diameter is 2. Then Lemma 7.3.1 implies $G[N(w/-)] \in S^*(1,1,k)$ and $G[N(-/w)] \in S^*(2,0,k)$. Hence, $G[N(w/-)]$ is a strongly regular with parameters $\left(\frac{(k + t)^2}{t} + 1, k + t, t - 1, t\right)$ for some positive integer $t$, and $G[N(-/w)]$ is a strongly regular with parameters $\left(\frac{(k + s^2)(k + s^2 - 1)}{k} + 1, k + s^2, k, k\right)$ for some positive integer $s$, by theorems 7.2.1 and 7.1.2, respectively.

We now establish that $G$ is a regular graph. Let $x \in N(w/-)$. Since $G[N(w/-)]$ is $(k + t)$-regular we have

$$n(w,x/-) = d_{G[N(w/-)]}(x) = k + t.$$ 

Now consider $x$. Using the above argument we can conclude that $G[N(x/-)]$ is $(k + t')$-regular for some positive integer $t'$. Since $w \in N(x/-)$ and $n(w,x/-) = k + t$ it follows that $t' = t$. Consequently, since $G \in S^*(2,1,k)$, $G[N(y/-)]$ is $(k + t)$-regular for every $y \in V(G)$. Therefore, since $G[N(w/-)]$ has $\frac{(k + t)^2}{t} + 1$ vertices, $G$ is $(\frac{(k + t)^2}{t} + 1)$-regular. Consequently, $G$ is a strongly regular graph.

Let $x \in N(w/-)$ and $y \in N(-/w)$ be non-adjacent vertices of $G$. Observe that $n(x,w/-) = \lambda = k + t$ and $n(x,y/-) = \mu$. Since $G \in S^*(2,1,k)$, $n(x,w/y) = k$ and $n(x,y/w) = k$. Therefore, $\mu = n(x,y/-) = k + t$. Hence, $G$ is a strongly regular graph with parameters

$$\nu = \frac{(k + t)^2}{t} + \frac{(k + s^2)(k + s^2 - 1)}{k} + 3,$$
$$r = \frac{(k + t)^2}{t} + 1.$$
\[ \lambda = k + t = \mu, \]

for some positive integers \( s \) and \( t \). Further, since \( y \in N(-/\omega) \) and \( G[N(-/\omega)] \) is \((k + s^2)\)-regular we have

\[ n(w,y/-) = \frac{(k + t^2)}{t} + 1 - (k + s^2). \]

Now, since \( \mu = k + t = n(w,y/-) \) we have

\[ \frac{k^2}{t} + 1 = s^2. \quad (7.3.1) \]

Since for any \( x \in N(w/-) \) and \( y \in N(-/\omega) \), \( n(x/w) = r - \lambda - 1 = \frac{k(k + t)}{t} \) and \( n(y,w/-) = \mu = k + t \), we have

\[ \frac{(k + t)^2}{t} + 1)\frac{k(k + t)}{t} = \frac{(k + s^2)(k + s^2 - 1)}{k} + 1)(k + t) \quad \text{(7.3.2)} \]

Equation (7.3.2) together with (7.3.1) yields \( k = 0 \), a contradiction. This completes the proof of the theorem. \( \square \)

7.4 Property \( P^*(n,k) \)

Recall that a graph \( G \) is said to have property \( P^*(n,k) \) if for any two sets \( A \) and \( B \) of vertices of \( G \) with \( A \cap B = \emptyset \) and \( |A \cup B| = n \), there are exactly \( k \) vertices not in \( A \cup B \) which are joined to every vertex of \( A \) but not joined to any vertex of \( B \). The class of graphs having property \( P^*(n,k) \) is denoted by \( \mathcal{G}^*(n,k) \). The cycle \( C_5 \) of length 5 is a member of \( \mathcal{G}^*(1,2) \). The PC-graph with parameters \((9,4,1,2)\), (see Figure 7.2.1) is a member of \( \mathcal{G}^*(1,4) \). Observe that if \( G \in \mathcal{G}^*(n,k) \), then \( \bar{G} \in \mathcal{G}^*(n,k) \).
Lemma 7.4.1: Let $n$ and $k$ be positive integers. Then

(a) for $n > 1$, $S^*(n,k) = \phi$, and

(b) for $n = 1$, $G \in S^*(1,k)$ if and only if $G$ is a $k$-regular graph on $2k + 1$ vertices.

Proof: (a) For $n = 2$, clearly $S^*(2,k) = S^*(2,0,k) \cap S^*(1,1,k) \cap S^*(0,2,k)$. But $S^*(2,0,k) \cap S^*(1,1,k) \cap S^*(0,2,k) = \phi$ (see sections 7.1 and 7.2), thus $S^*(2,k) = \phi$. Now, let $n \geq 3$. Since $S^*(n,k) \subseteq S^*(1,n-1,k) = \phi$ (by Theorem 7.3.3), then $S^*(n,k) = \phi$. This proves (a).

(b) Let $G \in S^*(1,k)$. Clearly $S^*(1,k) = S^*(1,0,k) \cap S^*(0,1,k)$. If $G \in S^*(1,0,k)$, then $G$ is a $k$-regular graph. If $G \in S^*(0,1,k)$, then $G$ is a $(n - k - 1)$-regular graph. Therefore, $G$ is a $k$-regular graph on $2k + 1$ vertices. The converse is obvious. \qed

Remark 7.4.1: (1) For odd $k$, $S^*(1,k) = \phi$.

(2) PC-graphs provide examples of graphs in the class $S^*(1,k)$. More specifically, if $G$ is a PC-graph with parameters $(4t + 1, 2t, t - 1, t)$, then $G \in S^*(1,2t)$.

(3) A strongly regular graph with parameters $(21,10,5,4)$ along with its complement is a member of $S^*(1,10)$. Note that [see Weisfeiler (1976), sections T and U], there is only one strongly regular graph with parameters $(21,10,5,4)$. Figure 7.4.1 shows the strongly regular graph with parameters $(21,10,5,4)$. 

154
Figure 7.4.1: The strongly regular graph with parameters $(21, 10, 5, 4)$. 
CHAPTER 8

SOME OPEN PROBLEMS

We conclude this thesis by highlighting some problems that have not yet been resolved. Many of these have been mentioned in the preceding Chapters.

Almost all of our work in this thesis (Chapter 4, 5 and 6) has been related to the Paley constructions. It would be of interest to study other classes of graphs. In Chapter 3, we constructed classes of graphs having property $P(1,n,k)$. However, for $m, n \geq 2$, the problem of constructing graphs with the property $P(m,n,k)$ seems to be difficult. To date the only published examples of such graphs are the Paley graphs. The "generalized" Paley graphs, described in Section 5.4, provide other examples of graphs in the class $\mathcal{V}(m,n,k)$. It would be interesting to find other classes of graphs with the property $P(m,n,k)$ for any $m, n$ and $k$.

Recall the following problems detailed in Chapter 1:

(1) Characterize the class $\mathcal{V}(m,n,k)$.

(11) Determine the functions

$$p(m,n,k) = \min\{\nu(G) : G \in \mathcal{V}(m,n,k)\}$$

and

$$q(\ell, (m,n,k)) = \min\{\epsilon(G) : \nu(G) = \ell \text{ and } G \in \mathcal{V}(m,n,k)\}.$$ 

The only result concerning the latter function is due to Erdös and Moser (1970) who determined $q(\ell, (m,0,1))$. We noted in
the introduction that Exoo and Harary (1980) established that for 
$n \leq 6$ the smallest order graphs in the class $\mathcal{G}(1,n,1)$ are the $(n+1,5)$-cages. Lemma 2.2.8 gave us the smallest graph in the class $\mathcal{G}(1,1,k)$. It would be of interest to establish the smallest order graphs in the class $\mathcal{G}(1,n,k)$ for any $n$ and $k$. In particular, it is of interest to prove:

For $n \geq 2$ and $n + k \leq 7$ the smallest order graphs in the class $\mathcal{G}(1,n,k)$ are the known $(n + k,5)$-cages.

In order to obtain a general proof that an $(n + k,5)$-cage is a smallest graph in the class $\mathcal{G}(1,n,k)$ for $n \geq 2$, Lemma 2.1.8 and the following conjecture would be useful.

Conjecture 8.1: For $n \geq 2$, if $G \in \mathcal{G}(1,n,k)$ and has girth at most $4$, then $\nu(G) \geq (n + k)^2 + (n + k)$.

Of course proving that the smallest graph in $\mathcal{G}(1,n,k)$ for $n \geq 2$ is a cage would be very difficult if no $(n + k,5)$-cage is known. However, Conjecture 8.1 is motivated by the following Table [see Wong (1982)]:

<table>
<thead>
<tr>
<th>degree</th>
<th>$\nu(G)$</th>
<th>Discovered by</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>10</td>
<td>Petersen</td>
</tr>
<tr>
<td>4</td>
<td>19</td>
<td>Robertson</td>
</tr>
<tr>
<td>5</td>
<td>30</td>
<td>Wegner</td>
</tr>
<tr>
<td>6</td>
<td>40</td>
<td>O'Keefe and Wong</td>
</tr>
<tr>
<td>7</td>
<td>50</td>
<td>Hoffman and Singleton</td>
</tr>
</tbody>
</table>

Table 8.1: Cages of girth 5.
Observe that for each graph $G$ given in Table 8.1, $\nu(G) \leq (n + k)^2 + (n + k)$. So the conjecture 8.1 might be useful for checking whether $(n + k, 5)$-cages which will be discovered in the future are also smallest graphs in the class $\mathcal{G}(1, n, k)$ for $n \geq 2$.

For $m = n = 2$, we know that, $34 \leq p(2, 2, 1) \leq 61$. We conjecture that:

Conjecture 8.2: $p(2, 2, 1) = 61$.

More generally, the following problem is of interest:

Problem 8.3: Determine $p(m, n, k)$ for $m, n \geq 2$.

Lower bounds for $p(m, n, k)$ were established in Section 2.2 (Theorem 2.2.11 and Corollary 2.2.12).

The following conjecture was suggested in Section 5.2.

Conjecture 8.4: Let $q = 1 \pmod{4}$ be a prime power. The Paley graph $G_q \in \mathcal{G}(1, 2, k) \cap \mathcal{G}(2, 1, k)$ if and only if $q \geq (1 + 2\sqrt{k})^2$.

We proved that (Corollary 5.2.3) if $q > (1 + 2\sqrt{k})^2$, then $G_q \in \mathcal{G}(1, 2, k) \cap \mathcal{G}(2, 1, k)$. We also have verified, by a computer, that if $q = 1 \pmod{4}$ is a prime power less than or equal to 1009 and $k$ a positive integer with $q < (1 + 2\sqrt{k})^2$, then $G_q \notin \mathcal{G}(1, 2, k) \cap \mathcal{G}(2, 1, k)$. Further, we have proved that (Remark 5.2.2) if $q < (-1 + 2\sqrt{2(k + 1)})^2$, then $G_q \notin \mathcal{G}(1, 2, k) \cap \mathcal{G}(2, 1, k)$. So the problem
is to look at \((-1 + 2\sqrt{2(k+1)})^2 \leq q \leq (1 + 2\sqrt{2}k)^2\).

Corollary 5.2.8 asserts that the Paley graph \(G_q \in \mathcal{G}(2, 2, 1)\) for all prime power \(q \equiv 137\). We have verified, by using a computer, that \(G_q \in \mathcal{G}(2, 2, 1)\) for all prime power \(q \equiv 1(\text{mod } 4)\) with \(61 \leq q \leq 1009\). It would be interesting to prove that \(G_q \in \mathcal{G}(2, 2, 1)\) if and only if \(q \equiv 61\) without the use of a computer. More generally, we have:

Problem 8.5: Determine the function \(f(m, n, k)\) such that \(G_q \in \mathcal{G}(m, n, k)\) if and only if \(q \geq f(m, n, k)\).

We have introduced the "generalized" Paley graphs in Section 5.4. Recall that for \(q\) and \(d\) with \(q\) a prime power and

\[
d > 1 \text{ odd or } \frac{(q - 1)}{d} \text{ even}
\]

we defined the "generalized" Paley graph \(G^{(d)}_q\) as follows. The vertices of \(G^{(d)}_q\) are the elements of the finite field \(F_q\). Two vertices \(a\) and \(b\) are adjacent if and only if \(a - b = y^d\) for some \(y \in F_q\). By using a computer we noted in Section 5.4 that for sufficiently large \(q\) the "generalized" Paley graphs \(G^{(3)}_q\) and \(G^{(4)}_q\) satisfy the property \(P(2, 2, k)\) for small \(k\). We conjecture that:

Conjecture 8.6: For any \(m, n\) and \(k\), all sufficiently large "generalized" Paley graphs satisfy the properties \(P(m, n, k)\) and \(P(n, k)\).

Recall that for \(q\) and \(d\) with \(q\) a prime power and

\[
d > 1 \text{ even and } \frac{(q - 1)}{d} \text{ odd}
\]

we defined the Paley digraph \(D^{(d)}_q\) as follows. The vertices of
$D^{(d)}_q$ are the elements of the finite field $\mathbb{F}_q$. Vertex $a$ joins to vertex $b$ by an arc if and only if $a - b = y^d$ for some $y \in \mathbb{F}_q$. We conjecture that:

Conjecture 8.7: For any given $m$, $n$ and $k$, all sufficiently large Paley digraphs $D^{(d)}_q$ satisfy the properties $Q(n,k)$ and $Q(m,n,k)$.

The following observation may be useful in considering the conjectures 8.6 and 8.7.

Let $q$ be a fixed primitive element of the finite field $\mathbb{F}_q$; that is $q$ is a generator of the cyclic group $\mathbb{F}_q^*$. For each $j = 0, 1, \ldots, q - 2$, define a function $\varphi_j$ by

$$\varphi_j(g^k) = e^{\frac{2\pi i j k}{q - 1}}, \text{ for } k = 0, 1, \ldots, q - 2;$$

where $i^2 = -1$. Hence, $\varphi_0 = \chi_0$ and it is easy to check that $\varphi_j$ is well-defined and is a character for $j = 0, 1, \ldots, q - 2$.

For an odd prime power $q$, put $j = \frac{q - 1}{2}$. Let $\eta = \varphi_{(q-1)/2}$. Then

$$\eta(g^k) = e^{k \pi i},$$

where $i^2 = -1$. Therefore, $\eta(c) = 1$ if $c$ is a square of an element of $\mathbb{F}_q^*$, $\eta(0) = 0$ and $\eta(c) = -1$ otherwise. That is, $\eta$ is the quadratic character of $\mathbb{F}_q^*$ defined in Chapter 5.

Recall that an interesting problem in Chapter 6 is that of determining the smallest integer $f(n,k)$ such that there exists a tournament $T_q$ of order $q$ which has property $Q(n,k)$ whenever $q \geq f(n,k)$. From (6.1.2) and Remark 6.2.3, we know that $47 \leq f(n,k) \leq 67$. We conjecture that:
Conjecture 8.8: $f(n,k) = 67$.

More generally, the following problem is of interest:

Problem 8.9: Determine $f(n,k)$ for any $n$ and $k$.

The following conjecture was suggested in Section 6.2.

Conjecture 8.10: Let $q \equiv 3 \pmod{4}$ be a prime power. The Paley tournament $D_q$ has property $Q(3,k)$ if and only if $q > (1 + 2\sqrt{2k})^2$.

We proved that (Corollary 6.2.3) if $q > (1 + 2\sqrt{2k})^2$, then $D_q$ has property $Q(3,k)$. We also have verified, by a computer, that if $q \equiv 3 \pmod{4}$ is a prime power less than or equal to 1031 and $k$ is a positive integer with $q \leq (1 + 2\sqrt{2k})^2$, then $D_q$ does not have property $Q(3,k)$. Further, we have proved that (Remark 6.2.2) if $q < (-1 + 2\sqrt{2(k+1)})^2$, then $D_q$ does not have property $Q(3,k)$. So the problem is to look at $(-1 + 2\sqrt{2(k+1)})^2 \leq q \leq (1 + 2\sqrt{2k})^2$.

Corollary 6.2.4 asserts that the Paley tournament $D_q$ has property $Q(4,1)$ for all prime power $q \geq 131$. We have verified, by using a computer, that $D_q$ has property $Q(4,1)$ for all prime power $q \equiv 3 \pmod{4}$ with $67 \leq q \leq 1031$ except 103. It would be interesting to prove that $D_q$ has property $Q(4,1)$ if and only if $q \geq 67$ except 103 without the use of a computer. More generally, we have:

Problem 8.11: Determine the function $g(n,k)$ such that $D_q$ has property $Q(n,k)$ whenever $q \geq g(n,k)$. 

161
REFERENCES


162


