Self-Complementary Arc-Transitive Graphs and Their Imposters

by

Natalie Mullin

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Combinatorics & Optimization

Waterloo, Ontario, Canada, 2009

Author's Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

This thesis explores two infinite families of self-complementary arc transitive graphs: the familiar Paley graphs and the newly discovered Peisert graphs. After studying both families, we examine a result of Peisert which proves the Paley and Peisert graphs are the only self-complementary arc transitive graphs other than one exceptional graph on 23^2 vertices. Then we consider other families of graphs which share many properties with the Paley and Peisert graphs. In particular, we construct an infinite family of self-complementary strongly regular graphs from affine planes. We also investigate the pseudo-Paley graphs of Weng, Qiu, Wang, and Xiang. Finally, we prove a lower bound on the number of maximal cliques of certain pseudo-Paley graphs, thereby distinguishing them from Paley graphs of the same order.

Acknowledgements

I would like to thank my advisor Chris Godsil for his guidance and instruction. I am also grateful to the Department of Combinatorics and Optimization for the academic opportunities they have afforded me both as an undergraduate and graduate student. Lastly, I would like to acknowledge the financial support of the National Science and Engineering Research Council of Canada.

Contents

List of Tables

Chapter 1

Introduction

Paley graphs are a remarkable family of graphs that have a variety of interesting properties. For example, Paley graphs are one of the most widely used examples of a family of deterministic graphs with random-like properties. They are also useful because their graph-theoretic properties relate to the number theory of quadratic residues. Moreover, their construction is surprisingly simple. Let $\mathbb{F}_q$ denote the field of order q such that $q \equiv 1 \pmod 4$. The Paley graph of order q is the graph constructed on the elements of $\mathbb{F}_q$ such that two elements are adjacent if and only if their difference is a nonzero square in $\mathbb{F}_q$.

Many of the properties possessed by Paley graphs are a consequence of their large automorphism group. In this thesis we are most interested in two well-known properties of Paley graphs. First we see that a Paley graph is isomorphic to its complement. We refer to graphs with this property as self-complementary. Second we see that the automorphism group of a Paley graphs act transitively on its arcs. We refer to such graphs as arc-transitive. These properties force strong conditions on the automorphism group of the Paley graph, and thus it is remarkable that the Paley graphs are an infinite family of graphs that are both self-complementary and arc-transitive. This prompts the following question: *Are there any other self-complementary arc-transitive graphs*?

Peisert provides an answer by explicitly describing another infinite family of self-complementary arc-transitive graphs, which we refer to as Peisert graphs. Similar to a Paley graph, a Peisert graph is defined as a graph on the elements of the finite field $\mathbb{F}_q$. However, it must be the case that $q = p^{2r}$ for some prime p such that $p \equiv 3 \pmod 4$. Suppose that ω is a multiplicative generator of $\mathbb{F}_q$. Two elements in the Peisert graph of order q are adjacent if and only if their difference is equal to ω^k for $k \equiv 0, 1 \pmod 4$. From this definition Peisert proves that Peisert graphs are self-complementary and arc-transitive. Using more elaborate algebraic techniques he confirms that Peisert graphs are distinct from Paley graphs, with the exception of the graph on 9 vertices [19].

With our own work, we see differences in the maximal clique structures of Paley and Peisert graphs. From a result of Blockhuis [2], we know that each pair of adjacent vertices in the Paley graph of order q^2 is contained in exactly one common clique of size q. However, in the Peisert graph of order q^2 where $q \equiv 1 \pmod 4$, this is not the case. For this graph, we prove that each pair of adjacent vertices contained in a common clique of size q is contained in at least two cliques of size q. Using a computer, we also find examples of Peisert graphs that do not contain maximal cliques of size q.

Impressively, Peisert does much more than find another family of self-complementary arc-transitive graphs. He also proves the following theorem.

Theorem. *A graph is self-complementary and arc transitive if and only if* $|G| = p^r$ *for some prime* p, $p^r \equiv 1 \pmod 4$, *and* G *is Paley graph or a Peisert graph or is isomorphic to an exceptional graph on* 23^2 *vertices.* □

In this thesis we study other families of graphs that share many properties with Paley and Peisert graphs. However, due to Peisert's result these graphs must not be self-complementary arc-transitive graphs. We attempt to distinguish these families from the Paley and Peisert graphs, thereby showing they are not self-complementary and arc-transitive.

In particular we focus on self-complementary strongly regular graphs. All self-complementary arc-transitive graphs are vertex transitive strongly regular graphs, but the reverse is not true. Thus Paley and Peisert graphs are examples of infinite families of self-complementary strongly regular graphs, but there may be other infinite families with these properties. In the spirit of the well-studied generalized Paley graphs, we define a new family of graphs that we refer to as generalized Peisert graphs. We also show that infinitely many generalized Peisert graphs are self-complementary and strongly regular, and using a computer we verify that small examples of these graphs are distinct from Paley and Peisert graphs.

While seeking out other imposters of Paley and Peisert graphs, we note the Paley graph construction can be mimicked on algebraic structures other than finite fields. It was recently shown by Weng, Qiu, Wang, and Xiang that the Paley construction works well on commutative semifields, which are algebraic systems that satisfy all of the field axioms except associativity of multiplication. The authors construct graphs on the elements of a finite commutative semifield where two elements are adjacent if and only if their difference is a nonzero square in the semifield. They refer to such graphs as pseudo-Paley graphs, and they show the graphs are strongly regular with the same parameter set as Paley graphs [24].

Weng, Qiu, Wang, and Xiang are able to distinguish small examples of pseudo-Paley graphs from Paley and Peisert graphs, and they conjecture this distinction holds true in general [24]. We devote the last chapter of this thesis to confirming that the pseudo-Paley graphs on Dickson semifields are distinct from the Paley graphs. From Blockhuis' result [2], we know the total number of cliques of size q in the Paley graph on q^2 vertices. By explicitly constructing more distinct cliques of size q in the graph on the Dickson semifield, we prove that Paley graph and Dickson semifield graph are not isomorphic. This successfully distinguishes Paley graphs from one family of imposters. We also include computational results which suggest similar methods could be applied to distinguish other families of pseudo-Paley graphs.

Chapter 2

Paley Graphs

A Paley graph is a graph constructed on the points of a finite field such that two vertices are adjacent if and only if their difference is a nonzero square in the field. Paley graphs possess many interesting properties that are a consequence of their large automorphism group. Paley graphs are especially useful because their graph-theoretic properties relate to the number theory of quadratic residues.

Paley graphs on a prime number of vertices are also one of the most widely used examples of a deterministic graphs with random-like properties. The randomness properties of such Paley graphs are established by Bollobás and Thomason [3] using estimates from Weil [23] and Burgess [4] for character sums. Chung, Graham, and Wilson show that Paley graphs on a prime number of vertices are *quasi-random*, thereby showing that such Paley graphs share a large number of graph properties with random graphs [6].

We begin our exploration of Paley graphs by defining them as Cayley graphs over the additive group of a finite field. From this definition we see two standard results concerning the symmetry of Paley graphs. We also note that Paley graphs are contained in the class of strongly regular graphs. Then we give an alternate construction of a Paley graph on a square number of vertices as a graph on the points of an affine plane. Finally, we see how this construction is used by Blokhuis to prove a result that determines all of the maximal cliques in Paley graphs with a square number of vertices [2].

2.1 Cayley Graphs

Our discussion of Cayley graphs follows the treatment given in Godsil and Royle's text [10]. For a group G, let S be a non-empty subset of G that is closed with respect to inverses and does not contain the identity. We define the Cayley graph $X(G, S)$ to be the undirected graph with the vertex set G where two vertices x and y are adjacent if and only if $xy^{-1} \in S$. We refer to S as the connection set of of G.

Since S is closed under taking inverses, we have

$$xy^{-1} \in S \iff yx^{-1} \in S.$$

This implies the graph $X(G, S)$ is undirected. Furthermore, since the connection set does not contain the identity, $X(G, S)$ will not have any loops. It is straightforward to see that the neighbours of the identity of G are precisely the elements in S. Also it is useful to prove that the automorphism group of a Cayley graph must act transitively on its vertices. We refer to graphs with this property as *vertex transitive*. The following result is standard.

2.1.1 Lemma. *Cayley graphs are vertex transitive.*

Proof. For any pair of elements u and v in G, there is a permutation $\tau_{u^{-1}v}$ of G defined by $\tau_{u^{-1}v} : x \mapsto xu^{-1}v$ that maps u to v. Let x and y be two elements in G, and let C be a nonempty inverse-closed subset of G that does not contain the identity. Note that $xu^{-1}v(yu^{-1}v)^{-1} = xy^{-1}$. From this it follows that $xy^{-1} \in C$ if and only $\tau_{u^{-1}v}(x)\tau_{u^{-1}v}(y)^{-1} \in C$. Therefore x is adjacent to y in $X(G, C)$ if and only if $\tau_{u^{-1}v}(x)$ is adjacent to $\tau_{u^{-1}v}(y)$. From this we conclude $\tau_{u^{-1}v}$ is an automorphism of X that maps a to b. Moreover, the subgroup $\{\tau_t : t \in G\}$ acts transitively on the vertices of $X(G, C)$. □

In this thesis we construct Cayley graphs on abelian groups, and therefore we use additive notation for the remainder of the thesis when describing such graphs.

2.2 Standard Construction and Properties

Let q be a prime power such that $q \equiv 1 \pmod 4$, and let $\mathbb{F}_q$ be the finite field of order q with primitive root ω. Let S denote the set of nonzero squares in $\mathbb{F}_q$. The Paley graph of order q, denoted $P(q)$ is the Cayley graph constructed on the additive group of $\mathbb{F}_q$ using S as the connection set. In other words, two vertices in the Paley graph are adjacent if and only if their difference is a nonzero square in $\mathbb{F}_q$.

Note that the set of all nonzero squares of $\mathbb{F}_q$ form a multiplicative subgroup of index two generated by ω^2. Since $q \equiv 1 \pmod 4$, it follows that -1 is contained in S. Thus S is a nonempty subset of $\mathbb{F}_q$ that is closed with respect to inverses, as required.

Let p denote the characteristic of $\mathbb{F}_q$. Define $f : \mathbb{F}_q \to \mathbb{F}_q$ by $f(x) = x^p$ for all x in $\mathbb{F}_q$. It is useful to note that f is an automorphism of $\mathbb{F}_q$. This automorphism is generally referred to as the Frobenius automorphism. It is a standard result that f generates the full group of automorphisms of $\mathbb{F}_q$.

Now we deduce several simple results from this definition of Paley graphs. For a graph X, we refer to an ordered pairs of adjacent vertices as an *arc* of X. If the automorphism group of X acts transitively on its set of arcs, then we refer to X as *arc-transitive*. The following result is standard.

2.2.1 Lemma. *Paley graphs are arc-transitive.*

Proof. Let θ denote the permutation of $\mathbb{F}_q$ defined by $\theta : x \mapsto \omega^2 x$. Recall that S is a multiplicative subgroup of $\mathbb{F}_q$ generated by ω^2, and so the subgroup of the permutation group generated by θ acts transitively on S. Suppose that x, y are adjacent vertices in $P(q)$, in which case $x - y = \omega^{2i}$ for some i. We see that

$$x - y = \omega^{2i} \iff \omega^2 x - \omega^2 y = \omega^{2(i+1)}.$$

Therefore x and y are adjacent if and only if $\theta(x)$ and $\theta(y)$ are adjacent. From this we see θ is a graph automorphism of $P(q)$ that fixes 0, and the subgroup generated by θ acts transitively on the neighbours of 0.

Using the fact that the automorphism group of every Cayley graph acts transitively on its vertices, we conclude that the automorphism group of $P(q)$ acts transitive on its arcs. □

Next we give a well-known proof that Paley graphs are isomorphic to their complements. We refer to graphs with this property as *self-complementary.*

2.2.2 Lemma. *Paley graphs are self-complementary.*

Proof. Let σ denote the permutation on $\mathbb{F}_q$ which maps x to ωx. Note that

$$x - y = \omega^{2i} \iff \sigma(x) - \sigma(y) = \omega^{2i+1}.$$

Recall that S is generated multiplicatively by ω^2, and so x and y are adjacent in $P(q)$ if and only if $\sigma(x)$ and $\sigma(y)$ are not adjacent. Therefore σ is an isomorphism from $P(q)$ to its complement. □

2.3 Strongly Regular Graphs

In this section we turn our focus to the adjacency properties of Paley graphs. First we specify the necessary adjacency properties of strongly regular graphs, and then we see that Paley graphs are strongly regular.

2.3.1 Definition. A graph X on n vertices is *strongly regular* with parameters (n, k, a, c) if the following conditions hold:

i) Each vertex has k neighbours where $k > 0$.

ii) Each pair of adjacent vertices has a common neighbours where $a < n-2$.

iii) Each pair of distinct, nonadjacent vertices has c common neighbours.

Note that the conditions on k and a restrict strongly regular graphs to graphs which have at least one edge and are not complete.

2.3.2 Example. The smallest example of a strongly regular graph is the 5-cycle. It can be easily shown that each vertex in the 5-cycle has two neighbours, each pair of adjacent vertices have no common neighbours, and each pair of distinct nonadjacent vertices has exactly one common neighbour.

Rather than proving that Paley graphs are strongly regular, we prove a stronger result which states that every self-complementary, arc-transitive graph is strongly regular. This proof follows directly from work in Godsil and Royle's text [10].

2.3.3 Lemma. *Self-complementary, arc-transitive graphs are strongly regular.*

Proof. Let X be a self-complementary, arc-transitive graph. Arc transitivity implies vertex transitivity, and so we consider the neighbourhood any vertex x in X without loss of generality. In particular, each vertex must have the same degree, and so the parameter k for X is well-defined.

Let y be a neighbour of x. By arc transitivity there is in automorphism of X which fixes x and maps y to any other neighbour of x. Therefore the number of common neighbours of x and y must be independent of the choice of y. This implies the parameter a is well-defined.

Let z be a vertex that is nonadjacent to x in X. Let $\overline{X}$ denote the complement of X. Clearly x is adjacent to z in $\overline{X}$. Since $\overline{X}$ is arc-transitive, the number of vertices that are nonadjacent to x and nonadjacent to z is independent of the choice of z. Therefore the number of common neighbours of x and any nonadjacent vertex in X is constant, and so the parameter c is well-defined. □

From this we immediately deduce that Paley graphs are strongly regular.

2.3.4 Corollary. *Paley graphs are strongly regular.* □

2.4 Affine Plane Construction

Now we give a construction of Paley graphs of square order using affine planes. This construction highlights the clique structure of the Paley graphs and enables us to determine the form of the largest cliques. We recall the properties of an affine plane.

2.4.1 Definition. An *affine plane* is a point-line incidence structure which satisfies the following conditions:

(i) Given any pair of points, there is exactly one line incident to both points.

(ii) Given a point p and a line l not incident to p, there is exactly one line l' through p which does not meet l.

(iii) There exists a set of four points, no three of which are incident to a common line.

Next we note that a graph can be defined on the points of the affine plane in the following way. First designate half of the parallel classes as special, and then define two points in the graph to be adjacent if and only they are incident to a common line that is contained in a special parallel class. For example, if we start with an affine plane with q^2 points, then each vertex in the resulting graph will have exactly $(q^2 - 1)/2)$ neighbours.

Using this method on the affine plane $AG(2, q)$ it is possible to choose a special set of parallel classes such that the resulting graph is isomorphic to the Paley graph $P(q^2)$. We give the details of this construction in the rest of this section. First we give an explicit correspondence between $AG(2, q)$ and the additive group of $\mathbb{F}_{q^2}$, and then we explain and justify the choice of special parallel classes.

2.4.1 Constructing $AG(2, q)$ from $\mathbb{F}_{q^2}$

First we consider $\mathbb{F}_{q^2}$ as a quadratic extension over $\mathbb{F}_q$. We can identify the elements of $\mathbb{F}_{q^2}$ with the following set.

$$\mathbb{F}_{q^2} = \{a + b\lambda : a, b \in \mathbb{F}_q\}$$

where $\lambda^2 = \alpha$ for some fixed nonsquare α in $\mathbb{F}_q$.

Next we consider $\mathbb{F}_{q^2}$ as a two-dimensional vector space over $\mathbb{F}_q$. We have the following isomorphism from this vector space into $\mathbb{F}_q \times \mathbb{F}_q$.

$$\psi : (a + b\lambda) \rightarrow (a, b) \tag{2.4.1}$$

It is straightforward to verify this map is a vector space isomorphism.

Lastly we construct the affine plane $AG(2, q)$ on the points of $\mathbb{F}_q \times \mathbb{F}_q$ by choosing the lines to be the translations of the one-dimensional vector spaces. Accordingly, q of the lines incident to $(0, 0)$ have the following form.

$$l_y = \{(c, cy) : c \in \mathbb{F}_q\} \tag{2.4.2}$$

for some fixed y in $\mathbb{F}_q$. We say a line l_y of this form has *slope* y and note the difference between any two points in l_y is a scalar multiple of $(1, y)$. The other line incident to $(0, 0)$ in $AG(2, q)$ is

$$l_\infty = \{(0, c) : c \in \mathbb{F}_q\} \tag{2.4.3}$$

We identify l_∞ with slope ∞ and note the difference between any two points in l_∞ is a scalar multiple of $(0, 1)$.

Every other line in $AG(2, q)$ is a translate of a line incident to $(0, 0)$. For each y in $\mathbb{F}_q \cup \infty$, we refer to the set of all q translates of l_y as a *parallel class* and say each line in this parallel class has slope y. We see that the set of all lines is partitioned into $q + 1$ parallel classes of size q.

2.4.2 Special Parallel Classes

Let ω denote a multiplicative generator of $\mathbb{F}_{q^2}$. Note that the unique subfield of order q is generated by ω^{q+1}. We are only interested in odd prime powers q, and so we assume that $q + 1$ is even. This implies that multiplication by any power of ω^{q+1} fixes the squares of $\mathbb{F}_{q^2}$. This further implies that the elements of the vector space $\mathbb{F}_q \times \mathbb{F}_q$ corresponding to squares of $\mathbb{F}_{q^2}$ are closed under scalar multiplication by elements of $\mathbb{F}_q$. Therefore $\psi^{-1}(1, y)$ is a square in $\mathbb{F}_{q^2}$ if and only if $\psi^{-1}(c, cy)$ is a square in $\mathbb{F}_{q^2}$ for all nonzero scalars c in $\mathbb{F}_q$. Note from our definition of ψ that $\psi^{-1}(0, 1)$ is not a square in $\mathbb{F}_{q^2}$.

Using these observations we partition the elements of $\mathbb{F}_q \times \mathbb{F}_q$ corresponding to the squares of $\mathbb{F}_{q^2}$ into $(q + 1)/2$ one-dimensional vector spaces. Each of these one-dimensional vector spaces corresponds to a line l_y in $AG(2, q)$ with slope y such that $\psi^{-1}(1, y)$ is a square in $\mathbb{F}_{q^2}$.

Recall that two vertices in the Paley graph constructed on $\mathbb{F}_q^2$ are adjacent if and only if their difference is a nonzero square. Identifying the elements of $\mathbb{F}_q^2$ as points of $AG(2, q)$, we see that two vertices in the Paley graph are adjacent if and only if they are incident to a common line with slope y in $\mathbb{F}_q$ such that $\psi^{-1}(1, y)$ is a square in $\mathbb{F}_{q^2}$. This verifies the following alternative construction of Paley graphs.

2.4.2 Construction. Let S denote the set of nonzero squares in $\mathbb{F}_{q^2}$. Let $\hat{S}$ denote the subset of slopes of $AG(2, q)$ such that

$$m \in \hat{S} \iff \psi^{-1}(1, m) \in S$$

Let G denote the graph constructed on the points of $AG(2, q)$, considered as elements of $\mathbb{F}_q \times \mathbb{F}_q$, where two points x and y are adjacent if and only if they are both incident to a line with slope m such that $m \in \hat{S}$. Then G is isomorphic to the Paley graph $P(q^2)$.

2.5 Maximal Cliques

We consider cliques in Paley graphs which are maximal with respect to size.

The size a maximal clique in $P(p)$ is known by a result of Graham and Ringrose [11] to be as large as $c \log p \log \log \log p$ for infinitely many primes p where c is some constant.

In general, it is a difficult problem to determine the size of a maximal clique in $P(q)$ unless q is a square. The Delsarte-Hoffman bound gives an upper bound for the size of the largest independent set in a regular graph in terms of the least eigenvalue of the adjacency matrix of the graph. We state the bound as the following lemma.

2.5.1 Lemma. *Let X be a k-regular graph on n vertices with least eigenvalue τ, and let $\alpha(X)$ denote the size of the largest independent set in X. Then*

$$\alpha(X) \leq \frac{n(-\tau)}{(k - \tau)}.$$

It can be shown that the least eigenvalue of the Paley graph $P(q)$ is $(-1 - \sqrt{q})/2$ (eg. [10]). Therefore by Lemma 2.5.1, we have the following.

$$\alpha(P(q)) \leq \frac{q(1 + \sqrt{q})}{(q + \sqrt{q})} = \sqrt{q}$$

Recall that Paley graphs are self-complementary, and therefore the maximal independent sets are in one-to-one correspondence with the maximal cliques by a self-complementing permutation. Thus the bound for $\alpha(P(q))$ given above is also a bound on the size of a maximal clique. For a Paley graph on a square number of vertices, say q^2, this bound is obtained by cliques of size q. The unique subfield of order q is an natural choice for such a clique.

2.5.2 Lemma. *The vertices corresponding to the unique subfield of order q in $\mathbb{F}_{q^2}$ form a q-clique in $P(q^2)$.*

Proof. Let ω be a primitive root of $\mathbb{F}_{q^2}$. Recall the subfield of order q that is multiplicatively generated by ω^{q+1} and $q+1$ is even. Therefore each element in the subfield is a square, and the difference between any two elements in the subfield is a square. □

From the construction of $P(q^2)$ given in Section 2.4, we see that certain lines of $AG(2,q)$ form cliques of size q. Let l_y denote a line with slope y where $\psi^{-1}(1,y)$ is a square in $\mathbb{F}_{q^2}$. Each pair of points incident to l_y are adjacent, and so the points incident to l_y form a clique of size q. If fact, we see that all the maximal cliques of $P(q^2)$ correspond to lines in $AG(2,q)$. This was first proved by van Lint and MacWilliams [22] for the case when q is a prime and was later generalized by Blokhuis [2] for all prime powers q. We review these proofs in the following sections.

2.5.1 q is a prime

When q is a prime, it can be shown using a theorem of Rédei [20] that the only clique of size q in $P(q^2)$ containing 0 and 1 in $P(q^2)$ is the subfield of order q. This result is due to van Lint and MacWilliams [22]. Using the fact that Paley graphs are arc-transitive, this result determines that all maximal cliques in $P(q^2)$ correspond to lines in $AG(2,q)$ when q is a prime. We give an elementary proof due to Lovász and Schrijver [15]. Throughout this work, we assume that p is a prime.

2.5.3 Definition. For a subset X of the points of $AG(2,p)$, we say that X *determines* a slope m if some two distinct points in X are incident to a common line with slope m.

Recall that each parallel class of $AG(2,p)$ contains p lines. Therefore if a subset X contains more than p points, each parallel class must contain a line incident to two points of X. This implies if $X > p$, then X must determine all $p+1$ possible slopes.

2.5.4 Theorem. *Let p be a prime and let X be a subset of the affine plane $AG(2,p)$, such that $|X| = p$ and X is not a line. Then X determines at least $(p+3)/2$ slopes.*

Proof. We assume that X does not determine all slopes, otherwise we are done. Therefore there is at least one parallel class such that each line in the parallel class contains exactly one point of X. This implies we can coordinatize $AG(2,p)$ in such a way that

$$X = \{(k, b_k) : k \in \mathbb{F}_p\}.$$

where $b_0, ..., b_{q-1}$ are elements of $\mathbb{F}_p$. Let U be the collection of slopes determined by X. Then

$$U = \left\{ \frac{b_k - b_m}{k - m} : k, m \in \mathbb{F}_p, k \neq m \right\}.$$

Suppose for a contradiction that $|U| < (p+3)/2$. Consider the polynomial

$$F_j(x) = \sum_{k \in \mathbb{F}_p} (b_k - kx)^j$$

for $j = 0, ..., p-2$. Note that $\sum_{k\in\mathbb{F}_p} k^j = 0$ if and only if $j = 0$ or $p-1$ does not divide j. Therefore the coefficient of x^j in F_j is zero, and so the degree of F_j is less than or equal to $j-1$ for nonzero j.

If x is a slope not contained in U, then the elements $b_k - kx$ for k in $\mathbb{F}_p$ are all distinct. This implies that $F_j(x) = 0$ if x is not contained in U. Since the degree of F_j is less than $j-1$, it follows that F_j is the zero polynomial if $j - 1 < p - |U|$. In particular, F_j is the zero polynomial if $j \leq (p-1)/2$.

Using the fact that every function over $\mathbb{F}_p$ is a polynomial of degree at most $p-1$, we can find elements c_i in $\mathbb{F}_p$ for $1 \leq i \leq m$ such that

$$b_k = c_m k^m + ... + c_2 k^2 + c_1 k + c_0 \tag{2.5.1}$$

where $c_m \neq 0$ and $m \leq p-1$. We have assumed that X is not a line, and so $m \geq 2$. Let $p - 1 = am + b$ where $a > 0$ and $0 \leq b \leq m-1$. Since $m \geq 2$, it follows that $a + b \leq (p-1)/2$ and so $F_{a+b} = 0$. In particular, the coefficient of x^b in F_{a+b} is 0. Utilizing Equation 2.5.1 we have

$$\begin{aligned} 0 &= \sum_k \binom{a+b}{b} b_k^a k^b \\ &= \binom{a+b}{b} \sum_k \left(c_m^a k^{am+b} + \sum_{j=b}^{p-2} d_j k^j \right) \\ &= \binom{a+b}{b} \left(\sum_k c_m^a k^{am+b} + \sum_{j=b}^{p-2} d_j \sum_k k^j \right) \\ &= \binom{a+b}{b} c_m^a \sum_k k^{p-1} \end{aligned}$$

where d_j is some element of $\mathbb{F}_p$ for $b \leq j \leq p-2$. Note that

$$\sum_{k \in \mathbb{F}_p} k^{p-1} = 1.$$

Therefore we have

$$0 = \binom{a+b}{b} c_m^a.$$

The right hand side of this equation is clearly nonzero by our choice of c_m, and so we have our desired contradiction. □

2.5.5 Corollary. *Let p be an odd prime. If a set of p vertices in the Paley graph $P(p^2)$ form a clique, then they are incident to a common line in $\mathbb{F}_{p^2}$ considered as the affine plane $AG(2,p)$.*

Proof. Using Construction 3.2.1 we construct $P(p^2)$ as a graph on the points of the affine plane $AG(2,q)$ where two points are adjacent if and only if they are incident to a common line with slope y in $\mathbb{F}_q$ such that $(1,y)$ corresponds to a square in $\mathbb{F}_{q^2}$. We have already seen that points incident to lines with designated slopes form a clique of size q. There are exactly $(q+1)/2$ such designated slopes, and so a set of points in $AG(2,q)$ that determine at least $(q+3)/2$ directions cannot form a q-clique in the Paley graph. The result follows. □

Rédei's original formulation of Theorem 2.5.4 is stated as follows.

2.5.6 Theorem. *If $f : \mathbb{F}_p \to \mathbb{F}_p$ is non-linear then the difference quotient*

$$\frac{f(x) - f(y)}{x - y}$$

takes on at least $(p+3)/2$ distinct values for x and y in $\mathbb{F}_p$ such that $x \neq y$. □

From this equivalent statement we prove one other interesting result due to Lovász and Schrijver [15]. This diverges temporarily from our discussion of maximal cliques.

Let $\tau_{a,b}$ denote the permutation of $\mathbb{F}_q$ defined as

$$\tau_{a,b}(x) = ax + b.$$

where a and b are elements of $\mathbb{F}_q$ such that $a \neq 0$. Again let S denote the set of nonzero squares of $\mathbb{F}_q$.

2.5.7 Corollary. *The automorphism group of the Paley graph $P(p)$ is precisely the following set of automorphisms*

$$\{\tau_{a,b} : a \in S, b \in \mathbb{F}_q\}$$

Proof. We have already seen that for a in S and b in $\mathbb{F}_p$, the map $\tau_{a,b}$ is an automorphism of the Paley graph. Suppose that θ is an automorphism of the Paley graph. For x and y in $\mathbb{F}_q$ we have

$$x - y \in S \iff \theta(x) - \theta(y) \in S.$$

For distinct x and y this implies that

$$\frac{\theta(x) - \theta(y)}{x - y} \in S.$$

Therefore the quotient takes on at most $(p+1)/2$ values. By Theorem 2.5.6 we deduce that f is a linear function. Thus for some b and nonzero c in $\mathbb{F}_p$ we have

$$\theta(x) = cx + b.$$

Since $\theta(x) - \theta(y) = c(x - y)$ is a square if and only if $x - y$ is a square, it must be the case that c is a nonzero square in $\mathbb{F}_p$. We conclude $\theta = \tau_{c,b}$. □

2.5.2 q is a prime power

Blokhuis generalized the previous result for all prime powers q [2]. We prove a series of lemmas that are a reproduction of Blokhuis' proof using graph theoretic terminology whenever possible.

Recall that the lines of $AG(2, q)$, considered as subsets of $\mathbb{F}_{q^2}$, can be partitioned into those with square differences in $\mathbb{F}_{q^2}$, say $\mathcal{L}_S$, and those with non-square differences in $\mathbb{F}_{q^2}$, say $\mathcal{L}_N$. There are $q + 1$ lines through 0 and exactly half of them correspond to lines in $\mathcal{L}_S$. Each line in $\mathcal{L}_S$ through 0 is incident to only square elements in $\mathbb{F}_{q^2}$, and each line in $\mathcal{L}_N$ through 0 is incident to only non-squares other than 0. Putting these simple observations together, we see that there are exactly $(q+1)/2$ non-squares on each line of $\mathcal{L}_S$ not passing through 0.

Let X be a clique in $P(q)$. Recall that if a is a nonzero square of $\mathbb{F}_{q^2}$, then

$$x - y \in S \iff ax - ay \in S$$

Thus aX is also a clique in $P(q)$. On the other hand, if a is a non-square in $\mathbb{F}_{q^2}$, then

$$x - y \in S \iff ax - ay \notin S$$

In this case, aX is an independent set in $P(q)$. For all a in $\mathbb{F}_{q^2}$ the set $X + a$ is a clique. Thus it suffices to consider cliques which contain 0. Otherwise we choose the translate of the clique which contains 0.

For notational purposes, let $\sigma_k(Y)$ denote the k^{th} elementary symmetric function of the finite set of vertices Y. In particular, we have the following.

$$\prod_{y \in Y}(1 + xt) = \sum_{k=0}^{|Y|} \sigma_k(Y) t^k.$$

Also, if 0 is an element of a finite set Y, let Y_0 denote the set $Y \setminus \{0\}$.

Now let X be a q-clique of $P(q^2)$. We assume that X contains 0, since otherwise we consider the q-clique $X - v$ for v in X that necessarily contains 0.

Define a polynomial $f(t)$ as follows.

$$f(t) := \prod_{x \in X_0}(t - x)$$

2.5.8 Lemma. *The vertices in X correspond to a line in $AG(2, q)$ if and only if the following equation holds.*

$$f(t) = t^{q-1} + \prod_{x \in X_0} x$$

Proof. Suppose that X corresponds to a line in $AG(2, q)$. From our earlier observations about $AG(2, q)$, we saw that each line though 0 is incident to the points $\{ia : i \in \mathbb{F}_q\}$ for some choice of nonzero a in $\mathbb{F}_{q^2}$. Therefore

$$\begin{aligned} f(t) &= \prod_{x \in X_0}(t - x) \\ &= \prod_{i \in \mathbb{F}_q}(t - ia). \end{aligned}$$

Choose an integer k such that $1 \leq k \leq q-1$, and let $\mathcal{H}$ denote the set of $q-k-1$-subsets of $\mathbb{F}_q^*$. Note that the coefficient of t^k can be expressed as

$$[t^k]f(t) = a^{q-1-k} \sum_{H \in \mathcal{H}} \prod_{i \in H} (-i).$$

Now we see that

$$f(t) = t^{q-1} + \prod_{x \in X_0} x.$$

On the other hand, suppose that

$$f(t) = t^{q-1} + \prod_{x \in X_0} x.$$

Since $f(x) = f(y) = 0$ for all x and y in X_0, we see that $x^{q-1} = y^{q-1}$ for all x and y in X_0. This implies that

$$X = \{ia : i \in \mathbb{F}_q\}$$

for some nonzero a. Therefore X is a line in $AG(2,q)$. □

Let A be a set of $(q+1)/2$ non-squares that form a clique in $P(q^2)$. An example of such a set is the non-squares incident to a line of $\mathcal{L}_S$ not passing through 0. We refer to such a set as a *special clique.* For two sets Y and Z, we define the set product as follows.

$$Y \cdot Z := \{yz : y \in Y, z \in Z\}$$

2.5.9 Lemma. *Let A be a special clique and let X be a q-clique containing 0. Then $A \cdot X_0$ is the set of all non-squares.*

Proof. Since the product of a non-square and a square in $\mathbb{F}_{q^2}$ is a non-square, every element in $A \cdot X_0$ is a non-square. There are $(q^2-1)/2$ products in $A \cdot X_0$, and so if each product is distinct, then $A \cdot X_0$ must contain all of the non-squares.

Suppose that

$$ax = by \tag{2.5.2}$$

for some a and b in A and some x and y in B. Subtracting bx from both sides from Equation 2.5.2 yields

$$(a-b)x = b(y-x).$$

Since a and b are in a clique, $a-b$ is a square, and so $(a-b)x$ is a square. Note that $b(y-x)$ is not a square unless $x=y$, but if $x=y$, then $a=b$. We conclude that $A \cdot X_0$ is the set of all nonzero squares. □

Now we define a second polynomial $f_a(t)$ for an element a from our special clique A.

$$f_a(t) := \prod_{x \in X_0} (t - ax)$$

2.5.10 Lemma. *For any special clique A, the following equation holds.*

$$\prod_{a \in A} f_a(t) = t^{\frac{1}{2}(q^2-1)} + 1$$

Proof. Let N denote the set of non-squares in $\mathbb{F}_{q^2}$. We apply Lemma 2.5.9 to our definition of $f_a(t)$.

$$\begin{aligned} f_a(t) &= \prod_{a \in A, x \in X_0} (t - ax) \\ &= \prod_{n \in N} (t - n) \\ &= t^{\frac{1}{2}(q^2-1)} + 1 \end{aligned}$$

Therefore the equality holds. □

We use this result to show that the k-th symmetric function of X_0 is 0 for small, positive k.

2.5.11 Lemma. *If X_0 is a q-clique in $P(q^2)$, then $\sigma_k(X_0) = 0$ for all positive k such that $k \leq (q^2-1)/2$.*

Proof. Let $m \leq (q-1)/2$ denote the smallest positive integer such that $\sigma_m(X) \neq 0$. If such an m does not exist, then we are done. Otherwise we express $f_a(t)$ in terms of a polynomial $p(t)$ of degree less than $q-1-m$.

$$f_a(t) = t^{q-1} + (-1)^m a^m \sigma_m(X_0) t^{q-m-1} + p(t)$$

Taking of the product of both sides over all a in A yields

$$\prod_{a \in A} f_a(t) = t^{\frac{1}{2}(q^2-1)} + (-1)^m \left(\sum_{a \in A} a^m \right) \sigma_m(X_0) t^{\frac{1}{2}(q^2-1)-m} + p'(t)$$

for a polynomial $p'(t)$ of degree less than $(q^2-1)/2 - m$.

Applying Lemma 2.5.10, we see that

$$t^{\frac{1}{2}(q^2-1)} + 1 = t^{\frac{1}{2}(q^2-1)} + (-1)^m \left(\sum_{a \in A} a^m \right) \sigma_m(X_0) t^{\frac{1}{2}(q^2-1)-m} + p'(t).$$

This implies

$$(-1)^m \left(\sum_{a\in A} a^m\right) \sigma_m(X_0) = 0.$$

However, we chose m such that $\sigma_m(X_0)$ was nonzero. Therefore

$$\sum_{a\in A} a^m = 0$$

for all special cliques A.

Define $A^{(s)}$ to be the following set.

$$A^{(s)} = \{a^s : a \in A\}$$

Suppose that a and b are in A, and so a and b are non-squares such that $a - b$ is a square. It follows that a^{-1} and b^{-1} are non-squares and

$$a^{-1} - b^{-1} = (ab)^{-1}(a - b)$$

is a square. Thus $A^{(-1)}$ is a special clique. Likewise a^q an b^q are both non-squares, and $a^q - b^q = (a - b)^q$ is also a non-square. Therefore $A^{(q)}$ is also a special clique.

From these observations we deduce that

$$\sum_{a\in A} a^{-qm} = 0$$

For any non-square n, we have

$$n^{(q^2-1)/2} = -1.$$

Combining this with our earlier result, we see that

$$\sum_{a\in A} a^{\frac{1}{2}(q^2-1)-qm} = 0$$

Let t be any element in $\mathbb{F}_{q^2}$ that is not contained in the $\mathbb{F}_q$ subfield, and let N denote the set of nonsquares of $\mathbb{F}_{q^2}$. All of the results shown thus far in this proof hold for any special clique A. Now we choose a specific special clique A such that

$$A = \{t + i : i \in \mathbb{F}_q, t + i \in N\}.$$

The following calculations hold.

$$\begin{aligned}0 &= 2\sum_{a\in A} a^{\frac{1}{2}(q^2-1)-qm}\\ &= 2\sum_{i\in\mathbb{F}_q, t+i\in N}(t+i)^{\frac{1}{2}(q^2-1)-qm}\\ &= \sum_{i\in\mathbb{F}_q}(t+i)^{\frac{1}{2}(q^2-1)-qm} + \sum_{i\in\mathbb{F}_q}(t+i)^{(q^2-1-qm)}\end{aligned}$$

Define the polynomial $F(t)$ to be the right hand side of the equation above. Note that $F(t) = 0$ for all t in $\mathbb{F}_{q^2}\setminus\mathbb{F}_q$. Since $F(t)$ has degree less that q^2-q, it follows that $F(t) = 0$ for all t in $\mathbb{F}_{q^2}$.

Finally, we consider the coefficient of t^{q^2-qm-q} in $F(t)$. It must be the case that

$$\binom{q^2-qm-1}{q-1}\sum_{i\in\mathbb{F}_q} i^{q-1} = 0$$

On the other hand, if we let p denote the characteristic of $\mathbb{F}_q$, then we see the that following two congruences hold:

$$\binom{q^2-qm-1}{q-1} \equiv 1 \pmod{p}$$

and

$$\sum_{i\in\mathbb{F}_q} i^{q-1} = q-1 \equiv -1 \pmod{p}.$$

This contradiction proves that no such m exists, which proves the lemma. □

Now we can apply Lemma 2.5.2 to prove the desired result.

2.5.12 Theorem. *If X is a maximal clique of $P(q^2)$, then X is a line of $\mathbb{F}_{q^2}$, considered as the affine plane $AG(2,q)$.*

Proof. Let X be a clique of size q in $P(q^2)$, and let x and y be two distinct vertices in X_0. Since x and y are both squares, it follows that x^{-1} and y^{-1} are both squares. Moreover, $x-y$ is a square, and so $x^{-1}y^{-1}(y-x)$ is also a square. Therefore $X_0^{(-1)}\cup 0$ is a q-clique. This implies that for positive m such that $m < \frac{1}{2}(q-1)$ we have

$$\sigma_{q-1-m}(X_0) = \prod_{x\in X_0} x\sigma_m(X_0^{(-1)}) = 0$$

From this we deduce $\sigma_m(X) = 0$ for all positive m such that $m < \frac{1}{2}(q-1)$ and

$$f(t) = t^{q-1} + \prod_{x \in X_0} x.$$

□

2.5.13 Corollary. *Each pair of adjacent vertices of $P(q^2)$ is contained in exactly one maximal clique.* □

Chapter 3

Peisert Graphs

As we saw in the previous section, Paley graphs have several remarkable properties. Most notably they are both self-complementary and arc-transitive. It is plausible to believe they are the only infinite family of self-complementary arc-transitive graphs. However, Peisert recently discovered a second infinite family of graphs that possess both properties [19]. We refer to this new family of graphs as Peisert graphs.

We proceed in a similar manner to Chapter 2. We begin by constructing Peisert graphs on the points of a finite field. Using this definition we show that Peisert graphs are self-compementary and arc-transitive. Then we give an alternate construction of Peisert graphs of order q^2 where $q \equiv 3 \pmod 4$ as graphs over the points of $AG(2,q)$. Using this second construction we apply Theorem 2.5.4 and Theorem 2.5.12 to obtain new information about the maximal cliques of those orders of Peisert graphs. For Peisert graphs of order q^2 where $q \equiv 1 \pmod 4$, we prove that any pair of vertices contained in a clique of size q must be contained in at least two cliques of size q. By Corollary 2.5.13, this new result implies that the number of cliques of size q in Peisert graphs in this cases differ from the corresponding number in Paley graphs. We also show that certain subgraphs of these Peisert graphs are isomorphic to the Paley graph of order q.

3.1 Standard Construction and Properties

The construction of Peisert graphs given in Peisert's paper is remarkably similar to the standard construction of Paley graphs. Let p be a prime such that $p \equiv 3 \pmod 4$, and let q denote an even power of p. Let ω denote a primitive root of $\mathbb{F}_q$, and let M be defined as follows.

$$M = \{\omega^i : i \equiv 0, 1 \pmod 4\}$$

The *Peisert graph* of order q, denoted $P^*(q)$, is the Cayley graph constructed on the additive group of $\mathbb{F}_q$ using M as the connection set.

Let M_0 denote the multipicative subgroup of $\mathbb{F}_q$ generated by ω^4. Note that the elements in M can be partitioned into M_0 and the multiplicative coset ωM_0. Our constraints on p and q imply that $q \equiv 1 \pmod 8$. Since $-1 = \omega^{\frac{q-1}{2}}$, it follows that $-1 \in M_0$. Therefore M is closed with respective to additive inverses, as required for the connection set of a Cayley graph.

There are many similarities between Peisert graphs and Paley graphs. The following result, due to Peisert [19], highlights the first similarity.

3.1.1 Lemma. *Peisert graphs are arc-transitive.*

Proof. Let θ denote the permutation of $\mathbb{F}_q$ defined by

$$\theta : x \mapsto \omega^4 x.$$

We see that $x - y = \omega^i$ for some $i \equiv 0, 1 \pmod 4$ if and only if

$$\theta(x) - \theta(y) = \omega^{i+4}.$$

This implies that θ is an automorphism of $P^*(q)$. Recall that $M = M_0 \cup \omega M_0$ and M_0 is generated multiplicatively by ω^4. It follows that the subgroup generated by θ fixes 0 and acts transitively on M_0, and so it also acts transitively on ωM_0.

Let p denote the characteristic of $\mathbb{F}_q$, and recall that $x \mapsto x^p$ is an automorphism of $\mathbb{F}_q$. Let γ denote the permutation of $\mathbb{F}_q$ defined by

$$\gamma : x \mapsto \omega x^p.$$

In order to show γ is an automorphism of $P^*(q)$, we consider two cases. First, if $x - y = \omega^{4k}$ for some k, then

$$\begin{aligned}\gamma(x) - \gamma(y) &= \omega x^p - \omega y^p \\ &= \omega(x - y)^p \\ &= \omega\omega^{4kp} \\ &= \omega^{4kp+1}.\end{aligned}$$

Second, if $x - y = \omega^{4k+1}$ for some k, then

$$\begin{aligned}\gamma(x) - \gamma(y) &= \omega(x-y)^p \\ &= \omega\omega^{4kp+p} \\ &= \omega^{4kp+p+1}.\end{aligned}$$

Recall that $p \equiv 3 \pmod 4$, and so $4kp + p + 1 \equiv 0 \pmod 4$. This implies that $\gamma(x) - \gamma(y) = \omega^{4s}$ for some s. From this we see that γ is an automorphism of $P^*(q)$ that interchanges M_0 and ωM_0. Therefore the subgroup generated by θ and γ fixes 0 and acts transitively on the neighbours of 0. Since the automorphism group of any Cayley graph acts transitively on the vertices, we conclude that the automorphism group acts transitively on the arcs of $P^*(q)$. □

Next we show Peisert graphs are also self-complementary. This result is also due to Peisert [19].

3.1.2 Lemma. *Peisert graphs are self-complementary.*

Proof. Let σ denote the permutation on $\mathbb{F}_q$ which maps x to $\omega^2 x$. Note that $x - y = \omega^i$ where $i \equiv 0, 1 \pmod 4$ if and only if $\sigma(x) - \sigma(y) = \omega^{i+2}$. This implies x and y are adjacent in $P^*(q)$ if and only if $\sigma(x)$ and $\sigma(y)$ are nonadjacent. Therefore σ is an isomorphism from $P^*(q)$ to its complement □

Finally, as a corollary to Lemma , we see that Peisert graphs are strongly regular.

3.1.3 Corollary. *Peisert graphs are strongly regular.* □

3.2 Affine Plane Construction

Similar to our affine plane construction of the Paley graph $P(q^2)$, we construct the Peisert graph $P(q^2)$ for $q \equiv 3 \pmod 4$ using affine planes.

First we consider the elements of $\mathbb{F}_{q^2}$ as points of the affine plane $AG(2, q)$ as described in Section 2.4. Recall that we have the following vector space isomorphism ψ from $\mathbb{F}_{q^2}$, considered as a two-dimensional vector space over $\mathbb{F}_q$, to $\mathbb{F}_q \times \mathbb{F}_q$.

$$\psi : (a + b\lambda) \to (a, b)$$

where $\lambda^2 = \alpha$ for some fixed nonsquare α in $\mathbb{F}_q$. Recall that lines in $AG(2, q)$ with slope y in $\mathbb{F}_q$ correspond to translates of the line

$$l_y = \{(c, cy) : c \in \mathbb{F}_q\}$$

The lines in $AG(2,q)$ with slope ∞ correspond to translates of the line

$$l_\infty = \{(0,c) : c \in \mathbb{F}_q\}$$

Let ω denote a multiplicative generator of $\mathbb{F}_{q^2}$, and recall that the q-subfield is generated by ω^{q+1}. Since $q \equiv 3 \pmod 4$, we see that $q+1 = 4k$ for some positive integer k. Therefore multiplication by any power of ω^{q+1} fixes the connection set M of $P^*(q^2)$. This implies that the elements of the vector space $\mathbb{F}_q \times \mathbb{F}_q$ corresponding to elements of M are closed under scalar multiplication by elements of $\mathbb{F}_q$. Therefore we have

$$\psi^{-1}(1,y) \in M \iff \psi^{-1}(c,cy) \in M$$

for all y in $\mathbb{F}_q$ and all nonzero c in $\mathbb{F}_q$. We also have

$$\psi^{-1}(0,1) \in M \iff \psi^{-1}(0,c) \in M$$

for all nonzero c in $\mathbb{F}_q$.

From these observations, it follows that we can partition the elements in the vector space corresponding to elements of M into $(q+1)/2$ one-dimensional vector spaces. Each of these one-dimensional vector spaces corresponds to a line l_y in $AG(2,q)$ with slope y such that $\psi^{-1}(1,y) \in M_0$ or $\psi^{-1}(1,y) \in \omega M_0$.

Recall that two vertices in the Peisert graph constructed on $\mathbb{F}_q^2$ are adjacent if and only if their difference is contained in M. Identifying the elements of $\mathbb{F}_q^2$ as points of $AG(2,q)$, we see that two vertices in the Peisert graph are adjacent if and only if they are incident to a common line with slope y in $\mathbb{F}_q$ such that $\psi^{-1}(1,y) \in M$ or they are incident to a common line with slope ∞ and $\psi^{-1}(0,1) \in M$. This verifies the following alternative construction of $P^*(q)$.

3.2.1 Construction. Let $q = p^r$ for some prime p such that $p \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$. Let ω denote a multiplicative generator of $\mathbb{F}_{q^2}$, and let M_0 denote the multiplicative subgroup generated by ω^4. Let $\hat{M}$ denote the subset of slopes of $AG(2,q)$ such that

$$m \in \hat{M} \iff \psi^{-1}(1,m) \in M_0 \cup \omega M_0.$$

Let G denote the graph constructed on the points of $AG(2,q)$, considered as elements of $\mathbb{F}_q \times \mathbb{F}_q$, where two points x and y are adjacent if and only if they are incident to a line with slope m such that $m \in \hat{M}$. Then G is isomorphic to the Peisert graph $P^*(q^2)$.

If $q \equiv 1 \pmod 4$, then $q+1 \equiv 2 \pmod 4$. Thus the elements of M in $P^*(q^2)$ are not closed under multiplication by all powers of ω^{q+1} in this case, and so we do have a straightforward construction of $P^*(q^2)$ using the lines of $AG(2,q)$ to define adjacency. However, we make the following observation.

3.2.2 Lemma. *The vertices in $P^*(q^2)$ corresponding to the unique subfield of order q in $\mathbb{F}_{q^2}$ induce a subgraph that is isomorphic to the Paley graph $P(q)$.*

Proof. Since $2k(q+1) \equiv 0 \pmod 4$ for all integers k, it follows that M is closed under multiplication by powers of $\omega^{2(q+1)}$. Notice that the subgroup generated by $\omega^{2(q+1)}$ is precisely the set nonzero squares of the subfield of order q. Therefore two points in $\mathbb{F}_q$ will be adjacent if and only if their difference is a nonzero square in $\mathbb{F}_q$. Thus the subgraph induced by the elements of $\mathbb{F}_q$ will be the Paley graph $P(q)$. □

This result implies that if we identify the vertices of $P^*(q^2)$ with the points of $AG(2,q)$ as above, then the lines of $AG(2,q)$ will all induce subgraphs isomorphic to the Paley graph $P(q)$.

3.3 Maximal Cliques

We have seen many similarities between the Paley and Peisert graphs, and so it is reasonable to expect the size of the maximal clique to be the same in $P(q^2)$ and $P^*(q^2)$. Recall from Section 2.5 that the largest clique in the Paley graph $P(q)$ has size q. The following result is useful to determine an upper bound on the size of a maximal clique in $P^*(q^2)$. We do not provide the details here, but the proof follows from results given in Godsil and Royle's text ([10] Ch. 10).

3.3.1 Lemma. *Let G be a self-complementary strongly regular graph on q^2 vertices. Then the least eigenvalue of the adjacency matrix of G is*

$$(-1-\sqrt{q})/2 \qquad \square$$

It follows from this lemma that the least eigenvalue of the Peisert graph $P^*(q^2)$ is $(-1-\sqrt{q})/2$, and thus from the application of Lemma 2.5.1 we deduce that the largest clique in $P^*(q^2)$ has size at most q.

If $q \equiv 3 \pmod 4$, then this bound is obtained. However, when $q \equiv 1 \pmod 4$ the size of a maximal clique may be less that q. We consider each case separately.

3.3.1 $q \equiv 3 \pmod 4$

For this case, it is easy to show that the subfield of order q forms a clique of size q.

3.3.2 Lemma. *When $q \equiv 3 \pmod 4$, the vertices corresponding to the unique subfield of order q in $\mathbb{F}_{q^2}$ form a clique of size q in $P^*(q^2)$.*

Proof. Let ω be a primitive root of $\mathbb{F}_{q^2}$. Recall that the subfield of order q is generated by ω^{q+1}. Since $q \equiv 3 \pmod 4$, this implies the elements in the subfield are all contained in the subgroup generated by ω^4. Therefore each element in the subfield is contained in M. Since the subfield is closed under addition and additive inverse, we conclude that the elements in the subfield form a clique of size q. □

From our work in Section 3.2, we see that when $q \equiv 3 \pmod 4$, we can construct $P^*(q)$ on the points of the affine plane $AG(2, q)$. Therefore the lines with slopes corresponding to elements in M form cliques of size q, and so we see that Peisert graphs have at least $(q + 1)/2$ maximal cliques on 0 in this case. In particular, if q is prime, then the following corollary to Theorem 2.5.4 implies that there are exactly $(q + 1)/2$ maximal cliques on 0 in this case.

3.3.3 Corollary. *Let p be an odd prime such that $p \equiv 3 \pmod 4$. If a set of p vertices in the Peisert graph $P^*(p^2)$ forms a clique, then they are incident to a common line in $\mathbb{F}_{p^2}$ considered as the affine plane $AG(2, p)$.* □

If q is a nontrivial prime power, then we apply Blockhuis' result to gain limited information about the cliques of size q. Recall that $M = M_0 \cup \omega M_0$ is the neighbourhood of 0, where we have

$$M_0 = \{\omega^{4k} : 0 \leq k \leq (q^2 - 1)/4\}.$$

Note that each element in M_0 is a square, and therefore we have the following corollary to Theorem 2.5.12.

3.3.4 Corollary. *Let X be a maximal clique of $P^*(q)$ where $q \equiv 3 \pmod 4$. If the difference between every distinct pair of elements of X is contained in M_0, then X is a line of $\mathbb{F}_{q^2}$, considered as the affine plane $AG(2, q)$.* □

The same result holds for a maximal clique X in $P^*(q^2)$ where the differences between distinct elements of X are completely contained in ωM. This does not completely characterize the maximal cliques as Blockhuis's result does for Paley graphs, but it is a start. It implies that any maximal cliques on 0 that do not correspond to a line of $\mathbb{F}_{q^2}$ must contain elements from both M_0 and ωM_0. Therefore, if we could eliminate the possibility of such cliques existing, then we could deduce that each maximal clique corresponds to a line.

3.3.2 $q \equiv 1 \pmod 4$

When $q \equiv 1 \pmod 4$ and q is prime, there is no Peisert graph of order q^2. Thus Rédei's result cannot be applied to any Peisert graphs in this case. Moreover, since we do not have a convenient construction of $P^*(q^2)$ on the points of $AG(2, q)$ when $q \equiv 1 \pmod 4$, we cannot easily get any information about the cliques using Blockhuis' result.

Peisert gives the following lower bound on the size of a maximal clique in $P(q^2)$ when $q \equiv 1 \pmod 4$ [13].

3.3.5 Lemma. *The size of a maximal clique in $P^*(q^2)$ where $q \equiv 1 \pmod 4$ is at least $q^{\frac{1}{4}}$.*

Proof. By the definition of Peisert graphs, we must have $q = p^r$ for some prime p such that $p \equiv 3 \pmod 4$. Since $q \equiv 1 \pmod 4$, it follows that r is even, and so $r = 2s$ for some positive integer s. Note that the unique subfield of order p^s in $\mathbb{F}_{q^2}$ is generated by ω^d where

$$\begin{aligned} d &= \frac{p^{4s} - 1}{p^s - 1} \\ &= (p^s + 1)(p^{2s} + 1). \end{aligned}$$

Therefore $d = 4k$ for some integer k, and it follows that the subfield of order p^s is contained in M_0, the multiplicative group generated by ω^4. It follows that the difference between any two elements in the subfield is contained in M_0, and so the elements of the subfield form a clique of size p^s. □

There are many cases of Peisert graphs $P^*(q^2)$ that obtain the upper bound with cliques of size q when $q \equiv 1 \pmod 4$. Here we show that if $P^*(q^2)$ has a clique of size q, then there are at least two cliques of size q on each pair of adjacent vertices in these graphs. This gives an elementary way to distinguish $P^*(q^2)$ from $P(q^2)$ when $q \equiv 1 \pmod 4$.

Recall that Peisert graphs are vertex-transitive, and therefore it suffices to consider maximal cliques containing 0. We refer to a clique containing 0 as a *central clique*. Here we prove that there are at least two maximal central cliques on each neighbour of 0 in $P^*(q^2)$ where $q \equiv 1 \pmod 4$. As a consequence, we show that the number of cliques of size q in $P^*(q^2)$ when $q \equiv 1 \pmod 4$ differs from the number in the Paley graph of the same order. This is original work.

3.3.6 Lemma. *Let $q = p^{2r}$ be a prime power such that $p \equiv 3 \pmod 4$. If $P^*(q^2)$ has at least one clique of size q, then each vertex in the neighbourhood of 0 in $P(q^2)$ is contained in at least two central cliques of size q.*

Proof. Suppose $P^*(q^2)$ has at least one clique of size q. This clique must be maximal with respect to size. Since $P^*(q^2)$ is vertex transitive, we can assume this clique contains 0. (Otherwise we consider a translation of the clique which contains 0.) Since Peisert graphs are arc-transitive, each vertex in M must be contained in the same number of maximal central cliques. Assume for a contradiction that each vertex in the neighbourhood of 0 is contained in exactly one maximal central clique. Using this observation, we partition M into $(q+1)/2$ sets of size $q-1$ corresponding to the maximal central cliques. Let C denote the unique clique in this set which contains 1.
Claim 1: $|C \cap M_0| = (q-1)/2$
Let r denote the number of elements in C that are contained in M_0. Suppose for a contradiction that $r > (q-1)/2$. It follows that C contains less than $(q-1)/2$ elements of ωM_0. Recall that $\omega^{4i}C$ is also a maximal central clique for all integers i. Since multiplication by ω^{4i} is an automorphism that fixes M_0 set-wise, there also must be exactly r elements of M_0 and $q-1-r$ elements of ωM_0 in $\omega^{4i}C$. Since each element of M_0 is contained in exactly one maximal central clique, the orbit of C under multiplication by ω^{4i} must have size at most $|M_0|/r$. On the other hand, since ω^{4i} is transitive on the elements of M_0, the orbit of C must have order exactly $|M_0|/r$. Note that $|M_0|/r < q+1$. This implies that the union of the sets in the orbit of C contains at most $(q+1)(q-1-r)$ elements of ωM_0.

Since $q \equiv 1 \pmod 4$, we see that $q-1$ does not divide $\frac{q^2-1}{2}$. Therefore $r < q-1$, and it follows that there must be at least one element of ωM_0 in a set in the orbit of C_0. Furthermore we see that

$$(q+1)(q-1-r) < (q^2-1)/2,$$

and so there must be at least one element of ωM_0 not contained in a set in the orbit of C_0. This contradicts the transitivity of ω^4 on ωM_0. Thus $r \leq (q-1)/2$.

If we assume that $r < (q-1)/2$, then we can apply the argument above to show that the number of elements of ωM_0 contained in C is less that $(q-1)/2$. From this we conclude that $r = (q-1)/2$, which proves the first claim.

Claim 2: *The set of elements in $M_0 \cap C$ form a multiplicative subgroup of $\mathbb{F}^*_{q^2}$.*
Let x and y be two elements of $C \cap M_0$. It follows that $x^{-1}y \in M_0$. Since multiplication by an element of M_0 is an automorphism of $P^*(q^2)$, the set $x^{-1}yC$ is a maximal central clique containing y. However, there is exactly one maximal central clique containing y, and so we must have $x^{-1}yC = C$. Therefore $x^{-1}y \in C$ for all elements x and y in C. Since $C \cap M_0$ contains 1, this proves the second claim.

Combining the results of Claim 1 and Claim 2, we see that $C \cap M_0$ is a multiplicative subgroup of $\mathbb{F}^*_{q^2}$ such that

$$\frac{|\mathbb{F}^*_{q^2}|}{|C \cap M_0|} = 2(q+1). \tag{3.3.1}$$

From Equation 3.3.1 we deduce that $C \cap M_0$ is generated multiplicatively by $\omega^{2(q+1)}$, and so $C \cap M_0$ contains the squares of multiplicative group of the subfield of order q. From our work with Paley graphs, we know that each nonsquare of F^*_q can be expressed as the difference of two squares. Therefore there must be two distinct elements elements of $C \cap M_0$ whose difference is ω^{q+1}. However, since $q \equiv 1 \pmod 4$, the element ω^{q+1} is not contained in $M_0 \cup \omega M_0$. This contradicts our assumption that C is a clique. Therefore each vertex must be contained in at least two maximal central cliques. □

3.4 Computational Results

The following computations were performed on a computer with a 2.8 Ghz processor using a combination of SAGE [21] and Cliquer [17] routines. The results for small Peisert graphs are shown in the table below. The graph on 7^4 is the smallest $P^*(q^2)$ that does not have a maximal clique of size q.

Table 3.1: **Peisert Graphs**

q^2	Max Clique Size	# Max Cliques on 0
3^2	3	2
7^2	7	4
3^4	3^2	10
11^2	11	6
19^2	19	10
23^2	23	12
7^4	17	15300

Chapter 4

Self-Complementary Arc-Transitive Graphs

We have seen that the Paley graphs and Peisert graphs are self-complementary and arc-transitive. In this section we see a complete description of all self-complementary arc-transitive graphs. First, we see a result of Zhang which states that self-complementary arc-transitive graphs must be Cayley graphs on the additive group of a vector space with a particular connection set. Then we see a result of Peisert which gives a stronger algebraic characterization of a self-complementary arc-transitive graphs in terms of the automorphism groups of the graphs. Finally we see how Peisert uses this characterization in conjunction with results about primitive permutation groups to show that Paley graphs, Peisert graphs, and one additional graph on 23^2 vertices are the only self-compementary arc-transitive graphs.

Before beginning, we clarify our use of terminology. Throughout this chapter, we refer to a graph as *symmetric* if it is both vertex transitive and arc-transitive. This definition is common in algebraic graph theory and is used in Biggs' text [1] and Godsil and Royle's text [10]. As a word of caution, we note that most of the works referenced in this chapter, including the papers of Peisert [19], Zhang [25], and Chao [5], define symmetric graphs as graphs that are vertex and edge transitive. An arc-transitive graph is edge transitive, but the converse is not true. This is discussed in more detail in Biggs' text [1]. However, a result of Zhang proves that any self-complementary vertex and edge transitive graph must also be arc-transitive [25]. Therefore the results presented in this chapter hold for both definitions of symmetric graphs.

4.1 Algebraic Characterization

The following lemma and theorem are due to Hong Zhang [25]. The theorem was the first major step towards a complete algebraic characterization of self-complementary symmetric graphs. The lemma gives another reason for the necessity of $q \equiv 1 \pmod 4$ for the Paley graph $P(q)$.

4.1.1 Lemma. *If a graph X on n vertices is self-complementary and symmetric, then $n \equiv 1 \pmod 4$.*

Proof. Since the graph X is vertex transitive, each vertex must have the same number of neighbours, say k. Furthermore, since X is self-complementary, each vertex in the complement of X must also have k neighbours. Therefore we have $k = (n-1)/2$, which implies n is odd. Moreover, there must be $n(n-1)/4$ edges in X. Since n is odd, it follows that $n \equiv 1 \pmod 4$. □

Zhang also proves that the automorphism group of a self-complementary symmetric graph must be a normal subgroup of index 2 in a doubly transitive group with index 2. Utilizing deep algebraic results, Zhang gives the following algebraic characterization of self-complementary symmetric graphs.

4.1.2 Theorem. *A graph is self-complementary and symmetric if and only if it is isomorphic to a Cayley graph $X(V_+, O_H)$, where*

a) V_+ is the additive group of the vector space V of dimension r over the finite field with p elements, and $p^r \equiv 1 \pmod 4$.

b) O_H is an orbit of a group H such that

i) $H \subset \hat{H} \subset GL(V)$

ii) $[\hat{H} : H] = 2$

iii) $\hat{H}$ is transitive on $V \setminus \{0\}$

iv) H is not transitive on $V \setminus \{0\}$ □

We have already seen the construction of the self-complementary symmetric Paley graphs on p^r vertices where p is an odd prime and r is a positive integer such that $p^r \equiv 1 \pmod 4$. Therefore the following corollary holds.

4.1.3 Corollary. *There exists a self-complementary symmetric graph on n vertices if and only if $n = p^r$ for some odd prime p and positive integer r such that $p^r \equiv 1 \pmod 4$.* □

Using Chao's classification of vertex- and edge-transitive graphs with a prime number of vertices [5], Peisert shows that the only self-complementary symmetric graphs on a prime number of vertices are Paley graphs [18]. If we consider self-complementary symmetric graphs that are circulants, then Zhang shows that the only such graphs are also Paley graphs of prime order [26].

In [19], Peisert gives a full description of self-complementary symmetric graphs and their automorphism groups.

For a graph G, denote the group of all automorphisms by $Aut(G)$. Let $\Gamma(G)$ denote the group of permutations on the vertex set generated by the group of automorphisms and the set of complementing permutations. Peisert gives the following one-to-one correspondence between the self-complementary symmetric graphs and permuation groups with special properties.

4.1.4 Lemma. *Let G be a self-complementary symmetric graph, $\mathcal{A} = Aut(G)$, and $\Gamma = \Gamma(G)$. Then the following hold:*

a) $|G| \equiv 1 \pmod 4$

b) Γ *is doubly transitive*

c) $\mathcal{A}$ *is a rank-3 group*

d) $[\Gamma : \mathcal{A}] = 2$

e) $|\mathcal{A}|$ *is even* □

Peisert also gives a partial converse to this lemma. To understand it, we introduce the following notation.

4.1.5 Definition. An *orbital* of a permutation group Γ on a set V is an orbit of Γ in its natural action on the Cartesian product $V \times V$.

If Γ is transitive, then the number of orbitals is the rank of Γ. If an orbital Δ is not the diagonal, then the digraph with vertex set V and edge set Δ is denoted by $Graph(\Delta)$. If for each element (x, y) in Δ, there exists an element (y, x) in Δ, then we identify $Graph(\Delta)$ with the corresponding undirected graph.

4.1.6 Lemma. *Let $\mathcal{A}$ and Γ be permutation groups satisfying conditions (b)-(e) of Lemma 4.1.4. Let G and G' be the nontrivial orbitals of $\mathcal{A}$. Then both $Graph(G)$ and $Graph(G')$ are undirected graphs, and G and G' are* *self-complementary, symmetric, and isomorphic to each other. Moreover, $\mathcal{A} \leq Aut(G)$ and $\Gamma \leq \Gamma(G)$. The equalities hold if and only if $\mathcal{A}$ is a maximal rank-3 group.* □

As an immediate consequence of Lemmas 4.1.4 and 4.1.6, Peisert gives the following algebraic characterization of self-complementary symmetric graphs.

4.1.7 Theorem. *Let Γ be a doubly transitive group, and let $\mathcal{A}$ be a subgroup of index 2 in Γ which is not doubly transitive and has even order. Then the orbitals of $\mathcal{A}$ are self-complementary symmetric graphs, and every self-complementary symmetric graph can be constructed in this way.* □

4.2 Possible Automorphism Groups

Using the necessary conditions for the automorphism groups of a self-complementary symmetric graph given in Lemma 4.1.4, Peisert narrows the possible automorphism groups of such graphs by applying deep results from permutation group theory.

4.2.1 Definition. The *socle* of a permutation group Γ is the subgroup of Γ generated by all the minimal normal subgroups.

Peisert uses the Burnside theorem and classification of finite simple groups to deduce that the automorphism group of every self-complementary symmetric graph is a rank-3 primitive group with equal subdegrees and an elementary abelian socle. Using Liebeck's classification, Peisert distinguishes four possible cases where the condition is satisfied.

Case 1 The group has degree 9.

This case is trivial. It can be verified that the Paley graph of order 9 is the only self-complementary vertex-transitive graph on 9 vertices.

Case 2 The group is contained in $A\Gamma L_1(p^r)$.

Before exploring this case, we clarify more useful notation. Let ω denote a fixed primitive root of $\mathbb{F}_{p^r}$ as well as denote the corresponding scalar multiplication which maps x to ωx. Let α denote the Frobenius automorphism of $\mathbb{F}_{p^r}$. That is, the automorphism α maps x to x^p. We let $\langle \omega, \alpha \rangle$ denote the subgroup of the automorphism group of $\mathbb{F}_{p^r}$ generated by ω and α.

4.2.2 Definition. Let $\gamma = \omega^{k_1}\alpha^{m_1}\omega^{k_2}\alpha^{m_2}\cdots\omega^{k_t}\alpha^{m_t}$ be an element of the subgroup generated by ω and α. We say that γ is *ω-even* (*ω-odd*) if $k_1 + \cdots + k_t$ is even (odd). A subgroup of $\langle\omega, \alpha\rangle$ will be called *ω-odd* if it contains at least one *ω-odd* element. Otherwise, it is *ω-even*.

It can be shown that the ω-parity of an element of $\langle\omega, \alpha\rangle$ does not depend on its representation and is preserved by conjugation. From these two observations, it is straightforward to see that a subgroup of $\langle\omega, \alpha\rangle$ is ω-even if and only if its generators are ω-even.

Consider the two-dimensional vector space over $\mathbb{F}_{p^r}$ and the underlying affine and projective groups. Let $\zeta : \Gamma L_2(p^r) \to P\Gamma L_2(p^r)$ be the natural homomorphism. Let T be the group of translations contained in $A\Gamma L_2(p^r)$. We use the notation TK to denote the subgroup of $A\Gamma L_2(p^r)$ which is a split extension of T by a subgroup K of ΓL_2. Since $\mathcal{A} \subseteq T$ and T is regular and normal in $A\Gamma L_1(p^r)$, it follows that $\mathcal{A}$ is the split extension $T\mathcal{A}_0$ of T by the stabilizer $\mathcal{A}_0 \subseteq \Gamma L_2(p^r)$.

4.2.3 Lemma. *Let G be a self-complementary symmetric graph whose automorphism group $\mathcal{A}$ is a ω-even subgroup of $A\Gamma L_1(p^r)$. Then G is a Paley graph and $Aut(G) = T\langle\omega^2, \alpha\rangle$.*

Proof. From our work in Chapter 2, we see that $T\langle\omega^2, \alpha\rangle$ is a subgroup of the automorphism group of $P(p^r)$. Moreover we can see that

$$|T\langle\omega^2, \alpha\rangle| = \frac{rp^r(p^r - 1)}{2}.$$

Since it is known that $|\mathcal{A}| = (rp^r(p^r - 1))/2$, we deduce that

$$\mathcal{A} = T\langle\omega^2, \alpha\rangle.$$

Note that all ω-even subgroups are contained in $T\langle\omega^2, \alpha\rangle$. By Lemmas 4.1.4 and 4.1.6, we know the automorphism group of a self-complementary graph must be a maximal rank-3 group. The result follows. □

A similar result can be proved for ω-odd groups, although we do not show the details here.

4.2.4 Lemma. *Let G be a self-complementary symmetric graph whose automorphism group $\mathcal{A}$ is a ω-odd subgroup of $A\Gamma L_1(p^r)$. Then G is a Peisert graph.* □

The automorphism groups of the Peisert graphs vary for different values of p^r. Thus it is not always the case that

$$Aut(P^*(p^r)) = T\langle \omega^4, \omega\alpha \rangle.$$

After more work, Peisert gives the following result about the automorphism groups of Peisert graphs.

4.2.5 Lemma. *If* $p^r \neq 3^2, 7^2, 3^4, 23^2$ *then*

$$Aut(P^*(p^r)) = T\langle \omega^4, \omega\alpha \rangle.$$

Furthermore, we have

$$|Aut(P^*(p^r))| = \frac{rp^r(p^r-1)}{4}. \qquad \square$$

Case 3 The group is solvable.

Peisert uses the Foulser's classification theorem [9] to explore two possible groups of degree 7^2 and 23^2. We reproduce the explicit construction of the graphs and summarize the proof that they are self-complementary and symmetric.

Recall that $\zeta : \Gamma L_2(n) \to P\Gamma L_2(n)$ is the natural homomorphism from $\Gamma L_2(n) \to P\Gamma L_2(n)$, and that T is the group of translations contained in $A\Gamma L_2(n)$.

Let S_4 denote the symmetric group of degree four, and let A_4 denote the subgroup of S_4 consisting of all even permutations. Let J and $\bar{J}$ be subgroups of $PSL_2(n)$ such that $J \subseteq \bar{J}$, $J \cong A_4$, and $\bar{J} \cong S_4$. The existence of such subgroups is known from Foulser [9]. Define

$$\mathcal{A}(n^2) = T\zeta^{-1}(J)$$

Also define

$$\Gamma(n^2) = T\zeta^{-1}(\bar{J}).$$

From Foulser and Kallaher [8], we see that for $n = 7$ or $n = 23$ the group $\mathcal{A}(n^2)$ is a maximal rank-3 group with order $12n^2(n-1)$. Again from Foulser [9], we see for these values of n that $\Gamma(n^2)$ is doubly transitive of order $24n^2(n-1)$. Therefore we must have

$$[\Gamma(n^2) : \mathcal{A}(n^2)] = 2.$$

By Lemma 4.1.6, we conclude the orbitals of the graphs are self-complementary symmetric graphs.

Utilizing more results from Foulser [9], it can be shown that this construction gives just one rank-3 group up to conjugation. The graphs constructed from these groups is denoted by $G(7^2)$ and $G(23^2)$, respectively.

Case 4 The exceptional group.

By a result from Liebeck [14], there is only one additional group satisfying the necessary requirements. Again we give the explicit construction and summarize the Peisert's proof that the constructed graph is indeed self-complementary and symmetric.

Since $PSL_2(9)$ is isomorphic to A_6, there exists a subgroup $J \leq PSL_2(9)$ such that J is isomorphic to A_5. From Foulser's work [9], we know that J has a unique minimal pre-image J^* under ζ. Let c be the scalar multiplication by a fixed primitive root of $\mathbb{F}_9$ and σ be a permutation defined as follows.

$$\sigma : (a, b) \to (a^3, b^3) \tag{4.2.1}$$

We define

$$\mathcal{A}(9^2) = T\langle J^*, c^2, \sigma\rangle$$

where $\langle J^*, c^2, \sigma\rangle$ denotes the subgroup of $\Gamma L_2(9)$ generated by J^*,c^2, and σ. Also define

$$\Gamma(9^2) = T\langle J^*, c, \sigma\rangle.$$

Again from Foulser's results [9], we have that $\mathcal{A}(9^2)$ is a maximal rank-3 group and $|\mathcal{A}(9^2)| = 60 \cdot 8 \cdot 81$. We also have that $\Gamma(9^2)$ is double transitive of order $\Gamma(9^2) = 2|\mathcal{A}(9^2)|$. By Lemma 4.1.6, we conclude that the nontrivial orbitals of $\mathcal{A}(9^2)$ are isomorphic self-complementary symmetric graphs. Using Foulser's work again we see that this construction gives us one rank three group, up to conjugation. We denote the corresponding graph by $G(9^2)$.

4.3 Isomorphisms

From cases presented in Section 4.2, we see that a self-complementary symmetric graph must be a Paley graph, Peisert graph, or one of the three exceptional graphs $G(7^2)$, $G(9^2)$, and $G(23^2)$. We wish to determine if there are duplications among this list.

First we distinguish between the Paley and Peisert graphs. When $p^r \neq 3^2$ and $p^r \neq 7^2$ a result of Foulser and Kallaher [8] can be applied to what is known about the automorphism groups from Section 4.2 to distinguish the corresponding Paley and Peisert graphs. We have already seen that $P^*(3^2)$ is isomorphic to $P(3^2)$. Peisert also shows that $P^*(7^2)$ is not isomorphic to $P(7^2)$. This leaves us with the following.

4.3.1 Lemma. *If $p \equiv 3 \pmod 4$, then $P^*(p^r)$ is not isomorphic to $P(p^r)$, except when $p^r = 3^2$.* □

It is known that there are only two self-complementary vertex transitive strongly regular graphs on 7^2 vertices [16]. Since the automorphism groups of $P(7^2)$ and $G(7^2)$ have different orders, it follows from Lemma 4.3.1 that $P^*(7^2)$ is isomorphic to $G(7^2)$.

Despite having an exceptional automorphism group, Peisert proves that $G(9^2)$ is isomorphic to $P^*(9^2)$. He then proves that $G^*(23^2)$ is not isomorphic to $G(23^2)$. Both of these results were obtained by distinguishing between the automorphism groups.

Putting all of this work together, Peisert proves the desired result.

4.3.2 Theorem. *A graph is self-complementary and arc-transitive if and only if $|G| = p^r$ for some prime p, $p^r \equiv 1 \pmod 4$, and G is a Paley graph or a Peisert graph, or is isomorphic to an exceptional graph on 23^2 vertices.* □

Chapter 5

Geometric Graphs

We have seen constructions of Paley and Peisert graphs, and we have also seen they are the only infinite families of self-complementary arc transitive graphs. Now we investigate graphs that are similar to Paley and Peisert graphs. We have already seen that Paley and Peisert graphs are strongly regular graphs. In this chapter we see that Paley and Peisert graphs have the same parameter set and are contained in a special subset of strongly regular graphs. We refer to graphs in this subset as conference graphs. We see a standard construction of other vertex transitive conference graphs on the points of an affine plane. Notably, we generalize the definition of a Peisert graph to describe a new infinite family of self-complementary conference graphs that we believe are distinct from the Paley and Peisert graphs.

5.1 Conference Graphs

First we recall that a graph X is strongly regular with parameter set (n, k, a, c) if the following conditions hold:

i) Each vertex has k neighbours, where $k > 0$.

ii) Each pair of adjacent vertices has a common neighbours, where $a < n - 2$.

iii) Each pair of distinct, nonadjacent vertices has c common neighbours.

The parameters of a strongly regular graph are not independent from each other. In particular, a simple condition can be derived from double counting the edges between the neighbours and nonneighbours of a specific vertex. The proof of this condition is given in Godsil and Royle's text [10]. We reproduce the result in the following lemma.

5.1.1 Lemma. *The parameter set (n, k, a, c) of a strongly regular graph must satisfy*

$$k(k-a-1) = (n-k-1)c$$

Proof. Let X be a strongly regular graph with parameters (n, k, a, c). Let x be a vertex of X, and let N denote the set of k vertices adjacent to x. Let $\overline{N}$ denote the set of $n-k-1$ vertices in $X \setminus \{x\}$ that are not adjacent to x. Each vertex in N is adjacent to $a+1$ vertices in $N \cup \{x\}$, and therefore each vertex in N must be adjacent to $k-a-1$ vertices in $\overline{N}$. Therefore there must be $k(k-a-1)$ edges between the vertices in N and $\overline{N}$. On the other hand, each vertex in $\overline{N}$ has c common neighbours with x, and so there must be $(n-k-1)c$ edges between the vertices in N and the vertices in $\overline{N}$. From this we conclude that $k(k-a-1) = (n-k-1)c$. □

Using this lemma we prove that the parameter set of any self-complementary strongly regular graph is determined by the size of its vertex set. Again, this result follows from work in Godsil and Royle's text [10].

5.1.2 Lemma. *A self-complementary strongly regular graph on n vertices has parameters $(n, \frac{n-1}{2}, \frac{n-5}{4}, \frac{n-1}{4})$.*

Proof. Let X be a strongly regular graph with parameters (n, k, a, c), and let $\overline{X}$ denote the complement of X. We begin by determining parameter set $(n, \bar{k}, \bar{a}, \bar{c})$ for $\overline{X}$ in terms of k,a, and c. Since each vertex in X has k neighbours, it follows that

$$\bar{k} = n-k-1.$$

Let x and y be adjacent vertices in $\overline{X}$. This implies x and y are not adjacent and have c common neighbours in X. It follows that there are $n-2-2k+c$ vertices in X that are not adjacent to x and not adjacent to y. Therefore x and y must have $\bar{a} = n-2-2k+c$ common neighbours in $\overline{X}$.

Let x and z be nonadjacent vertices in $\overline{X}$. There are a common neighbours to x and z in X, and so there are $\bar{c} = n-2k+a$ vertices which are nonadjacent to x and nonadjacent to z in X. □

Further suppose that X is self-complementary. The following three equations must hold:

(i) $k = n-k-1 = \bar{k}$

(ii) $a = n - 2 - 2k + c = \bar{a}$

(iii) $c = n - 2k + a = \bar{c}$

From equation (i), we immediately see that $k = \frac{n-1}{2}$. Substituting that expression for k into (ii) yields $a = c - 1$. Next, substituting those values for k and a into the equation proved in Lemma 5.1.1, we deduce that $c = \frac{n-1}{4}$ and $a = \frac{n-5}{4}$. Therefore the parameters of X are as claimed. □

We define a *conference graphs* to be a strongly regular graph with the parameter set

$$\left(n, \frac{n-1}{2}, \frac{n-5}{4}, \frac{n-1}{4}\right).$$

The next two corollaries follow immediately from our work above.

5.1.3 Corollary. *Paley graphs are conference graphs.*

5.1.4 Corollary. *Peisert graphs are conference graphs.*

5.2 Construction and Examples

Using a geometric approach, we construct strongly regular graphs on the points of an affine plane. We have already seen this method used in Sections 2 and 3 to construct Paley graphs and certain Peisert graphs. Now we give the general construction of a strongly regular graph on the points of $AG(2, q)$. Then we narrow the construction to produce conference graphs.

Before beginning with the construction, we recall the three defining properties of affine plane that were given Definition 2.4.1.

First, any two points uniquely determine a line. Second, given a line l and a point p not incident to l, there is a unique line l' through p parallel to l'. The last property states that an affine plane has at least four points, no three of which are collinear. This ensures there is more than one line and the plane is not a degenerate incidence structure.

It follows from these properties that each point is incident to a constant number of lines and each line is incident to a constant number of points. We say that an affine plane has order q if it has q^2 points and $q^2 + q$ lines. In such an affine plane each point is on $q + 1$ lines and each line is incident to q points. Given any line l in the affine plane there are $q - 1$ other lines that do not intersect l and are pairwise non-intersecting. These q lines form a *parallel class*. We note that there are $q + 1$ parallel classes in the affine plane.

We recall the method we use to construct a graph on the points of the affine plane. First we designate half of the parallel classes to be a special set, and then we define two points in the graph to be adjacent if and only they are incident to common line that is contained in one of the special parallel classes.

In particular, we use the affine plane $AG(2, q)$ derived from the two dimensional vector space $\mathbb{F}_q \times \mathbb{F}_q$. The points of this plane are ordered pairs of elements of $\mathbb{F}_q$, and the lines are translates of the one dimensional subspaces of the vector space. It is not difficult to see that any pair of points will be contained in exactly one coset. Also it can be shown that for a coset C and a point p not contained in C, there is exactly one coset disjoint from C containing that point. Therefore, $AG(2, q)$, as constructed from $\mathbb{F}_q \times \mathbb{F}_q$, satisfies the necessary conditions in Definition 2.4.1. An explicit description of the graph construction follows.

5.2.1 Construction. Let $AG(2, q)$ denote the affine plane of odd order q derived from the ordered pairs of $\mathbb{F}_q \times \mathbb{F}_q$. Let P denote a subset of $\mathbb{F}_q \cup \{\infty\}$. We define $G(P, q)$ to be a graph on the points of $AG(2, q)$ such that two points are adjacent if and only if the line incident to both points has slope m such that $m \in P$.

For example, if P is the empty set, then $G(P, q)$ has no edges. On the other hand, if $P = \mathbb{F}_q \cup \{\infty\}$, then $G(P, q)$ is the complete graph on q^2 vertices. In fact, we note that if $|P| > 1$, then $G(P, q)$ is connected. Also, it is useful to note that the complement of $G(P, q)$ is $G(P', q)$, where $P' = \mathbb{F}_q \cup \{\infty\}) \setminus P$.

Using a straightforward counting argument, we show that when P is a nontrivial subset of $\mathbb{F}_q \cup \{\infty\}$, then the resulting graph is strongly regular. This is a standard result.

5.2.2 Theorem. *A graph $G(P, q)$ constructed using Construction 5.2.1 where $0 < |P| < \frac{q+1}{2}$ is strongly regular with parameters*

$$(q^2, t(q-1), q-2+(t-1)(q-1), t^2-t)$$

where $t = |P|$.

Proof. Let L denote the set of tq lines contained in parallel classes of $AG(2, q)$ in with slopes in P. Note that two vertices in X are adjacent if and only if they are both incident to the same line in L. Consider a fixed point x in $AG(2, q)$. Each parallel class with slope contained in P contains exactly one line incident to x. Therefore x is incident to t lines in L, and each of those lines have only the point x in common. It follows that x is adjacent to $t(q-1)$ points in G.

Consider a neighbour y of x in G. Let l denote the unique line L incident to both x and y. There are $q-2$ other points on l, and each of those points is adjacent to both x and y. Moreover, each of the $t-1$ other lines through x in L is parallel to exactly one line incident to y. Therefore each of those $t-1$ lines intersect $t-2$ of the lines incident to y in $L \setminus \{l\}$. This implies there are $(t-1)(t-2)$ points adjacent to both x and y in G that are not incident to l in $AG(2,q)$. In total, x and y have $q-2+(t-1)(t-2)$ common neighbours in G.

Finally, consider a point z that is not a neighbour of x in $G(P,q)$. Obviously x is adjacent to z in $\overline{G}$, the complement of G. Let $P' = (\mathbb{F}_q \cup \{\infty\}) \setminus P$, and recall that $\overline{G} = G(P',q)$. Since $|(\mathbb{F}_q \cup \{\infty\}) \setminus P| = q+1-t$, it follows from our earlier work, that x and z have $q+2+(q-t)(q-t-1)$ common neighbours in $\overline{G}$. Also from our earlier work, we see that both x and z each have $(q+1-t)(q-1)$ neighbours in $\overline{G}$. This implies there are

$$2(q+1-t)(q-1)-2-(q+2+(q-t)(q-t-1)) = q^2+t-t^2-2$$

points adjacent to either x or z in $\overline{G}$. Therefore there are

$$q^2-2-(q^2+t-t^2-2) = t^2-t$$

points adjacent to both x and y in G. □

Recall that we wish to construct conference graphs. Therefore we we focus on graphs $G(P,q)$ such that $|P| = \frac{q+1}{2}$. From our previous result, we see the parameter set of such a graph is

$$(n, \frac{n-1}{2}, \frac{n-5}{4}, \frac{n-1}{4}).$$

For specific examples of graphs constructed using Construction 5.2.1, we revisit the affine plane constructions for Paley and Peisert graphs given in Sections 2.4 and 3.2, respectively.

5.2.3 Example. Let $q = p^r$ for some prime p such that $p \equiv 3 \pmod 4$. Let $\hat{S}$ denote the subset of $\mathbb{F}_q \times \mathbb{F}_q$ corresponding to the set of nonzero squares of $\mathbb{F}_{q^2}$. We choose P_1 to be the following set of slopes.

$$P_1 = \{y : (1,y) \in \hat{S},\, y \in \mathbb{F}_q\}$$

The graph $G(P_1,q)$ is isomorphic to the Paley graph $P(q)$.

5.2.4 Example. Let q denote a odd prime power, and let $\widehat{M}$ denote the subset of $\mathbb{F}_q \times \mathbb{F}_q$ corresponding to the set M of $\mathbb{F}_{q^2}$ where

$$M = \{\omega^i : i \equiv 0, 1 \pmod 4\}.$$

We choose P_2' to be the following set of slopes.

$$P_2' = \{y : (1, y) \in \widehat{M},\, y \in \mathbb{F}_q\}$$

If $(0, 1) \in \widehat{M}$, then we define $P_2 = P_2' \cup \{\infty\}$. Otherwise we define $P_2 = P_2'$. The graph $G(P_2, q)$ is isomorphic to the Peisert graph $P^*(q)$.

5.3 Generalized Peisert Graphs

In this section we give one more construction of strongly regular graphs that are similar to Paley and Peisert graphs. We revert to constructing graphs as Cayley graphs, but we note that certain instances of these graphs can also be constructed using affines plane. Thus using our work in Section 5.2, we prove those certain instances are conference graphs.

5.3.1 Generalized Paley Graphs

There is a natural generalization of Paley graphs. These graphs do not possess the particular properties we are interested in, but they do provide motivation for our forthcoming generalization of Peisert graphs.

We construct another family of graphs on the additive group of a finite field. Instead of using the set of nonzero squares as the connection set, we use larger powers. As an example we use the set of nonzero cubes as the connection set.

5.3.1 Example. Let q be a prime power such that $q \equiv 1 \pmod 3$. The *cubic Paley graph* of order q, denoted $P_{(3)}(q)$ is the graph on the points of $\mathbb{F}_q$ where two vertices x and y are adjacent if and only if

$$a - b \in \{y^3 : y \in \mathbb{F}_q\}.$$

The condition $q \equiv 1 \pmod 3$ ensures -1 is a cube in $\mathbb{F}_q$, and therefore $P_{(3)}(q)$ is a well-defined, undirected graph. We construct graphs using higher powers also.

5.3.2 Definition. Let q be a prime power such that $q \equiv 1 \pmod{n}$. The *n-th power Paley graph* of order q, denoted $P_{(n)}(q)$ is the graph on the points of $\mathbb{F}_q$ where two vertices x and y are adjacent if and only if

$$x - y \in \{a^n : a \in \mathbb{F}_q\}$$

We refer to the family of n-th power Paley graphs as *generalized Paley graphs*. These graphs are also known as cyclotomic graphs. It is known that the generalized Paley graph $P_{(n)}(q)$ is arc transitive, since the subgroup of the automorphism group that maps x to $\omega^n x$ fixes 0 and acts transitively on the neighbours of 0. However, we note that the number of edges in $P_{(n)}(p^r)$ is

$$|E(P_{(n)}(p^r)| = \frac{(p^r - 1)p^r}{2n}.$$

For $n > 2$, we have

$$|E(P_{(n)}(p^r)| < \frac{(p^r - 1)p^r}{4}$$

which implies there are more edges in the complement of $P_{(n)}(p^r)$ than in $P_{(n)}(p^r)$. Therefore non-trivial generalized Paley graphs are not self-complementary. Moreover, not all generalized Paley graphs are strongly regular, and those that are strongly regular do not have our desired parameter set. Therefore we turn our attention to a generalization of Peisert graphs.

5.3.2 Definition and Properties

Recall that Peisert graphs are Cayley graphs on $\mathbb{F}_q$ where the connection set is half of the cosets the multiplicative subgroup group of order $(q-1)/4$. Now we define a new family of graphs on the elements of $\mathbb{F}_q$ where the connection set is half of the cosets of a different multiplicative subgroup. We refer to this new family of graphs as *generalized Peisert graphs*.

5.3.3 Definition. Let n denote a positive even integer, and let q denote some odd prime power such that $q - 1 \geq n$ and $q \equiv 1 \pmod{n}$. The *n-th power Peisert graph* of order q, denoted $P^*_{(n)}(q)$, is the graph on the points of $\mathbb{F}_q$ where two vertices x and y are adjacent if and only if $x - y \in \widehat{M}$ where

$$\widehat{M} = \{\omega^{nk+i} : 0 \leq i \leq \frac{n}{2} - 1, k \in \mathbb{Z}\}.$$

For example, the graph $P^*_{(4)}(q)$ is precisely the Peisert graph $P^*(q)$ for appropriate q. Moreover, $P^*_{(2)}(q)$ is the Paley graph $P(q)$. For a concrete example, we consider the 10-th power Peisert graph of order 3^4.

5.3.4 Example. Let $q = 3^4$, and let $\widehat{M}$ denote the set

$$\widehat{M} = \{\omega^{10k+i} : 0 \leq i \leq 4, k \in \mathbb{Z}\}.$$

The graph $P^*_{(10)}(3^4)$ is the graph on the points of $\mathbb{F}_{3^4}$ where two vertices x and y are adjacent if and only if $x - y \in \widehat{M}$.

Let ω denote a multiplicative generator of $\mathbb{F}_{3^4}$, and consider the permutation

$$\gamma : x \to \omega^5 x.$$

Note that we have

$$x - y = \omega^{10k+i} \iff \gamma(x) - \gamma(y) = \omega^{10k+i+5}.$$

This implies

$$x - y \in \widehat{M} \iff \gamma(x) - \gamma(y) \notin \widehat{M}.$$

Therefore γ will be an isomorphism from $P^*_{(10)}(3^4)$ to its complement, which implies the graph is self-complementary.

In fact, the same results hold for all generalized Peisert graphs.

5.3.5 Lemma. *Generalized Peisert graphs are self-complementary.*

Proof. Let n denote a positive even integer, and let q denote some odd prime power such that $q - 1 \geq n$ and $q \equiv 1 \pmod{n}$. Let $P^*_{(n)}(q)$ be the generalized Peisert graph of order q. Recall that the connection set this graph is

$$\widehat{M} = \{\omega^{nk+i} : 0 \leq i \leq \frac{n}{2} - 1, k \in Z\}.$$

where ω is a primitive root of $\mathbb{F}_q$.

Let γ be the permutation on $\mathbb{F}_q$ defined as

$$\gamma : x \to \omega^{\frac{n}{2}} x.$$

We have that

$$x - y = \omega^{nk+i} \iff \gamma(x) - \gamma(y) = \omega^{nk+i+\frac{n}{2}}.$$

This implies

$$x - y \in \widehat{M} \iff \gamma(x) - \gamma(y) \notin \widehat{M}.$$

Therefore γ is an isomorphism from $P^*_{(n)}(q)$ to its complement. □

When q is a square and $n = \sqrt{q}+1$, we can construct the generalized Peisert graph $P^*_{(n)}(q)$ as an affine plane graph. This construction enables us to deduce that $P^*_{(n)}(q)$ is strongly regular for these values of q and n.

5.3.6 Lemma. *Let $q = p^{2r}$ for some odd prime p, and let $n = \sqrt{q}+1$. The generalized Peisert graph $P^*_{(n)}(q)$ is a conference graph.*

Proof. We begin by constructing $P^*_{(n)}(q)$ as an affine plane graph. Let ω denote a multiplicative generator of $\mathbb{F}_q$. Note that the subfield of order p^r is generated multiplicatively by ω^{p^r+1}.

Recall that the connection set of $P^{*(n)}(q)$ is

$$\widehat{M} = \{\omega^{(p^r+1)k+i} : 0 \leq i \leq (p^r+1)/2-1, k \in Z\}.$$

Therefore $\widehat{M}$ is closed under multiplication by powers of ω^{p^r+1}. From this we conclude that we can partition the points of $AG(2,q)$ corresponding to $\widehat{M}$ into $(q+1)/2$ lines incident to 0. Let P denote the set of slopes corresponding to those lines. We see that $G(P,q)$ as defined in Construction 5.2.1, will be isomorphic to $P^*_{(n)}(q)$. From Theorem 5.2.2, we conclude that $P^*_{(n)}(q)$ is strongly regular with parameter set

$$(n, \frac{n-1}{2}, \frac{n-5}{4}, \frac{n-1}{4}). \qquad \square$$

5.4 Computational Results

The generalized Peisert graphs are not always distinct from the Paley and Peisert graphs. As we pointed out earlier, $P^*_{(4)}(9)$ is isomorphic to $P^*(9)$. In fact, since there is only one vertex transitive self-complementary graph on 9 vertices, it follows that $P^*_{(4)}(9)$ is also isomorphic to $P(9)$. Using a computer and SAGE [21], we determine more information about these graphs. We summarize the information in the table below. Recall that for each graph on q^2 vertices, the maximum clique size is q. The third and fourth columns indicates whether the generalized Peisert graph is isomorphic to the corresponding Paley and Peisert graph, respectively.

Table 5.1: **Generalized Peisert Graphs**

q^2	# Max Cliques on 0	$\cong P(q)$?	$\cong P^*(q^2)$?
3^2	2	Yes	Yes
5^2	3	Yes	No
7^2	4	No	Yes
3^4	9	No	No
11^2	6	No	No
13^2	7	No	No
17^2	9	No	No
19^2	10	No	No
23^2	12	No	No
5^4	19	No	No
3^6	14	No	No

Chapter 6

Pseudo-Paley graphs

In this section we construct other families of vertex-transitive conference graphs that are self-complementary in some cases. These families were first studied by Weng, Qiu, Wang, and Xiang, who believe the families are distinct from the Paley and Peisert graphs [24].

First we note the one-to-one correspondence between the connection sets of strongly regular Cayley graph and partial difference sets. Then we give Weng, Qiu, Wang, and Xiang's construction of partial difference sets from algebraic structures known as semifields. Finally, we see specific examples of partial difference sets which are used to construct conference graphs.

6.1 Partial Difference Sets

We begin by deriving necessary conditions for the connection sets of strongly regular Cayley graphs on abelian groups.

Let $X(G, C)$ be a Cayley graph, and let x be a neighbour of 0 in X. Note that 0 and x have a common neighbour y if and only if there exist some element t such that $y, t \in C$ and $x + t = y$. Since C is necessarily closed under inverses, we see this is equivalent to having $y, -t \in C$ such that $y - (-t) = x$. Thus we see that the differences of elements in the connection set determine whether a Cayley graph is strongly regular. We use design theory terminology to describe these conditions.

6.1.1 Definition. Let G be a finite abelian group of order n. A k-element subset D of $G \backslash \{0\}$ is called a (n, k, a, c)-*partial difference set* if the following conditions hold:

(i) Each element of D is equal to $x - y$ for exactly a ordered pairs $x, y \in D$.

(ii) Each non-identity element of $G \setminus D$ is equal to $x - y$ for exactly c ordered pairs $x, y \in D$.

From this definition it is straightforward to see that a Cayley graph $X(G, C)$ is strongly regular with parameter set (n, k, a, c) if and only if C is an inverse-closed partial difference set of G. Recall that the set of nonzero squares of $\mathbb{F}_q$ is the connection set of the Paley graph of order q where $q \equiv 1 \pmod 4$. Recall the Paley graph $P(q)$ is a conference graph, and every conference graph has parameter set

$$\left(q, \frac{(q-1)}{2}, \frac{(q-5)}{4}, \frac{(q-1)}{4}\right).$$

It follows that the set of nonzero squares is a partial difference set of the additive group of $\mathbb{F}_q$ with the same parameter set. We refer to a partial difference set with these parameters as a *Paley-type partial difference set*.

6.2 Commutative Semifields

In order to construct other Paley-type partial difference sets, we consider the set of nonzero squares of a more general algebraic structure, a finite commutative semifield. The study of finite commutative semifields was started by Dickson in the early 1900s. Dickson is responsible for finding the first nonassociative examples.

6.2.1 Definition. A set $(K, +, *)$ equipped with two binary operations is a *commutative semifield* if the following five conditions hold:

(i) K is an abelian group with respect to $+$.

(ii) $x * y = y * x$ for all x and y in K.

(iii) $x * (y + z) = x * y + x * z$, $(x + y) * z = x * z + y * z$ for all x, y, z in K.

(iv) There exists 1 in K such that $1 * x = x * 1 = x$ for all x in K.

(v) If $x * y = 0$, then $x = 0$ or $y = 0$.

A finite fields is a simple example of a commutative semifield. It is not difficult to see that a finite commutative semifield with associative multiplication is a finite integral domain. Since finite integral domains are necessarily finite fields, it follows that finite commutative semifields with associative multiplication are finite fields. For this reason we are interested in commutative semifields with nonassociative multiplication, which we refer to as *proper semifields*. It can be shown that a finite semifield must have a prime power order, and a proper finite semifield of order q exists for all $q = p^r$ where p is prime and $r \geq 3$ if p is odd or $r \geq 4$ if $p = 2$ [7].

6.2.2 Example. Let q be an odd prime power, and let j be a nonsquare in $\mathbb{F}_q$. Let σ denote a nontrivial automorphism of $\mathbb{F}_q$. The *Dickson semifield* $(\mathbb{F}_q^2, +, *)$ is defined by the following multiplication:

$$(a, b) * (c, d) = (ac + jb^\sigma d^\sigma, ad + bc)$$

From this definition, we observe that the Dickson semifield is an additive group with respect to the usual addition, and the defined multiplication is commutative. It is also straightforward to verify that the element $(1, 0)$ is the multiplicative identity which satisfies condition (iv). Thus it suffices to show that conditions (iii) and (v) are met in Definition 6.2.1 in order to confirm the Dickson semifield is indeed a semifield.

Suppose that $x = (x_1, x_2)$, $y = (y_1, y_2)$, and $z = (z_1, z_2)$. First we show that the right-sided distributive law holds.

$$\begin{aligned} x * (y + z) &= (x_1, x_2) * (y_1 + z_1, y_2 + z_2) \\ &= (x_1y_1 + x_1z_1 + jx_2^\sigma y_2^\sigma + jx_2^\sigma z_2^\sigma, x_1y_2 + x_1z_2 + x_2y_1 + x_2z_1) \\ &= (x_1y_1 + jx_2^\sigma y_2^\sigma, x_1y_2 + x_2y_1) + (x_1z_1 + jx_2^\sigma z_2^\sigma, x_1z_2 + x_2z_1) \\ &= x * y + x * z \end{aligned}$$

Next we suppose that $x * y = 0$ for some $x \neq 0$, where $x = (x_1, x_2)$ and $y = (y_1, y_2)$. We must have the following.

$$(0, 0) = (x_1y_1 + jx_2^\sigma y_2^\sigma, x_1y_2 + x_2y_1)$$

Since $x \neq 0$, either x_1 or x_2 is nonzero. Suppose $x_1 \neq 0$. From the first coordinate of $x * y$, we must have

$$y_1 = -jx_2^\sigma y_2^\sigma x_1^{-1}$$

Substituting this expression into the second coordinate of $x * y$ yields

$$x_1y_2 = jx_2^{\sigma+1} y_2^\sigma x_1^{-1}$$

Since the squares of $\mathbb{F}_q$ are closed under multiplicative inversion, it follows that x_1 is a square if and only if x_1^{-1} is a square. Likewise, since the squares of $\mathbb{F}_q$ are closed under any automorphism, it follows that y_2 is a square if and only if y_2^σ is a square. Putting this together, we see that x_1y_2 is a square if and only if $y_2^\sigma x_1^{-1}$ is a square. Since $jx_2^{\sigma+1}$ is a non-square if x_2 is nonzero, this implies $x_2 = 0$. However, substituting $x_2 = 0$ into equation 6.2 yields $y_2 = 0$, and substituting $x_2 = 0$ into Equation 6.2 yields $y_1 = 0$. Therefore $(y_1, y_2) = (0, 0)$, as desired. We reach the same conclusion if we suppose that x_2 is nonzero.

Finally, we show that the Dickson semifield is not a field by demonstrating that the defined multiplication is not associative.

$$\begin{aligned}\{(a,b)*(c,d)\}*(e,f) &= (ac + jb^\sigma d^\sigma, ad + bc) * (e,f)\\ &= (ace + jeb^\sigma d^\sigma + j(ad+bc)^\sigma f^\sigma, acf + jfb^\sigma d^\sigma + ade + bce)\\ &= (ace + jb^\sigma d^\sigma e + ja^\sigma d^\sigma f^\sigma + jb^\sigma c^\sigma f^\sigma,\\ &acf + jfb^\sigma d^\sigma + ade + bce)\end{aligned}$$

Alternatively, we have

$$\begin{aligned}(a,b)*\{(c,d)*(e,f)\} = (&ace + jb^\sigma d^\sigma e^\sigma + jad^\sigma f^\sigma + jb^\sigma c^\sigma f^\sigma,\\ &acf + jbd^\sigma f^\sigma + abe + bce)\end{aligned}$$

From these computations, we notice that the multiplication associative if and only if $jb^\sigma d^\sigma e = jb^\sigma d^\sigma e^\sigma$ for all b, d, e in $\mathbb{F}_q$, which holds if and only if $e = e^\sigma$ for all e in $\mathbb{F}_q$. Since σ is chosen to be a nontrivial automorphism, it follows that the Dickson semifields are not associative, and therefore are not finite fields.

6.3 Semifield Graphs

We wish to construct a strongly regular graph on the additive group of a semifield that is a conference graph. Weng, Qiu, Wang, and Xiang show that the set of nonzero squares of a semifield form a Paley-type partial difference set [24]. Therefore the nonzero squares are an appropriate choice for the connection set of our graph. We give a slightly modified version of their proof in the lemmas and theorem that follow.

Let $(K, +, *)$ be a commutative semifield such that $|K| = n$, where n is an odd prime power. We utilize the notation $x^2 := x * x$, and we define the set D to be the set of nonzero squares of the semifield K such that

$$D = \{x^2 : x \in K \setminus \{0\}\}. \qquad (6.3.1)$$

6.3.1 Lemma. *For each y in D, there are exactly two distinct elements x and $-x$ in K such that $y = x^2 = (-x)^2$.*

Proof. Suppose y is an element in D. There must be at least one x in K such that $y = x^2$. Now suppose $x^2 = a^2$ for an element a of K. It follows that

$$x^2 - a^2 = (x - a) * (x + a) = 0.$$

Therefore either $a = x$ or $a = -x$. Since y is nonzero and $(K, +)$ is an additive group of odd order, the elements x and $-x$ are distinct. □

6.3.2 Corollary. *There are $\frac{n-1}{2}$ elements in D.* □

The next lemma uses the fact that each nonzero square has exactly two roots to establish a useful equation.

6.3.3 Lemma. *Let y denote an element of K. Let S_y denote the set of ordered pairs (z_1, z_2) in $K \times K$ such that $z_1^2 - z_2^2 = y$. The following equation holds*

$$|S_y| = \begin{cases} n-1 & \textit{if } y \neq 0, \\ 2n-2 & \textit{if } y = 0 \end{cases}$$

Proof. We consider both cases separately. First suppose that $y \neq 0$. We define the map $\phi : S_y \to K \setminus \{0\}$ as follows

$$(z_1, z_2) \mapsto (z_1 - z_2)$$

Note that if $\phi(z_1, z_2) = 0$, then $z_1 = z_2$. However, this implies $z_1^2 - z_2^2 = 0$, which contradicts our assumption that y is nonzero. Thus $\phi(S_y) \subseteq K \setminus \{0\}$, and so ϕ is well defined. Suppose $\phi(z_1, z_2) = \phi(z_3, z_4)$. This implies

$$z_1 - z_2 = z_3 - z_4 \tag{6.3.2}$$

Note that $z_1^2 - z_2^2 = (z_1 - z_2)(z_1 + z_2)$ and $z_3^2 - z_4^2 = (z_3 - z_4)(z_3 + z_4)$. Using the cancellation law that follows from the semifield axioms given in Definition 6.2.1, we have

$$z_1 + z_2 = z_3 + z_4 \tag{6.3.3}$$

Combining equations 6.3.2 and 6.3.3 yields $z_1 = z_3$ and $z_2 = z_4$. Therefore ϕ is one-to-one.

Let a be any element of $K \setminus \{0\}$. Consider the map $\Delta_a : K \to K$ defined as follows.

$$\Delta_a(x) = a^2 + 2ax$$

Notice that

$$\Delta(x) = \Delta(y) \iff 2ax = 2ay.$$

This implies $x = y$ and that Δ_a is a bijection from K to itself. It follows that for each y in K there is a uniquely corresponding x such that $\Delta_a(x) = y$. In other words, for each y in K there is a unique x such that

$$(a + x)^2 - x^2 = y.$$

Thus there exists an ordered pair $(a + x, x)$ in S_y such that $\phi(a + x, x) = a$. This implies ϕ in onto. We conclude that ϕ is a bijection between S_y and $K \setminus \{0\}$ and $|S_y| = n - 1$.

Next suppose that $y = 0$ and count the ordered pairs (z_1, z_2) in $K \times K$ such that $z_1^2 - z_2^2 = 0$. Choose x to be any nonzero element of K. From Lemma 6.3.1 we see there exists exactly two elements y and $-y$ such that

$$x^2 = y^2 = (-y)^2.$$

Furthermore, if we choose $x = 0$, then $y = 0$ is the only element of K such that $x^2 = y^2$. This implies there are $2(n - 1) + 1 = 2n - 1$ ordered pairs such that $z_1^2 - z_2^2 = 0$. □

The following theorem confirms that the set of nonzero squares of a commutative semifield is an appropriate choice for the connection set of a vertex-transitive conference graph.

6.3.4 Theorem. *The set of nonzero squares of a finite semifield of order q such that $q \equiv 1 \pmod 4$ forms a Paley-type partial difference set.*

Proof. For any y in $K \setminus \{0\}$, we recall that

$$S_y = \{(z_1, z_2) \in K \times K : z_1^2 - z_2^2 = y\}.$$

Also recall that

$$D = \{a^2 : a \in K \setminus \{0\}\}.$$

Now consider the set

$$T_y = \{(a, b) \in D \times D : a - b = y\}.$$

Each element in T_y corresponds to four distinct elements in S_y, namely

$$\{(z_1, z_2), (-z_1, z_2), (z_1, -z_2), (-z_1, -z_2)\}$$

where $z_1^2 = a$ and $z_2^2 = b$. Let U_y be the following set.

$$U_y = \{a \in D : a = y \text{ or } a = -y\}$$

Each element in U_y corresponds to two ordered pairs in S_y such that one coordinate is zero. It is easy to see that $|U_y| \leq 2$.

Putting these observations together, we have

$$|S_y| = 4|T_y| + 2|U_y| \tag{6.3.4}$$

From Lemma 6.3.3, we know that $|S_y| = n - 1$. Since $q \equiv 1 \pmod 4$, it follows that $|U_y| = 0$ or 2, depending on whether $y \in D$. Thus equation 6.3.4 can be rearranged to yield

$$|T_y| = \begin{cases} \frac{n-1}{4} & \text{if } y \notin D, \\ \frac{n-5}{4} & \text{if } y \in D \end{cases}$$

Note that T is precisely the set of pairs of D whose difference is y. Using Corollary 6.3.2, we conclude that D is a Paley-type partial difference set of the additive group of K. □

The following examples, together with Example 6.2.2, cover all known proper finite commutative semifields in a recent survey by Kantor [12]. Weng, Qiu, Wang, and Xiang construct Cayley graphs on the additive groups of these semifields using corresponding sets of nonzero squares as connection sets [24]. Their results given above confirm that the resulting graphs are conference graphs.

6.3.5 Example. The Dickson semifield described in Example 6.2.2 has the following set of nonzero squares.

$$D(q) = \{(x^2 + jy^{2\sigma}, 2xy) : (x, y) \in \mathbb{F}_q^2, (x, y) \neq (0, 0)\}$$

6.3.6 Example. Let $q = 3^r$ such that $r \geq 3$ and r is odd. The *Ganley semifield* $(\mathbb{F}_q^2, +, *)$ is defined by the following multiplication.

$$(a, b) * (c, d) = (ac - b^9 d - bd^9, ad + bc + b^3 d^3)$$

By Theorem 6.3.4, we see that the subset

$$G(q) = \{(x^2 + y^{10}, 2xy + y^6) : (x, y) \in \mathbb{F}_q^2, (x, y) \neq (0, 0)\}$$

is a Paley type partial difference set in $(\mathbb{F}_q^2, +)$.

6.3.7 Example. Let $q = 3^r$ such that $r \geq 2$, and let j be a nonsquare in $\mathbb{F}_q$. The *Cohen-Ganley semifield* $(\mathbb{F}_q^2, +, *)$ is defined by the following multiplication.

$$(a, b) * (c, d) = (ac + jbd + j^3b^9d^9, ad + bc + jb^3d^3)$$

By Theorem 6.3.4, we see that the subset

$$CG(q) = \{(x^2 + jy^2 + j^3y^{18}, 2xy + jy^6) : (x, y) \in \mathbb{F}_q^2, (x, y) \neq (0, 0)\}$$

is a Paley type partial difference set in $(\mathbb{F}_q^2, +)$.

6.3.8 Example. Let $q = 3^5$. The *Pentilla-Williams semifield* $(\mathbb{F}_q^2, +, *)$ is defined by the following multiplication.

$$(a, b) * (c, d) = (ac + b^9d^9, ad + bc + b^{27}d^{27})$$

By Theorem 6.3.4, we see that the subset

$$P(q) = \{(x^2 + y^{18}, 2xy + y^{54}) : (x, y) \in \mathbb{F}_q^2, (x, y) \neq (0, 0)\}$$

is a Paley type partial difference set in $(\mathbb{F}_q^2, +)$.

Note that the additive and multiplicative identities of the the semifields described in Examples 6.2.2, 6.3.6, 6.3.7, and 6.3.8 are $(0, 0)$ and $(1, 0)$, respectively. Moreover, each of the semifields contain $\mathbb{F}_q$ as the following subset equipped with the corresponding semifield operations.

$$\mathbb{F}_q \cong \{(a, 0) : a \in \mathbb{F}_q\}$$

We can easily verify this claim by noting that $(a, 0) + (c, 0) = (a + c, 0)$ and that $(a, 0) * (c, 0) = (ac, 0)$ for a and c in $\mathbb{F}_q$ using any of the above semifield operations.

We take special note that for the Dickson semifields, $\mathbb{F}_q \setminus \{0\}$ is contained in $D(q)$, the set of nonzero squares. For a in $\mathbb{F}_q$ such that $a = x^2$ for some x in $\mathbb{F}_q$, this containment is easy to see.

$$\begin{aligned}(a, 0) &= (x^2, 0) \\ &= (x, 0) * (x, 0)\end{aligned}$$

When a is a nonzero, it is slightly more complicated. Note that $a = jx^2$ for some x in $\mathbb{F}_q$, and let y be the element of $\mathbb{F}_q$ such that $y^\sigma = x$.

$$\begin{aligned}(a, 0) &= (jx^2, 0) \\ &= (jy^{2\sigma}, 0) \\ &= (0, y) * (0, y)\end{aligned}$$

Of the examples given above, the Dickson semifields are the only semifields which contain the subfield of size q in its set of squares.

Chapter 7

Dickson Semifield Graphs

In this chapter we study the graphs constructed on the Dickson semifield defined in Chapter 6.1. It is conjectured by Weng, Qiu, Wang, and Xiang that semifield partial difference sets are different from the connections sets of Paley and Peisert graphs [24]. Here we prove a new result about the number of cliques of size q in the Dickson semifield graph of order q^2. This result enables us to distinguish the Dickson semifield graphs from Paley graphs. This graph-theoretic result confirms that the corresponding partial difference sets are distinct.

7.1 Partial Difference Set Equivalence

We begin by giving two definitions of equivalence for partial difference sets.

7.1.1 Definition. Let D_1 and D_2 be two partial difference sets contained in a group G. We say the partial difference sets D_1, D_2 are *PDS-equivalent* if there exists and automorphism ϕ of G such that $\phi(D_1) = D_2$.

There is a weaker notion of equivalence that is more useful for our purpose.

7.1.2 Definition. Let D_1 and D_2 be two partial difference sets contained in a group G. We say the partial difference sets D_1, D_2 are *SRG-equivalent* if the corresponding Cayley graphs $X(G, D_1)$ and $X(G, D_2)$ are isomorphic.

Note that if ϕ is an automorphism of G such that $\phi(D_1) = D_2$, then ϕ is an isomorphism between $X(G, D_1)$ and $X(G, D_2)$. Therefore, if D_1 and D_2 are PDS-equivalent, then D_1 and D_2 are SRG-equivalent. The converse is not true, and there are examples of partial difference sets which are SRG-equivalent but not PDS-equivalent.

In order to show that the semifield partial difference sets are not PDS-equivalent and SRG-equivalent to the connection sets of Paley or Peisert graphs, it suffices to show that the corresponding Cayley graphs are distinct.

7.2 Uniqueness of Semifield Construction

We turn our attention to the graphs constructed from the Dickson semifields. Recall the definitions given in Examples 6.2.2 and 6.3.5.

7.2.1 Definition. Let q be an odd prime power, and let j be a nonsquare in $\mathbb{F}_q$. Let σ denote a nontrivial automorphism of $\mathbb{F}_q$. The *Dickson semifield* $(\mathbb{F}_q^2, +, *)$ is defined by the following multiplication:

$$(a,b) * (c,d) = (ac + jb^\sigma d^\sigma, ad + bc)$$

The set of nonzero squares in the Dickson semifield are

$$Dq = \{(x^2 + jy^{2\sigma}, 2xy) : (x,y) \in \mathbb{F}_q^2, (x,y) \neq (0,0)\}$$

It is useful to show that there is one Dickson semifield of order q^2 for each odd prime power q. In particular, we show that the structure of the Dickson semifield does not specifically depend upon the nontrivial field automorphism σ or nonsquare j used to define the multiplication. We prove this in the following two lemmas.

7.2.2 Lemma. *The Dickson semifields of order q^2 constructed in Example 7.2.1 are isomorphic regardless of the choice of nonsquare j.*

Proof. Suppose j_1 and j_2 be two distinct nonsquares in $\mathbb{F}_q$. Choose σ to be a nontrivial automorphism of $\mathbb{F}_q$. Let $K_1 = (\mathbb{F}_q^2, +, *_1)$ be the Dickson semifield defined by the following multiplication:

$$(a,b) *_1 (c,d) = (ac + j_1 b^\sigma d^\sigma, ad + bc)$$

Let $K_2 = (\mathbb{F}_q^2, +, *_2)$ be the Dickson semifield defined by the following multiplication:

$$(a,b) *_2 (c,d) = (ac + j_2 b^\sigma d^\sigma, ad + bc)$$

We wish to show the semifields K_1 and K_2 are isomorphic.

Recall that the elements $(0,0)$ and $(1,0)$ are the additive and multiplicative identities, respectively, of both K_1 and K_2 . To show K_1 is isomorphic to K_2, we must find a mapping θ from K_1 to K_2 that fixes the additive and multiplicative identity and preserves addition and multiplication in the following sense.

(i) $\theta((a,b)+(c,d)) = \theta(a,b)+\theta(c,d)$

(ii) $\theta((a,b) *_1 (c,d)) = \theta(a,b) *_2 (c,d)$

Since both j_1 and j_2 are nonsquares in $\mathbb{F}_q$, we know that $j_1(j_2)^{-1}$ is a nonzero square. Let r be an element of $\mathbb{F}_q$ such that $r^2 = j_1(j_2)^{-1}$. Define $\theta : K_1 \to K_2$ by $\theta(x,y) = (x, ry)$ for all $(x,y) \in K_1$. We consider the effect of θ on addition.

$$\begin{aligned}
\theta((a,b)+(c,d)) &= \theta(a+c, b+d) \\
&= (a+c, rb+rd) \\
&= (a, rb) + (c, rd) \\
&= \theta(a,b) + \theta(c,d)
\end{aligned}$$

Thus addition is preserved by θ. Next we consider the effect of θ on multiplication.

$$\begin{aligned}
\theta((a,b) *_1 (c,d)) &= \theta(ac + j_1 b^\sigma d^\sigma, ad+bc) \\
&= (ac + j_1 b^\sigma d^\sigma, rad + rbc) \\
&= (ac + j_2(rb^\sigma)(rd^\sigma), a(rd) + b(rc)) \\
&= \theta(a,b) *_2 \theta(c,d)
\end{aligned}$$

Therefore multiplication is preserved by θ, and we conclude that θ is an isomorphism from K_1 to K_2. □

7.2.3 Lemma. *The Dickson semifields of order q^2 constructed in Example 7.2.1 are isomorphic regardless of the choice of nontrivial automorphism σ.*

Proof. Suppose σ and ϕ are two distinct nontrivial automorphisms of $\mathbb{F}_q$. Choose j to be a nonsquare in $\mathbb{F}_q$. Let $K_1 = (\mathbb{F}_q^2, +, *_1)$ be the Dickson semifield defined by the following multiplication:

$$(a,b) *_1 (c,d) = (ac + jb^\sigma d^\sigma, ad+bc)$$

Let $K_2 = (\mathbb{F}_q^2, +, *_2)$ be the Dickson semifield defined by the following multiplication:

$$(a,b) *_2 (c,d) = (ac + jb^\phi d^\phi, ad+bc)$$

We proceed by showing that K_1 is isomorphic to another Dickson semifield K_3, and then we apply Lemma 7.2.2 to show that K_3 is isomorphic to K_2.

First note that the group of automorphisms of $\mathbb{F}_q$ forms an abelian group. Since both σ and ϕ are nontrivial automorphisms, there exists a nontrivial automorphism γ such that $(x^\sigma)^\gamma = x^\phi$ for all field elements x in $\mathbb{F}_q$.

Let $K_3 = (\mathbb{F}_q^2, +, *_3)$ be the Dickson semifield defined by the following multiplication:

$$(a, b) *_3 (c, d) = (ac + j^\gamma b^\phi d^\phi, ad + bc)$$

We wish to show K_1 is isomorphic to K_3 by finding an isomorphism θ from K_1 to K_2. Let θ be defined by $\theta(a, b) = (a^\gamma, b^\gamma)$. We proceed by showing that θ is an isomorphism, as desired.

We easily confirm that $\theta(0, 0) = (0, 0)$ and $\theta(1, 0) = (1, 0)$. Next we show that θ preserves addition.

$$\begin{aligned}
\theta((a, b) + (c, d)) &= \theta(a + c, b + d) \\
&= ((a + c)^\gamma, (b + d)^\gamma) \\
&= (a^\gamma + c^\gamma, b^\gamma + d^\gamma) \\
&= (a^\gamma, b^\gamma) + (c^\gamma, d^\gamma) \\
&= \theta(a, b) + \theta(c, d)
\end{aligned}$$

Now we consider the effect of θ on multiplication.

$$\begin{aligned}
\theta((a, b) *_1 (c, d)) &= \theta(ac + jb^\sigma d^\sigma, ad + bc) \\
&= ((a^c + jb^\sigma d^\sigma)^\gamma, (ad + bc)^\gamma) \\
&= (a^\gamma c^\gamma + j^\gamma (b^\sigma)^\gamma (d^\sigma)^\gamma, a^\gamma d^\gamma + b^\gamma + c^\gamma) \\
&= (a^\gamma c^\gamma + j^\gamma b^\phi d^\phi, a^\gamma d^\gamma + b^\gamma + c^\gamma) \\
&= (a^\gamma, b^\gamma) *_3 (c^\gamma, d^\gamma) \\
&= \theta(a, b) *_3 \theta(c, d)
\end{aligned}$$

From these computations we see that θ preserves addition and multiplication, and so we conclude that θ is an isomorphism from K_1 to K_3, as desired. From Lemma 7.2.2, we see K_3 is isomorphic to K_2, and therefore we conclude that K_1 is isomorphic to K_2. □

7.3 Cliques of Size q

Let K denote the Dickson semifield of order q^2. Our goal for this section is to show that the semifield graph $X(K, D(q))$ contains a different number of cliques of size q than $P(q^2)$ when q is a nontrivial prime power. As a consequence we prove that $X(K, D(q))$ is not isomorphic to $P(q^2)$.

Recall from the work of Blockuis shown in Section 2 that the largest cliques in $P(q^2)$ have size q. Furthermore, each vertex in the neighbourhood of 0 in $P(q^2)$ is contained in exactly one central maximal clique in $P(q^2)$. We show that some neighbours of 0 in $X(K, D(q))$ are contained in at least two central cliques of size q. We do this by constructing a family of central cliques of size q explicity.

7.3.1 Clique Construction

We define a family of q cliques of size q such that each element of $D(q)$ is contained in exactly two cliques in the family. Let $q = p^r$ for some prime p and positive integer r, and let σ denote a non-trivial automorphism of $\mathbb{F}_q$. Throughout this section we assume that the Dickson semifield has been constructed using a nonsquare j and the non-trivial automorphism σ. Let L denote the following set.

$$L = \{(x, 1) : x \in \mathbb{F}_q\} \cup \{(1, 0)\}$$

Note that $|L| = q + 1$. For each l in L we let C_l denote the following clique of size q.

$$C_l = \{(a * l) * l : a \in \mathbb{F}_q\}$$

where $*$ denotes the Dickson semifield multiplication.

For example, we have

$$C_{(1,0)} = \{(a, 0) : a \in \mathbb{F}_q\}.$$

Also for any $x \in \mathbb{F}_q$, we have

$$C_{(x,1)} = \{(ax, a) : a \in \mathbb{F}_q\}.$$

Finally, we define $\mathcal{C}$, our desired family of cliques.

$$\mathcal{C} = \{C_l : l \in L\} \tag{7.3.1}$$

7.3.2 Clique Verification

In order to prove that some elements in the neighbourhood of 0 in $X(K, D(q))$ are contained in at least two cliques of size q, we first verify that C_l is a clique contained in $D(q)$ for each l in L. Next we show that $\mathcal{C}$ contains q or $q+1$ distinct cliques, depending upon whether $q \equiv 1 \pmod 4$ or $q \equiv 3 \pmod 4$.

Recall from Section 6.3 that $C_{(1,0)} \subset D(q)$ and $C_{(1,0)}$ is an additive subgroup of the semifield. It immediately follows that $C_{(1,0)}$ is a clique of size q.

It requires more effort to prove that the other sets in $\mathcal{C}$ are cliques. We break up the work into several lemmas.

7.3.1 Lemma. *Let x be an element of $\mathbb{F}_q$. The set $C_{(x,1)}$ is an additive subgroup of the Dickson semifield of order q^2.*

Proof. Let a and b denote two elements of $\mathbb{F}_q$.

$$\begin{aligned}(ax, a) * (x, 1) - (bx, b) * (x, 1) &= (ax^2 + ja^\sigma, 2ax) - (bx^2 + jb^\sigma, 2bx)\\ &= ((a-b)x^2 + j(a-b)^\sigma, 2(a-b)x)\\ &= ((a-b)x, a-b) * (x, 1)\end{aligned}$$

Since $a - b \in \mathbb{F}_q$, we conclude $((a-b)x, a-b) * (x, 1) \in C_{(x,1)}$. □

Now we show that for each x and a in $\mathbb{F}_q$ such that $a \neq 0$, the nonzero semifield element $(ax, a) * (x, 1)$ in $C_{(x,1)}$ is contained in the set of nonzero squares $D(q)$. We do this by finding an element (c, d) such that

$$(ax, a) * (x, 1) = (c, d) * (c, d).$$

This is easy when a is a square.

7.3.2 Lemma. *Let a be a nonzero square in $\mathbb{F}_q$. The element $(ax, a) * (x, 1)$ is a nonzero square in the Dickson semifield of order q^2 for all x in $\mathbb{F}_q$.*

Proof. Since a is a nonzero square in $\mathbb{F}_q$, we can express $a = t^2$ for some nonzero element t. Then we see the following.

$$\begin{aligned}(ax, a) * (x, 1) &= (ax^2 + ja^\sigma, 2ax)\\ &= ((tx)^2 + j(t)^{2\sigma}, 2(tx)(t))\\ &= (tx, t) * (tx, t)\end{aligned}$$

We conclude $(ax, a) * (x, 1)$ is a nonzero square in the Dickson semifield. □

Now consider the case when a is not a square in $\mathbb{F}^q$. Before we prove that $(ax, a) * (x, 1)$ is a square, we need to do some preliminary work. Recall that we let S denote the set of nonzero squares in $\mathbb{F}_q^*$. We begin by defining a map f_a from S to $\mathbb{F}_q$ using the nonsquare j, and the nontrivial automorphism σ.

$$f_a(z) = ja^{-1}z(z-a)^{\sigma-1} \tag{7.3.2}$$

Next we prove that f_a is a permutation of S when a is a not a square in $\mathbb{F}_q$.

7.3.3 Lemma. *Let a be a nonzero nonsquare in $\mathbb{F}_q$. The function f_a is a permutation of S.*

Proof. By our assumption that a is nonzero, we see that f_a is well-defined on its domain S. Moreover, since a is not a square, for each square z in S, we see that $ja^{-1}z \in S$. Also, since σ is an odd prime power, we see that $(z-a)^{\sigma-1}$ is a square. Therefore $f_a(z) \in S$ for all z in S. Thus to show that f_a is a permutation of S, it suffices to show that f_a is one-to-one.

Suppose for a contradiction that $f_a(z_1) = f_a(z_2)$. there is an element x in $\mathbb{F}_q^*$ such that

$$x^2 = ja^{-1}z_1(z_1-a)^{\sigma-1} \tag{7.3.3}$$

and also

$$x^2 = ja^{-1}z_2(z_2-a)^{\sigma-1}. \tag{7.3.4}$$

Note that Equation 7.3.3 can be rearranged in the following way.

$$\begin{aligned} x^2 &= ja^{-1}z_1(z_1-a)^{\sigma-1} \\ &= ja^{-1}z_1(z_1-a)^{\sigma}(z_1-a)^{-1} \\ &= ja^{-1}z_1(z_1-a)^{\sigma}z_1^{-1}(1-az_1^{-1})^{-1} \\ &= j(z_1-a)^{\sigma}(a(1-az_1^{-1})^{-1} \end{aligned}$$

Therefore z_1 satisfies the following equation

$$ax^2 - a^2x^2z_1^{-1} = jz_1^{\sigma} - ja^{\sigma}.$$

This can be further rearranged to yield

$$ax^2 + ja^{\sigma} = a^2x^2z_1^{-1} + jz_1^{\sigma}.$$

Therefore if we let d_1 and c_1 denote elements of $\mathbb{F}_q$ such that $d_1^2 = z_1$ and $c_1 = axd_1^{-1}$ the following two equations hold.

$$\begin{aligned} (ax^2 + ja^{\sigma}, 2ax) &= (c_1^2 + jd_1^{2\sigma}, 2c_1d_1) \\ &= (c_1, d_1) * (c_1, d_1) \\ (ax^2 + ja^{\sigma}, 2ax) &= (c_1^2 + jd_1^{2\sigma}, -2c_1d_1) \\ &= (c_1, -d_1) * (c_1, -d_1) \end{aligned}$$

Now let d_2 and c_2 denote elements of $\mathbb{F}_q$ such that $d_2^2 = z_2$ and $c_2 = axd_2^{-1}$, then the following two equations also hold.

$$\begin{aligned}(ax^2 + ja^\sigma, 2ax) &= (c_2^2 + jd_2^{2\sigma}, 2c_2d_2)\\ &= (c_2, d_2) * (c_2, d_2)\\ (ax^2 + ja^\sigma, 2ax) &= (c_2^2 + jd_2^{2\sigma}, -2c_2d_2)\\ &= (c_2, -d_2) * (c_2, -d_2)\end{aligned}$$

Moreover since z_1 and z_2 are distinct, nonzero squares in $\mathbb{F}_q$, it follows that d_1, $-d_1$, d_2, and $-d_2$ are all distinct elements of $\mathbb{F}_q$. By the previous equation we see (c_1, d_1), $(c_1, -d_1)$, (c_2, d_2), and $(c_2, -d_2)$ are distinct elements of the Dickson semifield that have the same image under squaring. This contradicts Lemma 6.3.1, which states that $g(y) = y^2$ is a two-to-one function on the nonzero elements of a commutative semifield. □

7.3.4 Lemma. *Let a be a nonzero nonsquare in $\mathbb{F}_q$. The element $(ax, a) * (x, 1)$ is a nonzero square in the Dickson semifield of order q^2 for all x in $\mathbb{F}_q$.*

Proof. If $x = 0$, then we have

$$\begin{aligned}(ax, a) * (x, 1) &= (0, a) * (0, 1)\\ &= (ja^\sigma, 0)\end{aligned}$$

From our comments at the end of Section 6.3, we see that $(ja^\sigma, 0)$ is a square in the Dickson semifield for all a.

Now we consider the case when $x \neq 0$. By our result from Lemma 7.3.3, the function

$$f_a(z) = ja^{-1}z(z-a)^{\sigma-1}$$

is a permutation on $\mathbb{F}_q^*$. Therefore there exists an element z in S such that

$$f_a(z) = x^2.$$

If we let d and c denote elements of $\mathbb{F}_q$ such that $d^2 = z$ and $c = axd^{-1}$ then from our work in the proof of Lemma 7.3.3, we see that

$$(ax^2 + ja^{2\sigma}, 2ax) = (c^2 + jd^{2\sigma}, 2cx).$$

This implies.

$$(ax, a) * (x, 1) = (c, d) * (c, d)$$

□

We piece together these results to prove that the family of cliques constructed in 7.3.1 contains q distinct cliques of size q.

7.3.5 Lemma. *The family of sets $\mathcal{C}$, as defined in Equation 7.3.1, contains q distinct cliques of size q which contain 0.*

Proof. We have already shown that $C_{(1,0)}$ is a clique. From Lemmas 7.3.2 and 7.3.4, we see that for each x in $\mathbb{F}_q$ the set $C_{(x,1)}$ contains q semifield squares and is an additive subgroup of the semifield. Therefore we conclude that $C_{(x,1)}$ is a clique of size q.

Now we prove that q of these cliques are distinct. First we consider the cliques $C_{(1,0)}$ and $C_{(0,1)}$.

Note that

$$C_{(1,0)} = \{(a,0) : a \in \mathbb{F}_q\}.$$

Also note that

$$\begin{aligned} C_{(0,1)} &= \{(0,a) * (0,1) : a \in \mathbb{F}_q\} \\ &= \{(ja^\sigma, 0) : a \in \mathbb{F}_q\} \end{aligned}$$

Therefore $C_{(1,0)} = C_{(0,1)}$, and these cliques are not distinct. To show that the other $q-1$ cliques in $\mathcal{C}$ are distinct from $C_{(0,1)}$ and from each other, it suffices to show that $C_{(x,1)}$ is distinct from $C_{(y,1)}$ for distinct x and y in $\mathbb{F}_q$. Suppose for a contradiction that $C_{(x,1)} = C_{(y,1)}$ where $x \neq y$. Then for each a in $\mathbb{F}_q^*$, we must have a corresponding b in $\mathbb{F}_q^*$ such that

$$(ax^2 + ja^\sigma, 2ax) = (by^2 + jb^{2\sigma}, 2by)$$

Equality in the second coordinate implies $b = axy^{-1}$. Substituting this into the first coordinate implies

$$ax^2 + ja^\sigma = axy + ja^{2\sigma}x^{2\sigma}y^{-2\sigma}.$$

Rearranging this yields

$$ax^2 + ja^\sigma - axy + ja^{2\sigma}x^{2\sigma}y^{-2\sigma} = 0. \tag{7.3.5}$$

Recall that x and y are fixed elements of $\mathbb{F}_q^*$. Therefore the left hand side of 7.3.5 is a nonzero polynomial of a. Furthermore, each a in $\mathbb{F}_q^*$ must be a root of the polynomial on the left hand side of this equation. However, since the polynomial has degree 2σ, there must be at most 2σ roots.

Recall that p is an odd prime and $q = p^r$ for some positive integer r. Since σ is a nontrivial field automorphism, it follows that $\sigma = p^i$ for some $0 < i < r$. Moreover, we have $2\sigma < q - 1$. This contradiction confirms that $C_{(x,1)}$ is distinct from $C_{(y,1)}$. □

This allows us to prove the desired distinction between the partial difference sets corresponding to the nonzero squares of $\mathbb{F}_{q^2}$ and the nonzero squares of the Dickson semifield of order q^2.

7.3.6 Theorem. *Let q be a nontrivial odd prime power, and let G denote the additive group of $\mathbb{F}_{q^2}$, which is isomorphic to the additive group of the Dickson semifield of order q^2. Also let S denote the set of nonzero squares of $\mathbb{F}_{q^2}$, and let $D(q)$ denote the set of nonzero squares of the Dickson semifield. Then S is not SRG-equivalent to $D(q)$, and hence not PDS-equivalent to $D(q)$.*

Proof. From our comments in Section 7.1, it suffices to prove that the Cayley graphs $X(G, S)$ and $X(G, D(q))$ are not isomorphic. In Chapter 2, we saw that $X(G, S)$ contains exactly $(q + 1)/2$ distinct cliques of size q which contain 0. By the result of 7.3.5, we know that $X(G, D(q))$ contains at least q distinct cliques of size q which contain 0. Therefore the graphs are not isomorphic. □

7.4 Computational Results

As we did with Peisert Graphs, we use a computer to count the number of cliques which contain 0 and are maximal with respect to size. Again, the computations were performed on a 2.8 Ghz processor using a combination of SAGE and Cliquer routines.

For all of the cases that were small enough to test in a reasonable amount of time on a computer, we see that when $q \equiv 1 \pmod 4$, the q distinct cliques of size q from the family constructed in Section 7.3.1 are all of the maximal cliques. In the other case, when $q \equiv 3 \pmod 4$, there was one additional clique of the form

$$\{(0, a) : a \in \mathbb{F}\}.$$

However, at this time we are unable to prove in general that these are the only cliques of size q or even that the size of the maximal clique is q. We do not know if the semifield graphs are self-complementary in general. Thus we cannot apply the Delsarte-Hoffman bound to obtain a bound on the size of a maximal clique in the semifield graphs.

Weng, Qiu, Wang, and Xiang conjecture that semifield graphs are not self-complementary when the graph has more than 81 vertices [24]. We verified this holds in the small cases we tested.

Here we give a summary of our computational results for the semifield graphs described in Section 6.3. The computations were performed using a combination of SAGE [21] and Cliquer [17] routines. The columns labelled *SC?* indicate whether the corresponding graphs are self-complementary.

Table 7.1: **Dickson Semifield Graphs**

q^2	Max Clique Size	# Max Cliques on 0	SC?
3^4	3^2	3^2	Yes
5^4	5^2	5^2	No
3^6	3^3	3^3+1	No

Table 7.2: **Cohen-Ganley Semifield Graphs**

q^2	Max Clique Size	# Max Cliques on 0	SC?
3^4	3^2	3^2	Yes
3^6	3^3	3^3+1	No

Table 7.3: **Ganley Semifield Graphs**

q^2	Max Clique Size	# Max Cliques on 0	SC?
3^6	3^3	1	No

Chapter 8

Future Work

There are a number of ways the work presented in this thesis could be extended. First, it would be useful to prove that when $q \equiv 3 \pmod 4$ the only cliques of size q in Peisert graphs of order q^2 correspond to lines in $AG(2, q)$. where $q \equiv 3 \pmod 4$. This result is suggested by the computational results given in Section 3.4. A possible method of proof might be to modify Blockhuis' proof of the same result for Paley graphs. However, there does not seem to be a straightforward method of doing this, since the connection set of a Peisert graph is not closed under multiplication as it is in a Paley graph.

Second, it would be desirable to confirm that the generalized Peisert graphs described in Section 5.3 are distinct from Peisert and Paley graphs for infinitely many prime powers. This would answer a conjecture of Mathon [16].

Finally, it would be interesting to completely prove Weng, Qiu, Wang, and Xiang's conjecture that the pseudo-Paley graphs described in Section 6.3 are distinct from Paley and Peisert graphs [24]. We proved that the Dickson semifield graphs are distinct from Paley graphs by counting the number of cliques of size q in both families of graphs. If it could be shown that when $q \equiv 3 \pmod 4$ the only cliques in size q in Peisert graphs of order q^2 correspond to lines in $AG(2, q)$, then it would follow that the Dickson semifield graphs are distinct from Peisert graphs in this case. However, another method would need to be utilized to distinguish the Dickson semifield graphs from Peisert graphs of order q^2 where $q \equiv 1 \pmod 4$. It is possible that the clique counting method could be applied to distinguish other families of pseudo-Paley graphs from Paley and Peisert graphs.

Appendix A: SAGE Code

Below are the SAGE methods used to construct the graphs studied in this thesis. Note that SAGE has a Python-based interface [21].

1. This method constructs self-complementary generalized Peisert graphs. In particular, the method generates the $(q+1)$-th power Peisert graph of order q^2, which we have shown to be self-complementary and strongly regular in Section 5.3.

```
def GenPeisert(q):
   F.<a> = FiniteField(q^2)
   n = (q+1)/2
   pows = [a^(2*n*i+j) for i in [0..(p^2-1)/(2*n)-1] for j in [0..n-1]]
   return Graph([F, lambda i,j: i-j in pows])
```

2. This method constructs the Dickson semifield graph on p^{2r} vertices where p is a prime and $r > 1$.

```
def DicksonSRG(p,r):
   K.<a> = FiniteField(p^r)
   V = [(x,y) for x in K for y in K]
   D = [(x^2 + a*y^(2*p), 2*x*y) for x in K for y in K]
   return Graph([V, lambda i,j: i != j and subt(i,j) in D])
```

3. This method constructs Ganley semifield graph for $q = p^r$ where $p = 3$ and $r \geq 3$ and r odd.

```
def GanleySRG(q):
   K.<a> = FiniteField(q)
   V = [(x,y) for x in K for y in K]
   D = [(x^2 + y^10, 2*x*y + y^6) for x in K for y in K]
   return Graph([V, lambda i,j: i != j and subt(i,j) in D])
```

4. This method constructs Cohen-Ganley graph for $p = 3$ and $r \geq 2$.

```
def CGSRG(p,r):
   K.<a> = FiniteField(p^r)
   V = [(x,y) for x in K for y in K]
   D = [(x^2 + a*y^2 + a^3*y^18, 2*x*y + a*y^6) for x in K for y in K]
   return Graph([V, lambda i,j: i != j and subt(i,j) in D])
```

5. This method constructs the Pentilla-Williams semifield graph. The graph has 3^{10} vertices.

```
def PWSRG():
   K.<a> = FiniteField(3^5)
   V = [(x,y) for x in K for y in K]
   D = [(x^2 + y^18, 2*x*y + y^54) for x in K for y in K]
   return Graph([V, lambda i,j: i != j and subt(i,j) in D])
```

References

[1] Norman Biggs. *Finite groups of automorphisms.* Cambridge University Press, London, 1971. London Mathematical Society Lecture Note Series, 6.

[2] A. Blokhuis. On subsets of GF(q^2) with square differences. *Nederl. Akad. Wetensch. Indag. Math.*, 46(4):369–372, 1984.

[3] Béla Bollobás and Andrew Thomason. Graphs which contain all small graphs. *European J. Combin.*, 2(1):13–15, 1981.

[4] D. A. Burgess. On character sums and primitive roots. *Proc. London Math. Soc. (3)*, 12:179–192, 1962.

[5] Chong-yun Chao. On the classification of symmetric graphs with a prime number of vertices. *Trans. Amer. Math. Soc.*, 158:247–256, 1971.

[6] F. R. K. Chung, R. L. Graham, and R. M. Wilson. Quasi-random graphs. *Combinatorica*, 9(4):345–362, 1989.

[7] Stephen D. Cohen and Michael J. Ganley. Commutative semifields, two-dimensional over their middle nuclei. *J. Algebra*, 75(2):373–385, 1982.

[8] D. A. Foulser and Michael J. Kallaher. Solvable, flag-transitive, rank 3 collineation groups. *Geometriae Dedicata*, 7(1):111–130, 1978.

[9] David A. Foulser. The flag-transitive collineation groups of the finite Desarguesian affine planes. *Canad. J. Math.*, 16:443–472, 1964.

[10] Chris Godsil and Gordon Royle. *Algebraic Graph Theory*, volume 207 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2001.

[11] S. W. Graham and C. J. Ringrose. Lower bounds for least quadratic nonresidues. In *Analytic number theory (Allerton Park, IL, 1989)*, volume 85 of *Progr. Math.*, pages 269–309. Birkhäuser Boston, Boston, MA, 1990.

[12] William M. Kantor. Finite semifields. In *Finite geometries, groups, and computation*, pages 103–114. Walter de Gruyter GmbH & Co. KG, Berlin, 2006.

[13] Andrzej Kisielewicz and Wojciech Peisert. Pseudo-random properties of self-complementary symmetric graphs. *J. Graph Theory*, 47(4):310–316, 2004.

[14] Martin W. Liebeck. The affine permutation groups of rank three. *Proc. London Math. Soc. (3)*, 54(3):477–516, 1987.

[15] L. Lovász and A. Schrijver. Remarks on a theorem of Rédei. *Studia Sci. Math. Hungar.*, 16(3-4):449–454, 1983.

[16] Rudolf Mathon. On self-complementary strongly regular graphs. *Discrete Math.*, 69(3):263–281, 1988.

[17] Sampo Niskanen and Patric R. J. Östergård. *Cliquer User's Guide, Version 1.0.* Communications Laboratory, Helsinki University of Technology, Espoo, Finland, Tech. Rep. T48, 2003.

[18] Wojciech Peisert. Direct product and uniqueness of automorphism groups of graphs. *Discrete Math.*, 207(1-3):189–197, 1999.

[19] Wojciech Peisert. All self-complementary symmetric graphs. *J. Algebra*, 240(1):209–229, 2001.

[20] László Rédei. *Lückenhafte Polynome über endlichen Körpern.* Birkhäuser Verlag, Basel, 1970. Lehrbücher und Monographien aus dem Gebiete der exakten Wissenschaften, Mathematische Reihe, Band 42.

[21] William Stein. *Sage: Open Source Mathematical Software (Version 3.1.1).* The Sage Group, 2008. `http://www.sagemath.org`.

[22] Jacobus H. van Lint and F. Jessie MacWilliams. Generalized quadratic residue codes. *IEEE Trans. Inform. Theory*, 24(6):730–737, 1978.

[23] André Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent.* Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945). Hermann et Cie., Paris, 1948.

[24] Guobiao Weng, Weisheng Qiu, Zeying Wang, and Qing Xiang. Pseudo-Paley graphs and skew Hadamard difference sets from presemifields. *Des. Codes Cryptogr.*, 44(1-3):49–62, 2007.

[25] Hong Zhang. Self-complementary symmetric graphs. *J. Graph Theory*, 16(1):1–5, 1992.

[26] Hong Zhang. On edge transitive circulant graphs. *Tokyo J. Math.*, 19(1):51–55, 1996.

Index