Dissertation

Abstract Hyperovals, Partial Geometries, and Transitive Hyperovals

Submitted by

Benjamin C. Cooper

Department of Mathematics

In partial fulfillment of the requirements

For the Degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Summer 2015

Doctoral Committee:

Advisor: Timothy Penttila

Wim Bohm
Renzo Cavalieri
Jeanne Duflot

Abstract

Abstract Hyperovals, Partial Geometries, and Transitive Hyperovals

A hyperoval is a (q+2)- arc of a projective plane π, of order q with q even. Let G denote the collineation group of π containing a hyperoval Ω. We say that Ω is transitive if for any pair of points x, $y \in \Omega$, there exists a $g \in G$ fixing Ω setwise such that $x^g = y$. In 1987, Billotti and Korchmaros proved that if $4||G|$, then either Ω is the regular hyperoval in PG(2,q) for q=2 or 4 or $q = 16$ and $|G||144$. In 2005, Sonnino proved that if $|G| = 144$, then π is desarguesian and Ω is isomorphic to the Lunelli-Sce hyperoval. For our main result, we show that if G is the collineation group of a projective plane containing a transitive hyperoval with 4 $||G|$, then $|G| = 144$ and Ω is isomorphic to the Lunelli-Sce hyperoval. We also show that if $A(X)$ is an abstract hyperoval of order $n \equiv 2(mod\ 4)$, then $|Aut(A(X))|$ is odd. If $A(X)$ is an abstract hyperoval of order n such that $Aut(A(X))$ contains two distinct involutions with $|Fix_X(g)|$ and $|Fix_X(f)| \geq 4$. Then we show that $Fix_X(g) \neq Fix_X(f)$. We also show that there is no hyperoval of order 12 admitting a group whose order is divisible by 11 or 13, by showing that there is no partial geometry $pg(6, 10, 5)$ admitting a group of order 11 or of order 13. Finally, we were able to show that there is no hyperoval in a projective plane of order 12 with a dihedral subgroup of order 14, by showing that that there is no partial geometry $pg(7, 12, 6)$ admitting a dihedral group of order 14. The latter results are achieved by studying abstract hyperovals and their symmetries.

Acknowledgements

I am very grateful for the numerous conversations with Tim Penttila. He is a great mentor and true friend. I am also grateful for the love and support received from my father- B.C Cooper , my mother and stepfather- Marilyn and Roderick Fitzgerald, as well as my family and friends.

Last but not least, I would like to acknowledge my grandmother- Marian E. Lane ("Granny"). Whose humble beginnings- dirt poor, worked as a sharecropper in Mississippi as a child did not stop her from raising 10 children, and a few grandchildren as well. She realized the value of education and instilled it in my father- who in turn instilled it in me. She told me before she passed on my birthday last year: "I'm so proud of you Dr. Cooper! I can't believe my grandson is going to be a doctor of math! I always knew you would do great things in your life!" Her sacrifice for me will not be in vain. I love you Granny!

This dissertation is typset in LaTeX using a document class designed by Leif Anderson.

Table of Contents

CHAPTER 1

Introduction

In 1987, Biliotti and Korchmaros [9] showed that a hyperoval of a projective plane of even order that admits a group of order divisible by four is either a regular hyperoval in a Desarguesian plane of order 2 or 4 or is in a plane of order 16 and has group of order at most 144. In 2005, Sonnino [78] showed that a transitive hyperoval of a projective plane of order 16 with a group of order 144 is necessarily the hyperoval of the Desarguesian plane of order 16 constructed by Lunelli and Sce[60] in 1958. Here we rule out the remaining cases, completing the proof of the

Theorem 1.1. ***Main Theorem*** *A hyperoval of a projective plane of even order that admits a group of order divisible by four is either a regular hyperoval in a Desarguesian plane of order 2 or 4 or the Lunelli-Sce hyperoval of the Desarguesian plane of order 16.*

Our discussion will begin with a review of the relevant background material accompanied by a host of examples to aid in the absorption of the material. Next, we delve a little deeper into the theory of partial geometries focusing our attention on projective planes, hyperovals, and their automorphisms. Abstract hyperovals and their automorphisms our introduced at the next stage, as well as a few results- some of which are new. The proof of the main theorem is in the final chapter, where we'll also discuss transitive hyperovals, and the results (past and new) needed for proving our main result.

1.1. Opening Remarks

Finite geometry is concerned with the analysis of information representable through finite incidence structures. There is great power and elegance in a purely combinatorial or geometric proof; however, these results are notoriously tricky to conjure up. To date, many results in finite geometry are obtained through of a wealth of methods and tools from many areas of mathematics. In addition, even the most modest of modern results require vast amounts of CPU computations (and memory). Our methods combine old fashion blue-collar counting arguments with (less vast) CPU computations. The remainder of this chapter will focus on building up the vocabulary essential for understanding the ideas presented in the later chapters.

CHAPTER 2

Incidence Structures

By an *incidence structure* we mean a triple $S = (P, L, I)$ consisting of: a non-empty set, P, whose elements we call *points*, a non-empty set, L, disjoint from P, whose elements we call *blocks, lines, or edges*, and a binary relation I between P and L; that is, a subset of $P \times L$, which we call *incidence*. The converse I^* of I is $\{(l, X) \in L \times P \colon (X, l) \in I\}$, and it allows us to define the *dual* incidence structure $S^* = (L, P, I^*)$ of S.

2.1. t-Designs & Steiner Systems

When we use set membership as incidence, and when no blocks are incident with the same set of points, we may identify each block with the set of points incident with it. A $t - design$ or (t, v, k, λ)-*design* is an incidence structure $(P,\ B,\ \in)$ consisting of: a set P of points of cardinality v, as well as a set B of k element subsets of P called blocks with $I = \{(p, b)\ \in I\ \Leftrightarrow\ p \in b\}$ satisfying the following axiom:

- **TD 1:** any t points are contained in exactly λ blocks.

A **Steiner system** is a t-design with $\lambda = 1$.

Example 2.1.1

Let $P = \{a,\ b,\ c,\ d\}$, $B = \{\ \{\ a,\ b\ \}, \{a,\ b\ \}, \{\ a,\ d\ \}, \{\ b,\ c\ \}, \{\ b,\ d\ \}, \{\ c,\ d\ \}\ \}$. Then $S\ =\ (P, B, \in)$ is a Steiner System with $t = 2$.

Example 2.1.2

The previous example generalizes as follows. Let $K_n = (V, E)$ denote the complete graph on n vertices. Let $P = V$ (vertices of K_n) $= \{v_1, \ldots, v_n\}$. Let $B = E$ (edges of K_n). Define $S_{K_n} = (P, B, \in)$. To see that S_{K_n} is a Steiner system with $t = 2$, observe that **TD 1** follows directly from the from the definition of a complete graph. The correspondence with the complete graph on n vertices ($n > 1$) allows us to construct an infinite family of Steiner systems, $\{S_{K_n}\}_{n \in \mathbb{N} - \{1\}}$.

Example 2.1.3

Let $P = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Now the blocks are given by: $b_1 = \{1, 2, 3\}$, $b_2 = \{1, 4, 7\}$, $b_3 = \{1, 5, 9\}$, $b_4 = \{1, 6, 8\}$, $b_5 = \{2, 4, 9\}$, $b_6 = \{2, 5, 8\}$, $b_7 = \{2, 6, 7\}$, $b_8 = \{3, 4, 8\}$, $b_9 = \{3, 5, 7\}$, $b_{10} = \{3, 6, 9\}$, $b_{11} = \{4, 5, 6\}$, $b_{12} = \{7, 8, 9\}$. Then $(P, B, \in)$ is a Steiner system with $t = 2$.

2.2. Strongly Regular Graphs

A strongly regular graph Γ, with parameters, (n, k, λ, μ), is a graph with the following properties:

- Γ has n vertices,
- Γ is k-regular,
- any adjacent pair of vertices has exactly λ common neighbors, and finally
- Γ any pair of non-adjacent vertices has exactly μ neighbors in common.

Assume that Γ is a strongly regular graph on n vertices. The *adjacency matrix* of Γ which we denote A, is an $n \times n$ array of $a_{i,j}$ such that:

$$a_{i,j} \ = \ 1 \ if \ v_i v_j \ \in \ E(\Gamma), \ 0 \ otherwise.$$

Strongly regular graphs have interesting properties when observed through the lens of an adjacency matrix.

Claim: Suppose that Γ is a strongly regular graph with parameters (n, k, λ, μ), and let J denote the $n \times n$ all ones matrix. Then

- $$AJ \ = \ kJ$$
- $$A^2 \ + \ (\mu \ - \ \lambda)A \ + \ (\mu \ - \ k)I \ = \ \mu J$$

A great deal of work has gone towards the analysis of the eigenvalues of the adjacency matrix of a strongly regular graph. In fact, given the parameters one may determine the eigenvalues with multiplicity of the corresponding adjacency matrix. The adjacency matrix has three eigenvalues, k , the regularity of Γ, as well as two others, l and r, ($r > 0$ and $l < 0$) with

$$r \ + \ l \ = \ \lambda \ - \ \mu,$$

$$rl \ = \ \mu \ - \ k.$$

We list some of the known criteria for the existence of a strongly regular graph.

THEOREM 2.1. *If Γ is a strongly regular graph with parameters, (n, k, λ, μ) then the following is true:*

(1)

$$n \ - \ 2k \ + \mu \ - \ 2 \ \geq 0$$

(2)

$$k(k \ - \ \lambda \ - l) \ = \ \mu(n \ - \ k \ - \ 1)$$

(3) *Let f and g denote the multiplicity of the eigenvalues r and l, respectively. Then*

$$f \ = \ \frac{k(l \ + \ 1)(l \ - \ k)}{(k \ + \ rl)(r \ - \ l)}, \ g \ = \ \frac{k(r \ + \ 1)(k \ - \ r)}{(k \ + \ rl)(r \ - \ l)},$$

where f and g must both be integral and non-negative.

(4) *(The Krein Conditions)*

$$(r+1)(k+r+2rl) \ \leq \ (k+r)(l+1)^2,$$

$$(l+1)(k+l+2rl) \ \leq \ (k+l)(r+1)^2.$$

Example 2.2.1

Let S_6 denote the symmetric group on six points, and X its associated $G-Set$. Consider the graph with vertices the set of fixed point free involutions in S_6, $V = (1,2)(3,4)(5,6)^{S_6}$, and edge set $E = \{(a,b) \ \in \ V \times V : |Fix_X(a*b)| \ = \ 2.\}$. Then the resulting graph $\Gamma \ = \ (V, E)$ has the following properties.

(1) $|V| = 15$ ($n = 15$).

(2) Every vertex has exactly 6 neighbors ($k = 6$).

(3) Every pair of adjacent vertices share exactly 1 neighboring vertex ($\lambda = 1$).

(4) Every pair of non-adjacent vertices share exactly 3 neighboring vertices in common ($\mu = 1$).

It is worth noting that the previous graph was also an example of an abstract hyperoval, to be defined later in our discussion.

Example 2.2.2 The above example generalizes as follows. Let $A(X)$ denote an abstract hyperoval of order q, and S_{q+2} denote the symmetric group on $q+2$ points, and X its associated $G - Set$. Define $\Gamma = (V, E)$ with $V = A(X)$, and edge set $E = \{(a, b) \in V \times V : |Fix_X(a * b)| = 2.\}$. Then the resulting graph $\Gamma = (V, E)$ has the following properties.

(1) $|V| = q^2 - 1$ ($n = q^2 - 1$).

(2) Every vertex has exactly $\frac{(q-2)(q+2)}{2}$ neighbors ($k = \frac{(q-2)(q+2)}{2}$).

(3) Every pair of adjacent vertices share exactly $\frac{q^2-2q-6}{2}$ neighboring vertices ($\lambda = \frac{q^2-2q-6}{2}$).

(4) Every pair of non-adjacent vertices share exactly $\frac{q^2-4}{4}$ neighboring vertices in common ($\mu = \frac{q^2-4}{4}$).

We will later on show that we may construct an abstract hyperoval for each classical projective plane $PG(2, q)$. This provides us with a systematic method of constructing strongly regular graphs with these parameters whenever there exists a finite field of order q. Therefore, we obtain an infinite family of strongly regular graphs- one for each prime power q.

Example 2.2.3 The triangle graph $\mathcal{T}_n$ is the line graph of K_n. It is the graph corresponding to the dual of the incidence matrix of K_n. $\mathcal{T}_n$ may also be obtained by reversing the incidence containment relation which is induced by the map $I = V \times E \mapsto E \times V = I^*$, where $(e, v) \in I^* \Leftrightarrow e \ni v$. Denote this process as dualizing. We claim that $\mathcal{T}_n$ is strongly regular for any natural n.

To count the vertices of $\mathcal{T}_n$ we count the edges of K_n. In K_n every vertex shares an edge, and there are n vertices- this gives us $\binom{n}{2} = \frac{n(n-1)}{2}$ vertices for $\mathcal{T}_n$.

To compute the degree of a vertex of $\mathcal{T}_n$, we observe that any vertex of K_n is adjacent to n-1 other vertices. Therefore, there are n-1 edges incident with any vertex. Now any edge uv meets an additional n-2 edges at vertices u and v. Given that $\mathcal{T}_n$ is the dual of K_n, we see that the regularity $k = 2(n\text{-}2)$.

Consider two adjacent edges uv and vw which meet at the vertex v in K_n. To compute the number of edges adjacent to both uv and vw we write the vertices of $K_n - \{u, v, w\}$ as $x_1, \ldots, x_{n-3}$. It follows from the definition of the complete graph that there exist edges $x_1v,\ x_2v,\ \ldots,\ x_{n-3}v$ that are adjacent to both uv and vw at v. There is one additional edge, uw that is adjacent to both uv and vw. Adding them all up gives us a total of $n - 3 + 1 = n - 2 = \lambda$.

Finally, to compute the number of common edges shared by nonadjacent edges of K_n, we consider two non-adjacent edges uv & wx. Again, by the definition of K_n, we see that there are only four edges namely, uw, ux, vw, vx. Thus, $\mu = 4$.

At last, we have shown that $\{\mathcal{T}_n\}_{n\in\mathbb{N}}$ is an infinite family of strongly regular graphs with parameters $(\binom{n}{2}, 2(n\text{-}2), n - 2, 4)$.

2.3. Partial Geometries

A *partial geometry* $pg(s,t,\alpha)$ with parameters v, k, α is an partial linear space consisting of: a set P of points, a set L of lines satisfying the following axioms:

- any line is incident with s+1 points,
- any point is incident with exactly t+1 lines,
- if (p, L) is a non-incident point-line pair, there exists exactly α lines through p incident with a point incident with L.

This incidence structure was introduced by Bose [1963]. The following results are known about partial geometries, and can also be found in [**?**]:

- If $S = (P, B, I)$ is a partial geometry with parameters (s, t, α), then the dual structure $S^* = (P^*, B^*, I^*) = (B, P, I)$ with $s^* = t$, $t^* = s$, and $\alpha^* = \alpha$, is also a partial geometry.
- $$|P| \ = \ v \ = \ (s \ + \ 1)\frac{st \ + \ \alpha}{\alpha}, \ \&, \ |B| \ = \ ((t \ + \ 1)\frac{st \ + \ \alpha}{\alpha}$$
- The partial geometries with $\alpha = 1$ are generalized quadrangles.
- The partial geometries with $\alpha = s + 1$ or dually $\alpha = t + 1$ correspond to 2-(v, s + 1,1) designs and their duals.

The point graph of a partial geometry $S = pg(s,t,\alpha)$ is a graph $\Gamma(S)$, with

$$V(\Gamma(S)) \ = \ P,$$

and the following edge relation:

$$xy \ \in E(\Gamma(S)) \ \Leftrightarrow \ \exists \, b \ \in B : \{x, y\} \subset b.$$

The following result is due to [11] :

THEOREM 2.2. *The point graph of a partial geometry $pg(s,t,\alpha)$, is a strongly regular graph with parameters (n,k,λ,μ) such that:*

$$n = \frac{(s+1)(st+\alpha)}{\alpha},\ k = s(t+1),$$

$$\lambda = s-1+t(\alpha-1),\ \mu = \alpha(t+1).$$

A strongly regular graph having the parameters above, with

$$t \geq 1,\ s \geq 1,$$

$$1 \leq \alpha \leq s+1,\ \&\ 1 \leq \alpha \leq t+1$$

is called $pseudo-geometric$. It is worth pointing out that a strongly regular graph having the parameters above may not necessarily come from a partial geometry. In the case where a strongly regular graph Γ, with the parameters (n,k,λ,μ) corresponds to the point graph of a partial geometry, we say that Γ is *geometric*. Another result from Bose gives us a way to determine if a pseudo-geometric graph is geometric from the parameters.

THEOREM 2.3. *[11] A pseudo-geometric graph with parameters*

$$n = \frac{(s+1)(st+\alpha)}{\alpha},\ k = s(t+1),$$

$$\lambda = s-1+t(\alpha-1),\ \mu = \alpha(t+1)$$

is geometric if

$$2(s+1) > t(t+1) + \alpha(t+2)(t^2+1)$$

THEOREM 2.4. *If* Γ *is a pseudo-geometric graph with parameters* (s, t, α)*, then*

$$r = s - \alpha,$$

Let us review some important examples of partial geometries. Many of these can be found in [**?**].

Example 2.3.1 The Partial Geometry: S(Ω)

This infinite family was constructed by Thas and independently by Wallis [**?**]. Let π denote a projective plane of order q. Also, let Ω denote a maximal arc in π of degree d. We define the incidence structure $S(\Omega) = (P, B, I)$. The points of $S(\Omega)$ are the points of π that are not contained in Ω. The lines of $S(\Omega)$ are the lines of π that are incident with d points of Ω. The incidence is that of π. Then $S(\Omega)$ is a partial geometry with parameters,

$$t = q - \frac{q}{d},\ s = q - d,\ \alpha = q - \frac{q}{d} - d + 1.$$

The following example is an infinite family first constructed by Thas [**?**].

Example 2.3.2 The Partial Geometry: $\mathcal{T}_2^*(\mathcal{K})$

Let $\mathcal{K}$ be a maximal arc of degree d in $PG(2, q)$ over $GF(q)$. As $\mathcal{K}$, has only passants and d-secants, it will yield a linear representation of a partial geometry in $AG(3, q)$. This partial geometry $\mathcal{T}_2^*(\mathcal{K})$ has parameters:

$$t = (q + l)(d - 1),\ s = q\ 1,\ \alpha = d - 1.$$

For the previous example, it can be shown that in the case where q is a power of 2, that $\mathcal{T}_2^*(\mathcal{K})$ is a generalized quadrangle if and only if $\mathcal{K}$ is a hyperoval. The final example from this section is another infinite class of partial geometries constructed by De Clerck, Dye, and Thas [**?**].

Example 2.3.3 The Partial Geometry: $PQ^+(4n-1, 2)$

Define a spread Σ of the non-singular hyperbolic quadric

$$Q^+ \ = \ Q^+(4n-1, \ 2): \ n \ \geq \ 2,$$

in $PG(4n-1, \ 2)$ to be a maximal set of $2^{2n-1}+1$ disjoint $(2n-1)$-dimensional spaces on Q^+. Let Σ be a spread of Q^+ and let Ω be the set of all hyperplanes of the elements of Σ.

Define an incidence structure $\mathbf{PQ}^+(4n-1, \ 2) = (P, L, I)$, with points and lines given by:

- $P = \{x \ \in PG(4n-1, \ 2): \ \{x\} \cap Q^+ \ = \ \emptyset\}$,
- $L = \Omega$,
- $(x, \ell) \in I \Leftrightarrow x \in$ the polar space ℓ^* of ℓ with respect to Q^+.

The incidence structure given above is a partial geometry with parameters

$$s \ = \ 2^{2n-1}-1, \ t \ = \ 2^{2n-1}, \ \alpha \ = \ 2^{2n-2}.$$

2.4. Partial Linear Spaces

A *partial linear space* is an incidence structure $S = (P, L, I)$ consisting of points, lines satisfying the following axioms:

- any line is incident with at least two points, and
- two points are jointly incident with at most one line.

Example 2.4.1 Let $P = \{1,2,3,4,5\ \}$, $L = \{\ \{1,2\ \}, \{2,3\ \}, \{4,5\ \}\ \}$. Then $(P, L, \in)$ is a partial linear space.

Example 2.4.2 A **parallelism** of a plane is a partition of its point set into sets of parallel lines. Each parallelism induces a partial linear space which we denote S_m and construct as follows.

Let $(K, +, *)$ be a division algebra, and $P = K^2$. Define $L = \{\ell_b = \{(x,\ mx + b) \in K^2\}\ \}_{b \in K}$. This allows us to define incidence as $I = \{(P, \ell_b) \in P \times L :\ P = (x,\ mx + b)\}$. Then $S_m = (P, L, I)$ is a partial linear space for all $m \in K$ and thereby defines an infinite family of partial linear spaces parameterized by K.

Example 2.4.3 Let $P = \mathbb{S}^1 = \{(x, y) \in \mathbb{R}^2 |\ x^2 + y^2 = 1\}$. Define $L = \{\ell_\theta = \{(cos(\theta),\ sin(\theta)),\ (cos(\theta + \pi),\ sin(\theta + \pi))\} \subset \mathbb{R}^2\}\ \}_{b \in \mathbb{R}}$. This allows us to define incidence as $I = \{(P, \ell_\theta) \in P \times L :\ P \in \ell_\theta\}$. A quick inspection shows us that any line has exactly two points, and that two points are incident with at most one line. It follows that $S_{\mathbb{S}^1}$ is a partial linear space.

Example 2.4.4 Let $P = \mathbb{S}^1 = \{(x, y) \in \mathbb{R}^2 |\ x^2 + y^2 \leq 1\}$. Define $L = \{\ell_\theta = \{(x, (\frac{sin(\theta) - sin(\theta + \pi)}{cos(\theta) - cos(\theta + \pi)})x - cos(\theta)(\frac{sin(\theta) - sin(\theta + \pi)}{cos(\theta) - cos(\theta + \pi)}) + sin(\theta)) :\ x \in [-1, 1]\} \subset \mathbb{R}^2\}\ \}_{\theta \in [0, 2\pi]}$. This allows us to define incidence as $I = \{(P, \ell_\theta) \in P \times L :\ P \in \ell_\theta\}$. A quick inspection shows us that any line has at least two points, and that two points are incident with at most one line. It follows that $S_{\overline{\mathbb{D}^1}} = (P, L, I)$ is a partial linear space.

2.5. Linear Spaces

A *linear space* is an incidence structure $S = (P, L, I)$ consisting of points, lines, satisfying the following axioms:

- **LS1** any line is incident with least two points, and
- **LS2** every two points are jointly incident with a unique line.

Example 2.5.1 Let P = {1,2,3,4 }, L = { {1,2 }, {1,3 }, {1,4 }, {2,3 }, {2,4 }, {3,4 } }. Then $S = (P, L, \in)$ is a linear space.

Example 2.5.2 The previous example generalizes as follows. Let $K_n = (V, E)$ denote the complete graph on n vertices. Let $P = V$ (vertices of K_n) = $\{v_1, \ldots, v_n\}$. Let $L = E$ (edges of K_n). Define $S_{K_n} = (P, L, I)$. To see that S_{K_n} is a linear space, we observe that **LS1** is satisfied by the definition of an edge, and **LS2** follows from the definition of a complete graph. The correspondence with the complete graph on n vertices ($n > 1$) allows us to construct an infinite family of linear spaces, $\{S_{K_n}\}_{n \in \mathbb{N} - \{1\}}$.

2.6. Isomorphisms of Incidence Structures

Let $A = (P, L_A, I_A)$ and $B = (Q, L_B, I_B)$. An *isomorphism* of incidence structures is a map $\phi : A \mapsto B$ that is not only bijective on the points and lines of A and B, but also preserves incidence; that is $(\phi(P), \phi(l)) \in I_B$ if and only if $(P, l) \in I_A$. In other words,

(1) $\forall\ q \in Q$, $\exists!\ p \in P$ such that $\phi(p) = q$.

(2) $\forall\ m \in L_B$, $\exists!\ l \in L_A$ such that $\phi(l) = m$.

(3) Suppose $\phi(p_i) = q_i$ for $i \in$ 1,2. p_1 is incident $p_2 \Leftrightarrow q_1$ is incident with q_2.

An *isomorphism* of incidence structures is simply a relabeling of the point set that preserves incidence. Before we head off to the next section, let's discuss a few easy examples.

Example 2.6.1

Let P = {1,2,3,4 }, L = { {1,2 }, {1,3 }, {1,4 }, {2,3 }, {2,4 }, {3,4 } } . Let Q = {a,b,c,d }, L = { {a,b }, {a,c }, {a,d }, {b,c }, {b,d }, {c,d } }. Then the map ϕ: 1 $\mapsto$ a, 2 $\mapsto$ b, 3 $\mapsto$ c, 4 $\mapsto$ d , is an isomorphism of linear spaces.

Example 2.6.2

Let P = {0,1,2,3,4,5,6 }, L = { {1,2,4 }, {2,3,5 }, {3,4,6 }, {0,4,5 }, {1,5,6 }, {0,2,6 }, {0,1,3 }} . Let Q = { I, II, III, IV, V, VI, VII }, L = { { I, II, III }, {I, IV, V }, {I, VI, VII }, {II, IV, VI }, { II, V, VII }, {III, IV, VII }, {III, V, VI } } . Then the map ϕ: 0 $\mapsto$ I, 1 $\mapsto$ II, 2 $\mapsto$ III, 3 $\mapsto$ IV, 4 $\mapsto$ V, 5 $\mapsto$ VI, 6 $\mapsto$ VII , is an isomorphism of projective spaces.

2.6.1 Automorphisms of Incidence Structures

In the case where a map ϕ merely permutes the point set of an incidence structure A while preserving incidence, we say that ϕ is an *automorphism*. The set of all automorphisms of an incidence structure A form a group, $Aut(A)$, under compositions. Naturally, the structure of A and $Aut(A)$ are hopelessly intertwined. It is because of the aforementioned fact that one of our main tools for investigating incidence structures will be group theory. When the incidence structure is a projective plane, we use the classical term *collineation* for automorphism.

A **translation** is a collineation of an affine plane which acts freely on the parallel classes. A **translation plane** is an affine plane admitting a group of translations acting transitively on its points. We will revisit translation planes in the upcoming section on spreads, we close this chapter with an example of a collineation of $\mathbb{P}G(2,2)$.

Consider the previous example.

Example 2.6.3 Let $A = (P,\ L)$ Let P = {0,1,2,3,4,5,6 }, L = { {1,2,4 }, {2,3,5 }, {3,4,6 }, {0,4,5 }, {1,5,6 }, {0,2,6 }, {0,1,3 }} . Observe that each of the lines have the form {1 + k, 2 + k, 4 + k } where $k \in$ {0,1,2,3,4,5,6 }. Now assume that ϕ acts on the lines by $\phi : k \mapsto (k+1)(mod 7)$. It is easy to see that ϕ permutes the lines of A.

Now that we have had a chance to review some of the more basic topics of our discussion, we transition to the study of projective planes.

CHAPTER 3

Projective Geometries

3.1. Introduction

Let K be a division ring and V a (left) vector space over K. As usual, there are algebraic and geometric of a given projective geometry. The algebraic description is given by the lattice of all subspaces of V with subspace containment corresponding to incidence. We denote this space as $\mathbb{P}G(V)$. The geometric correspondence is natural: the 1-dimensional subspaces correspond to points, the 2-dimensional subspaces correspond to lines, 3-dimensional subspaces correspond to planes, and so forth. If $W \subset V$, the algebraic dimension of $\mathbb{P}G(W)$ is the cardinality of its basis in V, and the geometric dimension (sometimes denoted by g-dim) is one less than its algebraic dimension, (sometimes denoted by a-dim). For instance, if W is a subspace of V with a-dim m, $\mathbb{P}G(W)$ has g-dim m-1.

Counting Subspaces: Let $\mathbb{P}G(n,q)$ denote the n-dimensional projective geometry over $GF(q)$. We introduce the Gaussian binomial coefficient as a tool for enumerating the m-dimensional subspaces of $\mathbb{P}G(n,q)$. Define

$$\binom{n+1}{m+1}_q = \prod_{i=1}^{m+1} \frac{q^{n+1}-q^{i-1}}{q^{m+1}-q^{i-1}}.$$

We claim that $\binom{n+1}{m+1}_q$ is the number of m dimensional subspaces of $\mathbb{P}G(n,q)$. To see this, observe that the number of linearly independent $m+1$-tuples is given by the numerator. Dividing out by the number of spanning $m+1$-tuples (the denominator), we obtain the desired result.

For any projective geometry of g-dimension m, it is a well known fact that the space satisfies Desargues' Theorem (given below) when $m > 2$. As a result, given two projective geometries $\mathbb{P}G(V)$ and $\mathbb{P}G(V')$ with V and V' left vector spaces of dimension n and n' over division rings K and K' (respectively) we have that:

$$\mathbb{P}G(V) \simeq \mathbb{P}G(V') \textit{ whenever } n = n' \,\&\, K \simeq K'.$$

For this reason, we restrict our attention to projective geometries of g-dimension 2- the projective planes. However, there are techniques which use projective spaces of g-dim $>$ 2, to construct projective planes. We will discuss a few of these techniques later on in the chapter.

3.2. Affine Planes

An *affine plane* is an incidence structure satisfying the following axioms:

- **A1** Any two points are incident with a unique line.
- **A2** To any non-incident point line pair (P, ℓ), there exists a unique line through P not incident with ℓ.
- **A3** There exists a set of three non-collinear points.

Example 3.2.1 Let $(K, +, *)$ denote a division algebra. Define $P = K \times K$. We define lines as follows.

Let $L_0 = \{\ell_{(m,b)} = \{(x, mx + b) \in P \text{ for some fixed } m \text{ and } b \in K \}\}_{(m,b)\in K^2}$. Define $L_\infty = \{\ell_c = \{(c, y) \in P \text{ for some fixed } c \in K\}\}_{c\in K}$. Write $L = L_0 \cup L_\infty$. Then $(P, L, \in)$ is an affine plane and we denote it as $\mathbb{A}^2K$ *the affine plane coordinatized by* K.

3.3. Projective Planes

A *projective plane* is an incidence structure satisfying the following axioms:

- **P1** every line is incident with least two points,
- **P2** any two points are incident with a unique line.
- **P3** any two lines intersect at a unique point, and
- **P4** there exists a set of four points with no three collinear.

3.3.1. Projectivization. Write an affine plane $\mathbb{A}$ as $(P_{\mathbb{A}}, L_{\mathbb{A}}, I_{\mathbb{A}})$, and a projective plane $\mathbb{P}$ by $(P_{\mathbb{P}}, L_{\mathbb{P}}, I_{\mathbb{P}})$. For any point P, we denote the set of lines incident with P as (P). Given a line ℓ, we denote the set of points on ℓ as $[\ell]$ Every affine plane may be extended to a projective plane through the following process.

(1) Define an equivalence relation on $L_{\mathbb{A}}$ as follows:

$$\ell \sim m \Leftrightarrow [\ell] \ = \ [m] \ or \ [\ell] \cap [m] \ = \ \emptyset.$$

Denote $L_{\mathbb{A}}/\sim$ as $\bar{L_{\mathbb{A}}}$ with elements $\bar{\ell}$.

(2) Introduce a line (∞) such that for each $\bar{\ell} \in \bar{L_{\mathbb{A}}}$ there exists exactly one point $P_\ell \in (\infty)$ in which , $\forall\ m \in \bar{\ell}$, $[m]$ contains P_ℓ.

(3) Define $L_{\mathbb{P}}$ as the lines with point set $[m] \cup \{P_\ell\}$ for any $m \in \bar{\ell}$ as $\bar{\ell}$ ranges over $\bar{L_{\mathbb{A}}}$.

The resulting incidence structure $\mathbb{P}$ with point set $P_{\mathbb{P}} = P_{\mathbb{A}} \cup \{(\infty)\}$, line set $L_{\mathbb{P}}$, and corresponding incidence $I_{\mathbb{P}}$ is a projective plane. We denote this process as the projectivization of $\mathbb{A}$ and write $\mathbb{P}(\mathbb{A})$. This procedure is invertible when beginning with a projective plane, one need only designate a line at infinity and remove its points as well as the lines in which they are incident.

3.4. Spreads & Coordinatization

Biliotti, Jha, and Johnson give a nice introduction to spreads in [8]. We follow their outline in this portion of our exposition, beginning with the more natural of the two constructions of spreads.

Construction of Spreads via Vector Spaces

Let V be a $2n$-dimensional vector space over $GF(q)$. A **spread** on V is a partition of V into a collection $\mathcal{S}$ of pairwise trivially intersecting subspaces of dimension n. The associated collection of all cosets $v + \mathcal{S}$ where $v \in V$, is realized as the line-set of a translation plane of order q^n having V as its point-set.

Construction of Spreads via Groups

Let G be a group. A partition of G is a set $\mathcal{H} = \{H_1, H_2, \ldots\}$ such that

(1) $H_i \cap H_j = \{id_G\}$ *whenever* $i \neq j$, &

(2) $G = \bigcup_i H_i$

If all the subgroups $H_1, H_2, \ldots$ are normal in G, we say that $\mathcal{H}$ is a **normal partition** of G.

Recall that we say that G splits over M, $N \lhd G$ whenever $G = MN = NM$. Define a **normal splitting partition** to be a normal partition $\mathcal{N} = \{N_1, N_2, \ldots\}$, if N_i and N_j split G whenever $i \neq j$. Before we can move ahead in our discussion, we shall need the following results.

Theorem 3.1. *Let G be a group that admits a splitting normal partition $\mathcal{N}$, then G is Abelian. Moreover, the components N_i ($i = 1, 2, \ldots$) are mutually isomorphic.*

THEOREM 3.2. *Let* $\mathcal{N} = \{N_1, N_2, \ldots\}$ *be the components of a normal splitting partition of a group* G*. Then the following hold:*

(1) $(G, +)$ *is an Abelian group and* $G = N_1 \oplus N_2$ *with* $N_1 \cong N_2$ *and* $N_1 \neq N_2$*.*

(2) *Define an incidence structure on* G *by*

$$\pi(\mathcal{N}) := (G, \{x + N : x \in G, N \in \mathcal{N}\}),$$

The points are given by elements of G*. The lines are given by the cosets* $x + N$ *of the components* $N \in \mathcal{N}$*. Then* $\pi(\mathcal{N})$ *is an affine plane. The parallel postulate is confirmed by the observation that two lines of* $\pi(\mathcal{N})$ *are parallel whenever they are cosets of the same* $N \in \mathcal{N}$*.*

(3) *The translation group of* $\pi(\mathcal{N})$ *is simply the endomorphism group of* G *(i.e* $End(G)$*) of given by:*

$$\tau_G := \{\tau_g : x \mapsto x + g : g \in G\}.$$

(4) τ_G *has a regular action on* G*, therefore it must also have a regular action on the affine points of* $\pi(\mathcal{N})$*.*

We define an important subgroup, the **kernel of endomorphisms** of the partition $(\mathcal{K}, +, \circ)$ is a ring under addition and composition , and it is given by $\{\phi \in Hom(G, +) : \phi(N) = N, \forall N \subset \mathcal{N}\}$. The kernel will allow us to "see" the ground field of the translation plane obtained from a spread via the vector space construction. The following theorem and corollary provide us with precise statements of these ideas.

THEOREM 3.3. *Let* G *be a group that admits a splitting normal partition of* $\mathcal{N}$*. Then the kernel of endomorphisms is a division ring and* G *is a vector space over* $\mathcal{K}$ *under its standard action of* G*. Moreover, every component of* $\mathcal{N}$ *is a* $\mathcal{K}$*-subspace of* V*.*

COROLLARY 3.4. *Let G be a group admitting a normal splitting partition of $\mathcal{N}$, and let $\mathbf{0}_G$ denote the identity element. Then G is an Abelian group that becomes a vector space under the standard action of the kernel $\mathcal{K}$. Furthermore, the translation plane $\pi_{\mathcal{N}}$ admits $\mathcal{K}^{\times} = \mathcal{K} - \mathbf{0}_G$ as a group of homologies with center $\mathbf{0}_G$. In addition, the lines through $\mathbf{0}_G$ are the members of $\mathcal{N}$, and $\mathcal{K}$ is the largest subgroup of $Hom(G, +)$ that leaves invariant each of the lines through $\mathbf{0}_G$.*

3.4.1. PLANAR TERNARY RINGS. Given a nonempty set $A \supset \{0, 1\}$, suppose that we may define a ternary operation $T : A \times A \times A \longrightarrow A$ satisfying:

(1)

$$T(a, 1, 0) = T(1, a, 0) = a \; \forall \; a \in A;$$

(2)

$$T(0, 1, b) = T(1, b, 0) = b \; \forall \; b \in A;$$

(3)

$$T(a, b, 0) = a * b;$$

(4)

$$T(a, 1, b) = a + b.$$

We denote the pre-planar ternary ring over A as $\mathcal{A}^{pre}$. Define ($\mathcal{A}^{pre}$, +) to be the set { $c \in A$: $T(a, 1, b) = c$ for some $(a, b) \in A \times A$ }. Now, define ($\mathcal{A}^{pre}$, $*$) to be the set { $c \in A$: $T(a, b, 0) = c$ for some $(a, b) \in A \times A$ }. Then $\mathcal{A}$ is a planar ternary ring provided that ($\mathcal{A}^{pre}$, +) and ($\mathcal{A}^{pre}$-{0}, $*$) are both loops with identities 0 and 1 respectively. If $\mathcal{A}$ is left or right distributive, $\mathcal{A}$ is a quasifield. Furthermore, planar ternary ring is linear if $T(a, x, b) = ax + b$.

Here are a few well known properties of planar ternary rings.

- **PTR 1.** Given a,x, y in $\mathcal{A}$ $\exists!$ $b \in \mathcal{A}$ such that

$$T(a, x, b) \ = \ y.$$

- **PTR 2.** Given x, y, x', y' in $\mathcal{A}$ $\exists!$ ordered pair $(a,b) \in \mathcal{A}$ such that

$$T(a, x, b) \ = \ y \ \& \ T(a, x', b) \ = \ y'.$$

- **PTR 3.** Given a, b, a', b' in $\mathcal{A}$ ($a \neq a'$) $\exists!$ $x \in \mathcal{A}$ such that

$$T(a, x, b) \ = \ T(a', x, b').$$

Planar ternary rings are necessary for the coordinatization translation planes. Given a planar ternary ring $\mathcal{A}$, one may coordinatize a translation plane over $\mathcal{A}$ as follows.

- The point set is given by: $\{(a, b) : \ a, b \ \in \mathcal{A}. \}$
- The lines with defined slope are given by the point sets: $[m, b] = \{ \ (x, \ xm \ + \ b) : \ x \ \in \ \mathcal{A}. \}$
- The "vertical" lines are given by the point sets: $[c, x] = \{ \ (c, x) : \ x \ \in \ \mathcal{A}. \}$

3.4.2. Quasifields. A left or right quasifield $(\mathbb{Q}, +, *)$ is an abelian group under $+$ satisfying the following additional axioms under $*$. Assume 0 is the additive identity.

(1) $0 * a = a * 0 = 0$ for all $a \in \mathbb{S}$.

(2) $a * b \in \mathbb{S}$ whenever a, $b \in \mathbb{S}$ (closure under $*$).

(3) $a * (b + c) = a * b + a * c$ (right distributivity of $*$ over $+$) if and only if Q is a right quasifield.

(4) $(a + b) * c = a * c + b * c$ (left distributivity of $*$ over $+$) if and only if Q is a left quasifield.

(5) For every nonzero a, b, $\in \mathbb{S}$ there exists unique x and $y \in \mathbb{S}$ such that $x * a = b$ and $a * y = b$ (invertibility of non-zero elements).

3.4.3. Semifields. A semifield $(\mathbb{S}, +, *)$ is an abelian group under $+$ satisfying the following additional axioms under $*$. Assume 0 is the additive identity.

(1) $0 * a = a * 0 = 0$ for all $a \in \mathbb{S}$.

(2) $a * b \in \mathbb{S}$ whenever a, $b \in \mathbb{S}$ (closure under $*$).

(3) $a * (b + c) = a * b + a * c$ (right distributivity of $*$ over $+$).

(4) $(a + b) * c = a * c + b * c$ (left distributivity of $*$ over $+$).

(5) For every nonzero a, b, $\in \mathbb{S}$ there exists unique x and $y \in \mathbb{S}$ such that $x * a = b$ and $a * y = b$ (invertibility of non-zero elements).

We say that a semifield is proper if it is non-associative. A semifield is a linear planar ternary ring which is right and left distributive, or equivalently, a quasifield that is right and left distributive. Any semifield may be used to coordinatize a plane using the same method for planar ternary rings given above.

When a projective plane is coordinatized by a finite field of given order q, a projective plane is merely the projective geometry of g-dimension = 2 denoted by $PG(2, q)$. These are precisely the desarguesian planes. A result of Wedderburn showed that every associative division algebra is a finite field. However, for a general projective plane of order q, the planar ternary ring providing its coordinatization need only be a non-associative [1] division algebra.

[1]We define non-associative to mean not necessarily associative.

3.5. Projective Planes

Recall from the last section that a *projective plane* is an incidence structure (P, L, I) having the following incidence relation:

- P1: For any two points, there exists a unique line incident with both.
- P2: Every pair of lines intersect at a unique point.
- P3: There exist a set of four points with no three collinear.

. Though planes of infinite order exist, we shall focus on the finite case here. A projective plane of order q is a triple (P, L, I) with P a set of $q^2 + q + 1$ points, L a set of $q^2 + q + 1$ lines having having the following incidence relation:

- FP1: Every line contains $q + 1$ points
- FP2: Every point is incident with $q+1$ lines
- FP3: There exist a set of four points with no three collinear.

Every finite projective plane has an order.

Given a projective plane π, our coordinate free notation will denote points with uppercase letters A, B, ..., and lines by lower case letters a, b, ... Given any two lines a and b, there exists a unique point P which we shall denote as ab. In the dual case, given any two points P and Q there exists a unique line ℓ incident with both, hence we denote ℓ by PQ. Intersections of lines in the form PQ and $P'Q'$ will be written as $AB' \cap BA'$. This will be the notation used for the following properties of projective planes derived from a theorem of Pappus of Alexandria and a theorem of Girard Desaurgues.

3.5.1. Pappus' Theorem. We say that a projective plane is **pappian** if it satisfies Pappus' theorem.

For any pair of distinct lines ℓ and m containing the points $\{A, B, C\}$ and $\{A', B', C'\}$ respectively, we have that $AB' \cap BA'$, $AC' \cap CA'$, and $BC' \cap CB'$ are collinear. The following result (traditionally) credited to D. Hilbert shows that Pappian planes are coordinatized by fields.

Theorem 3.5. *A projective plane satisfies Pappus' theorem if and only if it is isomorphic to PG(2,F), for some field F.*

3.5.2. Desargues' Theorem. We say that a projective plane is **desarguesian** if it satisfies Desargues' theorem.

Let ABC, $A'B'C'$ denote two triangles (labeled so that AA' and CC' do not cross the interior of either triangle). There exists a point P for which $P = AA' \cap BB' \cap CC'$ if and only if there exists a line ℓ containing the points: $AB \cap A'B'$, $AC \cap A'C'$, and $BC \cap B'C'$. The following result, again (traditionally) credited to D. Hilbert shows that Desarguesian planes are coordinatized by division rings.

Theorem 3.6. *A projective plane satisfies Desargues' theorem if and only if it is isomorphic to PG(2,D), for some division ring D.*

In the finite case, a result of Wedderburn [84] shows us that finite Desarguesian planes are indeed coordinatized by finite fields.

Theorem 3.7. *[84] A finite division ring is a field.*

Given 3.5, 3.6, and 3.7, we may show the following two facts as corollaries.

(1) Corollary 3.7a A finite projective plane satisfies Desargues' theorem if and only if if it is isomorphic to PG(2,F), for some finite field F.

(2) Corollary 3.7b A finite projective plane that satisfies Desargues' theorem also satisfies Pappus' theorem.

3.5.3. Bruck-Ryser Theorem. It is an open question as to whether or not planes of non-prime power order exist. The theorem of Bruck and Ryser is one of the few results shedding some light on this question. We state it here:

Theorem 3.8. *If $n \equiv 1$ or 2 (mod 4) there cannot be a projective plane of order n unless n can be expressed as a sum of two integral squares.*

The previous theorem rules out 6 as well as infinitely many other orders (such as all orders congruent to 6 modulo 8). The smallest case left unresolved by the Bruck-Ryser theorem is 10.

3.6. Examples of Projective Planes

Example 3.6.1 PG(2,2) Assume points are in the form (x, y, z). Let $P = \{$(0,0,1), (0,1,0), (1,0,0), (1,0,1), (1,1,0), (0,1,1),(1,1,1)$\}$, $L = \{$ $[x = 0] = \{$ (0,0,1), (0,1,0), 0,1,1) $\}$, $[y = 0] = \{$ (0,0,1), (1,0,1),(1,0,0) $\}$, $[z = 0] = \{$(1,0,0), (0,1,0), (1,1,0) $\}$, $[x + y = 0] = \{$ (0,0,1), (1,1,0), (1,1,1) $\}$,$[x + z = 0] = \{$ (0,1,0), (1,0,1),(1,1,1) $\}$, $[y + z = 0] = \{$(1,0,0), (0,1,1), (1,1,1) $\}$, $[x + y + z = 0] = \{$(1,0,1), (1,1,0), (0,1,1) $\}\}$.

Example 3.6.2 PG(2,4)

In order to construct the projective plane over a finite field of order four, we look at the splitting field of $t^4 - t$ over the polynomial ring $\mathbb{Z}[t]/4\mathbb{Z}$. t^4-t splits as $t(t-1)(t^2+t+1)$. Since (t^2+t+1) is irreducible over $\mathbb{Z}_2$, it follows that our field is isomorphic to $\mathbb{Z}_2[t]/(t^2+t+1)$. We denote the field of order 4 as $\mathbb{F}_4$, and its elements are: $\{0, 1, t, t+1\}$. The addition and multiplication are done modulo (t^2+t+1) in a field of characteristic 2. The points of $PG(2,4)$ are given in the form (a, b, c):

$$\{(0,0,1),\ (0,1,0),\ (1,0,0),$$

$$(t,0,1),\ (0,1,t),\ (1,t,0),$$

$$(t+1,0,1),\ (0,1,t+1),\ (1,t+1,0),$$

$$(1,1,t),\ (1,t,1),\ (t,1,1),$$

$$(1,1,t+1),\ (1,t+1,1),\ (t+1,1,1),$$

$$(1,1,0),\ (1,0,1),\ (0,1,1),$$

$$(1,1,1),\ (1,t,t+1),\ (1,t+1,t)\}.$$

By duality we obtain the lines of $PG(2,4)$ given in the form $\langle x, y, z\rangle$. A point (a, b, c), lies on a line $\langle x, y, z\rangle$ if $ax + by + cz = 0$. Each line contains 4+1 = 5 points, and every point is incident with 5 lines. We list the following lines and the set of points with which it is incident.

(1) $\langle 0, 0, 1\rangle = \{(0,1,0), (1,0,0), (1,t,0), (1,t+1,0), (1,1,0)\}$

(2) $\langle 0,1,0\rangle = \{(0,0,1),\ (1,0,0),\ (t,0,1),\ (t+1,0,1),\ (1,0,1)\}$

(3) $\langle 1,0,0\rangle = \{(0,0,1),\ (0,1,0),\ (0,1,t),\ (0,1,t+1),\ (0,1,1)\}$

(4) $\langle t,0,1\rangle = \{(0,1,0),\ (t+1,0,1),\ (t+1,1,1),\ (1,1,t),\ (1,t+1,t)\}$

(5) $\langle 0,1,t\rangle = \{(1,0,0),\ (0,1,t+1),\ (1,1,t+1),\ (1,t,1),\ (1,t+1,t)\}$

(6) $\langle 1,t,0\rangle = \{(0,0,1),\ (1,t+1,0),\ (1,t+1,1),\ (t,1,1),\ (1,t+1,t)\}$

(7) $\langle t+1,0,1\rangle = \{(0,1,0),\ (1,0,t+1),\ (1,1,t+1),\ (1,t,t+1),\ (t,0,1)\}$

(8) $\langle 0,1,t+1\rangle = \{(1,0,0),\ (0,t+1,1),\ (1,t+1,1),\ (1,t,t+1),\ (0,1,t)\}$

(9) $\langle 1,t+1,0\rangle = \{(0,0,1),\ (t+1,1,0),\ (t+1,1,1),\ (1,t,0),\ (1,t,1)\}$

(10) $\langle 1,1,t\rangle = \{(1,1,0),\ (0,1,t+1),\ (1,t+1,1),\ (t+1,1,1),\ (t,0,1)\}$

(11) $\langle 1,t,1\rangle = \{(1,0,1),\ (t+1,1,1),\ (1,1,t+1),\ (0,1,t),\ (1,t+1,0)\}$

(12) $\langle t,1,1\rangle = \{(0,1,1),\ (1,t,0),\ (t+1,0,1),\ (1,t+1,1),\ (1,1,t+1)\}$

(13) $\langle 1,1,t+1\rangle = \{(1,1,0),\ (t+1,0,1),\ (1,t,1),\ (t,1,1),\ (0,1,t)\}$

(14) $\langle 1,t+1,1\rangle = \{(1,0,1),\ (1,t,0),\ (t,1,1),\ (1,1,t),\ (0,1,t+1)\}$

(15) $\langle t+1,1,1\rangle = \{(0,1,1),\ (t,0,1),\ (1,t+1,0),\ (1,t,1),\ (1,1,t)\}$

(16) $\langle 1,1,0\rangle = \{(1,1,0),\ (0,0,1),\ (1,1,1),\ (1,1,t),\ (1,1,t+1)\}$

(17) $\langle 1,0,1\rangle = \{(1,0,1),\ (0,1,0),\ (1,1,1),\ (1,t,1),\ (1,t+1,1)\}$

(18) $\langle 0,1,1\rangle = \{(0,1,1),\ (1,0,0),\ (1,1,1),\ (t,1,1),\ (t+1,1,1)\}$

(19) $\langle 1,1,1\rangle = \{(0,1,1),\ (1,0,1),\ (1,1,0),\ (1,t,t+1),\ (1,t+1,t)\}$

(20) $\langle 1,t,t+1\rangle = \{(1,1,1),\ (1,t+1,0),\ (1,t,t+1),\ (t+1,0,1),\ (0,1,t+1)\}$

(21) $\langle 1,t+1,t\rangle = \{(1,1,1),\ (1,t,0),\ (t,0,1),\ (0,1,t),\ (1,t+1,t)\}$

If we remove the line $z = 0$ from the previous example, $PG(2,4)$, we obtain the affine plane $AG(2,4)$. We obtain the coordinates by dehomogenization. Write $A = \frac{a}{c}$, and $B = \frac{b}{c}$. Then

$$(a,b,c) \ \approx \ \frac{1}{c}(A,B,1) \ \approx \ (A,B).$$

Example 3.6.3 PG(2, q)

Assume that $q = p^m$ and that p is prime. Let $K = \mathbb{F}_q$ denote the field with q elements, and $V = K^3$ with the standard basis. The set of points of $PG(2, q)$ is the set of all 1 dimensional subspaces of V through the origin. The set of lines is the set of all 2 dimensional subspaces of V. Incidence is given by containment.

Example 3.6.4 Derivation Planes

The following examples of projective planes are due to Hall. Let $GF(q^2)$ denote the finite field of order q^2, q a prime power, and $PG(2, q^2)$ denote the desarguesian plane of order q^2. Let $l_\infty \subset PG(2, q^2)$ denote the line at infinity. Now consider the affine plane $AG(2, q^2) = PG(2, q^2)$ - l_∞. We say that a set D of $q + 1$ points of l_∞ is a derivation set if for any two points x and y of $AG(2, q^2)$ and a line through x and y meeting D at a point, there exists a Baer subplane containing x, y and D. Define the points of the derived plane π, as the points of $PG(2, q^2)$. We define the lines of π as the lines of $AG(2, q^2)$ along with the Baer subplanes corresponding to some derivation set D. Observe that for any two points x and y in π we either have:

- a unique Baer subplane of $AG(2, q^2)$ corresponding to a line through x and y or
- x and y lie on l_∞.

Immediately, we see that this is a projective plane of order q^2. This is also referred to as a *derived plane* and is non-desarguesian for $q > 2$.

3.7. Duality in Projective Planes

The dual of a projective plane is a projective plane, which is of the same order if the plane is finite. An *incidence matrix* is a useful tool for investigating incidence structures. We give the definition here. The *incidence matrix* of an incidence structure π is an array of values of ordered pairs $a_{i,j} = 1$ if the i^{th} point is incident with the j^{th} line, and 0 otherwise. It is implicit from the definition that the entries of this matrix is dependent upon the choice of ordering of the points and lines.

It follows from the definition that the incidence matrix of a projective plane of order q is an element of $M_{q^2+q+1}(\mathbb{F}_2)$. Furthermore, if a projective plane of order q has the incidence matrix $A = [a_{i,j}]$, the incidence matrix of the dual is simply $A^t = [a_{j,i}]$.

Suppose that V is a three dimensional vector space over a field K. The points of $PG(V)$ correspond to lines through the origin, i.e solutions to:

$$ax \ + \ by \ + cz \ = \ 0.$$

But observe that if $X \ = (x, \ y, \ z)$ is a solution, then

$$akx \ + \ bky \ + ckz \ = \ 0,$$

and kX is a solution as well, $\forall \ k \in K$. Given the previous correspondence between points of $PG(V)$ and the 1 dimensional subspaces of V, the following characterization of lines in $PG(V)$ is intuitive. If we take the span of any two distinct subspaces of dimension 1 in V we get a subspace of dimension 2, a plane through the origin.

Choose a basis for V, let E denote the span of $\mathbf{e} = \langle e_1, e_2, e_3 \rangle$. Now choose a basis for V^*, $\mathbf{x} = \langle x_1, x_2, x_3 \rangle$. Observe that $\mathbf{x}$ is the image of a hyperplane in V under a polarity, $*$. We say that E is incident with x if and only if $\mathbf{e} \cdot \mathbf{x} = e_1x_1 + e_2x_2 + e_3x_3 = 0$, where $\cdot$ is the standard dot product.

3.8. Polarities

Let V and W be 3 dimensional vector spaces over a field K. Now let $PG(V)$ and $PG(W)$ denote their respective projective geometries. Suppose that $\phi : PG(V) \to PG(W)$ is a bijective map that reverses containment, i.e $R \subset S$ in V if and only if $\phi(S) \subset \phi(R)$. Then we say that ϕ is an anti-isomorphism. If $V = W$, we say that ϕ is a correlation or duality.

A *polarity* is a duality of order 2. An incidence structure S is *self dual* if it is isomorphic to its dual; that is, if the incidence matrix of S is similar to its transpose. The dual of a projective geometry $PG(V)$ is denoted by, $PG(V^*)$ and is the lattice of all subspaces of V with reverse containment. Thus, if V is a n dimensional W is an k dimensional vector subspace of V , then W^* is an $n - k$ dimensional enveloping vector space of V^*. If V is a right vector space, then V^* is a left vector space and vice-versa.

Theorem 3.9. *If V is a finite-dimensional vector space over a field K, then V always possess polarities.*

Let P be a point and ℓ be a line of a projective plane π, and ϕ be a polarity of π We say that a is a ϕ- *absolute point* if $\phi(a)$ is incident with a. Dually, we say that ℓ is a ϕ-*absolute line* if $\phi(\ell)$ is incident with ℓ.

3.9. Semilinear Transformations

Let V and W are vector spaces over a skew field K. Then we say that $\phi : V \to W$ is a *semilinear* transformation of vector spaces if there exists $\alpha \in Aut(K)$ such that:

(1) $\phi(u + v) = \phi(u) + \phi(v) \ \forall \ u, v \in V$, and

(2) $\phi(k * u) = k^{\alpha} * \phi(u) \ \forall \ k \in K$, and $\forall \ u \in V$.

The invertible semilinear transformations of V form a group $\Gamma L(V)$ under composition. When V is $\mathbb{F}_q^n$, we denote this by $\Gamma L(n, q)$.

3.10. Examples of Automorphism Groups of Projective Planes

Example 3.10.1 $P\Gamma L(2, 2)$

$P\Gamma L(2, 2)$is the collineation group of $PG(2, 2)$ and it consists of all invertible semi-linear transformations of $\mathbb{F}_2^3$.

Example 3.10.2 $PGL(3, q)$

Consider $GL(3, q)$, the group of all invertible linear transformations of $\mathbb{F}_q^3$. Note that scalar matrices are the kernel of the action on a projective space (and the center of $GL(3, q)$). If we take the quotient of $GL(3, q)$ with the scalar matrices we obtain the projective linear group of 3×3 matrices over $GF(q)$,

$$PGL(3, q) \ \cong \ GL(3, q)/Z(GL(3, q)).$$

Example 3.10.3 $P\Gamma L(3, q)$

Consider $\Gamma L(3, q)$, the group of all invertible semilinear transformations of $\mathbb{F}_q^3$. Note recall that scalar matrices are kernel of the action on a projective space. If we take the quotient

of $\Gamma L(3,q)$ with the scalar matrices we obtain the projective semilinear group

$$P\Gamma L(3,q) \cong \Gamma L(3,q)/Z(GL(3,q)).$$

3.11. Fundamental Theorem of Projective Geometry

We now state the fundamental theorem of projective geometry.

Theorem 3.10. *The collineation group of $PG(2,q)$ is $P\Gamma L(3,q)$.*

3.12. Non-existence of a plane of order 10

The nonexistence of a projective plane of order 10 completed by Lam, Thiel and Swiercz in 1989 [57] was carried out by computer. A major stepping stone to proving the non-existence of a projective plane of order 10, was the following result:

Theorem 3.11. *[57] There does not exist an abstract hyperoval of order 10.*

Abstract hyperovals will be defined later on in our discussion. It is in light of the result obtained by Lam, Thiel, Swiercz, and McKay, that we are encouraged to study projective planes by their hyperovals.

CHAPTER 4

Ovals and Hyperovals in Projective Planes

4.1. Arcs, and Lines

We are now ready to define and discuss certain substructures of projective planes. We begin with k-arcs. Let π denote a projective plane of order q. A $k-arc$ is a set of k points in such that no three are collinear. A *quadrangle* Q is 4-arc. Recall, that a frame of a projective plane, is also a set of four points with no three collinear. It follows, that every quadrangle of a projective plane is a frame and vice-versa.

Example 4.1.1 Example of a 4-arc of PG(2,2)

$$\langle 0,0,1\rangle\,,\ \langle 0,1,0\rangle\,,$$

$$\langle 1,0,0\rangle\,,\ \langle 1,1,1\rangle\,.$$

A k-arc A, is *maximal* when any point P of $\pi - A$ is collinear with two points of A. A natural question to ask would be: " are there any known bounds for k ? ", and the answer is in the affirmative. If q is odd, then $k \leq q+1$. An *oval* is a q+1 arc of π. It follows that an oval is a maximal arc when q is odd. If A is an oval, it follows from the definition that any line of π intersects A in either zero, one, or two points. A line that is non-incident with A is called an *external line* of A. A line that intersects A at a single point is called a *tangent line* of A. Any line that intersects A in two places is called a *secant line* of A.

Example 4.1.2 Example of an oval in PG(2,2)

$$\langle 0,0,1\rangle\,,\ \langle 0,1,0\rangle\,,\ \langle 1,0,0\rangle\,.$$

Example 4.1.3 Example of an oval in PG(2,q)

Consider the set of points in $PG(2,q)$ over $GF(q)$ of the form

$$\mathcal{O}\ =\ \{(1,t,t^2):\ t\ \in GF(q)\}\cup\{(0,0,10\}.$$

This is a conic, and it is an oval of $PG(2,q)$.

4.2. Hyperovals

Now assume that π is a projective plane of order q with q even. Let A be an oval in π. In a plane of even order, the set of all tangent lines of A intersect at a point called the *nucleus* which we denote by P. If one ponders the previous statement for a moment, one sees that any line through the P must be collinear with at most one point of A. Thus, $A\cup\{\ P\ \}$ is a $n+2$ arc. We define a *hyperoval* as a maximal n+2 arc (necessarily consisting of an oval and its nucleus). Furthermore, this arc is maximal, as the following theorem proves.

Theorem 4.1. *[10] Let A be a k-arc of a projective plane of order q. Then $k\leq q+2$, with equality if and only if q is even.*

Theorem 4.2. *[73] An oval of a projective plane of even order is contained inside of a unique hyperoval.*

Let us now review some of the known examples of hyperovals. Let $D(k)$, $k \in \mathbb{N}$ be the set of all points in $PG(2,q)$ over $GF(q)$ of the form

$$D(k) \ = \ \{(0,1,0),(0,0,1)\} \ \cup \ \{(1,t,t^k) : t \ \in \ GF(q)\}.$$

The set of points of $D(k)$ have the form $(1,t,f(t))$ where f is the so-called $o-polynomial$ of the hyperoval corresponding to $D(k)$.

Example 4.2.1 The regular hyperoval of PG(2,q)

A hyperoval of consisting of a conic along with its nucleus of $PG(2,q)$ is called a *regular hyperoval*. Let $q = 2^h$. these are due to [75].

$$D(2) \ = \ \{(0,1,0),(0,0,1)\} \ \cup \ \{(1,t,t^2) : t \ \in \ GF(q)\}.$$

Example 4.2.2 The regular hyperoval of PG(2,4)

Recall the elements of $GF(4) = \{0,1,t,t+1\}$

$$(0,0,1),\ (0,1,0),\ (1,x,x^2)|_{x=0} \ = \ (1,0,0),$$

$$(1,x,x^2)|_{x=1} \ = \ (1,1,1),\ (1,x,x^2)|_{x=t} \ = \ (1,t,t+1),$$

$$(1,x,x^2)|_{x=t+1} \ = \ (1,t+1,t).$$

Example 4.2.3 Translation Hyperovals of PG(2,q)

If $gcd(m, h) = 1$, then the map

$$\phi : t \mapsto t^{2^m}$$

is an automorphism of $GF(q)$, and the following subset of points of $PG(2, q)$ over $GF(q)$ form a hyperoval called the *translation* hyperoval.

$$D(2^m) = \{(0, 1, 0), (0, 0, 1)\} \cup \{(1, t, t^{2^m}) : t \in GF(q)\}.$$

These are also due to [75].

Example 4.2.4 Segre-Bartocci Hyperovals

Suppose that h is odd. The set

$$D(6) = \{(0, 1, 0), (0, 0, 1)\} \cup \{(1, t, t^6) : t \in GF(q)\}$$

is a hyperoval of $PG(2, q)$ over $GF(q)$.

Example 4.2.2 Glynn Hyperovals

Again, suppose that h is odd. We define two automorphisms of $GF(q)$ as follows:

$$\sigma : t \mapsto t^{\frac{h+1}{2}},$$

$$\gamma : t \mapsto t^{2^m} \; if \; h = 4m - 1, \; or$$

$$\gamma : t \mapsto t^{3m+1} \; if \; h = 4m + 1.$$

A result of [35] proved that

$$D(\sigma + \gamma) = \{(0,1,0),(0,0,1)\} \cup \{(1,t,t^{\sigma + \gamma}) : t \in GF(q)\}$$

as well as

$$D(3\sigma + 4) = \{(0,1,0),(0,0,1)\} \cup \{(1,t,t^{3\sigma + 4}) : t \in GF(q)\}$$

Example 4.2.3 Payne Hyperovals

Assume that h is odd. Define

$$\delta : GF(q) \to GF(q) \; as \; \delta : t \mapsto t^{\frac{1}{6}} + t^{\frac{1}{2}} + t^{\frac{5}{6}}.$$

The Payne hyperovals correspond to the the set

$$D(\delta) = \{(0,1,0),(0,0,1)\} \cup \{(1,t,t^{\delta}) : t \in GF(q)\}.$$

Example 4.2.4 Cherowitzo Hyperovals

Suppose that $h = 2s + 1$. Define

$$\sigma : GF(q) \to GF(q) \; as \; \sigma : t \mapsto t^{2^{s+1}}.$$

Now define

$$\zeta : GF(q) \to GF(q) \; as \; \zeta : t \mapsto t^{\sigma} + t^{\sigma+2} + t^{3\sigma+4}.$$

The Cherowitzo hyperovals correspond to the set:

$$D(\zeta) = \{(0,1,0),(0,0,1)\} \cup \{(1,t,t^{\zeta}) : t \in GF(q)\}.(\forall h \leq 9).$$

Example 4.2.4 Lunelli-Sce Hyperovals

Suppose that p is a primitive element of $GF(q)$ with $p^4 = 1$. Let

$$f(t) \;=\; t^{12} \;+\; t^{10} \;+\; p^{11}t^8 \;+\; t^6 \;+\; p^2t^4 \;+\; p^9t^2.$$

The Lunelli-Sce Hyperoval is given by:

$$D(f) \;\;=\;\; \{(0,1,0),(0,0,1)\} \;\cup\; \{(1,t,f(t)) : t \;\in\; GF(q)\}.$$

This hyperoval has the peculiar property of admitting a transitive automorphism group. It is a part of the following two infinite families.

Example 4.2.5 Subiaco Hyperovals

Suppose that $q = 2^h$. Also suppose that $\sigma \in GF(q)$ such that $\sigma^2 + \sigma + 1 \neq 0$ and trace($1/\sigma$) $= 1$. Define the o-polynomial f, as follows:

$$f(t) \;=\; \frac{\sigma^2(t^4 \;+\; t \;+(1+\sigma \;+\; \sigma^2)(t^3 \;+\; t^2))}{(t^2 \;+\; \sigma t \;+\; 1)^2} \;+\; t^{1/2}.$$

Then

$$D(f) \;\;=\;\; \{(0,1,0),(0,0,1)\} \;\cup\; \{(1,t,f(t)) : t \;\in\; GF(q)\}.$$

The Subiaco hyperovals discovered by Cherowitzo, Penttila, Pinneri and Royle.

Example 4.2.6 Adelaide Hyperovals

Let q be an even power of 2. Let $s \in GF(q^2)$ with $s \neq 1$ such that $s^{q+1} = 1$. Also, define

$$\phi : GF(q^2) \to GF(q^2),\ \phi : t \mapsto t^q\ -\ t.$$

Assume that

$$m\ \equiv\ \pm\frac{q-1}{3}(mod\ q+1).$$

Now define $f(t)$ as

$$\frac{\phi(s^m(t+1)}{\phi(s)} + \frac{\phi((st+s^q)^m)}{\phi(s)(t+\phi(s)t^{1/2}+1)^{m-1}} + t^{1/2}.$$

Then the Adelaide hyperovals are given by:

$$D(f)\ \ =\ \{(0,1,0),(0,0,1)\}\ \cup\ \{(1,t,f(t)) : t\ \in\ GF(q)\}.$$

CHAPTER 5

Collineations, Baer Subplanes, & Polar Spaces

A *collineation* is an automorphism of a projective plane. Collineations take points to points and lines to lines while preserving incidence. A point fixed linewise by a collineation α, is called is called the *center* of α. A line fixed pointwise by a collineation α , is called an axis of α.

5.1. Collineations

5.1.1. Properties and Examples of Collineations. As stated previously, a collineation is an automorphism of a plane- mapping points to points and lines to lines while preserving incidence. Given any projective plane π we define the group of collineations as $Aut(\pi)$. We list a few classical results on collineations.

Theorem 5.1. *A collineation has an axis if and only if it has a center.*

Theorem 5.2. *A non-identity collineation has at most one center and at most one axis.*

A collineation that has a center is called a *central collineation*.

Central collineations may fall into two categories.

(1) *Elations* are central collineations where the center is incident with the axis.

(2) *Homologies* are central collineations in which the axis is non-incident with the center.

The following result gives

Theorem 5.3. *In a projective plane of order n, a homology has order dividing n-1 and an elation has order dividing n.*

THEOREM 5.4. *The join of two fixed points is a fixed line, and dually the intersection of any two fixed lines is a fixed point.*

COROLLARY 5.5. *The fixed point and fixed lines of a collineation fixing a quadrangle form a subplane.*

A collineation fixing a quadrangle is called *planar*.

We now introduce an important substructure of finite projective planes. A *Baer subplane* is a projective plane of order $\sqrt{q}$ contained in a projective plane of order q. It is obvious that q must be a square in order for Baer subplanes to exist.

5.2. Baer Subplanes

Before we begin our discussion, we state the following theorem of *Baer*.

THEOREM 5.6. *A proper subplane of a projective plane of order n has order at most $\sqrt{n}$.*

If equality occurs, the subplane is called a *Baer subplane*. Planar collineations with fixed plane a Baer subplane are called *Baer collineations*. In particular, we are concerned with Baer collineations of order 2, called *Baer involutions*.

Baer subplanes can be used to deduce global properties as the following result of [59] *Lüneburg* demonstrates:

THEOREM 5.7. *Let π be a finite projective plane of order q. Then the following assertions are equivalent.*

- *π is a Desarguesian or a generalized Hughes plane.*

- *π contains a Baer subplane β such that for each line $\ell \in \beta$, there are exactly q elations of β induced by elations of π with axis ℓ.*
- *π has a proper subplane β such that for some $H = Stab_{Aut(\pi)}(\beta) < Aut(\pi)$, π - β admits a flag-transitive action.*
- *π contains a Bear subplane β with the property that $H = Stab_{Aut(\pi)}(\beta)$ is transitive on the points of β.*

In general, involutions in $Aut(\pi)$ can be wonderful tools for deducing properties of a projective plane π. Another advantage of working with involutions is that they have been completely classified as the next theorem shows.

THEOREM 5.8. *Let π be a projective plane of order n. An involution of π is either an elation (in which case n is even), a homology (in which case n is odd), or a Baer involution (in which case n is a square).*

Existence or non-existence of certain involutions may also be used to deduce properties of $Aut(\pi)$ as the theorem of Hughes given below shows. We prove an alternative version using abstract hyperovals in chapter 7.

THEOREM 5.9. *[41] Let π denote a projective plane of order n, with $n \equiv 2(mod\ 4)$ and $n > 2$. Then $Aut(\pi)$ has odd order.*

5.3. Polar Spaces

5.3.1. Sesquilinear and Bilinear forms. Let K be a field admitting an anti-automorphism ϕ, and V a vector space over K. We define a $\phi - sesquilinear\ form$ to be a function $f : V \times V \to K$ satisfying:

(1) $f(av + a'v', w) \;=\; af(v, w) \;+\; a'f(v', w)$,

(2) $f(v, aw + a'w') \;=\; a^{\phi}f(v, w) \;+\; a'^{\phi}f(v', w)$.

We say that f is non-singular if

(1) $\forall\ v \in V\ f(v, w) = 0 \Rightarrow w = 0$.

(2) $\forall\ w \in V\ f(v, w) = 0 \Rightarrow v = 0$.

Similarly, we define a bilinear form to be a 1_K-sesquilinear form. A bilinear form f is *alternating* if $f(v, v) = 0\ \forall\ v \in V$. A bilinear form is *reflexive* if $f(v, w) = -f(w, v)\ \forall$ $v,\ w \in V$. A ϕ-sesquilinear form is *Hermitian* if $f(v, w) = f(w, v)^{\phi}\ \forall\ v,\ w \in V$. Given a bilinear form f we may define a *quadratic form* as a map $q{:}V \to K$, where q is of degree two in each of the coordinates. It has the following properties:

$$q(av) \;=\; a^2q(v),\ \&\ q(v + w) \;=\; q(v) + q(w) + f(v, w).$$

Sesquilinear forms are related to polarities by the following theorem:

THEOREM 5.10. *Every correlation of $PG(n, K)$ is induced by a ϕ-sesquilinear form f, where ϕ is an anti-automorphism of K. The correlation is a polarity if and only if the form satisfies:*

$$(\forall v,\ w\ \in V)\ f(v, w) \;=\; 0 \;\Rightarrow\; f(w, v) \;=\; 0.$$

5.3.2. POLAR SPACES. Let f be a reflexive sesquilinear form on a vector space V over a field K, defining a polarity ϕ of the derived projective space. We say that a subspace $U \in V$ is *totally isotropic* if $f(U) = 0$, (i.e $U \subseteq U^{\phi}$). The totally isotropic subspaces of V form a subgeometry of the projective space called a *polar space*.

We list a few of the properties of polar spaces below:

- **PS1** Each totally isotropic space equipped with its lattice of totally isotropic subspaces, is isomorphic to a projective space of dimension of at most n-1.
- **PS2** The intersection of any family of totally isotropic subspaces is totally isotropic.
- **PS3** If U is a totally isotropic subspace of dimension n-1, and $p \in V - U$, then the set

$$L_p \ = \ \{q \ \in U : \ \textit{the line } pq \textit{ is totally isotropic}\},$$

  is a hyperplane in U, and the union of lines in L_p is a totally isotropic subspace of dimension n -1.

We now discuss an important family of polar spaces

5.3.3. Generalized Quadrangles. A polar space of rank 2 is a partial geometry satisfying the following properties:

- **GQ1** any line has at least three points;
- **GQ2** two points lie on at most one line;
- **GQ3** if a point p is not on a line ℓ, then p is collinear with a unique point of ℓ;
- **GQ4** no point is collinear with all others.

An incidence structure satisfying these properties is called a generalized quadrangle, or GQ for shorthand. GQs arising from this construction (i.e from polarities or quadratic forms) are called classical. However, not all GQs arise this way. This leads us to our next chapter on partial geometries.

CHAPTER 6

Abstract Ovals and Abstract Hyperovals

6.1. Abstract Ovals

In [15], Buekenhout recontextualized the study of ovals. He defined an **abstract oval** of order n on X to be a set $\Omega(X)$ of involutory permutations of a set X of cardinality $n+1 \geq 3$ such that

(1) each non-identity permutation has at most two fixed points, and the parity of the number of fixed points equals the parity of $n+1$

(2) for $A_1, A_2, B_1, B_2 \in X$ with $A_i \neq B_j$ there exists a unique $\sigma \in \Omega(X)$ with $\sigma(A_i) = B_i$ for $i = 1,2$.

Each oval X of a projective plane π of order n gives an abstract oval $\Omega(X)$ of order n, the set of all involutory permutations of X induced by the lines through the points P of π, not in X.

6.2. Abstract Hyperovals

Let X be a set of $n+2$ points. We define an *abstract hyperoval* on X and write $A(X)$ to denote a set of fixed point free involutions on X with the following property: For any four points $\{ a, b, c, d \} \subset X$, $\exists!\ u \in A(X)$ with

$$u : a \leftrightarrow b,\ c \leftrightarrow d.$$

The next few properties of abstract hyperovals may be deduced from the definition:

(1) $A(X)$ consists of n^2 - 1 fixed-point free involutions on X. Furthermore, any element of $A(X)$ is a product of $\frac{n+2}{2}$ transpositions.

(2) For any transposition t of points of X, there exists n-1 elements, $f \in A(X)$ such that $|Fix_X(f * t)| = 2$.

It follows from the definition of a hyperoval that we may always construct an abstract hyperoval from a hyperoval. Such an abstract hyperoval is called embeddable. Each abstract oval of even order can be uniquely extended to an abstract hyperoval, extending Qvist's result. (See, for example, [72]. [15] noted (without proof) the uniqueness of the abstract ovals of orders 2, 3, 4 and 5, and the non-existence of an abstract hyperoval of order 6. (As the latter is referred to as an experimental result, it may be computerbased.) A proof for the nonexistence of an abstract hyperoval of order 6 was given by [26]. [32] showed the uniqueness of the abstract oval of order 7 by computer.

Independently, [61] [31] [27] and [19], thesis [15], published 1985 [16]) constructed a nonembeddable abstract hyperoval of order 8 (giving two (non-embeddable) abstract ovals of order 8) : see also [33]. [61] classified abstract hyperovals of order 8 by computer : there are two of them (giving rise to 4 abstract ovals of order 8).

In 1980, John G. Thompson [71] initiated the study of abstract hyperovals of order 10, and he revisited the subject in 1981 [72]. Lam, Thiel, Swiercz and McKay (1983)[51] showed the non-existence of an abstract hyperoval of order 10 by computer, part of the proof of the nonexistence of a projective plane of order 10 completed by Lam, Thiel and Swiercz (1989)[50], also by computer.

Abstract ovals of order 9 were shown by computer to be embeddable by Giulietti and Montanucci (2009)[30]. (The projective planes of order 9 had previously been classified by computer by Lam, Kolesova and Thiel (1991)[49].) There are no known non-embeddable abstract ovals of odd order.

Similarly, each hyperoval X of a projective plane π of order n gives an abstract hyperoval $A(X)$ of order n, the set of all involutory permutations of X induced by the lines through the points P of π, not in X. Such an abstract hyperoval is called **embeddable**. The converse of the previous statement is false. As stated above, there exists one known example of an abstract hyperoval that cannot be embedded into any plane. We now pause to construct the abstract hyperoval of order 2 from the hyperoval of order 2 in $PG(2,2)$ over $GF(2)$.

Example 6.2.1 A Constructive Example

Recall the points of $PG(2,2)$ over $GF(2)$.

$$(0,0,1),\ (0,1,0),\ (1,0,0),\ (1,1,1),$$

$$(1,1,0),\ (1,0,1),\ (0,1,1).$$

The unique hyperoval X, is given by:

$$1\ =\ (0,0,1), 2\ =\ (0,1,0), 3\ =\ (1,0,0), 4\ =\ (1,1,1).$$

Consider the line in $PG(2,2)$ external to X,

$$E\ =\ x\ +\ y\ +\ z\ =\ 0.$$

$$E \;=\; \{(1,1,0),\ (1,0,1),\ (0,1,1)\}.$$

The secant lines through X incident with each of the points on E, pass through two points of X. The product of the transpositions fixing a unique point of E and interchanging two points of X are the fixed-point free involutions making up $A(X)$. We list them here: Let t and t' correspond to a transposition fixing (1,1,0). Then t and t' must interchange both 1 and 4, and 2 and 3. Thus, the fixed-point free involution corresponding to an element $a \in A(X)$ given by:

$$a \;=\; (1,4)(2,3).$$

Let u and u' correspond to a transposition fixing (1,0,1). Then u and u' must interchange both 1 and 3, and 2 and 4. Thus, the fixed-point free involution corresponding to an element $b \in A(X)$ given by:

$$b \;=\; (1,3)(2,4).$$

Finally, we let v and v' correspond to a transposition fixing (0,1,1). Then v and v' must interchange both 1 and 2, and 3 and 4. Thus, the fixed-point free involution corresponding to an element $c \in A(X)$ given by:

$$c \;=\; (1,2)(3,4).$$

We have now constructed the abstract hyperoval of order 2 given by:

$$(1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3).$$

THEOREM 6.1. *From any hyperoval, we may construct an abstract hyperoval.*

Example 6.2.2 Abstract Hyperoval of Order 4

$$A(X) := \{u_1 := (1,2)(3,4)(5,6), u_2 := (1,2)(3,5)(4,6),$$

$$u_3 := (1,2)(3,6)(4,5), u_4 := (1,3)(2,4)(5,6),$$

$$u_5 := (1,3)(2,5)(4,6), u_6 := (1,3)(2,6)(4,5),$$

$$u_7 := (1,4)(2,3)(5,6), u_8 := (1,4)(2,5)(3,6),$$

$$u_9 := (1,4)(2,6)(3,5), u_{10} := (1,5)(2,3)(4,6),$$

$$u_{11} := (1,5)(2,4)(3,6), u_{12} := (1,5)(2,6)(3,4),$$

$$u_{13} := (1,6)(2,3)(4,5), u_{14} := (1,6)(2,4)(3,5),$$

$$u_{15} := (1,6)(2,5)(3,4)\}.$$

6.3. Abstract Hyperovals and Partial Geometries

Given an abstract hyperoval $A(X)$ of order n, the incidence structure $S(A(X))$ with points the 2-subsets of X and lines the elements of $A(X)$ with the natural incidence is a partial geometry $pg(\frac{n}{2}, n-2, \frac{n-2}{2})$. Conversely, each $pg(s, 2s-2, s-1)$ arises in this way from an abstract hyperoval of order $2s$. This was established by De Clerck (1978, 1979)[22,23], building on the characterization of the triangular graphs $T(n+2)$ by their parameters for $n = 6$ by Connor (1958)[21], Shrikhande (1959)[69], Chang (1959)[13] and Hoffman (1960)[33], with all examples with the parameters of $T(8)$ determined by Chang (1960) [14]. (The triangular graph $T(m)$ has as vertices the subsets of size 2 of a set S of size m and edges the pairs of subsets meeting in a set of size 1.) Amongst other results, De Clerck (1979) [23] showed that the complements of the Chang graphs and $T(8)$ are not geometric, thereby showing the non-existence of a partial geometry $pg(3, 4, 2)$ and thus also of an abstract hyperoval of order 6.

CHAPTER 7

Using Abstract Hyperovals

The aim of this subsection is to familiarize the reader with certain preliminary facts and results we shall use throughout the section. Let Γ be a graph. We say that $C_m \subset \Gamma$ is a m-clique if $C_m \cong K_m$, the complete graph on m vertices. Throughout the section we identify $A(X)$ with a graph $\Gamma_{A(X)} = (V, E)$ where the vertices are given as

$$V \ = \ \{(x, y) : \ (x, y) \in X \times X - \{\cup_{x \in X}(x, x)\}$$

. (x, y) and (u, v) are adjacent if there exists an element $f \in A(X)$ such that

$$f : \ x \mapsto y, \ \& \ u \mapsto v$$

. Observe that f is distinct by the definition of an abstract hyperoval.

7.1. Minor Results

We now show the following results:

- C1: Each transposition appears in exactly n-1 elements of $A(X)$.
- C2: $|A(X)| = n^2$-1.
- C3: Let $\Gamma_{A(X)} = (V, \ E)$ with $V = (1, 2)^{S_{n+2}}$ and $E = (1, 2)(3, 4)^{S_{n+2}}$. $A(X)$ may be realized as the smallest set of $\frac{n+2}{2}$- cliques of Γ containing E.

We first prove $C1$.

PROOF. **C1:** Let $x, y \in X$. Let $A(X)|_{(x,y)}$ denote the set of elements in $A(X)$ having (x, y) as a factor. Let G be a group acting regularly on X-$\{x, y\}$, fixing x and y. The action of G on X induces a regular action on $A(X)|_{(x,y)}$. Since (x, y) was arbitrary, we conclude that each transposition appears

$$|G| \;=\; |X - \{x, y\}| \;=\; n - 1 \; times.$$

□

PROOF. **C2:** Consider a subset $U \subset A(X)$ whose elements are indexed by (x, y) $y \in X - \{x\}$. Observe that $|U| = n + 1$. Now act on $A(X)$ with the group G given above. We observe that the regular action of G on X-$\{x, y\}$ induces an action on $A(X)$. In particular, $U^G = A(X)$. To see this observe that any element either has the transposition (x, y) or the pair of transpositions (x, a), (y, b). The result follows by considering the regularity of the action of G on X-$\{x, y\}$ and the fact that this action is faithful and free on elements of $A(X)$(consider the orbits of elements indexed by (x, a), (y, b) for all $a, b \in X$-$\{x, y\}$). Thus,

$$|A(X)| \;=\; |U^G| \;=\; |U||G| \;=\; (n+1)(n-1) \;=\; n^2 - 1.$$

□

PROOF. **C3:** Let $A(X)$ be an abstract hyperoval of order n. Then $A(X)$ is a set fixed point free involutions on the points of X with the property that for any two pairs $\{a, b\}$ and $\{c, d\}$, there exists a unique fixed point free involution σ with

$$\sigma : a \leftrightarrow b, \; c \leftrightarrow d.$$

Let Γ be defined as before. Observe that each element of $A(X)$ corresponds to a set S of vertices of Γ such that the restricted graph S with edge set $E(S)$ is complete. This is precisely the definition of a clique.

Let C denote the set of $\frac{n+2}{2}$ cliques of Γ. We need only show that $A(X)$ corresponds to a set $M \subset C$, where M is minimal in the sense that it is the smallest subset of C containing $E(\Gamma)$. Recall that in M we must have each edge belonging to exactly one $\frac{n+2}{2}$-clique. Let $c \in C$. Then

$$|M| \;=\; \frac{|E(\Gamma)|}{|E(c)|} \;=\; \frac{\frac{(n+2)n(n^2-1)}{8}}{\frac{1}{2}\sum_{v\in c} d_M(v)} =$$

$$\frac{\frac{(n+2)n(n^2-1)}{8}}{\frac{n+2}{4}\frac{n}{2}} \;=\; n^2-1 \;=\; |A(X)|.$$

It follows from the string of equalities above that any set $N \subset C$ with less cliques than M would result in

$$|E(N)| \;<\; |E(M)| \;=\; |E(\Gamma)|.$$

Thus, $A(X)$ corresponds to a minimal subset of C.

Now suppose that M is a minimal set of C. We show that M corresponds to an abstract hyperoval. Since M is a minimal set of $\frac{n+2}{2}$-cliques of Γ, we know that each edge must be contained in at most one $\frac{n+2}{2}$-clique of M. If we identify the vertices of the $\frac{n+2}{2}$-cliques of M with fixed point free involutions on X, we see that M corresponds to a set of fixed point free involutions on X with the property that for any two pairs $\{a, b\}$ and $\{c, d\}$, there exists a unique fixed point free involution σ with

$$\sigma : a \leftrightarrow b,\; c \leftrightarrow d.$$

This is precisely the defining property of an abstract hyperoval. $\square$

The benefits of looking at abstract hyperovals in this way will be evident in the following section when we begin our investigation of one-factorizations in $A(X)$. We now show that a one-factorization of K_X can be realized as a subset $D \subset C$ that is minimal in the following sense: D is the smallest subset of C with $V(D) = V(\Gamma)$. An easy observation on the upper bound of D is that

$$|D| \leq n + 1 \ .$$

This is because there are only $\binom{n+2}{2} = (n+1)\frac{n+2}{2}$ transpositions, and each element is a product of $\frac{n+2}{2}$ of them.

C4: *Let $F(X)$ be a one-factorization of K_X. Then $F(X)$ can be realized as a set D of $n+1$ $\frac{n+2}{2}$-cliques of Γ.*

Proof. Let $F(X)$ be defined as above. Then $F(X)$ corresponds to a set of $n+1$ fixed point free involutions on X with $V(F(X)) = E(K_X)$. Thus, we may identify $F(X)$ with a set D of $\frac{n+2}{2}$-cliques of Γ. It is clear from the statement above that minimality is obtained when $|D| = n+1$.

If D is a subset of C with $V(D) = V(\Gamma)$, the identification of each element of D with a fixed point free involution on X gives us a set $F(X)$ of fixed point free involutions with each transposition on X appearing in exactly one element of $F(X)$. Thus, D corresponds to a one-factorization of K_X. □

7.2. Further Results

Lemma 7.1 (C. (2013)). *Let* $|X| = n+2$, $n \equiv 2(mod\ 4)$, *with* $n > 2$. *Let* $|Fix_X(g)| = m \in \{0, 2, 4\}$. *Consider the action of conjugation by* g, *an involution in* $Aut(A(X))$, *on* $C := (1, 2)(3, 4)^{S_X}$. *Then*

$$|Fix_C(g)| \ = \ 3\binom{\frac{n+2-m}{2}}{2} + \binom{m}{2}(\frac{n+2-m}{2}) + \frac{1}{2}\binom{m}{2}\binom{m-2}{2}.$$

Proof. Recall from Theorem 3 of [1], that if $m > 2$, then n is a square, which contradicts our assumption that $n \equiv 2(mod\ 4)$. So our formula need only be defined for $m \in \{0, 2\}$.

By assumption, g acts on $n + 2 - m$ points of X. Write $Fix_X(g) \ = \{f_1, \ldots, \ f_m\}$. Suppose g has a free action on $a, \ b, \ c, \ and \ d \ \in X$. Then for any pair of transpositions of g containing $\{a, \ b, \ c, \ d\}$, g fixes $(a, b)(c, d), \ (a, c)(b, d), \ \&, \ (a, d)(b, c)$. There are $\binom{\frac{n+2-m}{2}}{2}$ ways to select the transpositions of g. This gives us the term of

$$3\binom{\frac{n+2-m}{2}}{2}.$$

To count the number of ways g may fix a pair of transpositions with two elements from $Fix_X(g) \ \& \ X - Fix_X(g)$, we first observe that g does not fix any elements of the form $(f_1, a)(f_2, b)$ for

$$f_1, \ f_2 \ \in Fix_X(g), \ \& \ a, \ b \ \notin Fix_X(g).$$

Instead, g fixes a pair of transpositions with this property only if they have the form $(f_1, f_2)(a, b)$. There are $\binom{m}{2}$ ways to select $f_1, \ \&, \ f_2$, and for each of these ways there are $(\frac{n+2-m}{2})$ ways to select $a, \ b$. This yields the term of $\binom{m}{2}(\frac{n+2-m}{2})$.

Finally, we count the number of ways g may fix a pair of transpositions of points in $Fix_X(g)$. There are $\binom{m}{2}$ ways to select the first transposition and $\binom{m-2}{2}$ ways to select the second. This gives us a total of $\binom{m}{2}\binom{m-2}{2}$ pairs of transpositions of points in $Fix_X(g)$. Since,

$$(f_1, f_2)(f_3, f_4) \;=\; (f_3, f_4)(f_1, f_2),$$

we divide by 2 to obtain

$$\frac{1}{2}\binom{m}{2}\binom{m-2}{2}.$$

Summing over each case we obtain,

$$|Fix_C(g)| \;=\; 3\binom{\frac{n+2-m}{2}}{2} + \binom{m}{2}(\frac{n+2-m}{2}) + \frac{1}{2}\binom{m}{2}\binom{m-2}{2}.$$

□

LEMMA 7.2 (C. (2013)). $|Fix_{A(X)}(g)| \;=\; \frac{|Fix_C(g)|}{\binom{\frac{n+2}{2}}{2}}$.

PROOF. It follows from the definition of an abstract hyperoval that any pair of transpositions on X belong to a unique element of $A(X)$. If g fixes an element f in $A(X)$, g either:

(1) fixes a pair of transpositions of f or

(2) interchanges two transpositions of f.

Therefore, any element of $Fix_{A(X)}(g)$ contributes $\binom{\frac{n+2}{2}}{2}$ to the pairs of transpositions in $Fix_C(g)$. We obtain the number of elements of $A(X)$ fixed by g from dividing $|Fix_C(g)|$ by this contribution. Thus, $|Fix_{A(X)}(g)| \;=\; \frac{|Fix_C(g)|}{\binom{\frac{n+2}{2}}{2}}$. □

LEMMA 7.3 (C. (2013)). *Let $A(X)$ be an abstract hyperoval of order $n \equiv 2(mod\ 4)$. Suppose that $|Aut(A(X)|$ contains an involution, g. Then either $n \in \{2, 6\}$ or $|Fix_X(g)| < 2$.*

PROOF. Write

$$n \ = \ 4k + 2 \ (k \in \mathbb{Z}_{\geq 0}).$$

By 7.2

$$|Fix_{A(X)}(g)| \ = \ \frac{|Fix_C(g)|}{\binom{\frac{n+2}{2}}{2}}.$$

But when $|Fix_X(g)| \ = \ 2$, we have that:

$$\begin{aligned} |Fix_{A(X)}(g)| \ &= \frac{4(\frac{n}{2} + \frac{3}{4}(\frac{n}{2} - 1)n)}{(n+2)(\frac{n+2}{2} - 1)} \\ = \ &\frac{4(\frac{4k+2}{2} + \frac{3}{4}(\frac{4k+2}{2} - 1)(4k+2))}{((4k+2)+2)(\frac{(4k+2)+2}{2} - 1)} \\ = \ &\frac{3k+1}{k+1}. \end{aligned}$$

We immediately see that when $k \ \in \ \{0, 1\}$, $n \in \{2, \ 6\}$ and

$$|Fix_{A(X)}(g)| \ = \ \{1, 2\},$$

respectively. But for all $k \ > 1$,

$$\frac{3k+1}{k+1} \ \notin \ \mathbb{Z}.$$

To see this, observe that if $\frac{3k+1}{k+1} = c \in \mathbb{N}$,

$$1 \ < \ c \ = \ \frac{3k+1}{k+1} \ < \frac{3k+3}{k+1} \ = \ 3.$$

This implies the only possible value for c is 2. A quick calculation shows that the only value for k satisfying $c = 2$, is when k =1. We conclude that either $n \ \in \{2, \ 6\}$, or $|Fix_X(g)| < 2$. $\square$

LEMMA 7.4 (C. (2013)). *Let $A(X)$ be an abstract hyperoval of order $n \equiv 2(mod\ 4)$ with $n > 2$. Assume that g is an involutory automorphism on $A(X)$. Then $|Fix_X(g)| \neq 0$.*

PROOF. Suppose the contrary is true. Using 7.2 we compute:

$$|Fix_{A(X)}(g)| \ = \ \frac{|Fix_C(g)|}{\binom{\frac{n+2}{2}}{2}}$$

$$= \ \frac{3\binom{\frac{n+2-m}{2}}{2} + \binom{m}{2}\left(\frac{n+2-m}{2}\right) \ + \ \frac{1}{2}\binom{m}{2}\binom{m-2}{2}}{\binom{\frac{n+2}{2}}{2}}.$$

Set $m \ = \ 0$. To see that $|Fix_{A(X)}(g)| \ = \ 3$, we observe that when $m \ = \ 0$, the summands from the last two cases vanish. As a result, we have that

$$|Fix_{A(X)}(g)| \ = \ \frac{3\binom{\frac{n+2}{2}}{2}}{\binom{\frac{n+2}{2}}{2}} \ = \ 3.$$

Let f_i denote the unique element of $A(X)$ containing the transposition pair,

$$(1, \ g(1))(i, \ g(i)) \ for \ i \ \in \ \{2, \ 3, \ldots, \ \frac{n}{2}+1\}.$$

Write $n = 4k+2$, $(k \in \mathbb{Z}_{\geq 0})$. Observe that g must fix f_i for each $i \in \{2, 3, \ldots, \frac{n}{2}+1\}$. If $n > 2$, then $k > 0$. De Clerck proved the nonexistence of an abstract hyperoval of order 6 in 1979. The next largest value for $k > 1$. But if $k > 1$, we have that:

$$|Fix_{A(X)}(g)| \geq \frac{n}{2}$$

$$= \frac{4k+2}{2} \geq \frac{4(2)+2}{2}$$

$$= 5 > 3 = |Fix_{A(X)}(g)|,$$

a contradiction. As a consequence, we conclude that $|Fix_X(g)| \neq 0$. □

THEOREM 7.5 (C. (2013)). *Suppose that $A(X)$ is an abstract hyperoval of order $n \equiv 2(mod\ 4)$. Then $|Aut(A(X))|$ is odd.*

PROOF. Suppose that $|Aut(A(X))|$ is even. Then $Aut(A(X))$ must contain an involution, g. Note that $|Fix_X(g)|$ is even, as g is an involution and acts on an even number of elements of X. As a consequence of Theorem [3] of [1], if $Aut(A(X))$ contains an involution with four or more fixed points on X which fixes $A(X)$, then n is a square, which is impossible since $n \equiv 2(mod\ 4)$. The aforementioned fact along with previous lemmata imply that $|Fix_X(g)| \notin \mathbb{Z}_{\geq 0}$, which is impossible. Therefore, we must conclude that $|Aut(A(X))|$ is odd. □

THEOREM 7.6 (C. (2013)). *Let $A(X)$ be an abstract hyperoval of order n. Suppose that $G = Aut(A(X))$ contains two distinct involutions f & g such that*

$$|Fix_X(g)| \ \& \ |Fix_X(f)| \ \geq \ 4.$$

Then

$$Fix_X(f) \ \neq \ Fix_X(g).$$

PROOF. Suppose on the contrary that $Fix_X(f) \ = \ Fix_X(g)$. The preceeding lemmata along with Theorem 1 of [1] imply that

$$A(Fix_X(f)) \ = \ A(Fix_X(g))$$

is an embeddable abstract hyperoval of order $\sqrt{n}$. Therefore, there are

$$\frac{\sqrt{n}}{2}(\sqrt{n}-1)$$

external lines to $A(Fix_X(f))$, each corresponding to a one-factorization of $K_{\sqrt{n}+2}$. Furthermore, note that each of the one-factors correspond to an element of $Fix_{A(X)}(f) \cap Fix_{A(X)}(g)$.

Let

$$x \ \in \ (X \ - \ Fix_X(f)) \ = \ (X \ - \ Fix_X(g)).$$

There exist $\sqrt{n} \ + \ 1$ elements of $Fix_{A(X)}(f) \ \& \ Fix_{A(X)}(g)$ interchanging $\{x, \ g(x)\}, \& \ \{x, \ f(x)\}$, respectively. Since any two elements of an abstract hyperoval may share at most one transposition in common, we see that each set of $\sqrt{n} + 1$ elements of $Fix_{A(X)}(f)$ or $Fix_{A(X)}(g)$ interchanging $\{x, \ f(x)\} \ \& \ \{x, \ g(x)\}$, respectively, correspond to an external line of $A(Fix_X(f)) = A(Fix_X(g))$. Since any pair of external lines intersect exactly once, there exists an element,

$$t \in Fix_{A(X)}(f) \cap Fix_{A(X)}(g)$$

containing the transpositions $(x,\ g(x))$, & $(x,\ f(x))$. But t is a fixed point free involution. Therefore, $g = f$, on $X - Fix_X(g)$ a contradiction. As a result, we conclude that our initial assumption was false, and that

$$Fix_X(f) \neq Fix_X(g).$$

□

7.3. Automorphisms of Abstract Hyperovals

The *automorphism group* $Aut(A(X))$ of an abstract hyperoval $A(X)$ is the stabilizer of $A(X)$ in $Sym(X)$, acting via conjugation. The connection with partial geometries is functorial : the automorphism group of the corresponding partial geometry $\mathcal{P} = pg(\frac{n}{2}, n-2, \frac{n-2}{2})$ to an abstract hyperoval $A(X)$ of order n is isomorphic to $Aut(A(X))$. To see this, note that the automorphism group of $\mathcal{P}$ is the subgroup of the automorphism group of the point graph of $\mathcal{P}$ that takes lines to lines. The point graph Γ of the partial geometry is a strongly regular graph with the parameters of the complement of the triangular graph $T(n+2)$. By [25], [77], [17], [38], [26], it follows that Γ is isomorphic to the complement of $T(n+2)$. Since lines of $\mathcal{P}$ correspond to cliques of Γ of size $\frac{n+2}{2}$, these in turn correspond to fixed-point-free involutions of the point set X of $\mathcal{P}$. So $Aut(\mathcal{P})$ is the stabilizer of $A(X)$ in $Aut(\Gamma)$. It remains to show that $Aut(\Gamma)$ is $Sym(X)$. The triangular graph $T(m)$ is the line graph of the complete graph K_m, so $Aut(T(m)) = S_m$, by Theorem 8 of Whitney (1932) [85] (who calls line graphs *dual graphs*).

Studying projective planes and hyperovals via their automorphism groups has a long history. Baer (1946)[6] showed that a collineation of order 2 of a projective plane of finite order n is either a homology (in which case n is odd), an elation (in which case n is even) or the fixed points and lines form a subplane of order $\sqrt{n}$ (in which case n is a square). Biliotti and Korchmaros (1986)[9] show that a non-identity elation fixing a hyperoval has centre not on that hyperoval. Penttila and Royle (1995)[69] show that a non-identity elation fixing a hyperoval has axis a secant line of the hyperoval, if the order of the plane exceeds two.

Biliotti and Korchmaros (1986)[9] show that a non-identity collineation of a projective plane of order n stabilizing a hyperoval fixes at most $\sqrt{n}+2$ points of that hyperoval, and that equality implies the collineation is of order 2. They also show that a non-identity collineation of a projective plane fixes 1, 3 or an even number of points of the hyperoval, and that if it fixes at least 4 points, then the fixed points form a hyperoval in a subplane. We generalize these results to abstract hyperovals. To do this we need some notation : if the group G acts on the set Y, then $Fix_Y(g) = \{y \in Y : gy = y\}$. For an abstract hyperoval $A(X)$ on X, and $g \in Aut(A(X))$, we will need both $Fix_X(g)$ and $Fix_{A(X)}(g)$.

THEOREM 7.7. *Let $A(X)$ be an abstract hyperoval on X, and $g \in Aut(A(X))$ which fixes at least four points of X. Then $|Fix_X(g)|$ is even, and $A(Fix_X(g)) = \{t|_{Fix_X(g)} : t \in Fix_{A(X)}(g)\}$ is an abstract hyperoval on $Fix_X(g)$.*

PROOF. Let $\{a,b,c,d\} \subset Fix_X(g)$ with $|\{a,b,c,d\}| = 4$. Then there is a unique $t \in A(X)$, interchanging a and b and interchanging c and d. But gtg^{-1} also interchanges a and b and c and d, so it follows that $gtg^{-1} = t$. Thus $t \in Fix_{A(X)}(g)$, and so there is a unique $t \in A(Fix_X(g))$, interchanging a and b and interchanging c and d. □

THEOREM 7.8. *Let $A(X)$ be an abstract hyperoval on X of order n, and $g \in Aut(A(X))$. Then $|Fix_X(g)| \leq \sqrt{n}+2$, and equality implies that n is a square and g has order 2.*

PROOF. Let $m+2 = |Fix_X(g)|$ and $M = |Fix_{A(X)}(g)|$. Then, by the last theorem, $M = m^2 - 1$. Suppose $u \in Fix_{A(X)}(g), a \in X, a \notin Fix_X(g), a' = u(a)$. Then

$$g(a') = gu(a) = u(g(a)),$$

so, if $a' \neq g(a)$, a' determines u (as there is a unique $u \in A(X)$ interchanging a and a' and interchanging $g(a)$ and$g(a')$). Since a' is an element of $X \setminus Fix_X(g)$, not equal to a or $g(a)$ in this case, there are $(n+2)-(m+2)-2 = n-m-2$ possiblities for $u \in Fix_{A(X)}(g)$ with $u(a) \neq g(a)$. If $a' = g(a)$, and $b \in Fix_X(g)$ then $u(b) \in Fix_X(g)$, $u(b) \neq b$, so there are $m+1$ choices for $u(b)$ and so for u. Thus $M \leq n-1$, giving $m \leq \sqrt{n}$. If equality occurs, then each choice of $u(b) \in Fix_X(g) \setminus \{b\}$ gives rises to a $u \in A(X)$ interchanging a and $g(a)(= a')$, b and $b' = u(b)$ which commutes with g. But now $g(a') = u(g(a)) = u(a') = a$: g must interchange a and a', and this is true for all $a \in X \setminus Fix_X(g)$, so g is an involution. □

THEOREM 7.9. *Let $A(X)$ be an abstract hyperoval on X of order n, and $g \in Aut(A(X))$ of order 2 which fixes at least four points of X. Then n is a square,$|Fix_X(g)| = \sqrt{n}+2$, and $A(Fix_X(g))$ is an embeddable abstract hyperoval of order $\sqrt{n}$.*

PROOF. Let $x, x' \in X \setminus Fix_X(g)$ and $|Fix_X(g)| = m+2$. If $x' = gx$, then there are $m+1$ elements u of $Fix_{A(X)}(g)$ interchanging x and x', namely any element interchanging x and x' and two elements y, y' of $Fix_X(g)$. (For there are $\frac{(m+2)(m+1)}{2}$ choices for $\{y, y'\}$ and each u interchanges $\frac{m+2}{2}$ of them.)

If $x' \neq gx$, then there is a unique element u of $A(X)$ interchanging x and x' and gx and gx'. Since u^g also interchanges x and x' and gx and gx', it follows that $u^g = u$; that is, $u \in Fix_{A(X)}(g)$. There are $m^2 - 1$ elements of $Fix_{A(X)}(g)$ each of which interchanges $\frac{n-m}{2}$ pairs $\{x, x'\}$ with $x, x' \in X \setminus Fix_X(g)$, so

$$\frac{(m^2-1)(n-m)}{2} \geq \frac{(n-m)(m+1)}{2} + \frac{(n-m)(n-m-2)}{2},$$

giving

$$(m^2-1) \geq (m+1) + (n-m-2),$$

so

$$m^2 \geq n$$

.

Since, by Theorem 2, $m^2 \leq n$, it follows that $m^2 = n$.

Given $\{x, x' = g(x)\}$, the $m+1$ elements of $Fix_{A(X)}(g)$ interchanging x and x' form a 1-factorization of the complete graph on $Fix_X(g)$ (identifying fixed-point-free involutions with 1-factors of the complete graph), so we have a set $\mathcal{D}$ of $\frac{m^2-m}{2}$ 1-factorizations of $Fix_X(g)$ (they must be distinct, indeed they must meet in at most one 1-factor, for otherwise there would be two elements of $Fix_{A(X)}(g)$ arising from both $\{x, g(x)\}$ and $\{w, g(w)\}$). Thus, the hypotheses of the main theorem of Bose and Shrikhande (1973) [12] are satisified, with one component of the regular two-component pairwise balanced design being the lines of the dual of $\mathcal{S}(A(Fix_X(g))$ and the other component being $\mathcal{D}$. It follows from that theorem that $A(Fix_X(g))$ is embeddable. $\square$

Examples of embeddable hyperovals show that these results are, in some sense, best possible. For example, the collineation $g\colon (x,y,z) \mapsto (x^{2^a}, y^{2^a}, z^{2^a})$ stabilizes the regular hyperoval $H = \{(1,t,t^2) : t \in GF(2^{ab})\} \cup \{(0,1,0),(0,0,1)\}$ of $\mathrm{PG}(2,2^{ab})$, fixes 2^a+2 points of H and has order b and $Fix_H(g)$ is a hyperoval of the subplane $\mathrm{PG}(2,2^a)$ fixed by g.

The collineation $(x,y,z) \mapsto (cx,cy,cz)$ also stabilizes H and fixes 3 points of H and has order dividing $2^{ab}-1$, for $c \in GF(2^{ab}), c \neq 0$. The collineation $(x,y,z) \mapsto (x, x+y, x+z)$, stabilizes H and fixes 2 points of H and has order 2 and the collineation $(x,y,z) \mapsto (c^2z, cy+cdz, x+d^2z)$, where the polynomial x^2+cx+d is irreducible over $GF(2^{ab})$, stabilizes H and fixes 1 point of H, and has order dividing $2^{ab}+1$. Finally, the Lunelli-Sce hyperoval L of $\mathrm{PG}(2,16)$, the regular hyperoval H of $\mathrm{PG}(2,4)$, and the elliptic hyperoval of the translation plane over the semifield of order 16 with kernel $GF(2)$ (see [70]) admit elements of order 3 stabilizing the hyperoval and fixing no point of the hyperoval (also see Korchmaros (1978) [54]).

7.3.1. Abstract hyperovals of order 12. Just as for the problem of existence of a projective plane of order 12, the problem of existence of an abstract hyperoval of order 12 is presently out of computational reach. The standard path is to turn to a symmetry hypothesis: in a series of 17 papers by 10 authors over the period 1973-2009, it is shown that, if a projective plane of order 12 exists, its group is of order 1, 2 or 3 [3, 4, 7, 14, 39, 40, 43–52, 79]. This demonstrates that this kind of work has a long pedigree, even when just looking at order 12 (which is also the smallest open case for which the existence of a projective plane is undecided).

Turning to abstract hyperovals of order 12, Prince (1997)[71] showed by computer that there is no abstract hyperoval of order 12 admitting a Frobenius group of order 39. We improve his result :

THEOREM 7.10 (C., Penttila (2012)). *There is no abstract hyperoval of order 12 admitting a group of order 13. Equivalently, there is no partial geometry* $pg(6, 10, 5)$ *admitting a group of order 13.*

Our proof is also by computer.

PROOF. First we need a re-interpretation of an abstract hyperoval : an abstract hyperoval of order n is a set K of $n^2 - 1$ fixed-point-free involutions of degree $n + 2$ with the property that the product of any two distinct elements of K has 0 or 2 fixed points, and conversely.

In the light of that re-interpretation, the following definition will be useful.

An **abstract arc** is a set K of fixed-point-free involutions of degree $n + 2$ with the property that the product of any two distinct elements of K has 0 or 2 fixed points.

All subgroups of order 13 of the symmetric group of degree 14 are conjugate, being Sylow 13-subgroups. Of the 10395 orbits of a subgroup of order 13 on the set of fixed-point-free involutions of the symmetric group of degree 14, it turns out that 6600 are abstract arcs. The union of 3827948 pairs of these 6600 orbits are abstract arcs. The graph with vertices the 6600 orbits that are abstract arcs and edges the 3827948 pairs of orbits with unions that are abstract arcs has no clique of size 11. Therefore, there is no abstract hyperoval of order 12 admitting a group of order 13. The computations were done in Magma [13] and are in many ways similar to those in [71]. □

THEOREM 7.11 (C., Penttila (2012)). *There is no abstract hyperoval of order 12 admitting a group of order 11. Equivalently, there is no partial geometry* $pg(6, 10, 5)$ *admitting a group of order 11.*

Again, the proof is by computer.

PROOF. All subgroups of order 11 of the symmetric group of degree 14 are conjugate, being Sylow 11-subgroups. Of the 12285 orbits of a subgroup of order 11 on the set of fixed-point-free involutions of the symmetric group of degree 14, it turns out that 8445 are abstract arcs. The union of 6790170 pairs of these 8445 orbits are abstract arcs. The graph with vertices the 8445 orbits that are abstract arcs and edges the 6790170 pairs of orbits with unions that are abstract arcs has no clique of size 13. Therefore, there is no abstract hyperoval of order 12 admitting a group of order 11. The computations were again done in Magma. □

THEOREM 7.12. *[1] No abstract hyperoval of order 12 admits a dihedral group of order 14.*

PROOF. By Theorem 1 of [1], an element of order 7 that is an automorphism of an abstract hyperoval of order 12 is the product of two disjoint 7-cycles. A group of order 14 has a normal Sylow 7-subgroup, so is dihedral or cyclic. A dihedral subgroup of S_{14} of order 14, in which the Sylow 7-subgroup is generated by the product of two disjoint 7-cycles either acts regularly or has two orbits of length 7. If there are two orbits of length 7, then involutions have two fixed points, which by theorem 4 of [1], forces them to fix 11 elements of $A(X)$.

But then there are 11 orbits of length 7 on $A(X)$ & this is impossible, for there are only seven fixed point involutions that centralize a product of two disjoint 7-cycles; thus $A(X)$ is the union of orbits of length 14, 11 orbits of length 7 and some of these seven - which cannot make 143. Finally, a computer program in Magma rules out the transitive case : the cliques in the usual graph are not big enough. $\square$

CHAPTER 8

Transitive Hyperovals

A great deal of work has been done on the classification of the transitive hyperovals by Billotti, Korchmaros, Penttila, as well as Sonnino. In a paper published in 1987, Billotti and Korchmaros proved the following deep results.

Theorem 8.1. *Let π be a finite projective plane of even order, Ω a hyperoval of π, and G a collineation group of π which leaves Ω invariant and acts transitively on its points. If 4 $|$ G , then π has order 2, 4, or 16.*

Theorem 8.2. *Let π be a projective plane of even order $n \geq 8$ containing a transitive hyperoval Ω. If the order of the collineation group G preserving Ω is divisible by 4, then $n = 16$ and $|G|$ divides 144.*

Transitive hyperovals have been classified for Desarguesian planes. In a 2004 paper, Sonnino was able to show that:

Theorem 8.3. *Let π be a projective plane of order 16 containing a transitive hyperoval Ω. If the order of the collineation group G preserving Ω is equal to 144, then $\pi \cong PG(2, 16)$ and Ω is the Lunelli-Sce-Hall Hyperoval in $PG(2, 16)$.*

Observe that if π is a projective plane and Ω is a hyperoval of that plane, then we may derive the abstract hyperoval $A(\Omega)$ using the technique given above. Now observe that any collineation group on π acting on Ω induces an automorphism group on $A(\Omega)$.

Let $\mathcal{F}$ denote the set of all fixed-point free involutions on Ω. It is easy to see that $A(\Omega) \subset \mathcal{F}$. Let G denote the collineation group acting transitively on Ω. Let $A(G) \subset S_\Omega$ denote the induced automorphism group of $A(\Omega)$ induced by G. It is intuitively obvious to any casual observer that $A(\Omega)$ is preserved by $A(G)$.

Sonnino's approach was to use what Biliotti and Korchmaros proved about any transitive group of a hyperoval contained in a plane of order 16 to narrow down the possibilities of a group G of order 144. Then, he carried out a computer aided search for all abstract hyperovals (if any) whose underlying hyperoval admits a transitive action under G. We simply check whether or not $\mathcal{F}^G$ contained an orbit of size $|A(\Omega)|$. To find such an orbit would suggest the existence of a transitive group acting on Ω. If no such orbit exists, we may conclude that there cannot exist such a group.

8.1. Prior Results

We will need the classification of transitive permutation groups of degree 18, as well as the following theorems of 8.5 and 8.6

Theorem 8.4 (Hulpke (2005) [42]). *There are 983 transitive groups of degree 18.*

Theorem 8.5 (Biliotti-Korchmaros (1987)). *A transitive hyperoval in a finite projective plane of order n is either a regular hyperovals in* $\mathrm{PG}(2,2)$ *or* $\mathrm{PG}(2,4)$ *or $n = 16$. If $n = 16$, then the order of the group G of the hyperoval divides 144, the group fixes a Baer subplane π_0 disjoint from the hyperoval (and the pointwise stabilizer $G_{(\pi_0)}$ of π_0 in G has order at most 2) and G centralizes a unitary polarity of π_0 and acts transitively on the absolute points of that polarity in π_0. Moreover, G contains exactly nine involutions fixing two points of the hyperoval.*

THEOREM 8.6 (Sonnino (2005)). *A transitive hyperoval in a finite projective plane of order* 16 *with a group of order 144 is a Lunelli-Sce hyperoval in* $\mathrm{PG}(2,16)$.

We will follow Sonnino's methods closely, so it is necessary to describe them. The description in Theorem 8.5 of the group G of the hyperoval means that either G is the unique up to conjugacy subgroup of $P\Gamma U(3,4)$ of order 144 or the kernel of the action on the Baer subplane π_0 has order 2 and G^{π_0} is $AGL(1,9)$ or the semidirect product of $C_3 \times C_3$ by Q_8. Consideration of the possible transitive actions of degree 18 of these groups, it is feasible to mount a computer search for abstract hyperovals of order 18 admitting these actions.

Each such transitive action on a set X induces an action on the fixed-point-free involutions of degree 18, and any such abstract hyperoval $A(X)$ must be a union of orbits of this induced action. Many orbits O fail to satisfy the condition (necessary to be a subset of an abstract hyperoval) that whenever $a_1, a_2, b_1, b_2 \in X$ are distinct, there is at most one $\sigma \in O$ with $\sigma(a_1) = a_2$ and $\sigma(b_1) = b_2$.

Define a graph with vertices the orbits satisfying this condition and edges the unions O of a pair of vertices satisfying this condition. Then $A(X)$ corresponds to a clique of this graph; and mounting a clique search leads to all abstract hyperovals arising from a transitive hyperoval in a finite projective plane of order 16 with a group of order 144. It turns out that they all arise from a Lunelli-Sce hyperoval in $rmPG(2,16)$ and that such an abstract hyperoval embeds in a unique projective plane of order 16.

8.2. OUR METHODS

Sonnino's methods need to be sharpened a little to make the remaining cases computationally feasible. It turns out that good use can be made of the invariant Baer subplane.

LEMMA 8.7. *Let $A(X)$ be an abstract hyperoval of order 16 arising from a transitive hyperoval X in a finite projective plane π of order* 16 *with group G. Then there is an orbit U of G on $A(X)$ of size 9 and a union U' of orbits of G on $A(X)$ of size 12 such that if $B = U \cap U'$, we have the following:*

(1) *there is a set L of 9 subsets $\ell_1, \ldots, \ell_9$ of B of size 5 with $|Fix(\sigma\tau)| = 2$ for $\sigma \neq \tau$ in ℓ_i ($i = 1, \ldots, 9$),*

(2) *there is a set M of 12 subsets $m_1, m_2, \ldots, m_{12}$, of B of size 5 with $|Fix(\sigma\tau)| = 0$ for $\sigma \neq \tau$ in m_i ($i = 1, \ldots, 12$), and*

(3) *the incidence structure with point set B, line set $L \cup M$ and incidence set membership is a projective plane π_0' of order 4 and U is a unital of π_0'.*

PROOF. By Theorem 8.5, G leaves invariant a Baer subplane π_0 of π which is disjoint from X. The points of π not on X correspond to elements of $A(X)$ and the permutations groups $(G, \pi \setminus X)$ and $(G, A(X))$ are permutationally isomorphic via this correspondence. Moreover, π_0 is a union of G-orbits corresponding to the 9 absolute points of the G-invariant unitary polarity (which form a unital of π_0) and of G-orbits corresponding to the 12 non-absolute points of the G-invariant unitary polarity.

Every point of the hyperoval X lies on a unique line of π_0; this line is secant to X. Moreover, the points on this line and not on X correspond to element of $A(X)$ interchanging the points on the line on X; and hence there pairwise products fix these points. These 9 lines of π_0 secant to X give the set L via the correspondence between points not on X and elements of $A(X)$.

The remaining 12 lines of π_0 give the set M via the correspondence between points not on X and elements of $A(X)$; since they are external to X, the pairwise products of distinct elements corresponding to such a line are fixed-point-free. □

Like Sonnino, our programs were implemented in the computer algebra system Magma. It turns out to be far more efficient to search for the possible subsets U and U' arising from Lemma 8.7 of an abstract hyperoval of order 16 arising from a transitive hyperoval X in a finite projective plane π of order 16 first, and then to seek other orbits of the underlying group compatible with U and U'.

We ran through the list of transitive subgroups of degree 18 acting on $X = \{1, \ldots, 18\}$, first checking the conditions given by Theorem 8.5 for the groups, and, then, for each of the surviving groups G, finding the orbits O on fixed-point-free involutions such that whenever $a_1, a_2, b_1, b_2 \in X$ are distinct, there is at most one $\sigma \in O$ with $\sigma(a_1) = a_2$ and $\sigma(b_1) = b_2$.

The next step was to find the projective planes π'_0 of order 4 given by Lemma 8.7 invariant under G. Now, for each π'_0, we find the set V of orbits O on fixed-point-free involutions such that whenever $a_1, a_2, b_1, b_2 \in X$ are distinct, there is at most one $\sigma \in O \cup \pi'_0$ with $\sigma(a_1) = a_2$ and $\sigma(b_1) = b_2$.

Now we find the set E of pairs $\{O, O'\}$ with $O, O' \in V$ such that there is at most one $\sigma \in O \cup O' \cup \pi'_0$ with $\sigma(a_1) = a_2$ and $\sigma(b_1) = b_2$. Now the cliques of the graph $\Gamma = (V, E)$ are found, where the union of the elements of the clique contains 255 fixed-point-free involutions (255 is the size of an abstract hyperoval of order 16).

It turned out that all the abstract hyperovals arising from the search had a group of order 144, and so, by Theorem 8.6, X is a Lunelli-Sce hyperoval and π is Desarguesian. Together with Theorem 8.5, this proves the main theorem. $\diamond$

In more detail, 39 of the 983 transitive groups of degree 18 have orders divisible by 36 and dividing 144. By Theorem 8.6, we could restrict our attention to the 24 groups of order 36 or 72. Restricting our attention to groups contain no proper transitive subgroup of order divisible by 4 reduces this list to 9 groups. Applying Theorem 8.5, can reduce this still further to 5 groups, as the remaining groups are neither isomorphic to a subgroup of $P\Gamma U(3,4)$ nor have a normal subgroup of order 2 such that the quotient group is isomorphic to a subgroup of $P\Gamma U(3,4)$. One of the remaining groups does not contain 9 involutions with 2 fixed points, so can be eliminated by Theorem 8.5. The four surviving groups were $TransitiveGroup(18,i)$, for $i = 9, 10, 12, 28$, in the implementation of Hulpke's result on Magma. Each of these was fed into our algorithm.

By using the induced action on fixed-point-free involutions, it was possible to calculate the stabilizer of each abstract hyperoval that arose from running our software, and to check that its preimage in $Sym(X)$ was permutationally isomorphic to the group of the Lunelli-Sce hyperoval acting on the points of the Lunelli-Sce hyperoval. Now theorem 8.6 applies; the hyperoval X is a Lunelli-Sce hyperoval and π is Desarguesian.

Bibliography

[1] Cooper, B, Penttila, T. Abstract Hyperovals of order 12. In preparation.

[2] De Clerck, F., Een combinatorische studie van de eindige partiele meetkunden, Ph. D. thesis, Universiteit Gent, 1978.

[3] Akiyama, Kenzi, Suetake, Chihiro The nonexistence of projective planes of order 12 with a collineation group of order 8. J. Combin. Des. 16 (2008), 411-430.

[4] Akiyama, Kenzi, Suetake, Chihiro On projective planes of order 12 with a collineation group of order 9. Australas. J. Combin. 43 (2009), 133-162.

[5] Baer, Reinhold Polarities in finite projective planes. Bull. Amer. Math. Soc. **52** (1946) 77-93.

[6] Baer, Reinhold Projectivities with fixed points on every line of the plane. Bull. Amer. Math. Soc. **52**(1946), 273-286.

[7] Baumert, Leonard; Hall, Marshall, Jr. Nonexistence of certain planes of order 10 and 12. J. Combinatorial Theory Ser. A **14** (1973), 273-280.

[8] Biliotti, Mauro; Vikram, Jha; Johnson, Norman L; **Handbook of Finite Translation Planes** Chapman & Hall/ CRC, 2007. 5–11.

[9] Biliotti, Mauro; Korchmaros, Gabor Collineation groups strongly irreducible on an oval. Combinatorics '84 (Bari, 1984), 85-97, North-Holland Math. Stud., 123, North-Holland, Amsterdam, 1986.

[10] Bose, R. C. Mathematical theory of the symmetrical factorial design. Sankhy$\bar{a}$, **8** (1947). 107-166.

[11] Bose, R. C. Strongly regular graphs, partial geometries and partially balanced designs. Pacific J. Math. **13** (1963), 389-419.

[12] Bose, R.C, Shrikhande, S.S. Embedding the complement of an oval in a projective plane of even order. Discrete Math. **6** (1973), 305-312.

[13] Wieb Bosma, John Cannon, and Catherine Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput, **24** (1997), 235-265.

[14] Brown, Julia M. Nowlin On constructing finite projective planes from groups. Ars Combin. 16 (1983), A, 6185.

[15] Buekenhout, Francis Etudes intrinseque des ovales. Rend. Mat. e Appl. (5) 25 1966 333-393.

[16] Buekenhout, F. De Clerck and H. Van Maldeghem. **Handbook of Incidence Geometry: Buildings and Foundations.** North-Holland, 1995. 44-45, 437-444.

[17] Chang Li-ch'ien The uniqueness and nonuniqueness of the triangular association schemes. Sci. Record (N.S.) **3** (1959), 604–613.

[18] Chang Li-ch'ien Association schemes of partially balanced designs with parameters $v = 28, n_1 = 12, n_2 = 15 and p_{11}^2 = 4$. Sci. Record (N.S.) **4** (1960), 12-18.

[19] Cherowitzo,W. On the extension of pre-oval configurations, Ph. D. thesis, Columbia University, 1983.

[20] Cherowitzo, William Harmonic ovals of even order. Finite geometries (Winnipeg, Man., 1984), 6581, Lecture Notes in Pure and Appl. Math., 103, Dekker, New York, 1985.

[21] Cherowitzo, William α-flocks and hyperovals. Geom. Dedicata **72** (1998), 221-246.

[22] Cherowitzo, W., Kiel, D.I., Killgrove, R.B. Ovals and other configurations in the known planes of order nine, Congr. Numer. **55** (1986), 167–179.

[23] Cherowitzo, William E., O'Keefe, Christine M., Penttila, Tim A unified construction of finite geometries associated with q-clans in characteristic 2. Adv. Geom. **3** (2003), 1-21.

[24] Cherowitzo, W., Penttila, T., Pinneri, I., Royle, G. F. Flocks and ovals. Geom. Dedicata **60** (1996), 17-37.

[25] Connor, W. S. The uniqueness of the triangular association scheme. Ann. Math. Statist. **29** (1958), 262-266.

[26] De Clerck, F., Een combinatorische studie van de eindige partiële meetkunden, Ph. D. thesis, Universiteit Gent, 1978.

[27] De Clerck, F. The pseudogeometric and geometric (t,s,s1)-graphs. Simon Stevin **53** (1979), 301-317.

[28] De Clerck, F., Van Maldeghem, H. Some classes of rank 2 geometries, Chapter 10 of Buekenhout,F. (ed.), Handbook of Incidence Geometry, North-Holland, 1995.

[29] Dembowski, Peter **Finite Geometries**, Springer, Berlin (1997) (reprint of the 1968 edition).

[30] de Witte, Paul The exceptional case in a theorem of Bose and Shrikhande. J. Austral. Math. Soc. Ser. A 24 (1977), no. 1, 64-78.

[31] Faina, G.; Cecconi, G. A finite Buekenhout oval which is not projective. Simon Stevin **56** (1982), 121-127.

[32] Faina, Giorgio, Cecconi, Giorgio On the minimum order of nonprojective abstract (or Buekenhout) ovals and uniqueness of the abstract oval of order seven. Note Mat. **1** (1981), 93-111 (1982).

[33] Faina, Giorgio Example of a nonprojective abstract oval with Pascalian tangents whose automorphism group is solvable and doubly transitive. Barlotti, A., Marchi, M., Tallini, G. eds., Proceedings of the conference on combinatorial and incidence geometry: principles and applications (La Mendola, 1982), 289296, Rend. Sem. Mat. Brescia, 7, Vita e Pensiero, Milan, 1984.

[34] Giulietti, Massimo, Montanucci, Elisa Abstract ovals of order 9. Ars Combin. **91** (2009), 297-301.

[35] Glynn, David G. Two new sequences of ovals in finite Desarguesian planes of even order. Combinatorial mathematics, X (Adelaide, 1982), 217229, Lecture Notes in Math., 1036, Springer, Berlin, 1983.

[36] Hall, Marshall, Jr. Ovals in the Desarguesian plane of order 16. Ann. Mat. Pura Appl. (4) **102** (1975), 159-176.

[37] Hilbert, David (1899). **Grundlagen der Geometrie**. 2nd ed. Chicago: Open Court.

[38] Hoffman, A. J. On the uniqueness of the triangular association scheme. Ann. Math. Statist. **31** (1960), 492-497.

[39] Horvatic-Baldasar, K., Kramer, E., Matulic-Bedenic, I. Projective planes of order 12 do not have an abelian group of order 6 as a collineation group. Punime Mat. No. **1** (1986), 75-81.

[40] Horvatic-Baldasar, K., Kramer, E.,Matulic-Bedenic, I. On the full collineation group of projective planes of order 12. Punime Mat. No. **2** (1987), 9-11.

[41] D. Hughes, F. Piper. **Projective Planes**. Springer-Verlag, 1973. 202-204

[42] Hulpke, Alexander. Constructing Transitive Permutation Groups. J. Symbolic Comput. 39(2005), no. 1, 1-30.

[43] Janko, Zvonimir Projective planes of order 12 with a collineation group of order 27. Rad Jugoslav. Akad. Znan. Umjet. No. **408** (1984), 1-6.

[44] Janko, Zvonimir, Tran Van Trung On projective planes of order twelve and twenty. Math. Z. **173** (1980), 199-201.

[45] Janko, Zvonimir, Tran Van Trung On projective planes of order 12 which have a subplane of order 3. I. J. Combin. Theory Ser. A **29** (1980), 254-256.

[46] Janko, Zvonimir; Tran Van Trung Projective planes of order 12 do not have a nonabelian group of order 6 as a collineation group. J. Reine Angew. Math. 326 (1981), 152157.

[47] Janko, Zvonimir, Tran Van Trung On projective planes of order 12 with an automorphism of order 13. I. Kirkman designs of order 27. Geom. Dedicata **11** (1981), 257-284.

[48] Janko, Zvonimir, Tran Van Trung Projective planes of order 12 do not possess an elation of order 3. Studia Sci. Math. Hungar. **16** (1981), 115-118.

[49] Janko, Zvonimir, Tran Van Trung On projective planes of order 12 with an automorphism of order 13. II. Orbit matrices and conclusion. Geom. Dedicata **12** (1982), 87-99.

[50] Janko, Zvonimir, Tran Van Trung The full collineation group of any projective plane of order 12 is a 2,3-group. Geom. Dedicata **12** (1982), 101-110.

[51] Janko, Zvonimir, Tran Van Trung A generalization of a result of L. Baumert and M. Hall about projective planes of order 12. J. Combin. Theory Ser. A **32** (1982), 378-385.

[52] Janko, Zvonimir, Tran Van Trung Projective planes of order 12 do not have a four group as a collineation group. J. Combin. Theory Ser. A **32** (1982), 401-404.

[53] Järnefelt, G., Kustaanheimo, Paul An observation on finite geometries. Den 11te Skandinaviske Matematikerkongress, Trondheim, 1949, pp. 166182. Johan Grundt Tanums Forlag, Oslo, 1952.

[54] Korchmaros, Gabriele Collineation groups transitive on the points of an oval [$(q+2)$-arc] of $S_{2,q}$ for q even. Atti Sem. Mat. Fis. Univ. Modena **27** (1978), 89-105.

[55] Old and new results on ovals in finite projective planes, pp. 41–72 in Keedwell, A.D. ed., Surveys in Combinatorics, London Math. Soc. Lecture Note Series **166**, Cambridge University Press, 1991.

[56] Lam, C. W. H., Kolesova, G., Thiel, L. A computer search for finite projective planes of order 9. Discrete Math. **92** (1991), 187-195.

[57] Lam, C. W. H., Thiel, L., Swiercz, S. The nonexistence of finite projective planes of order 10. Canad. J. Math. **41** (1989), 1117-1123.

[58] Lam, C. W. H., Thiel, L., Swiercz, S., McKay, J. The nonexistence of ovals in a projective plane of order 10. Discrete Math. **45** (1983), 319-321.

[59] L*ü*neburg, H. Characterizations of the generalized Hughes planes, Canada. J. Math. **28** (1976), 376–402.

[60] Lunelli, L., Sce, M. k-archi completi nei piani proiettivi desarguesiani di rango 8 e 16. Centro di Calcoli Numerici, Politecnico di Milano, Milan 1958, 15 pp.

[61] Mathon, Rudolf The partial geometries pg(5,7,3). Proceedings of the Tenth Manitoba Conference on Numerical Mathematics and Computing, Vol. II (Winnipeg, Man., 1980). Congr. Numer. **31** (1981), 129-139.

[62] Mitchell,U.G., Geometry and collineation groups of the finite projective plane $\mathrm{PG}(2, 2^2)$, Ph. D. thesis, Princeton, 1910.

[63] Nizette, Noël Determination des ovales du plan de translation non arguesien et du plan de Hughes d'ordre neuf. Collection of articles honoring P. Burniat, Th. Lepage and P. Libois. Bull. Soc. Math. Belg. **23** (1971), 436-446.

[64] O'Keefe, Christine M., Penttila, Tim. Hyperovals in PG(2,16). European J. Combin. **12** (1991), 51-59.

[65] Payne, Stanley E. A new infinite family of generalized quadrangles. Proceedings of the sixteenth Southeastern international conference on combinatorics, graph theory and computing (Boca Raton, Fla., 1985). Congr. Numer. **49** (1985), 115-128.

[66] Penttila, Tim Configurations of ovals. Combinatorics, 2002 (Maratea). J. Geom. **76** (2003), 233-255.

[67] Penttila, Tim, Pinneri, Ivano Irregular hyperovals in PG(2,64). J. Geom. **51** (1994), 89-100.

[68] Penttila, Tim, Royle, Gordon F. Classification of hyperovals in PG(2,32). J. Geom. **50** (1994), 151-158.

[69] Penttila, Tim, Royle, Gordon F. On hyperovals in small projective planes. J. Geom. **54** (1995), 91-104.

[70] Penttila, Tim, Royle, Gordon F., Simpson, Michael K. Hyperovals in the known projective planes of order 16. J. Combin. Des. **4** (1996), 59-65.

[71] Prince, Alan R. Oval configurations of involutions in symmetric groups. Combinatorics (Rome and Montesilvano, 1994). Discrete Math. **174** (1997), 277-282.

[72] Polster, Burkard Abstract hyperovals and Hadamard designs. Australas. J. Combin. **16** (1997), 29-33.

[73] Qvist, B. Some remarks concerning curves of the second degree in a finite plane. Ann. Acad. Sci. Fennicae. Ser. A. I. Math.-Phys. 1952, (1952). no. **134**, 27 pp.

[74] Segre, Beniamino Ovals in a finite projective plane. Canad. J. Math. **7** (1955), 414-416.

[75] Segre, Beniamino Sui k-archi nei piani finiti di caratteristica due. Rev. Math. Pures Appl. **2** (1957), 289-300.

[76] Segre, B., Bartocci, U. Ovali ed altre curve nei piani di Galois di caratteristica due. Acta Arith. **18** (1971), 423-449.

[77] Shrikhande, S. S. On a characterization of the triangular association scheme. Ann. Math. Statist. **30** (1959), 39-47.

[78] Sonnino, Angelo Transitive hyperovals in finite projective planes. Australas. J. Combin. **33** (2005) 335-347.

[79] Suetake, Chihiro The nonexistence of projective planes of order 12 with a collineation group of order 16.

[80] J.A. Thas, On 4-gonal configurations. Geom. Dedicata **2**(1973) 317 - 326. J. Combin. Theory Ser. A **107** (2004), 21-48.

[81] Thompson, J. G. Fixed point free involutions and finite projective planes, 321-337 in (M. J. Collins, ed.) Finite Simple Groups II, Academic Press, 1980.

[82] Thompson, John G. Ovals in a projective plane of order 10. Combinatorics (Swansea, 1981), pp. 187190, London Math. Soc. Lecture Note Ser., 52, Cambridge Univ. Press, Cambridge-New York, 1981.

[83] Veblen, Oswald, Bussey, W. H. Finite projective geometries. Trans. Amer. Math. Soc. **7** (1906), 241-259.

[84] Wedderburn, J.H.M. A theorem on finite algebras. Transaction of the American Mathematical Society **6** (1905) 349-352.

[85] Whitney, Hassler Congruent Graphs and the Connectivity of Graphs. Amer. J. Math. **54** (1932), 150-168.