Flocks, Generalised Quadrangles and Hyperovals

Ivano Pinneri

This thesis is presented for the degree of
Doctor of Philosophy
of The University of Western Australia
Department of Mathematics
June 1996

Acknowledgments

Special thanks goes to Tim Penttila, my supervisor and one time drinking partner (and I have the medical certificates to prove it) and a pretty smart cookie to boot who has made "linking" my eternal quest of mathematics.

To my dearest friend Nick. Life on the PhD trail would have been pretty lonely and down right boring without you. May all your toast be crackin' and all your dwarves red.

A very special thanks to Gordon — he of the many questions and great programming flair. For being my defacto supervisor and much much more I thank you with a nice bottle of SB in my hand!

A big thanks to the secretaries for allowing me to disrupt their routine when I needed someone to talk to, keeping me sane while I wrote up and allowing me to have the room to myself after Nick went to Brisbane,[1] amongst other things!

Thanks to the Adelaide gang: Matt Brown and Cath Quinn for showing me that you can be human and still be in the PhD game; and especially Christine O'Keefe for her help and occasional confidence boosting.

Big thanks to Bill Cherowitzo, Franck De Clerck, Marialuisa de Resmini, Stan Payne and Jef Thas for making me feel like I'm actually doing something of importance and for just being nice!

Thanks go to my flatmate par excellence Cathy, the Message Moose and Kenneth. Oh! and Mum.

[1] The best place in the world, I hear.

Preface

In 1959 structures called generalised quadrangles were introduced by J. Tits [**132**] and much later Stan Payne [**92**] showed how certain generalised quadrangles of order (q^2, q) were related to a set of 2×2 matrices. P. Dembowski [**36**] popularised the term flocks in relation to a partition of an inversive plane, minus two points, into a set of disjoint circles. In turn the idea of partitioning quadrics of $PG(3, q)$ into disjoint conics occured. The concept of oval, or at least the study of these configurations in themselves, may have started with the paper [**8**] of Baer. The work expanded from the study of Bose [**16**] and a number of Finnish astronomers, most notably the work of Qvist [**114**]. Under the guide of Beniamino Segre and the numerous number of Italians who followed him, the area broadened in scope. Segre's theorem classifying ovals for q odd stimulated the area even further with most of the initial effort to proof a similar theorem for q even. Needless to say we are still working on that problem, (amongst others).

The relationship between generalised quadrangles and hyperovals originated (in the present form) in Stan Payne's paper [**93**] and the relationship between flocks of quadratic cones and generalised quadrangles by the work of Jef Thas [**127**], Bill Kantor [**67**] and Stan Payne [**93**]. Underlying these objects are the matrices forming a q–clan, a term invented by Payne. Together Thas, Kantor and Payne have made q–clans the central idea behind these structures to study.

This thesis deals more fully with the relationships between generalised quadrangles, flocks and hyperovals. The links have been investigated and added to, in particular with the introduction of the concept of a herd of ovals; concluding in the construction of the Subiaco family of ovals, flocks of quadratic cone, etc. for all q even.

The use of computers has been of extreme importance in this work. Most notably the construction of the first irregular hyperovals in $PG(2, 64)$ by Penttila and myself, and the introduction of the technique of "prime at a time". Special mention should go to Gordon Royle who pushed most of the computing techniques described here (and in the many papers co-authored by Royle) to present computing[2] power; and allowed me to extensively quote the results from these papers.

[2]It should be affordable computing power, both in time and money resources.

The thesis itself is in straightforward chapters. Unfortunately, due to the nature of this work a large amount of forward and backward referencing is made. It is virtually impossible to write this work without doing so.

Chapter I and II initially started as a Masters thesis, with a view of trying to write a definitive work on hyperovals in projective planes (Desarguesian and non-Desarguesian). I then transferred to a PhD and the original aim of the masters was discarded. But most of the original work on hyperovals has been included and an abridged version of the original notes on group theory as well. In these chapters most results are explained in detail, while the last two deal with the subject in a less thorough manner.

The main influences on this work have been: the paper [**93**] by Stan Payne, the book [**103**] by Jef Thas and Payne and the series of lectures Thas gave in 1992 at the University of WA. Also in need of special mention is Payne's work on the Subiaco constructions, most notably his feedback with proofs and counterexamples to Penttila's and my conjectures on the hyperovals in $PG(2,q)$, $q = 4^e$, e odd. Payne's Subiaco Notebook [**90**] were a source of great help in understanding the creature Bill Cherowitzo, Penttila, Royle and myself brought onto the world.

(The reader should be aware that Section 11 on page 159 gives a historical perspective on the ideas, and influences, of the Subiaco constructions.)

When I started this area Dembowski [**36**] and the first two volumes of projective geometries by Hirschfeld [**55**][**56**] were about the only decent books to find on projective geometry. Today the amount of material on the area has grown substantially. Of particular importance is the text called "The Handbook" [**24**]. The chapters by Thas (Chapter 8 and Chapter 9) and F. De Clerck and H. van Maldeghem (Chapter 10) in the Handbook are a main reference for this work.

The reader should be warned that for Chapters I, II and IV, groups are acting on the left, but in Chapter III they are acting on the right! The reason for this change in handiness is given on page 94.

Nearly all of the work in this thesis is collaborative. In particular, special mention must go to Tim Penttila, my supervisor. ALL results have his influence and most of them contain his original ideas. I have given credit to original sources for theorems that have not been published elsewhere.

In summary, this work investigates the connection between hyperovals, ovals, flocks of quadratic cones and generalised quadrangles and their subquadrangles.

Summary

This thesis is divided into five chapters:

Chapter 1: Introduction
Definitions of projective plane and spaces, generalised quadrangles, duality and other relevant material of an introductory nature are included (and in fact can be skipped for the more able reader). A small collection of group theoretical results are given and the important "Samosa Lemma" is proved.

Chapter 2: Hyperovals in Desarguesian planes
This chapter is an attempt at a comprehensive look at hyperovals in Desarguesian planes. Firstly, many results are stated for ovals and collineation groups of ovals and hyperovals in arbitrary projective planes. Results on when hyperovals can be stabilised by elations and generalised homologies are given. Secondly, a list and some properties of the known hyperovals are given. From then on most of the chapter is devoted to constructing the first two irregular hyperovals in $PG(2,64)$. The rest of the chapter is devoted to the very recent construction of hyperovals in other Desarguesian projective planes. The last section deals with related areas of hyperovals.

Chapter 3: Generalised Quadrangles
We first look at the parameters of a generalised quadrangle, classical GQs, regularity and other properties of GQs. Ovoids, spreads, subquadrangles and the concept of rosettes is introduced. Four-gonal families and q-clans are introduced with some pointers to the new ideas of tensor q-clan geometries. A specific look is given at rosettes and subquadrangles of the GQ of order (q,q^2) with $T_2(\mathcal{O})$, $\mathcal{O}$ a pointed conic of $PG(2,8)$, as a subquadrangle. The concept of herd is introduced and q–clan geometries and elation generalised quadrangles are described. The groups of the Subiaco GQs are investigated and the proof that there are two inequivalent hyperovals for $q=4^e$, $e>1$, odd is given.

Chapter 4: Flocks and Chapter 5: Open questions
Flocks of quadrics are discussed, with the rest of the introductory sections being devoted to flocks of cones, especially quadratic cones and a brief mention of translation oval cones. Most of the section is taken up with proofs of the Subiaco herds. A brief historical view of the Subiaco constructions forms the last part of the thesis with some open questions about hyperovals, flocks, generalised quadrangles and their links.

Contents

CHAPTER I

Introduction

1. Projective and Affine spaces

Throughout this work we will be dealing with incidence structures and some of the configurations within them. An **incidence structure**, $\mathscr{I}$, is a triple of objects, $(\mathscr{P}, \mathscr{B}, \mathrm{I})$, where $\mathscr{P}$ is a set of **points**, $\mathscr{B}$ is a set of **blocks**, with $\mathscr{P} \cap \mathscr{B} = \emptyset$ and $\mathscr{P}$, $\mathscr{B}$ are non-empty, and I is the relation $\mathrm{I} \subseteq \mathscr{P} \times \mathscr{B}$ called the **incidence relation**. We define the **dual** of an incidence structure $\mathscr{I} = (\mathscr{P}, \mathscr{B}, \mathrm{I})$, denoted $\hat{\mathscr{I}}$, with $\hat{\mathscr{I}} = (\mathscr{B}, \mathscr{P}, \hat{I})$ where $\hat{I} = \{(B, P) \mid (P, B) \in \mathrm{I}\}$.

We define a **projective plane** as an incidence structure $\mathscr{I} = (\mathscr{P}, \mathscr{L}, \mathrm{I})$, where $\mathscr{L}$ is a set of **lines**, such that $\mathscr{I}$ satisfies these axioms:

PP1: Any two distinct points are incident with a unique line.
PP2: Any two distinct lines are incident with a unique point.
PP3: There exists at least four points, no three collinear.

THEOREM 1 ([**46**]). *If $\mathscr{I}$ is a projective plane then so is $\hat{\mathscr{I}}$.*

A **finite projective plane** is a projective plane with $\mathscr{P}$ and $\mathscr{L}$ being finite.

THEOREM 2 ([**46**]). *Let $q \geq 2$ be an integer. In a projective plane, π, any one of the following implies the rest.*

(i) *One line contains exactly $q + 1$ points.*
(ii) *One point is on exactly $q + 1$ lines.*
(iii) *Every line contains exactly $q + 1$ points.*
(iv) *Every point is on exactly $q + 1$ lines.*
(v) *There are $q^2 + q + 1$ points in π.*
(vi) *There are $q^2 + q + 1$ lines in π.*

If any of the conditions of Theorem 2 are satisfied then the projective plane, π, has **order** q.

Theorem 3 ([**46**]). *A finite projective plane has order q, for some q.*

Similar treatment can be given to incidence structures called **affine planes**. This is an incidence structure $\mathscr{I} = (\mathscr{P}, \mathscr{B}, \mathrm{I})$ such that;

A1: Any two distinct points are incident with a unique line.
A2: Given a point P and a non-incident line l then there exists a unique line m incident with P but disjoint from l.
A3: There exists three points not all incident with the same line.

Two lines, l and m are **parallel** if they are equal or disjoint. Parallelism is an equivalence relation.

A **finite affine plane** is one where both $\mathscr{P}$ and $\mathscr{L}$ are finite sets.

It is well known [**36**] that one can get a projective plane from an affine plane and an affine plane from a projective plane.

2. Duality

We take a closer look at duality. Recall that the dual of an incidence structure $\mathscr{I} = (\mathscr{P}, \mathscr{B}, \mathrm{I})$ is $\hat{\mathscr{I}} = (\mathscr{B}, \mathscr{P}, \hat{I})$ where $\hat{I} = \{(B, P) \mid (P, B) \in \mathrm{I}\}$.

A finite projective plane, π, can be defined as a bipartite graph of girth 6 and diameter 3 (and a thickness condition), where one set of vertices are labelled points and the other set of vertices are labelled lines.

Given a theorem about finite projective planes if we swap the words "points" and "lines" (and reword incidence accordingly), then this theorem is now concerned with a bipartite graph where the labels of "points" and "lines" have been interchanged. Hence it is still a theorem about projective planes (with the same order).

We will use this fact throughout this work and say **dually**, to mean swap the words "lines" and "points" from a previous result to obtain the current result.

3. Projective Spaces and Collineation Groups

Let V be a finite dimensional vector space over a field $\mathbb{F}$. The **projective space**, $PG(V)$, associated with V is the space whose elements are proper subspaces of V and incidence is symmetrised inclusion. We have **points** being the one dimensional subspaces of V, **lines** being the two dimensional subspaces of V, **planes** being the three dimensional subspaces of V,..., and **hyperplanes** being the $\dim_{\mathbb{F}} V - 1$ subspaces of V. The **projective dimension** of a subspace W of V is $\dim_{\mathbb{F}} W - 1$. The **projective dimension** of $PG(V)$ is $\dim_{\mathbb{F}} V - 1$. Elements of $PG(V)$ are called

subspaces of the projective space. An isomorphism between projective spaces is a bijection preserving projective dimension and symmetrised inclusion.

THEOREM 4. *Let V, W be vector spaces. If $V \cong W$ then $PG(V) \cong PG(W)$ as projective spaces.*

We write $PG(d, \mathbb{F})$ for $PG(\mathbb{F}^{d+1})$ and $PG(d,q)$ for $PG(GF(q)^{d+1})$.

The points of $PG(d,q)$ are one dimensional subspaces $\langle(a_1, \dots, a_{d+1})\rangle$ of $GF(q)^{d+1}$. We use **homogeneous coordinates** for points, $\langle(a_1, \dots, a_{d+1})\rangle$, abbreviated to

$$(a_1, \dots, a_{d+1}) \text{ where } (a_1, \dots, a_{d+1}) \neq \mathbf{0}.$$

Hence

$$(\lambda a_1, \dots, \lambda a_{d+1}) = (a_1, \dots, a_{d+1}) \text{ for } \lambda \in GF(q),\ \lambda \neq 0.$$

The set of all invertible linear maps $V \to V$ is denoted $GL(V)$. The set of all semilinear maps $V \to V$ is denoted by $\Gamma L(V)$. We see that $GL(V) \triangleleft \Gamma L(V)$ and

$$\operatorname{Aut} \mathbb{F} \cong \frac{\Gamma L(V)}{GL(V)}$$

where $\mathbb{F}$ is the field V is defined over. Let $Z = \{\lambda I \mid \lambda \in \mathbb{F} \setminus \{0\}\}$ then Z is normal in $\Gamma L(V)$ and $GL(V)$. An **automorphism** of $PG(V)$ is an isomorphism $PG(V) \to PG(V)$. We define $\operatorname{Aut} PG(V)$ to be the set of all automorphisms, and is a group under composition.

By Theorem 4, p. 3, we have any $A \in GL(d+1,q)$ gives an automorphism

$$S \mapsto AS \text{ for all subspaces } S \text{ of } PG(d,q),$$

of $PG(d,q)$. Automorphisms of this form are called **homographies**. They form a group, $PGL(d+1,q)$,

$$PGL(d+1,q) \cong \frac{GL(d+1,q)}{Z}.$$

For an automorphism, α, of $GF(q)$, α acts on $GF(q)^{d+1}$ by

$$\alpha(a_1, \dots, a_{d+1}) = (\alpha(a_1), \dots, \alpha(a_{d+1})),$$

so α acts on subspaces S of $GF(q)^{d+1}$ by

$$\alpha(S) = \{\alpha(\boldsymbol{v}) \mid \boldsymbol{v} \in S\}$$

and

$$S \mapsto \alpha(S) \text{ for all subspaces } S \text{ of } PG(d,q)$$

is an automorphism of $PG(d,q)$, an **automorphic collineation**. The automorphic collineations and homographies form a group

$$S \mapsto A\alpha(S) \text{ for all subspaces } S \text{ of } PG(d,q)$$

called $P\Gamma L(d+1,q)$, the **collineations** of $PG(d,q)$,

$$P\Gamma L(d+1,q) \cong \frac{\Gamma L(d+1,q)}{Z}.$$

Let $SL(d,q)$ be the subgroup of elements of $GL(d,q)$ with determinant 1. Then we can define a subgroup, $PSL(d,q)$, of $PGL(d,q)$ as:

$$PSL(d,q) \cong \frac{SL(d,q)Z}{Z} \cong \frac{SL(d,q)}{SL(d,q)\cap Z}.$$

For reference we list the orders of the above groups:

$$\begin{aligned}
|GL(d,q)| &= q^{d(d-1)/2}\prod_{i=1}^{d}(q^i-1)\\
|PGL(d,q)| &= q^{d(d-1)/2}\prod_{i=2}^{d}(q^i-1) = \frac{|GL(d,q)|}{q-1}\\
|PSL(d,q)| &= \frac{q^{d(d-1)/2}\prod_{i=2}^{d}(q^i-1)}{(d,q-1)} = \frac{|PGL(d,q)|}{(d,q-1)}\\
|P\Gamma L(d,q)| &= |PGL(d,q)||\operatorname{Aut} GF(q)|
\end{aligned}$$

THEOREM 5 (Fundamental Theorem of Projective Geometry). *For $d > 1$ we have*

$$\operatorname{Aut} PG(d,q) = P\Gamma L(d+1,q).$$

An example of a projective space is the Desarguesian projective plane $PG(2,q)$. This incidence structure satisfies axioms **PP1**, **PP2**, and **PP3** and so **is** a projective plane. These projective planes satisfy the Theorem of Desargues (see [**59**]). We label points homogeneously as for projective spaces, and we label lines in $PG(2,q)$ homogeneously, so that the line

$$ax + by + cz = 0 \text{ for points } (x,y,z)$$

is denoted $[a,b,c]$ such that for any $\lambda \in GF(q)^*$ we have $[a,b,c] = [\lambda a, \lambda b, \lambda c]$.

We can construct an affine plane on a two dimensional vector space. Points are vectors of the space, lines are cosets of one-dimensional subspaces and incidence is inclusion. When the vector space is $GF(q)^2$ we call this affine space $AG(2,q)$.

4. Group theory results

LEMMA 6. *Let f be a polynomial defined over $GF(q)$. If $x-a \mid f(x)$ then $x-a \mid f(a)$.*

PROOF. By the remainder theorem we have

$$f(x) = g(x)(x-a) + f(a)$$

hence if $x-a$ divides $f(x)$ then it must divide $f(a)$. □

THEOREM 7 ([**136**]). *Let H and K be subgroups of G with $|G:H| = m$ and $|G:K| = n$ and $(m,n) = 1$. Then $|K:H\cap K| = m$ and $|H:H\cap K| = n$.*

COROLLARY 8. *Let G act transitively on X, let $H = G_x$ for some $x \in X$ and $|X| = n$. If $(|G:H|, n) = 1$ then H is transitive on X.*

Let G be a group and $H \leq G$. The normaliser of H in G is denoted $N_G(H)$, and the centraliser of H in G is denoted $C_G(H)$.

THEOREM 9. *Let G act on X and $H \leq G$. The normaliser of H in G permutes orbits of H on a set X of size m for all $m \in \mathbb{Z}^+$. Particularly, $N_G(H)$ permutes fixed points.*

THEOREM 10. *Let $H \lhd G$. Then*

(i) $C_G(H) \lhd N_G(H)$,
(ii) $N_G(H) \leq N_G(C_G(H)))$, *and*
(iii) $C_G(H) \leq N_G(C_G(H)))$.

THEOREM 11. *The number of conjugates of S under H is the index in H of the normaliser of S in H.*

THEOREM 12. *Let G be a group acting transitively on the set X. Then G is primitive on X if and only if G_x is a maximal subgroup of G, for all $x \in X$.*

THEOREM 13. *G acts on X and let $\alpha \in X$. If N is regular on X then $G = NG_\alpha$, and we say G_α is a **supplement** for N in G.*

If N was normal, then $G = N \rtimes G_\alpha$ and G_α is a **complement** for N in G.

The number of subsets of G conjugate to S is $|G:N_G(S)|$.

The number of elements in the conjugacy class that contains a is $|G:C_G(a)|$.

THEOREM 14 (Cauchy's Theorem). *Let G be a finite group and p be a prime divisor of $|G|$. Then G contains an element of order p.*

A subgroup H of a group G is called a **p-subgroup** of G if H is a p-group. Let G be a finite group of order $p^r m$ where $r \geq 1$ and p does not divide m. A p-subgroup H of G is called a **Sylow p-subgroup** of G if $|H| = p^r$, that is, if $|G:H|$ is coprime to p.

THEOREM 15 (Sylow's Theorem). *Let G be a finite group of order $p^r m$ where $r \geq 1$ and p does not divide m. Then*

(i) *Sylow p-subgroups of G exist;*
(ii) *any two Sylow p-subgroups of G are conjugate in G;*
(iii) *if H is any p-subgroup of G then H is contained in some Sylow p-subgroup of G;*
(iv) *the number of Sylow p-subgroups of G divides m and is congruent to 1 modulo p.*

The set of all Sylow p-subgroups of G is denoted by $\mathrm{Syl}_p(G)$.

COROLLARY 16. *Let $P \in \mathrm{Syl}_p(G)$. Then $P \lhd G$ if and only if P is the unique Sylow p-subgroup of G.*

COROLLARY 17 (Frattini Argument). *Let $H \lhd G$ and $P \in \mathrm{Syl}_p(H)$. Then*

$$G = HN_G(P).$$

THEOREM 18. *Let p be a prime and $p \,\big|\, |G|$. Let $P \in \mathrm{Syl}_p(G)$. If P is cyclic then there exists a unique conjugacy class of subgroups of G of order p^i for all i such that $p^i \,\big|\, |G|$.*

The below theorem is one of the most widely used in this work. Unfortunately, most references are obscure, either they are in German [**61**], or hard to find [**64**]. The proof of the theorem requires some knowledge of representation theory (see [**33**]) and primitive divisors. The so called **Samosa Lemma** is used to calculate $N_{\Gamma L(d,q)}(P)$ for any p-subgroup of $GL(d,q)$ where p is a q-primitive prime divisor of $q^e - 1$ for $e > d/2$. We concentrate on the case $|P| = p$, the others follow as a corollary.

A **q-primitive prime divisor**, or **q-ppd**, of $q^d - 1$ is a prime divisor of $q^d - 1$ which does not divide $q^e - 1$ for $1 \le e < d$. If p is a q-ppd of $q^d - 1$ then $(p, q) = 1$ so $q \in U(\mathbb{Z}_p)$ has an order. Let $|q|_p$ be the order of q as an element of $U(\mathbb{Z}_p)$. Then $|q|_p = d$ (obviously), hence $p \,\big|\, q^i - 1$ if and only if $d \,\big|\, i$.

A **q-primitive divisor**, or **q-pd** of $q^d - 1$ is a divisor which is coprime to $q^e - 1$ for $1 \le e < d$ (so q-ppd if and only if q-pd and prime). Let $\Phi^*_d(q)$ be the largest q-primitive divisor of $q^d - 1$, the **q-primitive part of** $q^d - 1$. Let

$$\Phi_n(x) = \frac{x^n - 1}{\left(x^n - 1, \prod_{i=1}^{n-1}(x^i - 1)\right)}$$

be the **nth cyclotomic polynomial** (see [**50**][**51**]). Then we have $\Phi^*_d(q) \,\big|\, \Phi_d(q)$, so if l is a prime and $l \,\big|\, \Phi_d(q)$ but $l \not\big|\, \Phi^*_d(q)$, then $l \,\big|\, d$.

THEOREM 19 ([**138**]). *We have*

$$\Phi^*_d(q) = \frac{1}{f^\alpha}\Phi_d(q),$$

where $f = (d, \Phi_d(q))$ and $f^\alpha \,\big|\, \Phi_d(q)$ but $f^{\alpha+1} \not\big|\, \Phi_d(q)$. In particular, $\Phi^*_d(q) \neq 1$ for $d \ge 2$ unless (d, q) equals $(6, 2)$ or $(2, 2^a - 1)$ for some a.

Suppose a prime $p \,\big|\, |GL(d,q)|$ with $p \not\big|\, q$ then there exists an $e \le d$ such that $p \,\big|\, q^e - 1$. If we choose e to be minimal such that $p \,\big|\, q^e - 1$ implies that p is a q-ppd of $q^e - 1$. So primes not the characteristic of q can be classified by e.

Suppose $(d/2) < e$. Then $|q|_p = e$ with $p \,\big|\, q^i - 1$ if and only if $e \,\big|\, i$, in fact, since $(d/2) < e$, we have that $p \,\big|\, q^i - 1$ for some i, $1 \le i \le d$, if and only if $e = i$. Hence

$$\left(p, \frac{|GL(d,q)|}{q^e - 1}\right) = 1, \text{ if } |q|_p = e > \frac{d}{2}. \tag{1}$$

Let $V = GF(q)^d$. Let U be a subspace of dimension e, with W a complement of U in V such that $V = U \oplus W$. So $U \cong GF(q)^e$ and identify U with $GF(q^e)$. Multiplication in $GF(q^e)$ is $GF(q)$-linear, thus there exists a $C_{q^e-1} \leq GL(U)$ via Singer's Theorem (page 27). We can extend this linearity to the whole space (namely $C_{q^e-1} \times I_W$) so there exists a $C_{q^e-1} \leq GL(V)$.

Let $P \in \mathrm{Syl}_p(C_{q^e-1})$. By Eq. (1) we have $P \in \mathrm{Syl}_p(GL(d,q))$. All p-subgroups of $GL(d,q)$ are cyclic; any two of the same order are conjugate: Since if P_1, P_2 are p-subgroups of $GL(d,q)$ of equal order implies that there exists P_1^* and P_2^* from $\mathrm{Syl}_p(GL(d,q))$ with $P \leq P_1^*$ and $P_2 \leq P_2^*$ by Sylow's Theorem which, also by Sylow's Theorem, implies there exists a $g \in GL(d,q)$ such that $gP_1^*g^{-1} = P_2^*$ so $gP_1g^{-1} \leq P_2^*$ of order $|P_2|$. So P_2^* is cyclic implies that there is a unique subgroup of each order dividing $|P_2^*|$. Hence $gP_1g^{-1} = P_2$.

A **representation** of a group G is a homomorphism $G \to GL(V)$ for a vector space V. Two representations $T_1\colon G \to GL(V)$, $T_2\colon G \to GL(W)$ are **equivalent** if there exists an invertible linear map $\varphi\colon V \to W$ such that

$$\varphi T_1(g)\varphi^{-1} = T_2(g) \text{ for all } g \in G$$

that is,

$$\varphi T_1(g) = T_2(g)\varphi \quad \text{for all } g \in G.$$

An **intertwiner** (or G**-endomorphism**) between T_1 and T_2 is a linear map $\varphi\colon V \to W$ such that

$$\varphi T_1(g) = T_2(g)\varphi \quad \text{for all } g \in G.$$

(We note that the zero map is always an intertwiner.)

A subspace is G**-invariant** if for all $g \in G$ we have $T(g)W = W$.

A representation $T\colon G \to GL(V)$ is **reducible** if there is a non-zero, proper subspace W of V such that W is G-invariant. Otherwise we say T is irreducible.

Let $T\colon G \to GL(V)$ be a representation, then

$$\mathrm{End}_G(V) = \{\text{intertwiners between } T \text{ and } T\}$$

is a division ring under addition and composition by Schur's Lemma [**72**]. Now

$$\begin{aligned} U(\mathrm{End}_G(V)) &= \{\varphi \in GL(V) \mid \varphi T(g) = T(g)\varphi \text{ for all } g \in G\} \\ &= C_{GL(V)}(T(G)) \end{aligned}$$

Theorem 20 (Samosa Lemma). *Let q and d be integers strictly greater than 1. Let p be a q-ppd of $q^e - 1$ with $e > (d/2)$. Let P be a p-subgroup of $GL(d,q)$. Then*

$$N_{GL(d,q)}(P) \cong (GF(q^e)^* \times GL(d-e,q)) \rtimes \mathrm{Gal}\left(\frac{GF(q^e)}{GF(q)}\right).$$

$$N_{\Gamma L(d,q)}(P) \cong (GF(q^e)^* \times GL(d-e,q)) \rtimes \mathrm{Aut}\, GF(q^e).$$

$$C_{GL(d,q)}(P) \cong GF(q^e)^* \times GL(d-e,q).$$

Proof. We have P acting on $V = U \oplus W$ with $\dim U = e$ as $gw = w$ for all $g \in P$ and for all $w \in W$. Now $GF(q^e)^*$ acts regularly on $U - \{0\}$ implies that P acts semiregularly on $U - \{0\}$ which implies that all orbits of P on $U - \{0\}$ have length $|P|$. (Noting that p divides $q^i - 1$ if and only if e divides i for $i > 0$.) Let $\{0\} \neq U' \leq U$ be P-invariant. Then $|U'| = 1 + pn$ for some n. Let $e' = \dim U' \neq 0$. Then $q^{e'} - 1 = pn$ which implies p divides $q^{e'} - 1$ which implies e divides e'. But $e' \leq e$ so $e' = e$. Hence P is irreducible on U (strictly speaking $T(P)$ is).

Now $N_{\Gamma L(V)}(P)$ permutes fixed vectors of P, so $N_{\Gamma L(V)}(P)$ fixes W. Also $N_{\Gamma L(V)}(P)$ permutes the fixed subspaces of P and preserves irreducibility, so $N_{\Gamma L(V)}(P)$ fixes U (there are no other irreducible subspaces of dimensions not equal to one).

We now look at the action of $N_{\Gamma L(V)}(P)$ on U.

What is the kernel of this action? The kernel acts trivially on U so implying that its companion automorphism is 1, hence kernel is a subgroup of $GL(V)$. Fix W and we have the kernel a subgroup of $I_U \times GL(W)$. Now

$$I_U \times GL(W) \leq C_{GL(V)}(P) \cap \text{kernel}.$$

Hence the kernel of the action is equal to $I_U \times GL(W)$.

Now we look at the action induced on U. Without loss of generality let $V = U$ and $d = e$. By Schur's Lemma [**72**], $\mathrm{End}_P(U)$ is a division ring and so by Wedderburn's Theorem [**72**], $\mathrm{End}_P(U)$ is a field. Hence $\mathrm{End}_P(U) \cong GF(q^e)$. (Since $\mathrm{End}_P(U)^*$ is cyclic and so abelian, it acts faithfully on V implying that it acts semiregularly on $U - \{0\}$. So we have $|\mathrm{End}_P(U)^*|$ dividing $|U - \{0\}| = q^e - 1$. Now P is cyclic and so abelian, making P a subgroup of $C_{GL(V)}(P)$, giving that p divides $|\mathrm{End}_P(U)^*|$. But p is primitive, so given $\{\lambda I \mid \lambda \in GF(q)\} \leq \mathrm{End}_P(U)$ we have $\mathrm{End}_P(U) \cong GF(q^{e'})$ for some e' with $e' \geq 1$. Hence p divides $q^{e'} - 1$ so e divides e' so $e = e'$.)

This gives $C_{GL(U)}(P) = GF(q^e)^* \cong C_{q^e-1}$. Now $C_{GL(U)}(P)$ is normal in $N_{GL(U)}(P)$ and

$$\frac{N_{GL(U)}(C_{q^e-1})}{C_{GL(U)}(C_{q^e-1})} \leq \mathrm{Aut}\, C_{q^e-1} \cong U(\mathbb{Z}_{q^e-1}).$$

Let $n \in N_{GL(U)}(C_{GL(U)}(P))$, $n1 = 1$ under the identification of U with $GF(q^e)$ so $n\colon \lambda \mapsto \lambda^j$ for some j. Now n is additive so $j = q_0^k$ for some k where q_0 is the characteristic of $GF(q)$. Also since n preserves $GF(q)$-scalars we have that $j = q^l$ for some l.

Hence

$$N_{GL(U)}(P) \leq GF(q^e)^* \rtimes \mathrm{Gal}\left(\frac{GF(q^e)}{GF(q)}\right),$$

and

$$N_{\Gamma L(U)}(P) \leq GF(q^e)^* \rtimes \mathrm{Aut}\, GF(q^e).$$

The theorem follows. ☐

5. The Exponential Convention

We shall need to compute within the field $GF(q)$, q even, with functions $f\colon GF(q) \to GF(q)$. It will prove to be very convenient to use **exponential notation** for functions f of the form $f\colon x \mapsto x^n$, for some integer n, that is, for **monomial** functions.

The natural map from polynomials to polynomial functions is a ring homomorphism from $GF(q)[x]$ onto the ring of all functions $GF(q) \to GF(q)$ (with pointwise operations) with kernel the principal ideal generated by $x^q - x$. It follows that, for integers m and n the polynomials x^m and x^n map to the same function if and only if $m = n = 0$ or $m \equiv n \pmod{q-1}$. For this reason we set $\mathbb{Z}_{q-1} = \{1, 2, \ldots, q-1\}$.

For $n \in \mathbb{Z}_{q-1}$ we denote the function $x \mapsto x^n$ from $GF(q)$ to $GF(q)$ by n. With this convention for m, $n \in \mathbb{Z}_{q-1}$, $m + n$ is the pointwise product of the functions $x \mapsto x^m$ and $x \mapsto x^n$, while mn is their composition.

If u is a unit of $\mathbb{Z}_{q-1}$ we denote its inverse in $\mathbb{Z}_{q-1}$ by $1/u$ (since $\mathbb{Z}_{q-1}$ is commutative). Now u is a unit in $\mathbb{Z}_{q-1}$ if and only if the function $x \mapsto x^u$ is invertible and in this case $1/u$ denotes the inverse function. Also the function $q/2$ is equal to the function $1/2$, and $q-2$ is equal to -1.

6. The Trace Equation

Let $q = 2^e$. The map $\mathrm{trace}_{GF(q)\to GF(q_0)}\colon GF(q) \to GF(q_0)$ defined to be

$$\operatorname*{trace}_{GF(q)\to GF(q_0)}(x) = \sum_{\alpha \in \mathrm{Gal}\left(\frac{GF(q)}{GF(q_0)}\right)} x^\alpha = \sum_{i=0}^{e'-1} x^{q_0^i},$$

where $q_0 = 2^{e'}$, $x \in GF(q)$, is the **trace map from $GF(q)$ to $GF(q_0)$**.

Let $GF(q) = GF(q_0^h)$ with h odd. Then

$$\operatorname*{trace}_{GF(q_0)\to GF(2)}(x) = \operatorname*{trace}_{GF(q)\to GF(2)}(x)$$

for all $x \in GF(q_0)$. If h was even then we have $\mathrm{trace}_{GF(q)\to GF(2)}(x) = 0$ for all $x \in GF(q_0)$.

We define the map $\mathrm{trace} = \mathrm{trace}_{GF(q)\to GF(2)}\colon GF(q) \to GF(2)$ to be

$$\mathrm{trace}(x) = \sum_{i=0}^{e-1} x^{2^i}$$

for $x \in GF(q)$, and simply call this the **trace map** (sometimes referred to as the **absolute trace** map).

Let K be the kernel of the trace map.

Theorem 21 ([**108**]). (i) *The trace map is additive.*

(ii) *The trace map is invariant under automorphisms of* $GF(q)$.

(iii) *We have* K *being a subgroup of* $(GF(q), +)$ *of index* 2 *and* trace *has image* $GF(2)$.

(iv) *We have* K *being automorphism invariant.*

(v) *There are* $q-1$ *subgroups of* $(GF(q), +)$ *of index* 2, *namely,* aK *for* $a \in GF(q)^*$ *and if* $aK = bK$ *then* $a = b$.

(vi) *The only subgroup of* $(GF(q), +)$ *of index* 2 *which is automorphism invariant is* K.

(vii) *For* $\alpha \in \operatorname{Aut} GF(q)$, *the set*

$$\{x^\alpha + x \mid x \in GF(q)\} \subseteq K$$

with equality if and only if α *generates* $\operatorname{Aut} GF(q)$.

(viii) *For* $a \neq 0$ *we have* $ax^2 + bx + c$ *being irreducible over* $GF(q)$ *if and only if*

$$\operatorname{trace}\left(\frac{ac}{b^2}\right) = 1 \text{ and } b \neq 0.$$

7. Spreads and Reguli

Let Π be a projective space of odd dimension $2t-1$. Let $\mathcal{S}$ be a collection of $(t-1)$-dimensional projective subspaces of Π. Then $\mathcal{S}$ is a **spread** of Π if each point of Π is contained in one and only one member of $\mathcal{S}$.

If $\Pi = PG(2t-1, q)$, then a spread of Π is a collection of $q^t - 1$ distinct $(t-1)$-dimensional subspaces having no points in common.

Let R be a set of $q+1$ pairwise skew lines of $PG(3, q)$. A line l is a **transversal** of R if it meets all elements of R. A transversal meets every element of R in a unique point, and conversely.

Let Π be a projective space of dimension greater or equal to three. A **regulus** is a set of transversals to three pairwise skew lines.

Given a regulus R, and l_1, l_2, $l_3 \in R$, distinct lines, the transversals to l_1, l_2, l_3 are transversal to all the lines of R. This regulus is called the **opposite regulus** to R.

Hence any triple of pairwise skew lines lies on a unique regulus.

8. Bruck-Bose Construction

In this section we mention a way of constructing affine planes (and, hence, projective planes) from projective spaces.

Theorem 22 (Bruck-Bose Construction [20][2]). *Let $\mathcal{S}$ be a $t{-}1$-spread of $PG(2t-1,q)$. Embed $PG(2t-1,q)$ as a hyperplane, H, of $PG(2t,q)$. Let*

(i) *Let $\mathcal{P}$ equal the points of $PG(2t,q)$ not on H.*
(ii) *Let $\mathcal{L}$ be the subspaces of $PG(2t,q)$ of dimension t which meet H in an element of $\mathcal{S}$.*
(iii) *Let I be the natural incidence of $PG(2t,q)$.*

Then $\mathscr{I} = (\mathscr{P}, \mathscr{L}, \mathrm{I})$ is an affine plane of order q^t. Note $\mathscr{I}$ may be non-Desarguesian.

9. Generalised Quadrangles

We say two points, x and y, are **collinear** or **adjacent**, denoted $x \sim y$, if there exists a line they are both incident to. If no such line exists then we say x and y are **non-collinear** or **non-adjacent**, denoted $x \nsim y$. Two lines, L and M, are **concurrent** or **intersect**, denoted $L \sim M$, if there exists a point incident with both. If no such point exists then we say that the lines L and M are **non-concurrent** or **disjoint**, denoted by $L \nsim M$.

A **firm generalised quadrangle**, abbreviated to **firm GQ**, is an incidence structure (see page 1), $\mathscr{I} = (\mathscr{P}, \mathscr{B}, \mathrm{I})$, with the following axioms:

GQ1: Two points are incident with at most one line;

GQ2: If a point x is not incident with a line L, then there exists a unique point, y, and a unique line, M, such that x is incident with M which is incident with y which in turn is incident with L.

ptGQ: There exists no point that is collinear with all points.

Axiom **GQ2** is sometimes referred to as "there are no triangles" axiom.

From **GQ1**, **GQ2** and **ptGQ** we can get the dual axioms:

GQ1*: Two lines are concurrent with at most one point;

GQ2*: If a point x is not incident with a line L, then there exists a unique point, y, and a unique line, M, such that x is incident with M which is incident with y which in turn is incident with L. That is **GQ2**.

ptGQ*: There exists no line that is concurrent with all other lines.

Theorem 23. *We can determine the axioms* **GQ1***, **GQ2*** *and* **ptGQ*** *from the axioms* **GQ1**, **GQ2** *and* **ptGQ**.

Proof. As **GQ1*** and **GQ2*** are straightforward we will prove **ptGQ***.

Suppose that there exists a line L that is concurrent with all lines of the firm generalised quadrangle. Let y be a point of the firm generalised quadrangle not incident to L (this exists else we would contradict **ptGQ**). By **GQ2** there exists a line M and a point x such that $x \mathrm{\ I\ } L \mathrm{\ I\ } y \mathrm{\ I\ } M$. By **ptGQ** there is a point z that is not collinear with x and y. By **GQ2** there exists a line N such that $z \mathrm{\ I\ } N \mathrm{\ I\ } x \mathrm{\ I\ } M$. But as L is concurrent with all lines of the firm generalised quadrangle then y is collinear with two points on L contradicting **GQ2**. So **ptGQ*** is true. □

Hence the dual of a firm generalised quadrangle is a firm generalised quadrangle.

A firm generalised quadrangle has at least two points incident with every line and two lines incident with every point (from now on we will rephrase comments like the one above to "... at least two points incident with every line and dually," taking advantage of the fact that the dual of a firm GQ is a firm GQ). Suppose not: Then there is a line L with only one point on it, p say. By axiom **GQ2** every point not on L must be collinear with p (as this is the only point on L), and so p is collinear with all points, contradicting axiom **ptGQ**.

Two examples of firm generalised quadrangles are complete bipartite graphs and their duals, grids. A **grid** of type (s, s'), $s, s' > 0$, is a set of $s + s' + 2$ lines and $(s+1)(s'+1)$ points such that every point is on exactly two lines and that there are $s+1$ lines with $s'+1$ points on each line and $s'+1$ lines with $s+1$ points on each. The dual of a grid is a **complete bipartite graph** of type (t, t'), $t, t' > 0$, denoted $K_{t+1,t'+1}$, with every line having two points and a partitioning of points into two sets, one of size $t+1$ and one of $t'+1$; additionally, every point in the set of size $t+1$ is adjacent to every point of the set of size $t'+1$ and conversely.

A **generalised quadrangle** is a firm generalised quadrangle with two extra axioms:

thickGQ: There are at least three points on every line, and
thickGQ*: There are at least three lines on every point.

These are referred to as the **thickness** axioms. Thickness is self-dual(!), so again, we have that the dual of a generalised quadrangle is a generalised quadrangle. A firm generalised quadrangle need not be a generalised quadrangle.

THEOREM 24 (Thickness implies order [**13**]). *In a generalised quadrangle the number of points on a line is a constant and the number of lines on a point is a constant (not necessarily the same constant).*

PROOF.
(1) Let L and M be disjoint lines of the generalised quadrangle (existence via **ptGQ** axiom). For every point p on L there is a unique point, p', on M, and conversely. So there is a one-to-one correspondence of points between disjoint lines. Hence disjoint lines have the same cardinality.

(2) Suppose L and M meet at a point y (by axiom **GQ1** there are no more points of intersection). Let x be a point on neither L or M and not collinear with y. By **GQ2** there is one line on x meeting L and another line meeting M. By thickness there exists another line, N, which is disjoint from L and M (else we will have triangles). So we use part (1) to get that L has the same cardinality as N and similarly for M.

Dually every point has the same number of lines on it. □

We say that the constants of the above theorem are the **parameters** of the generalised quadrangle. A **finite generalised quadrangle** is a generalised quadrangle where the parameters are finite. We say a finite generalised quadrangle has **order** (s,t) where the number of points on a line is $s+1$ and the number of lines on a point is $t+1$ (note: one line having $s+1$ points implies all lines have $s+1$ points, and dually). If $s=t$ then we say the generalised quadrangle has order s. The dual of a generalised quadrangle of order (s,t) is a generalised quadrangle of order (t,s).

NOTE. Payne and Thas [**103**] define a generalised quadrangle as an incidence structure satisfying **GQ1**, **GQ2** with the existence of the parameters s and t (as above) for $s,t\geq 1$.

For a grid of type (s,s) we have a firm generalised quadrangle with a constant number of points on every line (equal to $s+1$) and a constant number of lines on every point (equal to two), hence this is a Payne and Thas generalised quadrangle of order $(s,1)$, but it is not a generalised quadrangle. For a complete bipartite graph of type (t,t) we have a firm generalised quadrangle with a constant number of lines on a point (equal to $t+1$) and a constant number of points on a line (equal to two). Again this is not a generalised quadrangle, but it is a Payne and Thas generalised quadrangle of order $(1,t)$.

THEOREM 25 (A poor man's classification of firm GQs). *A firm generalised quadrangle is either*

(i) *a grid, or*
(ii) *a complete bipartite graph, or*
(iii) *a generalised quadrangle.*

PROOF. Let L and M be disjoint lines of the generalised quadrangle. By **GQ2** there is a one-to-one correspondence between the points of L and M. Let $s+1$ be the number of points on disjoint lines. Let the line N meet L. This line can not meet any other line meeting L, else this will contradict **GQ2**. Let y be the point of intersection of L and N. Any other line meeting L, other than at point y, is disjoint from N, so there is a one-to-one correspondence between the points of N and the other line by **GQ2**. We let $s'+1$ be the number of points on N.

If we have thickness then $s=s'$ (as there is a line disjoint from L and N, and so by **GQ2**, we have that there is one-to-one correspondence with the lines L and N), so we have a generalised quadrangle.

If no such line exists, then all lines meet L or N. From a consequence of axiom **ptGQ** we have at least two lines on any point. So a point not on L or N must have one line meeting L and the other meeting N, (with **GQ2** forbidding both lines from the point meeting only L or N). Hence we have a grid.

Dually, we arrive at a constant number of lines through a point (and a generalised quadrangle) or we have a complete bipartite graph. □

COROLLARY 26. *A firm generalised quadrangle with only two points on any line is a complete bipartite graph, or if dually, then the firm generalised quadrangle is a grid.*

10. End Notes

NOTES ON SECTION 1, P. 1. Incidence structures that satisfy **PP1**, **A3** and every line has at least two points are called **linear spaces**. A large body of work has been written about such spaces, of particular interest is the work of F. Buekenhout (see [**12**] for an overview of finite linear spaces).

The results in this Section are well known.

NOTES ON SECTION 2, P. 2. The results in this Section are well known.

NOTES ON SECTION 3, P. 2. The definition of collineation on page 3 is equivalent to that on page 23 due to the Fundamental Theorem of Projective Geometry (Theorem 5, p. 4).

The results in this Section are well known.

NOTES ON SECTION 4, P. 4. Theorem 20, p. 7, is a specific case of the more general theorem that says for a given irreducible W we have

$$\mathrm{End}(W^n) = M_n(\mathrm{End}(W)).$$

The results in this Section are well known, though Theorem 20 is hard to find.

NOTES ON SECTION 5, P. 9. The results in this Section are well known.

NOTES ON SECTION 6, P. 9. The results in this Section are well known.

NOTES ON SECTION 7, P. 10. The results in this Section are well known.

NOTES ON SECTION 8, P. 10. The results in this Section are well known.

NOTES ON SECTION 9, P. 11. The results in this Section are well known. The author's treatment is different from the standard text [**103**] as the author prefers synthetic definitions without assuming order.

CHAPTER II

Hyperovals in Desarguesian Planes

1. Arcs in Arbitrary Projective Planes

Let $\mathcal{K}$ be a set of k points, a k**-set**, in a projective plane of order q. For each i with $0 \leq i \leq q+1$, let

$$t_i = |\{ \text{ lines } l \mid |l \cap \mathcal{K}| = i\}|.$$

A k-set $\mathcal{K}$ has **class** $[m_1, m_2, \dots, m_s]$ if $0 \leq m_1 < m_2 < \cdots < m_s \leq q+1$ and $\{i \mid t_i \neq 0\} \subseteq \{m_1, m_2, \dots, m_s\}$; it has **type** $(m_1, m_2, \dots, m_r)$ if $0 \leq m_1 < m_2 < \cdots < m_r \leq q+1$ and $\{i \mid t_i \neq 0\} = \{m_1, m_2, \dots, m_r\}$.

THEOREM 27 ([**118**] [**55**]). *Let $\mathcal{K}$ be a set of k points of a projective plane π. Then*

$$\text{(1)} \qquad \sum_{i=0}^{q+1} t_i = q^2 + q + 1.$$

$$\text{(2)} \qquad \sum_{i=1}^{q+1} i t_i = k(q+1).$$

$$\text{(3)} \qquad \sum_{i=2}^{q+1} i(i-1) t_i = k(k-1).$$

PROOF.

(1) Count the number of lines in two ways.

(2) Count $|\{(P, l) \mid P \in \mathcal{K},\ P \mathrel{\mathrm{I}} l\}|$ in two ways: For each of the k points P of $\mathcal{K}$, there are $q+1$ lines on P; for each of the t_i lines l with $|l \cap \mathcal{K}| = i$, there are i points of $\mathcal{K}$ on l.

(3) Count $\{(P, Q, l) \mid P, Q \in \mathcal{K},\ P \neq Q,\ P \mathrel{\mathrm{I}} l,\ Q \mathrel{\mathrm{I}} l\}|$ in two ways; for each of the k points P of $\mathcal{K}$, there are $k-1$ points Q of $\mathcal{K}$ with $P \neq Q$, and each pair (P, Q) has a unique line on it; for each of the t_i lines l with $|l \cap \mathcal{K}| = i$, there are i points P of $\mathcal{K}$ on l and $i-1$ points Q of $\mathcal{K}$ on l with $Q \neq P$. $\square$

An **arc** in a finite projective plane is a set of points where no three are collinear. A k**-arc** is an arc containing k points. A **quadrangle** is another way of referring to a 4-arc and **triangle** for a 3-arc.

Secant, **tangent**, and **external** lines are lines that meet an arc in exactly 2, 1 or 0 points, respectively.

Hence a k-arc is of class $[0, 1, 2]$.

THEOREM 28 ([**16**]). *A k-arc in a projective plane of order q has $k \leq q+2$. When equality holds there are no tangent lines to the arc.*

PROOF. Let P be a point of the k-arc. Each line on P is incident with at most one point from the arc (other than P) as no three are collinear. We have $q+1$ lines on P, so that there are at most $q+1$ points on the arc not including P. Hence $k \leq (q+1)+1 = q+2$.

Suppose we have a $(q+2)$-arc, $\mathcal{H}$. Let P be a point on $\mathcal{H}$. Let l be a line on P. Each line on P meets $\mathcal{H} - \{P\}$ in exactly one point. Therefore l meets $\mathcal{H} - \{P\}$ in exactly one point. Hence l meets $\mathcal{H}$ in exactly two points. Thus every line that meets $\mathcal{H}$ is secant to $\mathcal{H}$. □

We call a $(q+2)$-arc a **hyperoval**. The proof above shows that any hyperoval has type $(0, 2)$.

THEOREM 29 ([**16**]). *If there exists a hyperoval in a projective plane of order q then q is even.*

PROOF. Let $\mathcal{H}$ be a hyperoval. Choose a point P not on $\mathcal{H}$. This point exists as $q^2+q+1 > q+2$. By Theorem 28, each line on P meets $\mathcal{H}$ in zero or two points. Hence the lines on P partition $\mathcal{H}$ into sets of size two. Hence 2 divides $q+2$, which implies 2 divides q, which implies that q is even. □

COROLLARY 30 ([**16**]). *In a projective plane of order q, q odd, a k-arc has $k \leq q+1$.*

Irrespective of whether q is odd or even, a $(q+1)$-arc in a projective plane of order q is called an **oval**.

LEMMA 31 ([**114**]). *In a projective plane of order q every point of an oval has a unique tangent on it.*

PROOF. Let P be a point of an oval $\mathcal{O}$. Then

$$\begin{aligned} \text{number of tangents on } P &= (q+1) - \text{number of secants on } P \\ &= (q+1) - |\mathcal{O} - \{P\}| \\ &= (q+1) - q \\ &= 1. \quad \square \end{aligned}$$

Hence the number of tangents of an oval in a projective plane of order q is $q+1$.

THEOREM 32 ([**114**]). *In a projective plane of order q, with q odd, every point not on the oval is on zero or two tangents of the oval.*

PROOF. Let $\mathcal{O}$ be an oval in a projective plane of odd order q. The number of points on $\mathcal{O}$ is even. Thus every point not on $\mathcal{O}$ lies on an even number of tangent lines. Now let l be a tangent line to $\mathcal{O}$. Every point on l not in $\mathcal{O}$ lies on at least one other tangent line to $\mathcal{O}$. Since there are q tangent lines to $\mathcal{O}$ other than l and q points on l not in $\mathcal{O}$ each point on l not in $\mathcal{O}$ lies on exactly one tangent line other than l.

So every point not in $\mathcal{O}$ either lies on no tangent lines to $\mathcal{O}$ or exactly two tangent lines to $\mathcal{O}$. □

We call all points not on the oval $\mathcal{O}$ that have two tangents to $\mathcal{O}$ **external points** to $\mathcal{O}$, and those with no tangents to $\mathcal{O}$ the **internal points** to $\mathcal{O}$. In fact, we can see that all points in our projective plane of order q, q odd, can be characterised as external points, internal points, or the $q+1$ points of $\mathcal{O}$.

Let P be a point of the oval $\mathcal{O}$. Then there is a unique tangent line, l, to P of $\mathcal{O}$. The line l has q points different from P, with these points being incident with another tangent line to $\mathcal{O}$ not equal to l. Hence there are $\frac{1}{2}q(q+1)$ external points in a projective plane of order q, q odd. Since there are $q+1$ points on $\mathcal{O}$, this gives $\frac{1}{2}q(q-1)$ internal points.

REMARK. Theorem 32, says that for q odd, the tangent lines to an oval form an oval of the dual plane.

THEOREM 33 ([**114**]). *In a projective plane of order q, q even, an oval, $\mathcal{O}$, has $q+1$ tangents all concurrent in a point.*

PROOF. By Lemma 31, we have $q+1$ tangents. Since $q+1$ is odd, each point lies on an odd number of tangents to $\mathcal{O}$. Let l be a secant line to $\mathcal{O}$. Each point of l lies on at least one tangent to $\mathcal{O}$, but there are only $q+1$ tangents so each lie on exactly one tangent. Hence any point incident with two (or more) tangents is incident with no secant lines, and so is on $q+1$ tangents.

Equivalently any intersection of two tangents does not lie on a secant of $\mathcal{O}$. So all the lines on a point of intersection of two tangents are tangents. □

COROLLARY 34 ([**114**]). *In a projective plane of order q, with q even, every oval can be uniquely completed to form a hyperoval.*

PROOF. All the tangents of the oval $\mathcal{O}$ meet in a point N and this point lies on no secant line to $\mathcal{O}$. Hence $\mathcal{O} \cup \{N\}$ is a hyperoval. This is unique by Lemma 31. □

In a plane of even order, we call the point of intersection of all the tangents from an oval the **nucleus** of the oval.

Theorem 35 ([**114**]). *Let $\mathcal{K}$ be a k-arc contained in a hyperoval with $k > q/2+1$. If $\mathcal{K} \cup \{P\}$ is a $(k+1)$-arc, then P is on the hyperoval containing $\mathcal{K}$.*

Proof. Let $\mathcal{K} \cup \{P\}$ be an arc with P not on the hyperoval containing $\mathcal{K}$, which we shall call $\mathcal{H}$. Then all the lines from P must meet $\mathcal{H}$ in two or no points by Theorem 28, p. 16. But as $\mathcal{K}$ has more than $q/2+1$ points on it, there must be a line from P, intersecting $\mathcal{H}$, that meets $\mathcal{K}$ in two points, contradicting the fact that $\mathcal{K} \cup \{P\}$ is an arc. Hence P is on $\mathcal{H}$. □

2. Conics

We investigate a special example of an oval. The reader should be familar with the area of sesquilinear forms and Witt's Theorem. See [**124**] for an introduction.

The **radical** of a sesquilinear form $f\colon V \times V \to GF(q)$ on a vector space V is

$$\mathrm{Rad}\, f = V^{\perp} = \{\boldsymbol{w} \in V \mid f(\boldsymbol{v}, \boldsymbol{w}) = 0 \text{ for all } \boldsymbol{v} \in V\}.$$

A form f is **nondegenerate** if $\mathrm{Rad}\, f = \{\boldsymbol{0}\}$, otherwise f is **degenerate**.

A **quadratic form** on a vector space V is a function $Q\colon V \to GF(q)$ with $Q(c\boldsymbol{v}) = c^2 Q(\boldsymbol{v})$ for all $\boldsymbol{v} \in V$ and $c \in GF(q)$ and we define f_Q the symmetric bilinear form associated with Q as

$$f_Q(\boldsymbol{v}, \boldsymbol{w}) = Q(\boldsymbol{v}+\boldsymbol{w}) - Q(\boldsymbol{v}) - Q(\boldsymbol{w}) \text{ for all } \boldsymbol{v},\, \boldsymbol{w} \in GF(q).$$

The **singular radical** of a quadratic form Q is

$$\{\boldsymbol{v} \in \mathrm{Rad}\, f_Q \mid Q(\boldsymbol{v}) = 0\}.$$

A quadratic form is **nondegenerate** (or **nonsingular**) if the singular radical is $\{\boldsymbol{0}\}$, **degenerate** (or **singular**) otherwise.

For q odd, Q is nondegenerate if and only if f_Q is nondegenerate. For q even, there are nondegenerate quadratic forms Q with a degenerate form f_Q.

A quadratic form Q on V defines a **quadric**,

$$\mathcal{Q} = \{\langle \boldsymbol{x} \rangle \mid Q(\boldsymbol{x}) = 0\}$$

in $PG(n,q)$ where $\dim_{GF(q)} V = n+1$. The one-dimensional subspaces $\langle \boldsymbol{x} \rangle$ where $Q(\boldsymbol{x}) = 0$ are called **totally singular points** of $\mathcal{Q}$, since they are points of $PG(n,q)$. When a nondegenerate quadratic form Q has f_Q degenerate, then the radical of f_Q is called the **nucleus** of $\mathcal{Q}$. Quadrics in $PG(2,q)$ are called **conics**.

Example. Let Q be the quadratic form on $GF(q)^3$ defined by

$$Q(x,y,z) = ax^2 + by^2 + cz^2 + dxy + exz + fyz.$$

Then Q defines a conic in $PG(2,q)$. The corresponding form is

$$\begin{aligned} f_Q(\boldsymbol{x},\boldsymbol{x}') &= Q(x+x',y+y',z+z') - Q(x,y,z) - Q(x',y',z') \\ &= \begin{pmatrix} x & y & z \end{pmatrix} \begin{pmatrix} 2a & d & e \\ d & 2b & f \\ e & f & 2c \end{pmatrix} \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}, \end{aligned}$$

with f_Q being non-degenerate if and only if

$$\begin{vmatrix} 2a & d & e \\ d & 2b & f \\ e & f & 2c \end{vmatrix} \neq 0.$$

Now suppose that $\mathcal{Q}$ is a degenerate conic. We define $\bar{f}_Q$ over $GF(q)^3/\operatorname{Rad} f_Q$ so $\bar{f}_Q$ is nondegenerate.

Let q be even. Then $\dim(V/\operatorname{Rad} f_Q)$ is even so $\dim \operatorname{Rad} f_Q$ is odd. If $\dim \operatorname{Rad} f_Q = 3$ then $f_Q = 0$ so $Q(x,y,z) = ax^2 + by^2 + cz^2 = (\sqrt{a}x + \sqrt{b}y + \sqrt{c}z)^2$, a repeated line, or the whole plane. If $\dim \operatorname{Rad} f_Q = 1$ then $\operatorname{Rad} f_Q$ is the singular radical of Q since Q is degenerate. Then $\bar{Q}$ defined on $GF(q)^3$ over the singular radical of Q has dimension two. If it is of plus type we have two distinct concurrent lines, if it is of minus type then it is a point (see [**124**]).

Let q be odd. If $\dim \operatorname{Rad} f_Q = 3$ then $Q = 0$ and $\mathcal{Q}$ is the whole plane. If $\dim \operatorname{Rad} f_Q = 2$ then $\bar{Q}$ is a one dimensional non-degenerate form with no singular points, hence $\mathcal{Q}$ is a repeated line. When $\dim \operatorname{Rad} f_Q = 1$ we have the same situation as for q even.

Hence we can say that a degenerate conic is one of the following:

(i) The whole plane,
(ii) a point,
(iii) two concurrent distinct lines, or
(iv) a repeated line.

THEOREM 36 (see [**55**] Lemma 7.2.3). *A nondegenerate conic is an oval of $PG(2,q)$.*

PROOF. A nondegenerate conic is the set of totally singular points with respect to a nondegenerate quadratic form Q. Given a line l (that is, a two-dimensional subspace of $GF(q)^3$) the restriction $Q|_l$ of Q to l is a (possibly degenerate) quadratic form. Since Q has **Witt index** 1, that is, the common dimension of the maximal totally singular subspaces is 1, then $Q|_l \neq 0$. If $Q|_l$ is nondegenerate, it has either zero or two singular points on l, since $Q|_l$ is isometric to $O^-(2,q)$ or $O^+(2,q)$, respectively [**124**]. If degenerate, the radical is one-dimensional, and is the only totally singular point. Hence every line l meets the conic in 0, 1, or 2 points. The form Q is similar to $xz - y^2$ which has $q+1$ totally singular points, those being $\{(1,t,t^2) \mid t \in GF(q)\} \cup \{(0,0,1)\}$. $\square$

THEOREM 37. *Let $q = 2^e$. Let i satisfy $(i, e) = 1$ and $\alpha = 2^i$ be an automorphism of $GF(q)$. Then (in the notation of Section 6, p. 46) we have*

$$\mathcal{D}(\alpha) - \{(0,1,0)\} = \{(1,t,t^\alpha) \mid t \in GF(q)\} \cup \{(0,0,1)\},$$

being an oval.

PROOF. The lines on the point $(0,0,1)$ are of the form $[0,1,0]$ and $[1,b,0]$ where $b \in GF(q)$. These only meet the oval in at most one other point. What is left to show is that no three points of $\{(1,t,t^\alpha) \mid t \in GF(q)\}$ are collinear.

Suppose the points $(1,x,x^\alpha)$, $(1,y,y^\alpha)$, and $(1,z,z^\alpha)$ are collinear for distinct x, y, $z \in GF(q)$. Then

$$\frac{x^\alpha + y^\alpha}{x+y} = \frac{x^\alpha + z^\alpha}{x+z} = \frac{y^\alpha + z^\alpha}{y+z},$$

which implies that $(x+y)^{\alpha-1} = (x+z)^{\alpha-1} = (y+z)^{\alpha-1}$ as $\alpha \in \operatorname{Aut} GF(q)$. Since $(\alpha - 1, q - 1) = (2^i - 1, 2^e - 1) = 2^{(i,e)} - 1 = 1$ we have $\alpha - 1$ being one-to-one. Hence $x + y = x + z = y + z$. Contradiction. Hence $\mathcal{D}(\alpha) - \{(0,1,0)\}$ is an oval. □

LEMMA 38 (Lemma of Tangents [**55**]). *Assume $\mathcal{Q}$ is a q-arc of $PG(2,q)$, q odd. Let $t_1, \ldots, t_r$ be tangents of $\mathcal{Q}$ passing through the point P. Put $Q_i = t_i \cap \mathcal{Q}$ and denote by s_i the second tangent of $\mathcal{Q}$ through Q_i. Then there is a conic $\mathcal{C}$ of $PG(2,q)$ containing all the Q_i and such that s_i is a tangent of $\mathcal{C}$ for all i.*

In 1949 Järnefelt and Kustaanheimo [**62**] conjectured that for q odd every oval is a conic. Marshall Hall Jr. wrote when reviewing the article [**45**] "The reviewer finds this conjecture implausible." This moved Segre into proving the conjecture and he announced the proof in 1954 in Italian and 1955 in English [**116**].

THEOREM 39 (Segre's Theorem). *Let $\mathcal{O}$ be an oval in $PG(2,q)$, q odd. Then $\mathcal{O}$ is a conic.*

PROOF. This theorem is true if $q = 3$, so assume $q \geq 5$.

Pick $P \in \mathcal{O}$. Then all the secants of $\mathcal{O}$ through P are tangents of the q-arc $\mathcal{O} - \{P\}$. Hence there is a conic $\mathcal{C}$ with $\mathcal{C} \supseteq \mathcal{O} - \{P\}$, such that all the tangents of $\mathcal{O}$ which have their points of tangency in $\mathcal{C} \supseteq \mathcal{O} - \{P\}$ are also tangents of $\mathcal{C}$ by Lemma 38, p. 20.

Pick $Q \in \mathcal{O} - \{P\}$. The same argument yields a conic $\mathcal{C}'$ with $\mathcal{C}' \supseteq \mathcal{C} - \{Q\}$, such that the tangents of $\mathcal{C}'$ through points of $\mathcal{C} - \{Q\}$ are also tangents of $\mathcal{C}$. Hence $\mathcal{C}$ and $\mathcal{C}'$ have at least $q - 1 \geq 4$ points and at least as many tangents in common.

This is more than enough to make $\mathcal{C} = \mathcal{C}'$. □

A hyperoval in $PG(2,q)$, q even, is **regular** if it is the union of a conic and the nucleus of the conic. A **pointed conic** is an oval equal to $\mathcal{C} \cup \{N\} - \{P\}$ where $\mathcal{C}$ is a conic with nucleus N and P is a point of the conic.

LEMMA 40. *A regular hyperoval in $PG(2,q)$ contains a unique conic if $q \geq 8$.*

Proof. By definition there exist a conic, $\mathcal{C}$, such that $\mathcal{H} = \mathcal{C} \cup \{N\}$, where N is the nucleus of the conic. Suppose $\mathcal{C}' \subseteq \mathcal{H}$. Then $|\mathcal{C} \cap \mathcal{C}'| \geq q \geq 5$, and since there exists a unique conic on a 5-arc ([**55**] corollary to theorem 7.2.1) we have $\mathcal{C} = \mathcal{C}'$. □

The quadrangle $\{(0,0,1),(0,1,0),(1,0,0),(1,1,1)\}$ is referred to as the **fundamental quadrangle**.

Lemma 41 ([**55**], theorem 8.4.2, corollary 6). *Let $\mathcal{H}$ be a regular hyperoval in $PG(2,2)$ then $P\Gamma L(3,2)_{\mathcal{H}} \cong S_4$. In particular, all hyperovals in $PG(2,2)$ are regular.*

Proof. In $PG(2,2)$ $\mathcal{H}$ is a 4-arc. As $P\Gamma L(2,2) = PGL(2,2)$ is regular on ordered quadrangles we have $P\Gamma L(3,2)_{\mathcal{H}} \cong S_4$, so all hyperovals are equivalent in $PG(2,2)$. The four hyperovals, $\mathcal{C} \cup \{N\}$, for a conic $\mathcal{C}$ and nucleus N, on the fundamental quadrangle are:

(i) $\mathcal{C}$ defined as $xy + xz + yz = 0$ with nucleus $N = (1,1,1)$.
(ii) $\mathcal{C}$ defined as $x^2 + yz = 0$ with nucleus $N = (1,0,0)$.
(iii) $\mathcal{C}$ defined as $y^2 + xz = 0$ with nucleus $N = (0,1,0)$.
(iv) $\mathcal{C}$ defined as $z^2 + xy = 0$ with nucleus $N = (0,0,1)$. □

Lemma 42 ([**55**], theorem 8.4.2, corollary 6). *Let $\mathcal{H}$ be a regular hyperoval in $PG(2,4)$, then $P\Gamma L(3,4)_{\mathcal{H}} \cong S_6$. In particular, all hyperovals in $PG(2,4)$ are regular.*

Proof. Let $q = 4$. Let $\mathcal{Q}$ be a 4-arc in $PG(2,4)$. There are two points P_1 and P_2 of $PG(2,4)$ such that $\mathcal{Q} \cup \{P_i\}$ is a 5-arc for $i = 1, 2$. In fact $\mathcal{Q} \cup \{P_1, P_2\}$ is the unique hyperoval on $\mathcal{Q}$. Hence there exists a unique hyperoval on $\mathcal{Q}$. Since $PGL(3,4)$ is regular on 4-arcs then there exists a unique $g \in PGL(3,4)$ such that $g\mathcal{Q}_1 = \mathcal{Q}_2$ with $\mathcal{Q}_1$ and $\mathcal{Q}_2$ being 4-arcs contained in a hyperoval $\mathcal{H}$. Since there is a unique hyperoval on each 4-arc we have $g\mathcal{H} = \mathcal{H}$. Hence $PGL(3,4)_{\mathcal{H}}$ is sharply 4-transitive on $\mathcal{H}$. Hence $PGL(3,4)_{\mathcal{H}} \cong A_6$, so $G \cong S_6$.

Let ω be a primitive element of $GF(4)$ such that $\omega^2 = \omega + 1$. Let

$$\mathcal{Q} = \{(1,0,0),(0,1,0),(0,0,1),(1,1,1)\}$$

with $\{P_1, P_2\} = \{(1,\omega,\omega^2),(1,\omega^2,\omega)\}$, so

$$\mathcal{Q} \cup \{P_1, P_2\} = \{(1,t,t^2) \mid t \in GF(q)\} \cup \{(0,1,0),(0,0,1)\}$$

so $\mathcal{Q} \cup \{P_1, P_2\}$ is equal to a conic, $\mathcal{C}$, plus its nucleus N. Then we have the conics and nuclei being:

(i) $\mathcal{C}\ xy + \omega xz + \omega^2 yz = 0$ with nucleus $N = (1,\omega^2,\omega)$.
(ii) $\mathcal{C} : \omega^2 xy + \omega xz + yz = 0$ with nucleus $N = (1,\omega,\omega^2)$.
(iii) $\mathcal{C} : x^2 + yz = 0$ with nucleus $N = (1,0,0)$.
(iv) $\mathcal{C} : y^2 + xz = 0$ with nucleus $N = (0,1,0)$.
(v) $\mathcal{C} : xy + xz + yz = 0$ with nucleus $N = (1,1,1)$.
(vi) $\mathcal{C} : z^2 + xy = 0$ with nucleus $N = (0,0,1)$. □

Hence Lemma 40, p. 20, needs $q \geq 8$.

THEOREM 43 ([**55**], theorem 8.4.2, corollary 6). *The stabiliser of a regular hyperoval, $\mathcal{H}$ in $PGL(3,q)$ is isomorphic to*

$$\left\{ \begin{pmatrix} a^2 & 0 & b^2 \\ ac & ad+bc & bd \\ c^2 & 0 & d^2 \end{pmatrix} \;\middle|\; a,b,c,d \in GF(q), ad+bc \neq 0 \right\}.$$

since this is the stabiliser of $\mathcal{D}(2)$ (in the notation of Section 4, p. 41).

PROOF. If A is the set of all field automorphisms of $GF(q)$ (acting on $PG(2,q)$ as in Section 3, p. 2) then

$$P\Gamma L(3,q)_{\mathcal{H}} = \langle PGL(3,q)_{\mathcal{H}}, A\rangle.$$

Also $PGL(3,q)_{\mathcal{H}}$ is generated by these matrices:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & t & 0 \\ 0 & 0 & t^2 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ t & 1 & 0 \\ t^2 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad t \in GF(q).$$

The first two types of matrices generate a maximal subgroup in $PGL(3,q)_{\mathcal{H}}$. The proof follows:

Let

$$H = \left\langle \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & t & 0 \\ 0 & 0 & t^2 \end{pmatrix} \;\middle|\; t \in GF(q) \right\}, \left\{ \begin{pmatrix} 1 & 0 & 0 \\ t & 1 & 0 \\ t^2 & 0 & 1 \end{pmatrix} \;\middle|\; t \in GF(q) \right\} \right\rangle,$$

so $H \leq PGL(3,q)_{\mathcal{H},(0,0,1)}$. Since $|PGL(3,q)_{\mathcal{H}}| = (q+1)q(q-1)$ and $|PGL(3,q)_{\mathcal{H}} : PGL(3,q)_{\mathcal{H},(0,0,1)}| = q+1$ with $PGL(3,q)_{\mathcal{H}}$ transitive on points of the conic, we conclude that $|PGL(3,q)_{\mathcal{H},(0,0,1)}| = q(q-1)$, so $H = PGL(3,q)_{\mathcal{H},(0,0,1)}$. Since $PGL(3,q)_{\mathcal{H}}$ is 2-transitive on points of the conic, then $PGL(3,q)_{\mathcal{H}}$ is primitive on points of the conic and so $H = PGL(3,q)_{\mathcal{H},(0,0,1)}$ is a maximal subgroup of $PGL(3,q)_{\mathcal{H}}$ by Theorem 12, p. 5. □

THEOREM 44 ([**55**], lemma 7.2.3, corollary 7). *The action of $P\Gamma O(3,q)$ on the set of totally singular points of the $O(3,q)$ polar space is equivalent to the action of $P\Gamma L(2,q)$ on the points of $PG(1,q)$.*

PROOF. The bijection from $PG(1,q)$ to $O(3,q)$ with form $xz = y^2$

$$f : \begin{cases} (1,t) \leftrightarrow (1,t,t^2) \\ (0,1) \leftrightarrow (0,0,1) \end{cases}$$

plus the isomorphism from $PGL(2,q)$ to $PGO(3,q)$ (with field automorphisms acting coordinate wise)

$$\psi : \begin{pmatrix} a & b \\ c & d \end{pmatrix} Z_2 \leftrightarrow \begin{pmatrix} a^2 & 2ab & b^2 \\ ac & bc+ad & bd \\ c^2 & 2cd & d^2 \end{pmatrix} Z_3$$

(where Z_d is the centre of $GL(d,q)$) form an equivalence since $\psi(g)f(x) = f(gx)$ for all $x \in PG(1,q)$ and all $g \in P\Gamma L(2,q)$.

Let

$$D = \begin{pmatrix} a^2 & 2ab & b^2 \\ ac & bc+ad & bd \\ c^2 & 2cd & d^2 \end{pmatrix}.$$

Since $\mathcal{D}(2) \supseteq$ quadrangle (for $q > 2$) then

$$f \begin{pmatrix} a & b \\ c & d \end{pmatrix} f^{-1} \text{ and } D$$

agree on a quadrangle, and so

$$f \begin{pmatrix} a & b \\ c & d \end{pmatrix} f^{-1} = D|_{\mathcal{D}(2)},$$

with D unique. □

NOTE. Let $\mathcal{O}$ be a conic in $PG(2,4)$ and $\mathcal{H} = \mathcal{O} \cup \{N\}$, where N is the nucleus of $\mathcal{O}$. So there are 15 secant lines and hence 6 external lines to $\mathcal{H}$ in $PG(2,4)$; these external lines make a dual hyperoval. Since $P\Gamma L(3,4)_{\mathcal{O}} \cong S_5 \cong PGL(2,4)$ and by Witt's Theorem [**124**], $P\Gamma L(3,4)_{\mathcal{O}}$ is transitive on external lines to $\mathcal{H}$.

THEOREM 45. *Let $\mathcal{H}$ be a regular hyperoval in $PG(2,q)$. Let $G = P\Gamma L(3,q)_{\mathcal{H}}$. Then for $q \geq 8$ we have $G \cong P\Gamma L(2,q)$.*

PROOF. Let $q \geq 8$. By Lemma 40, p. 20, we have a unique conic $\mathcal{C}$, such that, $\mathcal{H} = \mathcal{C} \cup \{N\}$ where N is the nucleus of $\mathcal{C}$. Hence $G = P\Gamma L(3,q)_{\mathcal{C}\cup\{N\}} = P\Gamma L(3,q)_{\mathcal{C}}$. The result follows from Theorem 44, p. 22. □

3. Collineation Groups

A **collineation** of a projective plane, π, is an automorphism of π. We quite happily use both collineation and automorphism interchangeably.

Let P and Q be points of a projective plane π. Let g be a collineation of π. Let l be the line, PQ, joining P and Q. Then gl is the unique line joining gP and gQ, that is,

$$g(PQ) = (gP)(gQ).$$

Dually, if l and m are lines of π with $l \neq m$, then

$$g(l \cap m) = (gl) \cap (gm).$$

We will define lines by the points on them, so $P \in l$ is equivalent to saying $P \mathrm{~I~} l$.

3.1. Fixed Configurations

Let G be a group of collineations of a projective plane π with P a point and l a line of π.

(i) If $gP = P$ for all $g \in G$ then P **is fixed under** G.
(ii) If $gl = l$ for all $g \in G$, that is, $\{P \mid P \in l\} = \{gP \mid P \in l\}$, then l **is fixed under** G.
(iii) l is **fixed!pointwise** by G if $gP = P$ for all $P \in l$, for all $g \in G$.
(iv) P is **fixed!linewise** by G if $gl = l$ for all l incident with P, for all $g \in G$.

The **fixed configuration** for a group G of collineations is the configuration of fixed lines and fixed points under G.

We call a subset of points $\mathscr{P}'$ and a subset of lines $\mathscr{L}'$ of a projective plane a **closed configuration** if

(i) Given P, $Q \in \mathscr{P}'$ with $P \neq Q$ then $PQ \in \mathscr{L}'$, and
(ii) given l, $m \in \mathscr{L}'$ with $l \neq m$ then $l \cap m \in \mathscr{P}'$.

THEOREM 46 ([**134**]). *Let G be a group of collineations of a projective plane π. Then for all $g \in G$*

(i) *If distinct points P and Q are fixed then so is the line PQ.*
(ii) *If distinct lines l and m are fixed so is the point $l \cap m$.*
(iii) *If the distinct lines l and m are fixed pointwise with $l \neq m$, then $g = 1$.*
(iv) *If the distinct points P and Q are fixed linewise with $P \neq Q$, then $g = 1$.*

PROOF. (i) $g(PQ) = gPgQ = PQ$ as P and Q are fixed.
(ii) Dually.
(iii) Let $O = l \cap m$. Let P be any point not on l or m. Then take two lines r and s through P distinct from PO (these exist as there are at least three lines on any point).

Let $R = l \cap r$, $S = l \cap s$, $C = m \cap s$ and $U = m \cap r$. Since $gR = R$ and $gU = U$ we have $gr = r$. Similarly, $gs = s$. Hence P is fixed by (ii). Since P is any arbitrary point not initially fixed by g, it follows that $g = 1$.
(iv) Dually. □

A fixed configuration of a group of collineations G is always a closed configuration. In fact the incidence structure of a fixed configuration satisfies axioms **PP1** and **PP2**.

A **subplane**, π', of a projective plane, π, is a closed configuration that contains a quadrangle. A subplane π' is a **Baer subplane** if every point of π is on a line of

π' and every line of π is on a point of π'. If a collineation has a subplane as a fixed configuration then we say the collineation is **planar**, those planar collineations whose fixed subplane is Baer are called **Baer collineations**.

COROLLARY 47. *Let g be a collineation of a projective plane such that*

(i) *l is fixed pointwise by g, and*

(ii) *$gP = P$ and $gQ = Q$ with $P \notin l$ and $Q \notin l$,*

then $g = 1$.

PROOF. Take any point R not on l and PQ. Let $U = RP \cap l$ and $V = RQ \cap l$. Since U, V, P and Q are fixed, the lines UP and VQ are fixed. Hence $R = UP \cap VQ$ is fixed. Since R was arbitrary, the line UR is fixed pointwise as well as l. Since we have two distinct lines UR and l being fixed pointwise by Theorem 46, we have $g = 1$. □

Let $\mathscr{I} = (\mathscr{P}, \mathscr{B}, \mathrm{I})$ be a projective plane of order q. An **incidence matrix** A for $\mathscr{I}$ is a matrix with rows indexed by points, columns indexed by lines with entry in row P and column l being 1 if $P \mathrel{\mathrm{I}} l$ and 0 if $P \not\mathrel{\mathrm{I}} l$.

LEMMA 48 ([**46**]). *Suppose that $\mathscr{I} = (\mathscr{P}, \mathscr{B}, \mathrm{I})$ is a finite projective plane of order q then*

$$AA^T = qI + J,$$

where J is the all one's matrix. Also A is invertible.

PROOF. For P_1, $P_2 \in \mathscr{P}$, the entry in row P_1 and column P_2 of AA^T is

$$|\{l \in \mathscr{B} \mid P_1 \mathrel{\mathrm{I}} l \mathrel{\mathrm{I}} P_2\}| = \begin{cases} 1 & \text{if } P_1 \neq P_2, \\ q+1 & \text{if } P_1 = P_2. \end{cases}$$

So $AA^T = qI + J$. Now $\det(qI + J) = (n+1)^2 n^{n^2+n} \neq 0$ so A is invertible. □

THEOREM 49 ([**46**]). *In a finite projective plane the permutation σ of points and τ of lines of a collineation has the same cycle structure.*

PROOF. Let $\mathscr{I} = (\mathscr{P}, \mathscr{L}, \mathrm{I})$ be a point-line incidence structure with a point-line incidence matrix A. Let $g \in \mathrm{Sym}(\mathscr{P} \cup \mathscr{L})_{\mathscr{P} \cup \mathscr{L}}$. Then $g \in \mathrm{Aut}\,\mathscr{I}$ if and only if we have $gP \in gl \iff P \in l$. Let $g = (\sigma, \tau)$ where $\sigma = g|_{\mathscr{P}}$ and $\tau = g|_{\mathscr{L}}$. So $g \in \mathrm{Aut}\,\mathscr{I}$ if and only if $\sigma P \in \tau \iff P \in l$.

Let the permutation matrix of σ be S and τ have permutation matrix T. Then $PSATl = PAl$ for all points P and all lines l, hence $SAT = A$.

By Theorem 48 A is invertible so

$$S = AT^{-1}A^{-1} \implies S \sim T^{-1}. \quad \square$$

COROLLARY 50 ([**46**]). *In a finite projective plane a collineation fixes the same number of points and lines.*

By Corollary 50, in a group generated by a collineation (that is, a cyclic group of collineations) the number of fixed points equals the number of fixed lines. It is necessary that the group be cyclic since the group $AGL(2,q)$ fixes no points of $PG(2,q)$ but does fix a line.

If g fixes a line l pointwise then we say that g has **axis** l. If g fixes a point linewise then we say that g has **centre** P.

If g is not equal to the identity then it has at most one axis and centre by Theorem 46.

Let $g \neq 1$ have axis l and centre P, then g is an **elation** if $P \mathrel{\mathrm{I}} l$ and a **homology** if not. By convention, the identity is both an elation and a homology.

NOTES. (i) For a collineation g with axis l and centre P, apart from l, only lines through P are fixed. Since, if we suppose there exists a line n not through P fixed by g and a line m through P with $l \neq m$, then $m \cap n$ is fixed, giving a contradiction.

(ii) Given P and l the set of all collineations with centre P and axis l form a group. We have $(\mathrm{Aut}\,\pi)_{(P,l)}$ acting on $\{\text{lines on } P\} \cup \{\text{points on } l\}$. The kernel of the action equals $\{\text{collineations with centre } P \text{ and axis } l\} \lhd (\mathrm{Aut}\,\pi)_{(P,l)}$.

(iii) If $gP = P$ then for any collineation h, we have

$$(hgh^{-1})(hP) = hP,$$

so hP is fixed by hgh^{-1}.

(iv) Given a collineation g with axis l and centre P and h a collineation, then hgh^{-1} is a collineation with centre hP and axis hl, since, if $P \in hl$, then $h^{-1}P \in l$. Also

$$\begin{aligned} hgh^{-1}(P) &= hg(h^{-1}P) \\ &= h(h^{-1}P) \\ &= P, \end{aligned}$$

so hl is fixed pointwise by hgh^{-1}. Similarly, we can prove hP is fixed linewise by hgh^{-1}.

The (cyclic) group generated by an elation or a homology acts semiregularly on points not equal to the centre and not on the axis by Corollary 47.

THEOREM 51 ([**36**]). *In a projective plane of order q.*

(i) *The order of an elation divides q.*

(ii) *The order of a homology divides $q-1$.*

PROOF. Look at a line l on the centre but not on the axis. Since l is on the centre it is fixed, so has q points not fixed on l if it is an elation, and $q-1$ points not fixed on l if it is a homology. ☐

THEOREM 52. *A non-trivial homology does not stabilise a hyperoval in a projective plane of order q.*

PROOF. Let g be a homology with axis l and centre C. Let P be a point not on l and distinct from C, then C, P, gP are collinear. So the orbits of P under $\langle g \rangle$ are collinear (on a line incident with the centre C). The length of this orbit is equal to $|g|$, since g acts semi-regularly. Since q is even we have $q-1$ being odd, so $|g|$ is odd, hence as g is non-trivial $|g| \geq 3$ (Theorem 51), hence the orbits under g are not arcs. □

This is the reason we concentrate on elations more than homologies.

We say l is a **translation line** if for all P I l we have for every pair of distinct points Q, R where Q, R, P collinear and Q, R not on l, there exists an elation g with centre P and axis l such that $gQ = R$.

If a projective plane, π, has a translation line then we say π is a **translation plane**. The projective plane $PG(2,q)$ is a translation plane where every line is a translation line.

In a projective plane, π, of order q a **translation q-arc**, $\mathcal{K}$, is a q-arc whose stabiliser in the full automorphism group of π contains a group of elations acting transitively on its q points. A **translation hyperoval** is a hyperoval that contains a translation q-arc $\mathcal{K}$. Since the group is transitive, the axis of the group of elations is external to $\mathcal{K}$.

A **semi-translation hyperoval** [**112**] is a hyperoval with an elation group with common axis in its stabiliser each of whose orbits not on the axis, together with the points of the hyperoval on the common axis forms a translation hyperoval of a Baer subplane (cf. Ostrom's definition [**89**] of a semi-translation plane).

THEOREM 53 ([**36**]). *Let g and h be elations with common axis l but distinct centres C and B, respectively, with $g \neq h \neq 1 \neq g$. Then $gh = hg$.*

PROOF. Take a point P. If $P \in l$ then $gh(P) = hg(P)$. So suppose $P \notin l$. Then C, P, and gP are collinear, and B, P, and hP are collinear. Let $U = ChP \cap BgP$. Then $hP = BP \cap CU$, so $ghP = g(BP) \cap g(CU) = BgP \cap CU = U$. Now $gP = BU \cap CP$, so $hgP = h(BU) \cap h(CP) = BU \cap ChP = U$. So $gh = hg$. □

THEOREM 54 (Singer's Theorem [**122**]). *A Desarguesian plane π of order q has a cyclic collineation group of order q^2+q+1 which is regular on the points and also on the lines.*

An **involution** is a collineation of order 2.

THEOREM 55. *An elation stabilising a hyperoval is involutory.*

PROOF. The group generated by the elation acts semi-regularly on the non-fixed points, but interchanges the points of secancy on any non-axial secant line on the centre; thus the group has order 2. □

Example. The complement of a line is a hyperoval in $PG(2,2)$. It is stabilised by all elations with centre on the line. Those with axis different from the line have axis secant to the hyperoval, while those with axis equal to the line have axis external to the hyperoval. The stabiliser of the hyperoval is S_4 (see Theorem 41, p. 21). The elations with axis external to the hyperoval generate a Klein four group C_2^2. The elations with axis secant to the hyperoval generate the whole stabiliser. Each point not on the hyperoval is the centre of exactly three elations stabilising the hyperoval.

Let $\mathrm{Fix}(G)$ denote the configuration of fixed points and lines of the group G and let $\mathrm{Fix}(g)$ denote the configuration of fixed points and lines of the cyclic group generated by the element g.

Theorem 56 ([**9**]). *An involutory collineation, g, of a projective plane of order q is*

(i) *an elation and q is even; or*
(ii) *a homology and q is odd; or*
(iii) *a Baer collineation (that is,* $\mathrm{Fix}(g)$ *is a Baer subplane) and q is square.*

Proof. Every non-fixed line contains a fixed point (namely, the intersection of the line and its image under g). Thus, if the collineation is planar, then it is Baer. If it is not planar, then it is a generalised homology or a generalised elation (see page 31), and so it is a homology or an elation, by above. □

Theorem 57 ([**58**]). *If π is a projective plane of order $q \equiv 2 \pmod 4$ and if π possess a collineation of order two, then $q = 2$.*

Theorem 58 ([**111**]). *An elation stabilising a hyperoval has centre not on the hyperoval and, if the plane has order greater than two, has axis secant to the hyperoval.*

Proof. By the proof of Theorem 55, the centre is not on the hyperoval. By Theorems 55 and 57, the order of the plane is not congruent to 2 modulo 4 if it is bigger than 2. Thus, there are an odd number of secant lines on the fixed point not equal to the centre of the elation, from which it follows that the unique fixed line on this point (namely, the axis) is a secant line. □

Theorem 59. *A planar collineation fixing a hyperoval either has its fixed subplane disjoint from the hyperoval or they intersect in a hyperoval of the fixed subplane.*

Proof. If a fixed line contains a fixed point on the hyperoval, then it is a secant line, so it contains two fixed points. Thus the set of fixed points on the hyperoval is set of points of the fixed subplane of class $[0,2]$, so is either empty or a hyperoval. □

Example. A regular hyperoval in $PG(2,4)$ has stabiliser isomorphic to S_6 (see Theorem 42, p. 21). It has three types of involutions in its stabiliser: Baer involutions fixing no points of the hyperoval, Baer involutions fixing four points of the hyperoval and elations fixing two points of the hyperoval. Each point not on the hyperoval is the centre of exactly three elations stabilising the hyperoval.

THEOREM 60 ([**15**]). *Two distinct nonidentity elations stabilising a hyperoval in a projective plane of order q with $q > 4$ have distinct centres.*

PROOF. If not, then, for each secant line on the common centre that is not the axis of either of the elations, the points of secancy are interchanged by both elations, so their product fixes an arc of size at least $q - 2$ which is greater than $\sqrt{q} + 2$, so lies in no proper subplane. Thus their product is the identity, contrary to their being distinct. □

THEOREM 61 ([**15**]). *Two distinct Baer involutions fixing a hyperoval have distinct fixed planes.*

PROOF. If not, any point P of the hyperoval not in the common fixed subplane has the line joining it and its image (under either of the involutions) in the subplane. This is a secant line and the image of P under each involution must therefore be the other point of secancy, so P is fixed by the product of the involutions; thus the fixed configuration of the product of the involutions is the whole plane, that is, the product is the identity, that is, the involutions are not distinct. □

THEOREM 62 ([**113**]). *The product of two involutorial elations, the centre of each of which is not incident with the axis of the other, fixes no point not on the line joining the two centres and not equal to the intersection of the two axes.*

PROOF. Suppose not and let g be the product of the two involutions. Then, since the intersection P of the axes, the line l joining the centres, and some point Q not on the line are fixed by g, g fixes the line $m = PQ$, and so the point R of intersection of l and m. Thus g fixes three collinear points on m. It follows that if g is not planar, then m is the unique line containing more than two fixed points of g. The elations invert g, but do not both fix m, so g is planar. Thus the elations fix the fixed subplane π_0 of g. They induce involutions of π_0 with all fixed points collinear, so these must be elations. But these induced involutions commute, contrary to the original hypothesis and the axes and centres. □

THEOREM 63 ([**113**]). *The group H generated by the product of two involutorial elations g and h, the centre of each of which is not incident with the axis of the other, acts semiregularly on the points not on the line joining the two centres and not equal to the intersection of the two axes.*

PROOF. Let G be the group generated by g and h. Then G is a dihedral group with H as a cyclic subgroup of index 2. Each nonidentity element of H is the product of two distinct elements of G that are not in H. Each of the elements of G that are not in H are involutions that are conjugate either to g or to h, and so are elations.

Moreover, any two such have the property that the centre of each of them is not incident with the axis of the other. Thus Theorem 62 applies, and any nonidentity element of H fixes no point not on the line joining the two centres and not equal to the intersection of the two axes. □

THEOREM 64 ([**113**]). *The product of two involutorial elations g and h of a projective plane of order q, the centre of each of which is not incident with the axis of the other, has order dividing $q^2 - 1$ and not equal to one.*

PROOF. This follows from Theorem 63. □

THEOREM 65 ([**15**]). *If two distinct elations stabilise a hyperoval in a plane of order q, then one of the following situations occurs:*

(i) *the elations have different centres but the same axis, which is a secant line to the hyperoval, and the product of the two elations is an involutory elation with the same axis but a different centre; or*

(ii) *the axes are distinct and meet at a point of the hyperoval, the centres are distinct and the line joining the centres is*

  (a) *a secant line and the product of the elations has order dividing $q - 1$; or*

  (b) *an external line, and the product of the elations has order dividing $q + 1$; or*

(iii) *the axes are distinct secant lines which meet at a point not on the hyperoval, the centres are distinct and the line joining them is external to the hyperoval, the product of the elations has order 3, and q is congruent to 1 modulo 3; or*

(iv) *q is 2 or 4.*

PROOF. Suppose that $q > 4$, so that we are not in case (iv). Then by Theorem 58, p. 28, the axes are secant lines. If they are distinct, then, by Theorem 60, p. 29, they have different centres and case (i) arises. If they are distinct then their intersection is not the centre of either of the elations, as then, conjugating the first elation (which has centre the intersection of the two axes) by the second elation we obtain an elation with the same centre as the first elation but a different axis. Thus there would be two elations with the same centre fixing the hyperoval contrary to Theorem 60, p. 29. Now Theorems 63 and 64, apply, and the group generated by their product has order dividing $q^2 - 1$ and acts semi-regularly on the points of the hyperoval not on the line joining the centres and not the intersection of the axes. If the axes meet at a point of the hyperoval, then either the line joining the centres is secant and the order of the product divides $q - 1$ or the line joining the centres is external and the order of the product divides $q + 1$, which are cases (ii)(a) and (ii)(b), respectively. If the axes meet at a point not on the hyperoval, then the line joining the centres cannot be a secant line, for then the order of the product would be a nontrivial divisor of $q^2 - 1$ and q, which are coprime. So it is external and the order of the product is a nontrivial divisor of q^2-1 and $q+2$, from which it follows that it is 3 and that q is congruent to 1 modulo 3. This is case (iii). □

The examples after Theorems 55, p. 27 and Theorem 59, p. 28 show that case (iv) in the above theorem is genuinely exceptional.

EXAMPLES. (i) Translation hyperovals and semi-translation hyperovals (see Section 3.1, p. 27) give examples of (i) of Theorem 65.

(ii) Regular hyperovals in Desarguesian plane give examples of (ii)(a) of Theorem 65.

(iii) Regular hyperovals and the first class of Subiaco hyperovals (see Section 9, p. 149), for $q=4^e$, e odd, give examples of (ii)(b) of Theorem 65.

(iv) The regular hyperoval in $PG(2,4)$ and the Lunelli-Sce hyperoval (see Section 9, p. 149) in $PG(2,16)$ give examples of (iii) of Theorem 65.

THEOREM 66 ([**15**][**105**]). *If q is not congruent to* 1 *modulo* 3 *and not equal to* 2 *then there is no hyperoval in a projective plane of order q which is stabilised by three elations whose axes form a triangle.*

PROOF. In these cases, (i), (iii) and (iv) cannot apply to any two of these elations, so that (ii) holds (referring to the cases in Theorem 65). But now two of the elations generate a dihedral group containing an odd number of elations, all with distinct axes, all meeting at a point on the hyperoval; the third elation cannot have axis meeting all of these axes on the hyperoval. □

THEOREM 67 ([**113**]). *In a group of a projective plane of order $q>4$ containing involutory elations and fixing no point or line all elations are conjugate.*

Let $g \in \operatorname{Aut}\pi$, with $t+1$ fixed points on l and $t+1$ fixed lines on C, with $C \notin l$. Then g is a **generalised homology (of order t)**. We say g has **pseudo-axis** l and **pseudo-centre** C. If $t=2$ then the centre and axis are not unique for a generalised homology. Similarly we can define a **generalised elation (of order t)** with centre C incident with axis l. Note, the terms centre and axis have different meanings here to those on page 26, but the context will make it clear which definition we will be using.

THEOREM 68 ([**105**], cf Theorem 52, p. 27). *Any nonidentity generalised homology of prime order stabilising a hyperoval in a projective plane of order q has at most $(q+2)/2$ fixed points. If it has more than three fixed points, then it has order* 3, *and q is congruent to* 1 *modulo* 3.

PROOF. A generalised homology of a projective plane containing a hyperoval has odd order. Thus, if the generalised homology is not the identity, every orbit of points on a fixed line that is not just a fixed point contains a triple of collinear points. If the generalised homology has more than three fixed points then it has unique centre and axis, the centre is not on the hyperoval and the axis is external to the hyperoval. (If the centre were on the hyperoval, then each fixed line on the centre would be secant to the hyperoval, so each fixed point of the axis would be on the hyperoval, so the axis would meet the hyperoval in more than two points. So the centre is not on the hyperoval, making the fixed lines on the centre external, and so the axis external.) There are $(q+2)/2$ secant lines on the centre, none of which are fixed. So there are at most $q/2$ fixed lines on the centre, giving at most $(q+2)/2$ fixed points. The group generated by the generalised homology acts semi-regularly on the $(q+2)/2$ secant lines through the centre. Thus the generalised homology has order 3, since a generalised homology of prime order has order dividing $q-1$. □

Example ([**112**]). In the dual Hall plane of order 16, there is a hyperoval stabilised by a generalised homology of order 3 with 6 fixed points. The full stabiliser is dihedral of order 6 with the involutions being Baer. In the dual Dempwolff plane of order 16, there is a hyperoval stabilised by a generalised homology of order 3 with 9 fixed points, which gives equality in the bound. The full stabiliser is cyclic of order 6 with the involution being Baer. In the semifield plane of order 16 with kernel $GF(2)$, there is a hyperoval stabilised by a generalised homology of order 3 with 6 fixed points. In this case, the full stabiliser has order 3. These are the only hyperovals in the known planes of order 16 stabilised by generalised homologies with more than three fixed points.

Theorem 69 (cf [**78**]). *Let $\mathcal{H}$ be a hyperoval in a projective plane π of order q, q even, and let $G = (\mathrm{Aut}\,\pi)_{\mathcal{H}}$. The ovals obtained by deleting the points P and Q of $\mathcal{H}$ are equivalent if and only if P and Q lie in the same orbit of G in $\mathcal{H}$.*

Proof. Straightforward. □

Theorem 70 (cf [**78**]). *Let $\mathcal{O}$ be an oval of projective plane π of order q, q even, with nucleus N, so that $\mathcal{H} = \mathcal{O} \cup \{N\}$. Let $G = (\mathrm{Aut}\,\pi)_{\mathcal{H}}$ and suppose that the orbit of G on $\mathcal{H}$ which contains N has n points. Then the stabiliser J in $\mathrm{Aut}\,\pi$ of $\mathcal{O}$ has order $|G|/n$.*

3.2. Collineations of $PG(2,q)$

$P\Gamma L(3,q)$ acts faithfully on $PG(2,q)$. We have $PGL(3,q)$ being regular on ordered 4-arcs in $PG(2,q)$, and $PGL(2,q)$ being sharply 3-transitive on points of $PG(1,q)$. In fact, $PGL(n,q)$ is 2-transitive on points of $PG(n-1,q)$

The stabiliser of any three distinct points of $PG(1,q)$ in $PGL(2,q)$ is trivial.

Theorem 71 ([**36**]). *If a homography of $PG(2,q)$ fixes three collinear points then it fixes every point on the line joining them.*

Proof. Let l be a line in $PG(2,q)$. Then we have

$$PGL(3,q)_l^l \cong PGL(2,q)^{PG(1,q)} \cong PGL(2,q)_{PG(1,q)}^{PG(1,q)}.$$

We have for a line l, $PGL(3,q)_l^l$ is sharply 3-transitive on the points of l. So if $h \in PGL(3,q)_l^l$ fixes three distinct points of l, then $h = 1$. So if $h \in PGL(3,q)_l$ fixes three distinct points of l, then h has an axis. If $h \in PGL(3,q)$ fixes three collinear points, then h has axis l. □

So we can say that if h is a non-trivial homography its fixed configuration does not contain a quadrangle.

Let $A \in PGL(3,q)$. We would like to know what is the image of the line $[a,b,c]$ under A. Now

$$\begin{aligned}(x,y,z) \ \mathrm{I}\ [a,b,c] &\iff ax+by+cz=0\\ &\iff \begin{pmatrix} a & b & c\end{pmatrix}\begin{pmatrix} x\\ y\\ z\end{pmatrix} = 0\end{aligned}$$

Since collineations preserve incidence we have $(x,y,z)\ \mathrm{I}\ [a,b,c]$ if and only if $A(x,y,z)\ \mathrm{I}\ A[a,b,c]$. Let $A(x,y,z) = (x',y',z')$, so $(x,y,z) = A^{-1}(x',y',z')$. So

$$\begin{aligned}\begin{pmatrix} a & b & c\end{pmatrix}\begin{pmatrix} x\\ y\\ z\end{pmatrix} = 0 &\iff (x',y',z')\ \mathrm{I}\ A[a,b,c]\\ &\iff \begin{pmatrix} a & b & c\end{pmatrix} A^{-1}\begin{pmatrix} x'\\ y'\\ z'\end{pmatrix} = 0.\end{aligned}$$

Hence $A[a,b,c]$ is defined to be $\begin{pmatrix} a & b & c\end{pmatrix} A^{-1}$. So the action of $GL(3,q)$ on the dual of $PG(2,q)$ is via A^{-T}.

A **flag** is an incident point-line pair. An **antiflag** is a nonincident point-line pair.

We have $PGL(3,q)$ being transitive on flags of $PG(2,q)$. The centre and axis of an elation is a flag hence without loss of generality the flag is $((0,1,0),[1,0,0])$ up to conjugation.

Theorem 72.

$$G = \left\{ \begin{pmatrix} 1 & 0 & 0\\ a & 1 & 0\\ 0 & 0 & 1\end{pmatrix} \mid a \in GF(q) \right\},$$

is the set of all elations with centre $(0,1,0)$ *and axis* $[1,0,0]$. *G is transitive on the q points of* $[1,0,0]$ *not equal to* $(0,1,0)$.

Proof. We have (x, y, z) I $[1, 0, 0]$ if and only if $x = 0$, and

$$\begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ y \\ z \end{pmatrix},$$

so $[1, 0, 0]$ is the axis.

Now $(0, 1, 0)$ I $[d, e, f]$ if and only if $e = 0$. So we look at the points on the lines $[d, 0, f]$. Since (x, y, z) I $[d, 0, f]$ if and only if $dx + fz = 0$ and elements of G take (x, y, z) to $(x, ax+y, z)$, we have (x, y, z) I $[d, 0, f]$ if and only if $(x, ax+y, z)$ I $[d, 0, f]$. So the lines $[d, 0, f]$ are fixed, that is, $(0, 1, 0)$ is the centre.

Let a, $b \in GF(q)^*$. Then

$$\begin{aligned} \begin{pmatrix} 1 & 0 & 0 \\ 0 & b/a & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & b/a & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-1} &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & b/a & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & a/b & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 \\ b & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \quad \square \end{aligned}$$

The above proof shows that all non-identity elations are conjugate.

By the above techniques we can see that the map

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

has centre $(0, a, b)$ and axis $[1, 0, 0]$. Hence

$$\left\{ \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & 0 & 1 \end{pmatrix} \;\middle|\; a,\ b \in GF(q) \right\} = AGL(3, q)_{([1,0,0])}.$$

Let

$$U = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{pmatrix} \;\middle|\; a,\ b,\ c \in GF(q) \right\}.$$

Since $|U| = q^3$ then $U \in \mathrm{Syl}_p(PGL(3, q))$, where $q = p^e$, with U fixing a unique flag $((0, 0, 1), [1, 0, 0])$. Hence

$$\begin{aligned} N_{PGL(3,q)}(U) &= \left\{ \begin{pmatrix} \lambda & 0 & 0 \\ a & \mu & 0 \\ b & c & \nu \end{pmatrix} \;\middle|\; a,\ b,\ c \in GF(q),\ \lambda,\ \mu,\ \nu \in GF(q)^* \right\} \\ &= PGL(3, q)_{(0,0,1),[1,0,0]}. \end{aligned}$$

The subgroup of Aut $PG(2, q)$ generated by the collection of all elations is $PSL(3, q)$.

$PGL(3,q)$ is transitive on antiflags. As the centre and axis of a homology is an antiflag, we can without loss of generality let the antiflag be $((1,0,0),[1,0,0])$. Then

$$\left\{ \begin{pmatrix} \lambda & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; \lambda \in GF(q)^* \right\}$$

is all such homologies. All homologies of order r with $r \,|\, q-1$ are conjugate.

EXAMPLE (Generalised Homologies in $PG(2,q)$). Let $\alpha \in \operatorname{Aut} GF(q)$ and $\alpha \neq \mathrm{id}$. Then

$$g\colon \begin{pmatrix} x \\ y \\ z \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \lambda \end{pmatrix} \begin{pmatrix} x^\alpha \\ y^\alpha \\ z^\alpha \end{pmatrix}$$

with $\lambda \neq 1$ is a generalised homology (except when it's planar for $\alpha = 2$ and $q = 4$) with pseudo-axis $[0,0,1]$ and pseudo-centre $(0,0,1)$ with the fixed points on the axis being

$$\{(1,t,0) \mid t^\alpha = t\} \cup \{(0,1,0)\}.$$

So g has $2+q_0$ fixed points and $2+q_0$ fixed lines if

$$\alpha\colon x \mapsto x^{q_0}.$$

Claim: All generalised homologies with more than three fixed points in $PG(2,q)$ are conjugate to one of these. Proof: Without loss of generality let h have axis $[0,0,1]$ and centre $(0,0,1)$, and greater than three fixed points. Since there exist three collinear fixed points we have $h^{[0,0,1]} \in P\Gamma L(2,q)$ fixing at least three points. Without loss of generality $(1,0,0)$, $(0,1,0)$, $(1,1,0)$ are fixed (by the results on page 32). Hence $h^{[0,0,1]}\colon (x,y,0) \mapsto (x^\alpha, y^\alpha, 0)$ for some $\alpha \in \operatorname{Aut} GF(q)$ and since h is not a homology then $\alpha \neq 1$. We have

$$\ker P\Gamma L(3,q)^{[0,0,1]}_{(0,0,1),[0,0,1]} = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \lambda \end{pmatrix} \mid \lambda \in GF(q)^* \right\}.$$

So

$$h\colon \begin{pmatrix} x \\ y \\ z \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \lambda \end{pmatrix} \begin{pmatrix} x^\alpha \\ y^\alpha \\ z^\alpha \end{pmatrix},$$

for some $\lambda \in GF(q)^*$ and $\lambda \neq 1$.

THEOREM 73 ([**37**]). *In $PG(2,q)$. We have $D_{2(q+1)} \leq PGL(2,q)$.*

THEOREM 74 ([**84**]). *Let $\mathcal{K}$ be a $(q+1)$-arc in $PG(2,q)$, q even, and suppose that $\mathcal{K}$ has a transitive homography stabiliser. Then it is a nondegenerate conic.*

We make use of the below theorem constantly through Section 8, p. 55.

LEMMA 75 ([**84**]). *Let J be a cyclic subgroup of order $q+1$, q even, of $P\Gamma L(3,q)$. Suppose that J fixes a point and fixes a line not on the point. Then the orbits of J on the points of $PG(2,q)$ are the fixed point, the fixed line and $q-1$ nondegenerate conics.*

PROOF. The stabiliser K in $PGL(3,q)$ of a non-incident point-line pair in $PG(2,q)$ is isomorphic to $GL(2,q)$. Now a cyclic subgroup of $GL(2,q)$ of order $q+1$ induces a cyclic subgroup of $PGL(2,q)$ of order $q+1$, as $(q-1, q+1) = 1$. By inspection of Dickson's list of subgroups of $PGL(2,q)$ [**37**] we see that any two cyclic subgroups of order $q+1$ of $PGL(2,q)$ are conjugate. Since q is even, this forces any two cyclic subgroups of order $q+1$ of $GL(2,q)$ to be conjugate. For if $K_1 = \langle k_1 \rangle$ and K_2 are subgroups of order $q+1$, conjugate in $PGL(2,q)$, there exists $g \in PGL(2,q)$, $k_2 \in K_2$ and $\lambda \in GF(q)$ such that $g^{-1}k_1 g = \lambda k_2$. Since k_1 and k_2 have order $q+1$, it follows that $\lambda^{q+1} = \lambda^2 = 1$ so that $\lambda = 1$. Since $PGL(3,q)$ is transitive on antiflags, any two antiflags have conjugate stabilisers. Hence any two cyclic subgroups of order $q+1$ of $PGL(2,q)$ which fix an antiflag are conjugate, so any two cyclic subgroups of order $q+1$ of K are conjugate (since $K \cong GL(2,q)$).

It is therefore enough to display a cyclic subgroup of order $q+1$ of $PGL(3,q)$, q even, whose orbits on $PG(2,q)$ are a point, a line and $q-1$ nondegenerate conics. We consider the following pencil of conics:

$$\lambda(x^2 + axy + y^2) + \mu z^2 = 0$$

for λ, $\mu \in GF(q)$, not both zero and $\mathrm{trace}(1/a) = 1$. The degenerate conic given by $\mu = 0$ is the point $(0,0,1)$ and the degenerate conic given by $\lambda = 0$ is the line $z = 0$. The other $q-1$ conics of the pencil are nondegenerate. The $q+1$ conics of the pencil are pairwise disjoint and cover $PG(2,q)$.

Let F be the following set of homographies:

$$f = \left\{ \begin{pmatrix} f & g & 0 \\ g & f+ag & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid f,\ g \in GF(q),\ \text{not both zero} \right\}.$$

A conic of the pencil is fixed by an element of F provided the matrix has determinant $f^2 + afg + g^2 = 1$. Now F is a cyclic subgroup of order q^2-1 of $GL(3,q)$, since the 2×2 submatrices formed by the first two rows and columns form a field under addition and multiplication of matrices (adjoining the zero matrix), so they form a cyclic group under multiplication. But these 2×2 matrices determine the multiplicative structure of F. Thus $F \cap SL(3,q)$ is a cyclic subgroup of order $q+1$ of $GL(3,q)$ (as it is the kernel of the homomorphism defined by the determinant map, which is onto $GF(q)^*$ as can be seen by considering the matrices with $g = 0$). So $F \cap SL(3,q)$ gives rise to a cyclic subgroup of order $q+1$ of $PGL(3,q)$. Also, J has orbits on the points of $PG(2,q)$ a point, a line and $q-1$ nondegenerate conics, as required. $\square$

LEMMA 76 (T. Penttila, private communication). *Up to conjugacy, there is a unique cyclic subgroup of $PGL(3,q)$ of order $q+1$ for q odd. It's orbits are: a point C, two orbits of length $(q+1)/2$ together forming a line l, and $q-1$ nondegenerate conics, with respect to each of which C and l are the pole-polar relationship.*

PROOF. Existence: The stabiliser of a nondegenerate conic in $PGL(3,q)$ is isomorphic to $PGL(2,q)$, which has a cyclic subgroup of order $q+1$ by Singer's Theorem 54, p. 27.

Uniqueness: As $q+1$ is even, so a cyclic subgroup G of that order contains and centralises an element of order 2 which must be a homology. Hence it fixes the centre C and the axis l of the homology. Since $(q-1, q+1) = 2$, the kernel of the action on l has order 2, so the group induced on l has order $(q+1)/2$. By Dickson's List [**37**], there is, up to conjugacy, a unique cyclic subgroup of $PGL(2,q)$ of order $(q+1)/2$, and it follows that G is determined up to conjugacy.

Orbits: The stabiliser of an internal point in the stabiliser of a conic is dihedral of order $2(q+1)$ and so contains a cyclic subgroup of order $q+1$, which is transitive on the conic, fixes the internal point C and its polar line l and has two orbits of length $(q+1)/2$ on that polar line.

Identifying $GF(q^2)$ with $AG(2,q)$ we see that there is a cyclic subgroup of $PGL(3,q)$ of order q^2-1, fixing a point C, a line l and transitive on the points of the plane other than C and l. Hence all orbits of a cyclic group of order $q+1$, other than C and the two orbits on l, are nondegenerate conics. □

3.3. Fixed configurations for $PGL(3,q)$

Let g be a non-trivial homography of $PG(2,q)$ and let $|g| = r$. If there exists a triple of collinear fixed points of g then by Theorem 71, p. 32, g has an axis, and so centre. If the centre is on an axis then g is an elation and no further fixed points as then it would fix a quadrangle. If the centre is not on the axis then we have a homology. Otherwise, no three fixed points are collinear, and dually no three fixed lines are concurrent. So there are at most three fixed points, else we have a fixed quadrangle.

If we have three fixed points then we have the fixed configuration of Figure 1, a **triangle element**, and hence $r \mid q-1$.

If we have two fixed points then we have the configuration of Figure 2, and hence $r \mid q$ and $r \mid q-1$. Hence the order of the collineation cannot be a prime.

If we have one fixed point then we have the configuration of Figure 3. If we have no fixed points then we have the empty configuration and hence $r \mid q^2+q+1$.

NOTE. The above requires the use of homographies, as collineations have the counterexample of a subplane.

In Section 8, p. 55 we use the above results extensively.

3.4. Subgroups of $PGL(3,q)$

Let Y be a set of points of $PG(2,q)$ and let $H = P\Gamma L(3,q)_Y$, then $P\Gamma L(3,q)_{gY} = gHg^{-1}$ for $g \in P\Gamma L(3,q)$. Since g can be thought of as a **change of coordinates**, if we only study points up to a change of coordinates, then we only study their group of symmetries up to conjugation. If $r \,\big|\, |H|$, r prime, we have by Cauchy's Theorem 14, p. 5, there exists $R \leq H$ with $|R| = r$.

Suppose there are t conjugacy classes of subgroups of $P\Gamma L(3,q)$ of order r with representatives $R_1, \ldots, R_t$. Then $R = g^{-1}R_i g$ for some i. Hence gY has stabiliser gHg^{-1} with subgroup $gRg^{-1} = R_i$. So by changing coordinates we can assume that

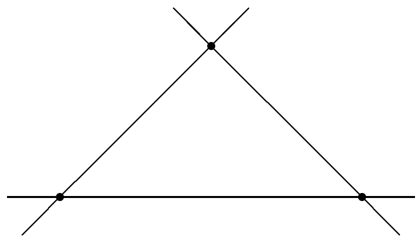

FIGURE 1.

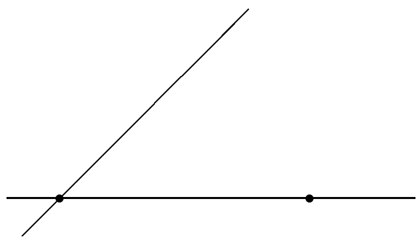

FIGURE 2.

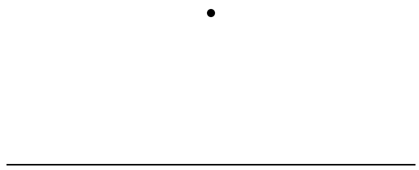

FIGURE 3.

Y has a stabiliser with subgroup R_i for some i. Note the above can be replaced by $PGL(3, q)$ since it is normal in $P\Gamma L(3, q)$.

Now suppose we have $T \leq H$. If we change coordinates by an element g we need to know if $T \leq gHg^{-1}$. Since it is possible that T may equal H we can only change coordinates with an element g such that $gTg^{-1} = T$, that is, by elements of $N_{P\Gamma L(3,q)}(T)$. See Section 8, p. 55, for motivation of the above few paragraphs.

THEOREM 77. *If r is a prime, $r \neq 3$, dividing $q^2 + q + 1$ then there is a unique conjugacy class of subgroups of $PGL(3, q)$ of order r^i for all i with $r^i \,\big|\, |PGL(3, q)|$.*

PROOF. From Singer's Theorem 54, p. 27, there exists a cyclic subgroup of $PGL(3, q)$ of order $q^2 + q + 1$ which is regular on points (and lines) of $PG(2, q)$. Hence a Sylow r-subgroup of $PGL(3, q)$ is cyclic, since $r \not| \; (q^2 + q)q^2(q - 1)^2$ as $r \neq 3$. If R_1 and R_2 are subgroups of $PGL(3, q)$ with $|R_1| = |R_2| = r^i$ for some i, then $R_1 \leq S_1$ and $R_2 \leq S_2$ with S_1, S_2 being Sylow r-subgroups of $PGL(3, q)$. So by Sylow's Theorem there exists a $g \in PGL(3, q)$ with $gS_1g^{-1} = S_2$. Hence $gR_1g^{-1} \leq S_2$ with $|gR_1g^{-1}| = r^i$. Since S_2 is cyclic it has a unique subgroup of order r^i, so $gR_1g^{-1} = R_2$. □

COROLLARY 78. *If r is a prime dividing $q + 1$, $r \neq 2$, then there is a unique conjugacy class of subgroups of order r^i for all i with $r^i \,\big|\, |PGL(3, q)|$.*

PROOF. By Singer's Theorem 54, p. 27, there exists a cyclic subgroup of $PGL(2, q)$ of order $q + 1$ and hence one of $PGL(3, q)$ of order $q^2 - 1$ and so has a subgroup of order $q + 1$. Hence a Sylow r-subgroup is cyclic since $r \not| \; (q^2 + q + 1)q^2(q - 1)^2$ as $r \neq 2$. Then proceed similar to the last part of the proof of Theorem 77. □

THEOREM 79. *If r is a prime dividing $q - 1$ then there is a unique conjugacy class of subgroups generated by homologies of order r^i for $r^i \,\big|\, q - 1$.*

PROOF. Without loss of generality we denote the centre as (1,0,0) and the axis as [1,0,0], this gives the homology, g, as

$$g = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

with $\lambda^{r^i} = 1$ and $\lambda^n \neq 1$ for $n < r^i$. Since $GF(q)^*$ is cyclic this determines $\langle g \rangle$. □

NOTE. If r is a prime dividing $q-1$ then there are about $(r-2)/6$ conjugacy classes of subgroups of order r with generators having three fixed points with representatives of the form

$$g_i = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda^i \end{pmatrix},$$

with $\lambda^r = 1$, $\lambda \neq 1$ and $i \neq 1, 0 \pmod{r}$. We have

$$g_i,\ g_{1-i},\ g_{1/i},\ g_{i/(i-1)},\ g_{1/(1-i)},\ g_{(i-1)/i},$$

generating groups conjugate to this, hence explaining the dividing by six part of the above note.

THEOREM 80. (i) *If $r = 3 \mid q^2+q+1$ then there exists a unique conjugacy class of subgroups of $PGL(3,q)$ of order 3 with generator having no fixed points.*

(ii) *If $r = 2 \mid q-1$ then there exists a unique conjugacy class of subgroups of $PGL(3,q)$ of order 2; this subgroup is generated by a homology.*

(iii) *If $r = p = 2$ then there exists a unique conjugacy class of subgroups of $PGL(3,q)$, where $q = p^e$, of order 2; it is generated by an elation.*

(iv) *If $r = p \neq 2$ then there exists two subgroups of $PGL(3,q)$, where $q = p^e$, of order p; one is generated by an elation and the other by an element having one fixed point.*

3.5. Polarities

A **correlation** of a projective plane is a permutation of the lines and points of the plane. A correlation is a collineation if it maps points to points and lines to lines, else it is a **duality** of the projective plane. If a duality has order two then it is a **polarity**.

THEOREM 81 ([**8**]). *A polarity Δ of a finite projective plane has absolute points. If the plane has order q then the number of absolute points is $(q+1) + r\sqrt{q}$ for some $r \in \mathbb{Z}$.*

PROOF. Label the points of the projective plane of order q as $P_1, \ldots, P_{q^2+q+1}$ and the lines $\Delta P_1, \ldots, \Delta P_{q^2+q+1}$. With this ordering let A be the incidence matrix of the plane so

$$A_{ij} = \begin{cases} 1 & \text{if } P_i \mathrel{\mathrm{I}} \Delta P_j \\ 0 & \text{if } P_i \mathrel{\not{\mathrm{I}}} \Delta P_j \end{cases}$$

Then A is symmetric since $P_i \mathrel{\mathrm{I}} \Delta P_j \iff \Delta P_i \mathrel{\mathrm{I}} \Delta^2 P_j \iff \Delta P_i \mathrel{\mathrm{I}} P_j$. The number of absolute points of Δ is $\operatorname{trace}(A)$. We find

$$\operatorname{trace}(A) = q + 1 + (q^2 + q - 2d)\sqrt{q}$$

where d is the multiplicity of the eigenvalue of $-\sqrt{q}$. □

THEOREM 82 ([**8**]). *Let $r \geq 0$. If q is not a square then $r = 0$. If $r = 0$ then*

(i) *If q is even the absolute points are the points of a non-absolute line l and the absolute lines are the lines concurrent to Δl.*

(ii) *If q is odd then the absolute points are the points of an oval and the absolute lines are the tangent lines to the oval.*

PROOF. Firstly we can not have two absolute points on an absolute line. Suppose P and Q are absolute points on an absolute line l. Let $Z \not\mathrm{I}\, l$. Then Z I ΔP and Z I ΔQ, so P I ΔZ and Q I ΔZ this implies that ΔZ I l, but l is absolute and $\Delta l \neq Z$.

Let P be an absolute point so P I ΔP. Let l be a line through P. Then Δl is on ΔP, so l is not absolute. Hence every absolute line lies on exactly one absolute point and dually.

Now we want to prove that the number of non-absolute points incident with a non-absolute line is even. Let l be a non-absolute line. Define a map, g, on the points of l by $g(P) = \Delta P \cap l$ where P I l. Then g is a permutation of order 2, since $g(P)$ I ΔP implies P I $\Delta g(P)$ we have $P = \Delta g(P) \cap l = g(g(P)) = g^2(P)$. The fixed points of g are the absolute points on l. So we have that there is an even number of non-absolute points on an non-absolute line.

Let q be even. Then every line has at least one absolute point. Hence there are at least $q+1$ absolute points in the plane. Suppose there are $q+1$ absolute points.

Let l be a line with a point P which is not absolute. Since q is even every line has at least one absolute point on it, different from P, and the lines have no absolute point in common. Hence every line on P contains exactly one absolute point. So if any point of a line is not absolute then that line only has one absolute point on it. Since two absolute points are on a line this line has all its points absolute. As this line has $q+1$ absolute points on it there are no other absolute points. So for q even the set of absolute points is a line.

Let q be odd. By Theorem 81, p. 40, there exists an absolute point P. Let l be a line on P different from ΔP. Since l has one absolute point already and l is non-absolute and $q+1$ is even then l has another absolute point. So there are at least $q+1$ absolute points.

Suppose there are $q+1$ absolute points. Then every line l on an absolute point P such that $l \neq \Delta P$ is on exactly two absolute points. As P was arbitrary we have that the set of absolute points is an oval, with the absolute lines being the tangent lines. □

4. Hyperovals in $PG(2,q)$

Since $P\Gamma L(3,q)$ is transitive on 4-arcs we can map a hyperoval $\mathcal{H}'$ to a hyperoval $\mathcal{H}$ containing the points $\{(0,0,1),(0,1,0),(1,0,0),(1,1,1)\}$, the fundamental quadrangle. We say any two sets, X_1, X_2, of points are **equivalent** if one is the image of another under some element of $P\Gamma L(3,q)$, and we write $X_1 \cong X_2$.

THEOREM 83 ([**55**]). *A hyperoval, $\mathcal{H}$, in $PG(2,q)$, q even, $q > 2$, is equivalent to*

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

such that f is a permutation polynomial with $f(0) = 0$ and $f(1) = 1$ *(see Section 5.1, p. 43)*.

When we can describe a hyperoval by such an f we say that f is an **o-polynomial** and the hyperoval is denoted $\mathcal{D}(f)$. We say o-polynomials are **equivalent** when their respective hyperovals are equivalent, and we write $f \cong g$ if f and g are equivalent.

THEOREM 84 ([**55**]). *Let f be a permutation polynomial of $GF(q)$ with $f(0) = 0$ and $f(1) = 1$. For $s \in GF(q)$ define a polynomial, f_s, on $GF(q)$ as $f_s(0) = 0$ and $f_s(x) = (f(x+s)+f(s))/x$ for $x \in GF(q)^*$. Then f is an o-polynomial when f_s is a permutation polynomial for all $s \in GF(q)$.*

THEOREM 85 ([**55**]). *If $\mathcal{D}(f)$ with $f(x) = \sum_{i=1}^{q-2} a_i x^i$ is a hyperoval in $PG(2,q)$, q even, $q > 2$, then $a_i = 0$ for i odd, that is*

$$f(x) = \sum_{j=1}^{\frac{q-2}{2}} a_{2j} x^{2j}.$$

THEOREM 86 ([**29**]). *Given f an o-polynomial, then the set of points $\mathcal{D}(f)$, under the following list of images of S_4 implicitly define o-polynomials equivalent to f where the maps are; (x,y,z) maps to:*

(a)	$(x+y,x,x+z)$	*(b)*	$(y+z,x+z,z)$	*(c)*	$(x+y,y,y+z)$
(d)	$(x,x+z,x+y)$	*(e)*	$(x+z,x+y,x)$	*(f)*	$(y+z,x+y,y)$
(g)	$(y,y+z,x+y)$	*(h)*	$(x+z,z,y+z)$	*(i)*	$(x,x+y,x+z)$
(j)	$(x+y,x+z,x)$	*(k)*	(z,x,y)	*(l)*	$(x+y,y+z,y)$
(m)	$(y+z,z,x+z)$	*(n)*	(z,y,x)	*(o)*	$(y,x+y,y+z)$
(p)	$(x+z,x,x+y)$	*(q)*	(x,z,y)	*(r)*	$(y+z,y,x+y)$
(s)	(y,z,x)	*(t)*	$(z,x+z,y+z)$	*(u)*	$(z,y+z,x+z)$
(v)	(y,x,z)	*(w)*	$(x+z,y+z,z)$	*(x)*	(x,y,z)

The maps (k), (n), (q), (s), (v) fix the point $(1,1,1)$; the maps (a), (c), (i), (o), (v) fix $(0,0,1)$; the maps (e), (n), (u), (w) fix $(0,1,0)$; the maps (c), (h), (l), (q), (w) fix $(1,0,0)$. The maps (c), (i), (n), (q), (v) and (w) are involutions. In particular, the following polynomials g are o-polynomials equivalent to a given o-polynomial f:

(i) $g(x) = f^{-1}(x)$, *by map (q),*
(ii) $g(x) = xf(x^{-1})$, $g(0) = 0$, *by map (v),*
(iii) $g(x) = f(x+1)+1$, *by map (i),*
(iv) $g(x) = (x+1)f((x+1)^{-1})+1$, $g(1) = 1$, *by map (o),*
(v) $g(x) = x + xf(1+x^{-1})$, $g(0) = 0$, *by map (a),*
(vi) $g(x) = x + (x+1)f(x(x+1)^{-1})$, $g(1) = 1$, *by map (c).*

as well as with each of the above with f replaced with f^{-1}, which are arrived by the maps (x), (k), (d), (t), (p) and (h), respectively.

When an o-polynomial $f(x) = x^k$ for some k we denote the hyperoval of f as $\mathcal{D}(k)$.

THEOREM 87 ([**55**]). *If $\mathcal{D}(k)$ is a hyperoval then $(k, q-1) = (k-1, q-1) = 1$ and*

$$\mathcal{D}(k) \cong \mathcal{D}(1-k) \cong \mathcal{D}(k^{-1}) \cong \mathcal{D}(1-k^{-1}) \cong \mathcal{D}((1-k)^{-1}) \cong \mathcal{D}(k(k-1)^{-1}).$$

PROOF. k, $1-k$, k^{-1}, $1-k^{-1}$, $(1-k)^{-1}$, $k(k-1)^{-1}$ are integers modulo $q-1$. As $(k, q-1) = 1$, k^{-1} is well-defined, and as $(k-1, q-1) = 1$, then $(1-k)^{-1}$ and $(k-1)^{-1}$ are well-defined.

From Theorem 86 use the maps (v), (q), (k), (s), and (n). □

COROLLARY 88 ([**55**]). *Let $\mathcal{D}(k)$ be a hyperoval. Then it is regular if and only if $k = 2$, $1/2$ or -1.*

THEOREM 89 ([**81**]). *When $q \geq 8$ the $q+2$ equivalent o-polynomials representing a regular hyperoval are exactly*

(i) *the 3 monomials x^2, $x^{1/2}$, x^{-1},*
(ii) *the $q-1$ polynomials*

$$g_s(x) = \sum_{i=1}^{(q-2)/2} (s+1)s^{2i-1}x^{2i},$$

for $s \in GF(q)^*$.

COROLLARY 90 ([**55**]). *The only ovals of $PG(2,8)$ are translation ovals (in fact, conics and pointed conics).*

LEMMA 91. *A hyperoval in $PG(2,q)$, $q = 2^e$, is represented by an o-polynomial written over $GF(q_0)$, $q_0 = 2^h$, if and only if it is stabilised by the group of order e/h generated by*

$$(x, y, z) \mapsto (x^{q_0}, y^{q_0}, z^{q_0}).$$

5. Glynn's Inequality

5.1. Lagrange Interpolation

Let $g\colon GF(q) \to GF(q)$ be any function. Then g corresponds to a unique polynomial f over $GF(q)$ and of degree less than or equal to $q-1$. Then $f(t) = \sum_0^{q-1} a_i t^i$ with

$a_i \in GF(q)$, where $a_0 = g(0)$, $a_r = -\sum_{x\in GF(q)^*} g(x)x^{-r}$ for $1 \le r \le q-2$, and $a_{q-1} = -\sum_{x\in GF(q)} g(x)$. This is known as **Lagrange interpolation**.

We use the techniques of Lagrange interpolation to generate polynomial functions. The concept of delta functions is used to construct the polynomials from the given data (used in Section 9, p. 62). To think of a polynomial as a function is to think of a ring homomorphism, ϕ, from $GF(x)[x]$ to $GF(q)^{GF(q)}$ with kernel $(x^q - x)$ (see Section 5, p. 9, Chapter I). Now $f(t) = 0$ for all t if and only if $x - t \mid f(x)$ for all t if and only if $\prod_{t\in GF(q)}(x-t) \mid f(t)$. If $h(x) = x^q - x$ then $h(t) = 0$ for all $t \in GF(q)$ so h is in the kernel of ϕ. So $\prod_{t\in GF(q)}(x-t) \mid h(t)$. Hence $x^q - x = \prod_{e\in GF(q)}(x-t) = x\prod_{e\in GF(q)^*}(x-t)$ gives that $x^{q-1}-1 = \prod_{t\in GF(q)^*}(x-t)$, hence we have $\prod_{t\in GF(q)^*}(-t) = -1$.

Define the **delta function** as

$$\delta_b(t) = \begin{cases} 0 & \text{if } t \ne b, \\ 1 & \text{if } t = b. \end{cases}$$

Now $g(x) = (x^q - x)/(x-b)$ implies that $g(t) = 0$ if $t \ne b$. From above, we have

$$g(b) = \prod_{\substack{t\in GF(q)\\ t\ne b}} (b-t) = \prod_{c\in GF(q)^*} c = -1.$$

Hence $\delta_b = -g$, that is,

$$\delta_b(x) = -\left(\frac{x^q - x}{x-b}\right).$$

For q even, if $b \ne 0$ we have

$$\delta_b(x) = x^{q-1} + bx^{q-2} + \cdots + b^{q-2}x,$$

and if $b = 0$ then

$$\delta_0(x) = x^{q-1} + 1.$$

5.2. Glynn's inequality

Define a partial ordering $\precsim$ on the set of integers $N_q = \{n \mid 0 \le n \le q-1\}$, with $q = 2^e$, with $a, b \in N_q$ as

$$a \precsim b \iff a = \sum_0^{r-1} a_i 2^i,\ b = \sum_0^{r-1} b_i 2^i$$
$$\text{with } a_i, b_i \in \{0,1\} \text{ for all } i, \text{ and } a_i \le b_i \text{ for all } i.$$

In other words $a \precsim b$ if and only if all terms appearing in the binary expansion of a also appear in the binary expansion of b. This is Glynn's [**44**] partial ordering.

Result 92. If $k \in \mathbb{Z}$ then the expansion of

$$(1+t)^k \pmod{t^q - t} \text{ over } GF(q)$$

is calculated as follows:

1st: If $k = 0$ then $(1+t)^k = 1$.

2nd: If $k \neq 0$, let $k = k \pmod{q-1}$ so $1 \leq k \leq q-1$, then

$$(1+t)^k = \sum_{\substack{c \precsim k \\ c \in N_q}} t^c \pmod{t^q - t}.$$

Theorem 93 ([**44**]). *$\mathcal{D}(k)$ is a hyperoval of $PG(2,q)$ if and only if $d \not\precsim kd$, for all $d \in \{1,2,\ldots,q-2\}$, where dk is reduced modulo $q-1$ to lie in N_q.*

Proof. Let $k \in \{1,2,\ldots,q-2\}$ and $(k,q-1) = (k-1,q-1) = 1$. Then

$$\begin{aligned}
&\mathcal{D}(k) \text{ is a hyperoval of } PG(2,q) \\
&\iff f_k(t) = \frac{(t+1)^k + 1}{t} \text{ is a permutation polynomial} \\
&\iff [f_k(t)]^r \pmod{t^q - t} \text{ has zero coefficient for } t^{q-1} \\
&\qquad\qquad \text{for all } r \in \{1,\ldots,q-2\} \\
&\iff \sum_{\lambda \in GF(q)^*} ((\lambda+1)^k + 1)\lambda^{-1})^r = 0 \text{ for all } r \in \{1,\ldots,q-2\} \\
&\iff \text{coefficients of } t^r \text{ in } ((t+1)^k+1)^r \text{ is zero for all } r \in \{1,\ldots,q-2\} \\
&\iff \sum_{d \precsim r} (t+1)^{kd} \text{ has zero coefficient for } t^r \text{ for all } r \in \{1,\ldots,q-2\} \\
&\iff \sum_{d \precsim r} \sum_{g \precsim kd} t^g \text{ has zero coefficient for } t^r \text{ for all } r \in \{1,\ldots,q-2\} \\
&\iff \sum_{d \precsim r \precsim kd} t^r = 0 \text{ for all } r \in \{1,\ldots,q-2\} \\
&\iff |\{d \mid d \leq r \leq kd\}| \cong 0 \pmod 2 \text{ for all } r \in \{1,\ldots,q-2\} \\
&\iff d \not\precsim kd \text{ for all } d \in \{1,\ldots,q-2\}.
\end{aligned}$$

Now $d \not\precsim kd$ for all $d \in \{1,\ldots,q-2\}$ implies that $(k,q-1) = (k-1,q-1) = 1$, since if $(k,q-1) = l \neq 1$, then $m = (q-1)/l$ satisfies $m \in \{1,\ldots,q-2\}$ and $mk \cong q-1 \pmod{q-1}$. Hence $m \precsim mk$. Similarly if $(k-1,q-1) = n \neq 1$ then $p = (q-1)/n$ satisfies $p(k-1) \cong 0 \pmod{q-1}$. Hence $p \cong pk \pmod{q-1}$ and so $p \precsim pk$, $p \in \{1,\ldots,q-2\}$. ☐

Theorem 94 ([**44**]). *A polynomial f of degree at most $q-2$ satisfying $f(0) = 0$ and $f(1) = 1$ is an o-polynomial if and only if the coefficient of x^c in $f(x)^b \pmod{x^q - x}$ is zero for all pairs of integers (b,c) satisfying $1 \leq b \leq c \leq q-1$, $b \neq q-1$, and $b \precsim c$.*

THEOREM 95 ([**81**]). *Let* $f(x) = \sum_{i=1}^{q-2} a_x x^i$ *and suppose that* $\sum_{i=1}^{q-2} a_i = 1$. *Then* f *is an o-polynomial if and only if for all* b *with* $1 \le b \le q-2$ *and all* c *with* $b \precsim c$

$$\sum \prod_{k=1}^{n} a_{i_k}^{\alpha_k} = 0,$$

where $b = \alpha_1 + \cdots + \alpha_n$, *the* α_j *are distinct powers of* 2 *and the sum is over all* i_k *with* $c = \sum_{k=1}^{n} i_k \alpha_k \pmod{q-1}$.

PROOF. Straightforward, use Theorem 94. □

6. Known Hyperovals

We list the known hyperovals immediately and go into further detail later.

Regular: Discussed in Section 2, p. 18, and on page 46.
Translation: See page 47.
Lunelli-Sce: See page 47.
Segre-Bartocci: See page 49.
Glynn: See page 50.
Payne: See page 50.
Cherowitzo: See page 51.
O'Keefe-Penttila: See page 53.
Irregular hyperovals in $PG(2,64)$: See page 54 for the two constructed by Penttila and Pinneri and page 67 for the hyperoval constructed by Penttila and Royle.
Subiaco: See page 108 and page 149.
Cyclic q–clan: See page 68 for the one constructed in $PG(2,256)$ by Penttila and Royle, and page 121 for those constructed by cyclic q–clans in $PG(2,q)$ for $q = 256$, 1024, 4096 and 16384.

We now go into some detail for the above hyperovals.

6.1. Regular hyperovals

We continue our investigation of the regular hyperovals from Section 2, p. 18.

THEOREM 96 ([**81**]). *If* $q = 2$, 4 *or* 8 *then every hyperoval is a regular hyperoval.*

PROOF. For $q = 2$ see Theorem 41 and for $q = 4$ see Theorem 42, p. 21.

We prove that every hyperoval in $PG(2,8)$ is regular by showing each o-polynomial describes a regular hyperoval. For $q = 8$ an o-polynomial will have degree being 2, 4 or 6 by Theorem 85, p. 42.

For $f(x) = a_2x^2$ we have $f(1) = 1$ so $a_2 = 1$, hence $f(x) = x^2$, and so equivalent to $\mathcal{D}(2)$.

For $f(x) = a_2x^2 + a_4x^4$ with $a_4 \neq 0$ we have as $f(x) = 0$ implies $x = 0$ so $a_2 = 0$; with $f(1) = 1$ we have $a_4 = 1$.

For $f(x) = a_2x^2 + a_4x^4 + a_6x^6$ with $a_6 \neq 0$ we have $a_2 + a_4 + a_6 = 1$. Consider the equations of Theorem 95, for the cases $b = 3$, $c = 3$ and $b = 3$, $c = 7$, which are

$$a_4^2a_2 + a_2^2a_6 = 0 \text{ and } a_6^2a_2 + a_4^2a_6 = 0$$

respectively. There are 10 solutions (a_6, a_4, a_2) with $a_6 + a_4 + a_2 = 1$ to this system of equations. This can be seen by noting that the system can be rewritten as

$$(a_4^2 + a_2a_6)a_2 = 0 \text{ and } (a_4^2 + a_2a_6)a_6 = 0$$

so that the solutions are the point $(0, 1, 0)$ together with the points of the conic $a_4^2 = a_2a_6$. Since Theorem 89, p. 43, constructs 10 o-polynomials representing regular hyperovals, it follows that they are the only o-polynomials for $PG(2, 8)$. $\square$

6.2. Translation hyperovals

The first irregular hyperovals to be found were the **translation** hyperovals [**117**] equivalent to $\mathcal{D}(2^i)$ where $(i, e) = 1$ with $1 < i$ and since $\mathcal{D}(2^i) \cong \mathcal{D}(2^{e-i})$, we have $i < \frac{e}{2}$. A translation hyperoval has a stabiliser in $P\Gamma L(3, q)$, $q = 2^e$, of order $q(q-1)e$.

Note that this is a translation hyperoval under the definition on page 27, since the map

$$(x, y, z) \mapsto (x, y + cx, z + c^{2^i}x),$$

for all $c \in GF(q)$ for the translation hyperoval $\mathcal{D}(2^i)$, is an elation fixing the translation hyperoval.

THEOREM 97 ([**84**]). *Let $q \geq 8$ be even, let $\mathcal{H}$ be a hyperoval of $PG(2, q)$ and let S be a Sylow 2-subgroup of the homography stabiliser H of $\mathcal{H}$. If $|S| = q$ then $\mathcal{H}$ is a translation hyperoval.*

COROLLARY 98 ([**84**]). *Let $\mathcal{K}$ be a q-arc in $PG(2, q)$, with $q \geq 8$ even, and suppose that it has a transitive homography stabiliser. Then $\mathcal{K}$ is a translation q-arc.*

THEOREM 99 ([**84**]). *An irregular translation hyperoval in $PG(2, q)$, $q = 2^e \geq 8$, has homography stabiliser of order $q(q-1)$ isomorphic to $AGL(1, q)$, that is, $C_2^e \rtimes C_{q-1}$. The orbits on the hyperoval have lengths 1, 1 and q.*

6.3. Lunelli-Sce hyperoval

In 1958 the Lunelli-Sce [**75**] hyperoval was found in $PG(2, 16)$ with the use of a computer. The hyperoval is equivalent to $\mathcal{D}(f)$ with $f(x) = x^{12} + x^{10} + \eta^{11}x^8 + x^6 +$

$\eta^2 x^4 + \eta^9 x^2$, where η is a primitive element of $GF(16)$ satisfying $\eta^4 = \eta + 1$. This was the first case of a hyperoval not being equivalent to one described by a monomial o-polynomial.

THEOREM 100 ([**32, 47**]). *The Lunelli-Sce hyperoval in $PG(2,16)$ has a transitive homography stabiliser of order 36 isomorphic to $C_3^2 \rtimes C_4$. The full collineation stabiliser has order 144 which is isomorphic to $((C_3 \times C_3) \rtimes C_8) \times C_2$.*

The derived group of the full collineation group of the Lunelli-Sce hyperoval is the unique Sylow 3-subgroup, which is elementary abelian of order 9, with all elements of order 3 having a fixed configuration being a triangle with no fixed points on the hyperoval; there are 9 Sylow 2-subgroups each of which are isomorphic to $C_8 \times C_2$. In a Sylow 2-subgroup, there are four involutions: two Baer and one an elation. The Baer involutions have no fixed points on the hyperoval. The whole group has centre of order 2, which is generated by a Baer involution. Thus the full group is that stated in the above theorem.

We have classified all hyperovals with transitive stabiliser by the below theorem.

THEOREM 101 ([**68**]). *Let $\mathcal{H}$ be a hyperoval of $PG(2,q)$. Suppose G the collineation stabiliser of $\mathcal{H}$ is transitive on $\mathcal{H}$. Then $\mathcal{H}$ is either a regular hyperoval of $PG(2,2)$ or $PG(2,4)$ or it is the Lunelli-Sce hyperoval of $PG(2,16)$.*

PROOF. Let $q = 2^e$. Since G is transitive on $\mathcal{H}$, then $q+2 \,\big|\, |G|$, and also divides $|P\Gamma L(3,q)| = (q^2+q+1)(q-1)^2 q^3 (q+1)e$. By Lemma 6, p. 4, we have $q+2$ divides $((-2)^2 - 2 + 1)(-3)^2(-2)^3(-1)$ which means $q+2$ divides $3^3 \cdot 2^3 e = 216e$. Hence $2^e + 2 \leq 216e$ so $e \leq 11$. Since $2^h + 2 \,\big|\, 216e$ we have $e = 1$, 2 or 4. Every hyperoval for $e = 1$ and $e = 2$ is regular. For $e = 4$ there are only the regular and the Lunelli-Sce hyperoval (see below), and only the Lunelli-Sce hyperoval has a transitive stabiliser. □

A more general theorem to the one above can be stated not just for Desarguesian projective planes but for projective planes of Lenz type greater than I, that is, a projective plane of order 2^e where a flag (P,l) with elation group with centre P and axis l has order 2^e.

THEOREM 102 ([**106**]). *If a projective plane of Lenz type greater that I and order a power of two contains a transitive hyperoval then the plane has order 2, 4 or 16.*

PROOF. Suppose not. Let $\mathcal{H}$ be a G-transitive hyperoval in a projective plane of order $2^e > 16$ (we know that the order is not 8, as the unique projective plane $PG(2,8)$ of order 8 contains no transitive hyperovals). Let p be a primitive prime divisor of $2^{2e-2} - 1$ (this exists, as $e > 4$). Then p divides $2^{e-1} + 1$, so divides $2^e + 2 = |\mathcal{H}|$. Thus there is an element g of G of order p and p is not 3, as $e > 4$. So p is coprime to $2^{2e} + 2^e + 1$, $2^e + 1$, 2^e and $2^e - 1$. It follows that g is planar. Since the plane has Lenz type greater than I, it follows from a theorem of Roth [**115**] that the order of the fixed subplane of g is 2^i for some i. So p divides $2^e - 2^i$, giving p divides $2^{e-i} - 1$, contrary to being a primitive prime divisor. □

Hall [**47**] by computer and O'Keefe-Penttila [**80**] without the use of a computer proved that the only hyperovals in $PG(2,16)$ are the regular and Lunelli-Sce hyperovals.

6.4. Segre-Bartocci hyperoval

The Segre-Bartocci (announced in [**120**], proved in [**121**]) is the hyperoval equivalent to $\mathcal{D}(x^6)$ when q is not a square and $q > 8$. The order of the stabiliser of these hyperovals in $P\Gamma L(3,q)$, $q = 2^e$, is $3(q-1)e$ for $e = 5$ and $(q-1)e$ for $e \geq 7$.

THEOREM 103. *We have $\mathcal{D}(6)$ being a hyperoval in $PG(2,q)$, $q = 2^e$, whenever e is odd.*

PROOF. We use the results from Chapter III, p. 81. We first show that the matrices

$$A_t = \begin{pmatrix} t & t^3 \\ 0 & t^5 \end{pmatrix},$$

with $t \in GF(q)$, $q = 2^e$, e odd, form a q–clan. That is, we prove that

$$\operatorname{trace}\left(\frac{(t+u)(t^5+u^5)}{(t^3+u^3)^2}\right) = 1, \text{ for all } t \neq u.$$

We have

$$\begin{aligned}\frac{(t+u)(t^5+u^5)}{(t^3+u^3)^2} &= \frac{t^6+tu^5+t^5u+u^6}{(t^3+u^3)^2} \\ &= 1 + \frac{tu^5+ut^5}{(t^3+t^3)^2} \\ &= 1 + \frac{t^2u+tu^2}{t^3+u^3} + \frac{t^4u^2+t^2u^4}{t^6+u^6}\end{aligned}$$

So $\operatorname{trace}\left((t+u)(t^5+u^5)/(t^3+u^3)^2\right) = \operatorname{trace}(1)$, and $\operatorname{trace}(1) = 1$ if and only if e is odd. Hence A_t is a q–clan if and only e is odd.

Following Section III.11, p. 104: Let $\boldsymbol{a} = (1,0)$ then $(a\boldsymbol{a}, g_t(a\boldsymbol{a}), t^3 a\boldsymbol{a}) = a(\boldsymbol{a}, t^{1/2}, t^3\boldsymbol{a})$ where $g_t(\boldsymbol{a}) = \sqrt{\boldsymbol{a}A_t\boldsymbol{a}^T}$. In the basis $(\boldsymbol{a},0,0)$, $(0,1,0)$ and $(0,0,\boldsymbol{a})$ we have $a(\boldsymbol{a}, t^{1/2}, t^3\boldsymbol{a})$ being equivalent to the point $(1, t^{1/2}, t^3)$ in $PG(2,q)$ and the set of points $\{(1,t^{1/2},t^3) \mid t \in GF(q)\} \cup \{(0,1,0),(0,0,1)\}$ being a hyperoval. This set of points is equivalent to $\mathcal{D}(6)$, hence $\mathcal{D}(6)$ is a hyperoval. □

6.5. Glynn hyperovals

Independently Hirschfeld in 1975 [**54**] and Eich and Payne [**38**] in 1972 constructed a hyperoval equivalent to $\mathcal{D}(x^{20})$ in $PG(2,128)$. The order of its stabiliser is 2667.

Glynn constructed two infinite families of hyperovals in 1983 [**42**]. They are equivalent to the hyperovals

(I): $\mathcal{D}(x^{3\sigma+4})$, where $e \geq 9$ with $\sigma^2 \equiv 2 \pmod{q-1}$, and

(II): $\mathcal{D}(x^{\sigma+\lambda})$ where $e \geq 7$ with $\sigma^2 \equiv 2 \pmod{q-1}$ and $\lambda^2 \equiv \sigma \pmod{q-1}$,

with $q = 2^e$ not a square, where σ and λ are automorphisms of $GF(q)$. The order of the stabiliser in $P\Gamma L(3,q)$, $q = 2^e$, for the Glynn hyperoval I is $(q-1)e$ and for the Glynn hyperoval II is $3(q-1)e$ for $e = 7$ and $(q-1)e$ for $e > 7$. Note the Glynn hyperoval II generalises the Hirschfeld-Eich-Payne hyperoval. A proof of the Glynn hyperovals using flocks of translation oval cones is given in [**27**].

6.6. Payne hyperoval

Payne [**93**] constructed a hyperoval equivalent to $\mathcal{D}(x^{1/6} + x^{3/6} + x^{5/6})$, for $q = 2^e$ with $e \geq 5$ odd and where the exponents are read modulo $q-1$. The order of the stabiliser for the Payne hyperoval in $PG(2,q)$, $q = 2^e$, is $2e$ [**131**] (see also [**87**]).

Theorem 104 ([**93**]). *Let $q = 2^e$ with $e \geq 5$ odd, the Payne hyperovals are an infinite family.*

Proof. For e odd, $(6, q-1) = 1$ so $x \mapsto x^{1/6}$ exists. Now $\mathcal{D}(1/6)$ and $\mathcal{D}(5/6)$ are equivalent to the hyperoval $\mathcal{D}(6)$. We use the ideas of Chapters III, p. 81 and IV, p. 141, to prove $\mathcal{D}(x^{1/6} + x^{1/2} + x^{5/6})$ is a hyperoval. We let $f(x) = x^{1/6}$ and $g(x) = x^{5/6}$. We show

$$\operatorname{trace}\left(\frac{(x^{1/6}+y^{1/6})(x^{5/6}+y^{5/6})}{x+y}\right) = 1, \text{ for all } x \neq y.$$

We let $X = x^{1/6}$ and $Y = y^{1/6}$, so we have

$$\begin{aligned}\operatorname{trace}\left(\frac{(X+Y)(X^5+Y^5)}{X^6+Y^6}\right) &= 1 + \operatorname{trace}\left(\frac{XY^5+X^5Y}{X^6+Y^6}\right)\\ &= 1 + \operatorname{trace}\left(\frac{XY(X^4+Y^4)}{X^6+Y^6}\right)\\ &= 1 + \operatorname{trace}\left(\frac{XY(X^2+Y^2)}{(X^2+XY+Y^2)^2}\right)\end{aligned}$$

Now

$$\frac{XY(X^2+Y^2)}{(X^2+XY+Y^2)^2} = \frac{XY}{X^2+XY+Y^2} + \left(\frac{XY}{X^2+XY+Y^2}\right)^2,$$

so this has trace zero. Hence for e odd, since trace$(1) = 1$, we have $\mathcal{D}(x^{1/6}+x^{1/2}+x^{5/6})$ being a hyperoval. $\square$

6.7. Cherowitzo hyperoval

Let $f_{\mathcal{C}}(x) = x^{\sigma} + x^{\sigma+2} + x^{3\sigma+4}$. Then we have the Cherowitzo ([**29**] and [**27**]) hyperovals equivalent to $\mathcal{D}(f_{\mathcal{C}})$, where $q = 2^e$ with e odd and σ is an automorphism of $GF(q)$ with $\sigma^2 \equiv 2 \pmod{q-1}$. The order of the stabiliser in $P\Gamma L(3,q)$, $q = 2^e$, for $e = 5$ is e [**85**] and for $e \geq 7$ is divisible by e [**29**]. It should be added that only recently has $\mathcal{D}(f_{\mathcal{C}})$ been proved to be a hyperoval for all e odd [**27**].

We will prove that the Cherowitzo hyperovals are new; the Theorem below will be central to that proof.

Theorem 105 ([**87**]). *Let $q = 2^e$ where $e \geq 7$ is odd. Let $\mathcal{H}$ be a Cherowitzo hyperoval. A collineation which fixes $\mathcal{H}$ and which fixes either $(0,1,0)$ or $(0,0,1)$ must be an automorphic collineation.*

Lemma 106 ([**85**]). *For $q = 32$ the Cherowitzo hyperoval is not equivalent to the listed hyperovals.*

The proof below is quite long.

Theorem 107 ([**106**]). *The Cherowitzo hyperovals in $PG(2,q)$, $q = 2^e$, e odd, are new for $e > 3$.*

Proof. We show the Cherowitzo hyperovals, $\mathcal{C} = \mathcal{D}(f_{\mathcal{C}})$, are new by first showing that for any known non-Cherowitzo hyperoval, $\mathcal{H}$, in $PG(2,2^e)$, e odd, if $\mathcal{C} \cong \mathcal{H}$ then the equivalence is a homography stabilising the fundamental quadrangle (FQ), and then using Theorem 105.

By Theorem 89, p. 43 the only o-polynomials over $GF(2)$ representing regular hyperovals are x^2, $x^{1/2}$ and $x^2 + x^4 + \cdots + x^{q-2}$. Hence $\mathcal{C}$ is not equivalent to a regular hyperoval, for $q > 8$.

Let $\mathcal{H}$ be an irregular translation hyperoval. Then the stabiliser, H, of $\mathcal{H}$ in $P\Gamma L(3,q)$ is isomorphic to $A\Gamma L(1,q)$ (Theorem 99, p. 47). Since the group has orbits on $\mathcal{H}$ of lengths 1, 1 and q, and is 2-transitive on the orbit of length q, it follows that all quadrangles on $\mathcal{H}$ containing the two fixed points are equivalent under the stabiliser of $\mathcal{H}$.

Now suppose that f is an o-polynomial over $GF(2)$ representing a hyperoval $\mathcal{D}(f)$ equivalent to $\mathcal{H}$. Then the stabiliser, H', of $\mathcal{D}(f)$ is conjugate in $P\Gamma L(3,q)$ to H. Since H' contains the automorphic collineations, which fix only the points of the fundamental quadrangle, H must contain a group A conjugate to the automorphic collineations fixing a quadrangle on $\mathcal{H}$, and no further points. Thus A fixes a quadrangle on the fixed points of $\mathcal{H}$. Without loss of generality, $\mathcal{H} = \mathcal{D}(\alpha)$, for some generator $\alpha \in \operatorname{Aut} GF(q)$. By the transitivity on quadrangles containing the fixed points noted above, without loss of generality, A fixes the FQ. Thus the equivalence between $\mathcal{D}(f)$ and $\mathcal{D}(\alpha)$ stabilises the FQ and, without loss of generality, is a homography. If $\mathcal{C} \cong \mathcal{H}$ then $\mathcal{C}$ is stabilised by an involution fixing the FQ and two points of the FQ. Hence by Theorem 105, p. 51 we have the homography being the map $(x, y, z) \mapsto (x, z, y)$, that is, we have $f_{\mathcal{C}} = f_{\mathcal{C}}^{-1}$. By lemma 18 in [**27**] we have that if $f(x) = x + x^{\sigma-1} + x^{\sigma+1}$ then

$$f^{-1}(x) = \frac{x^{\sigma+1}}{1 + x^2 + x^{\sigma}}.$$

Now $g(x) = x^{\sigma+2}$ then we have $f_{\mathcal{C}} = f \circ g$. Hence $f_{\mathcal{C}}^{-1} = g^{-1} \circ f^{-1}$ so

$$\begin{aligned} f_{\mathcal{C}}^{-1}(x) &= \left(\frac{x^{\sigma+1}}{1 + x^2 + x^{\sigma}}\right)^{\frac{1}{\sigma+2}} \\ &= \left(\frac{x^{\sigma+1}}{1 + x^2 + x^{\sigma}}\right)\left(\frac{1 + x^2 + x^{\sigma}}{x^{\sigma+1}}\right)^{\frac{1}{\sigma}} \\ &= \frac{x^{\sigma+1}(1 + x^{\sigma} + x)}{(1 + x^2 + x^{\sigma})(x^{1+\frac{1}{\sigma}})} \\ &= \frac{x^{\sigma-\frac{1}{\sigma}}(1 + x + x^{\sigma})}{1 + x^2 + x^{\sigma}}. \end{aligned}$$

Hence

$$f_{\mathcal{C}}^{-1}(x) = \frac{x^{1/\sigma}(1 + x + x^{\sigma})}{1 + x^2 + x^{\sigma}}.$$

So if $f_{\mathcal{C}}(x) = f_{\mathcal{C}}^{-1}(x)$ then

$$x^{1/\sigma} + x^{1+1/\sigma} + x^{\sigma+1/\sigma} = x^{\sigma} + x^{2\sigma} + x^{\sigma+4} + x^{2\sigma+2} + x^{3\sigma+4} + x^{3\sigma+6} + x^{4\sigma+4}.$$

Hence the right hand side must collapse to three terms. That is, we require two more cancellations. It is easy to verify that the required cancellations only occur when $q \leq 8$.

Now suppose $\mathcal{H}$ is a Payne hyperoval. Then by [**131**] [**85**] the stabiliser of the Payne hyperoval in $PG(2, q)$, $q = 2^e$, e odd is cyclic of order $2e$. The group has an involution fixing the FQ and moving two points. If $\mathcal{C} \cong \mathcal{H}$ then by [**87**] the involution is $(x, y, z) \mapsto (x, z, y)$ so we have $f_{\mathcal{C}} = f_{\mathcal{C}}^{-1}$. From above we see that this only occurs when $q \leq 8$.

Let $\mathcal{H}$ be the Subiaco hyperoval. We are only interested in the case when $q = 2^e$, e odd. We argue as for the Payne hyperoval.

Let $\mathcal{H}$ be a known monomial, non-translation hyperoval. In [**84**] the group H of any known monomial non-translation hyperoval $\mathcal{H}$ in $PG(2, q)$ is shown to be isomorphic to $\Gamma L(1, q)$ for $q > 128$. Since this group has orbits on $\mathcal{H}$ of lengths 1, 1, 1, $q - 1$, and is transitive on the orbit of length $q - 1$, it follows that all quadrangles on $\mathcal{H}$ containing the three fixed points are equivalent under the stabiliser of $\mathcal{H}$.

Now suppose that f is an o-polynomial over $GF(2)$ representing a hyperoval $\mathcal{D}(f)$ equivalent to $\mathcal{H}$. Then the stabiliser H' of $\mathcal{D}(f)$ is conjugate in $P\Gamma L(3,q)$ to H. Since H' contains the automorphic collineations, which fix only the points of the FQ, H must contain a group A conjugate to the automorphic collineations fixing a quadrangle on $\mathcal{H}$, and no further points. Thus A fixes a quadrangle on the fixed points of $\mathcal{H}$. Without loss of generality, let $\mathcal{H} = \mathcal{D}(n)$ where n is 6, $\sigma + \lambda$ or $2\sigma + 4$ where σ and λ are defined as for the Glynn hyperoval (page 50). By transitivity on quadrangles containing the fixed points, as noted above, then without loss of generality, A fixes the fundamental quadrangle. Thus the equivalence between $\mathcal{D}(f)$ and $\mathcal{D}(n)$ stabilises the FQ, and without loss of generality, is a homography. So if $\mathcal{C} \cong \mathcal{H}$ then there is a homography taking the FQ to the FQ. But $\mathcal{D}(n)$ has homography group C_{q-1} fixing three points of the FQ. Thus there exists a nontrival homography of $\mathcal{C}$ fixing three points of the FQ. Hence at least one of $(0,1,0)$ and $(0,0,1)$ is fixed contrary to Theorem 105.

For $q = 32$ and $q = 128$ the stabiliser, H, of some non-translation monomial hyperoval has order $3(q-1)$ [**84**]. This hyperoval, $\mathcal{H}$, is equivalent to $\mathcal{D}(6)$ for $q = 32$ and equivalent to $\mathcal{D}(20)$ for $q = 128$. Now suppose that f is an o-polynomial over $GF(2)$ representing a hyperoval $\mathcal{D}(f)$ equivalent to $\mathcal{H}$ for $q = 32$ or 128. As in the previous paragraph, H must contain a group A conjugate to the automorphic collineations fixing a quadrangle on $\mathcal{H}$, and no further points. Thus A fixes a quadrangle on the fixed point of $\mathcal{H}$. We have $|A|$ being 5 or 7 for $q = 32$ or $q = 128$, respectively, so the set of four fixed points of H must be those fixed by A. Now 31 and 127 are prime, and 3 is coprime to 5 and 7, so any subgroup conjugate to A is a Sylow 5-subgroup or Sylow 7-subgroup for $q = 32$ or $q = 128$, respectively. For $h \in H$ the fixed points of hAh^{-1} is equal to h(fixed points of A) which is equal to

$$h(\text{orbit of length 3}) \cup \{P\} = (\text{orbit of length 3}) \cup \{P'\}$$

for points P, P' on $\mathcal{H}$. We have $A \leq H' = P\Gamma L(3,q)_{\mathcal{D}(f)}$. For $g \in P\Gamma L(3,q)$ we have $gAg^{-1} \leq H$. Since for $A \in \mathrm{Syl}_e(H)$ then $gAg^{-1} \in \mathrm{Syl}_e(H)$ for $e = 5$, 7. This implies that $gAg^{-1} = hAh^{-1}$ for some $h \in H$. So if $\mathcal{C} \cong \mathcal{H}$ we have that there exists a nontrivial homography of $\mathcal{C}$ fixing 3 points of the FQ. Hence at least one of $(0,1,0)$ and $(0,0,1)$ is fixed, contrary to Theorem 105. □

6.8. O'Keefe-Penttila hyperoval

The O'Keefe-Penttila [**82**] hyperoval in $PG(2,32)$ is equivalent to $\mathcal{D}(f)$, where $f(x) = x^4 + \omega^{11}x^6 + \omega^{20}x^8 + \omega^{11}x^{10} + \omega^6x^{12} + \omega^{11}x^{14} + x^{16} + \omega^{11}x^{18} + \omega^{20}x^{20} + \omega^{11}x^{22} + \omega^6x^{24} + \omega^{11}x^{26} + x^{28}$, with ω being a primitive root of $GF(32)$ satisfying $\omega^5 = \omega^2 + 1$. The stabiliser of the O'Keefe-Penttila hyperoval in $P\Gamma L(3,32)$ has order 3 [**82**].

Penttila-Royle [**110**] have done an exhaustive computer search in $q = 32$ and have found that there are no further hyperovals in $PG(2, 32)$. The hyperovals are the regular, translation, Segre-Bartocci, Payne, Cherowitzo, and O'Keefe-Penttila hyperovals.

6.9. Irregular hyperovals in $PG(2, 64)$

The smallest q for which hyperovals have not been classified is 64. In fact for many years an open question (see for example [**55**]) was whether or not there existed irregular hyperovals in $PG(2, 64)$, as the only hyperovals in the list above for $q = 64$ are the regular ones.

The next sections will resolve this question by describing two inequivalent irregular hyperovals in $PG(2, 64)$. The two hyperovals and the order of their stabiliser in $P\Gamma L(3, 64)$ are:

(I): equivalent to $\mathcal{D}(f)$ with $f(x) = \omega^{42}x^2 + \omega^{21}x^4 + \omega^{42}x^6 + x^8 + \omega^{21}x^{10} + x^{12} + \omega^{21}x^{14} + \omega^{21}x^{16} + x^{20} + x^{22} + \omega^{42}x^{26} + \omega^{42}x^{28} + \omega^{21}x^{30} + \omega^{42}x^{32} + \omega^{42}x^{36} + \omega^{21}x^{38} + \omega^{42}x^{40} + x^{42} + \omega^{21}x^{44} + \omega^{21}x^{48} + x^{52} + \omega^{21}x^{54} + \omega^{21}x^{56} + \omega^{21}x^{58} + \omega^{21}x^{60} + \omega^{21}x^{62}$ with order 15, and

(II): equivalent to $\mathcal{D}(f)$ with $f(x) = \omega^{21}x^4 + \omega^{42}x^6 + \omega^{21}x^8 + \omega^{21}x^{10} + \omega^{42}x^{12} + \omega^{21}x^{14} + \omega^{21}x^{16} + \omega^{42}x^{18} + \omega^{42}x^{20} + x^{24} + \omega^{42}x^{26} + x^{30} + \omega^{42}x^{32} + \omega^{21}x^{34} + \omega^{42}x^{36} + \omega^{21}x^{38} + \omega^{21}x^{40} + \omega^{42}x^{42} + \omega^{21}x^{44} + \omega^{21}x^{46} + \omega^{42}x^{48} + \omega^{42}x^{50} + \omega^{21}x^{52} + \omega^{21}x^{54} + \omega^{21}x^{58} + \omega^{21}x^{60} + x^{62}$ with order 60,

where ω is a primitive element of $GF(64)$ satisfying $\omega^6 = \omega + 1$.

7. Fano Configuration

Every 4-arc on a hyperoval $\mathcal{H}$ determines a Fano plane, containing six lines secant to $\mathcal{H}$ of the 4-arc, and a further 7th line. This line is called the **diagonal line** of the 4-arc. Now, this diagonal line can either be external to $\mathcal{H}$ or secant to $\mathcal{H}$, by Theorem 28, p. 16, in which case we refer to the 4-arc itself as being **external** or a **secant** 4-arc, respectively. Now for each point P on $\mathcal{H}$ we can count the number of secant 4-arcs on P, and call this the **height** of P. This associates a number with each point, in such a way that points in the same orbit of the stabiliser of $\mathcal{H}$ must be assigned the same number. Therefore these numbers induce a partition on $\mathcal{H}$ which respects the orbit partition, but may be coarser. This multiset of numbers is called a **profile** of $\mathcal{H}$.

The above result yields a quick method for distinguishing hyperovals, though profiling a hyperoval is a order q^4 computation (since there are $\binom{q+2}{4}$ quadrangles on $\mathcal{H}$). It turns out that hyperovals (so far) are in fact distinguished by the coarser invariant consisting of the total number of external 4-arcs and secant 4-arcs.

Since any automorphism of a hyperoval preserves the partition of the points of $\mathcal{H}$ by their heights, by working in the stabiliser of one of the smaller cells, it is often possible to identify the automorphism group of the hyperoval.

8. Irregular Hyperovals in $PG(2,64)$

In this section we will talk about the methods used to construct the first irregular hyperovals in $PG(2,64)$.

The overall picture is this: Assume that the hyperoval has symmetry. We make this assumption as weak as possible by assuming the symmetry stems from a subgroup of prime order. So by Cauchy's Theorem page 5 we investigate each prime that divides the order of $P\Gamma L(3,q)$. Now the hyperovals are a union of orbits of this prime subgroup, the orbits either having length the prime or one (fixed points). We conveniently start with the largest prime and then the next largest and so on. Firstly, we determine if the hyperoval *can* be a union of orbits and fixed points of the prime subgroup. If so, we go onto the next step, which involves determining conjugacy classes of the prime subgroup etc. These techniques we call "**prime at a time**."

Now

$$|P\Gamma L(3,64)| = 73.19.13.7^2.5.3^5.2^{24}.$$

So the feasible primes are 73, 19, 13, 7, 5, 3, 2.

Immediately we discard 73, since $73 > 66$, which is the size of a hyperoval in $PG(2,64)$, and it's impossible to fix 66 points.

We have $19 \mid q^2+q+1$, so the subgroup of order 19 is generated by a power of a Singer cycle and so has no fixed points, so all orbits are of length 19 on $PG(2,64)$. But $19 \not| \ 66$ so a hyperoval can not be the union of orbits of length 19.

We find that the primes 13, 7, 5, 3 and 2 can be used to construct hyperovals. Below we give a detailed account of the primes 13, 7 and 5, and a summary of the work done on 3, 2 and the no symmetry hypothesis.

For the rest of this section let ω be a primitive element of $GF(64)$ satisfying $\omega^6 = \omega + 1$.

8.1. Hyperovals, $\mathcal{H}$, in $PG(2,64)$ with $|P\Gamma L(3,64)_{\mathcal{H}}|$ divisible by 13.

An element of order 13 in $P\Gamma L(3,64)$ has one fixed point and (hence) one fixed line by Section 3.3, p. 37. The hyperoval $\mathcal{H}$ is a union of five orbits of length 13 and contains the fixed point.

Now $13 \mid |P\Gamma L(3,64)|$ but $13^2 \nmid |P\Gamma L(3,64)|$, so by Sylow's Theorem all subgroups of order 13 are conjugate in $P\Gamma L(3,64)$. Hence we can study our favourite subgroup of order 13.

Let

$$T = \left\langle \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & \omega^{58} \end{bmatrix} \right\rangle,$$

then $|T| = 13$.

Let $\mathcal{H}$ denote the hyperoval we are looking for. Suppose $13 \mid |PGL(3,64)_{\mathcal{H}}|$. Then without loss of generality we can say $T \leq PGL(3,64)_{\mathcal{H}}$, applying the remarks in Section 3.4, p. 38.

THEOREM 108. *If* 13 *divides the order of the stabiliser of a hyperoval in* $PG(2,64)$ *then the hyperoval is regular.*

PROOF. By computer. Note that by the remarks above we need only determine the hyperovals fixed by T. Also since $N_{P\Gamma L(3,64)}(T)$ is transitive on the 13-arcs fixed by T, we need only determine the hyperovals fixed by T on a given 13-arc fixed by T. In fact a quick computation shows that all 39-arcs in $PG(2,64)$ stabilised by a collineation of order 13 lie on a regular hyperoval. □

8.2. Hyperovals, $\mathcal{H}$, in $PG(2,64)$ with $|P\Gamma L(3,64)_{\mathcal{H}}|$ divisible by 7.

Suppose 7 divides the stabiliser of the hyperoval $\mathcal{H}$. Then the hyperoval is constructed from nine orbits of length 7 and 3 fixed points, a total of 66 points.

An element of order 7 has a fixed configuration of 3 fixed points and 3 fixed lines forming a triangle. Since $P\Gamma L(3,64)$ is transitive on triangles, without loss of generality, we can assume that the fixed points are $(0,0,1)$, $(0,1,0)$ and $(1,0,0)$. Then we can construct a matrix

$$g = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda^i \end{bmatrix}, \text{ where } \lambda^7 = 1,\ \lambda \neq 1, \text{ and } i \in \mathbb{Z}_7,$$

(by the note after Theorem 79, p. 39, since $7 \mid q-1$), so $|g| = 7$.

We investigate the conjugacy classes of the group generated by g.

Let S be the subgroup of $P\Gamma L(3,64)$ of order 7 generated by g. Then $S = \langle g \rangle = \langle g^j \rangle$ for all j with $1 \leq j \leq 6$. So for some j, we have,

$$g^j = g_i = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega^9 & 0 \\ 0 & 0 & \omega^{9i} \end{bmatrix}$$

with $i \in \mathbb{Z}_7$ since $\langle\lambda\rangle$ is the unique subgroup of order 7 of $GF(64)^*$, we have $\lambda^j = \omega^9$, for some j. As a non-trivial homology cannot stabilise a hyperoval i cannot be 0 or 1.

The fixed points of S are $(0,0,1)$, $(0,1,0)$ and $(1,0,0)$. By permuting these fixed points , we see that g_i is conjugate to g_j where

$$j \equiv \frac{1}{i} \equiv 1-i \equiv \frac{i}{i-1} \equiv \frac{1}{1-i} \equiv \frac{i-1}{i} \pmod 7.$$

Hence $\langle g_2\rangle = \langle g_6\rangle$ and $\langle g_3\rangle = \langle g_4\rangle = \langle g_5\rangle$ so without loss of generality we can say $i = 2$ or 3.

Let a point of $PG(2,64)$ be called **admissible** if $\{P\} \cup \{(1,0,0),(0,1,0),(0,0,1)\}$ is a 4-arc. There are $(64-1)^2$ such points. We have $N_{P\Gamma L(3,64)}(S)$ being transitive on admissible points, since

$$N_{P\Gamma L(3,64)}(S) = C_{P\Gamma L(3,64)}(S) \geq \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & \mu & 0 \\ 0 & 0 & \nu \end{pmatrix} \,\middle|\, \mu,\ \nu \in GF(64)^* \right\},$$

with the $(64-1)^2$ matrices acting regularly on the admissible points. So $N_{P\Gamma L(3,64)}(S)$ permutes the orbits of S, hence transitive on the orbits of S, so all orbits, not on the sides of the triangle $(0,0,1)$, $(0,1,0)$ and $(1,0,0)$, are equivalent, so equivalent to the orbit containing $(1,1,1)$. Now since $7 = 2^3 - 1$ we then have the orbit

$$\{(1,\omega^9,\omega^{9\cdot 3}) \mid |\omega^9| = 7\}$$

being contained in $PG(2,8)$. Thus the orbit of $(1,1,1)$ is an arc if and only if

$$\mathcal{D}(i) = \{(1,t,t^i) \mid t \in GF(8)\} \cup \{(0,1,0),(0,0,1)\}$$

is a hyperoval of $PG(2,8)$. This can only occur if i is congruent to 2, 4 or 6 modulo 7 (see Section 88, p. 43). Hence $S = \langle g_3\rangle$ can not stabilise a hyperoval.

THEOREM 109. *If 7 divides the order of the stabiliser of a hyperoval in $PG(2,64)$ then the hyperoval is regular.*

PROOF. By computer. Note that by the remarks above we need only determine the hyperovals fixed by S where $i = 2$. Also since $N_{P\Gamma L(3,64)}(S)$ is transitive on the 7-arcs fixed by S, we need only determine the hyperovals fixed by S on a given 7-arc fixed by S. A computation shows that all 31-arcs in $PG(2,64)$ stabilised by a collineation of order 7 lie on a regular hyperoval. □

8.3. Hyperovals, $\mathcal{H}$, in $PG(2,64)$ with $|P\Gamma L(3,64)_{\mathcal{H}}|$ divisible by 5.

An element of order 5 in $P\Gamma L(3,64)$ has one fixed point and one fixed line. By Lemma 75, p. 36 the fixed line and fixed point form an antiflag.

As for a stabiliser of order divisible by 13, we can construct a group

$$F = \left\langle \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & \omega^{21} \end{bmatrix} \right\rangle,$$

which has order 5. Subgroups of $P\Gamma L(3,64)$ of order 5 are conjugate to F by Sylow' Theorem. Now F has fixed point $P = (1,0,0)$ and fixed line $l : x = 0$.

(We note that

$$\begin{pmatrix} \omega^{21} & \omega^{21} & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & \omega^{21} \end{pmatrix} \begin{pmatrix} \omega^{21} & \omega^{21} & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & \omega^{21} & 0 \\ 0 & \omega^{42} & 1 \end{pmatrix} = g$$

where $g \in PGL(3,64)$ is the element of order 5 used on page 113, Chapter III.)

Notice that $\{0, 1, \omega^{21}, \omega^{42}\} \subseteq GF(64)$ is isomorphic to $GF(4)$.

Let $C = C_{PGL(3,64)}(F)$, the centraliser of F in $PGL(3,64)$. Then C permutes the fixed points and fixed lines of F, and so fixes the point $(1,0,0)$ and fixes the line $x = 0$.

We now determine the normaliser of F in $P\Gamma L(3,64)$ by using the Samosa Lemma (Theorem 20, p. 7). Let the group P of the Samosa Lemma be $F \cong C_5$. Firstly we need to determine d of the Samosa Lemma. We have

$$64^m - 1 \equiv 4^m - 1 \pmod 5 \equiv (-1)^m - 1 \pmod 5 \equiv 0 \pmod 5 \text{ if and only if } 2 \,\big|\, m.$$

Hence $5 \,\big|\, 64^m - 1$ implies that $2 \,\big|\, m$ So for $F \leq PGL(3,64)$ we have $5 \not| \; 64 - 1$ but $5 \,\big|\, 64^2 - 1$ giving $d = 2$. Then we have a representation $T' \colon C_5 \to GL(3,64)$. Let $W = GF(q)^3$, then $W = U \oplus V$ where U is a fixed one-dimensional subspace and V is a fixed two-dimensional subspace, that is, a fixed point and a fixed line, respectively. Now $C_{GL(W)}(T'(C_5))$ fixes U and V. Let $C_5 = \langle g \rangle$. Then

$$T'(g) = \begin{pmatrix} 1 & 0 \quad 0 \\ 0 & \\ 0 & T \end{pmatrix}$$

with $T \colon G \to GL(V)$ irreducible. Also

$$C_{GL(W)}(T'(C_5)) = \left\{ \begin{pmatrix} \lambda & 0 \quad 0 \\ 0 & \\ 0 & A \end{pmatrix} \;\Big|\; A \in C_{GL(V)}(T(C_5)) \right\}.$$

So $C_{GL(W)}(T'(C_5)) = GF(64)^* \times GF(64^2)^* \geq \{\lambda I \mid \lambda \in GF(64)^*\}$, hence

$$C_{PGL(W)}(T'(C_5)) = \frac{GF(64)^* \times GF(64^2)^*}{\{\lambda I \mid \lambda \in GF(64)^*\}}.$$

So C_5 fixes l (the subspace V). Choose coordinates so that $l = [0,0,1]$ and $P = (0,0,1)$ (the one-dimensional subspace U). Now C_5 fixes l which implies that

$C_5 \leq AGL(2,64)$, identified with $PGL(2,64)_l$ as usual. Also C_5 fixes P implying $C_5 \leq GL(2,64)$. Hence $C_{GL(2,64)}(C_5)$ is regular on $PG(2,64) - (l \cup \{P\})$.

Let $N = N_{P\Gamma L(3,64)}(F)$ then by Theorem 20, p. 7, we have

$$\begin{aligned} N &\cong GF(64^2)^* \rtimes \operatorname{Aut} GF(64^2) \\ &\cong C_{4095} \rtimes C_{12} \end{aligned}$$

with $C \lhd N$ acting regularly on the points of $PG(2,64)$ not on l and not equal to P. We identify C with $GF(64^2)^* = \langle \eta \rangle$, where $\eta^2 = \omega^{22}\eta + \omega^{10}$. Since C acts regularly on points of $PG(2,64)$ not on l and not equal to P, we identify points not on l with elements of $GF(64^2)$, with P corresponding to 0. Then F corresponds to the group generated by multiplication by η^{819} and C is generated by multiplication by η. Hence

$$N \cong C \rtimes \langle \eta^i \mapsto \eta^{2i} \rangle$$

As C is transitive on orbits of F not on l, not equal to P, we may suppose that $1 \in \mathcal{H}$.

Explicitly, $\operatorname{Aut} GF(64^2) = \langle x \mapsto x^2 \rangle$ and $\eta^i \mapsto \eta^{2i}$ takes orbit

$$\{\eta^i, \eta^{i+819}, \eta^{i+1638}, \eta^{i+2457}, \eta^{i+3276}\} \mapsto \{\eta^{2i}, \eta^{2i+1638}, \eta^{2i+3276}, \eta^{2i+819}, \eta^{2i+2457}\}$$

Identifying the orbit of η^i under F with i for $i \in \mathbb{Z}_{819}$, the map is now $i \mapsto 2i$ with $i \in \mathbb{Z}_{819}$.

There is a unique subgroup of C of order 63, consisting entirely of homologies, namely

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}$$

with $\lambda \in GF(64)^*$.

Let $G = P\Gamma L(3,64)_{\mathcal{H}}$ with $\mathcal{H}$ irregular. Then $|C \cap G| = 5$. (Note $|C| = 13.5.7.3^2$. If $g \in C$, g non-trivial, and $|g| \mid 63$, then g is a homology which by Theorem 52, p. 27, does not stabilise a hyperoval. Alternatively, $g \in C$ and $|g| = 13$, then we have shown from Theorem 108, p. 56, that g does not stabilise an irregular hyperoval. Hence $|g| = 5$ or 1.)

Now $C \cap G = C_G(F)$, and $N \cap G = N_G(F)$. We have

$$\frac{N_G(F)}{C_G(F)} \cong \frac{N \cap G}{C \cap G} \cong \frac{(N \cap G)C}{C} \lesssim \frac{N}{C},$$

so

$$\frac{N_G(F)}{C_G(F)}$$

is cyclic of order dividing 12. Hence $|N_G(F)|$ divides 60.

THEOREM 110. *If $\mathcal{H}$ is a hyperoval in $PG(2,64)$, $G = P\Gamma L(3,64)_{\mathcal{H}}$, $F \le G$ with $|F| = 5$ and 60 divides $|N_G(F)|$, then $\mathcal{H}$ is a regular hyperoval or the hyperoval $\mathcal{H}_1$ equivalent to*

$$\begin{aligned} f(x) &= \omega^{21}x^4 + \omega^{42}x^6 + \omega^{21}x^8 + \omega^{21}x^{10} + \omega^{42}x^{12} + \omega^{21}x^{14} + \omega^{21}x^{16} \\ &\quad + \omega^{42}x^{18} + \omega^{42}x^{20} + x^{24} + \omega^{42}x^{26} + x^{30} + \omega^{42}x^{32} + \omega^{21}x^{34} \\ &\quad + \omega^{42}x^{36} + \omega^{21}x^{38} + \omega^{21}x^{40} + \omega^{42}x^{42} + \omega^{21}x^{44} + \omega^{21}x^{46} + \omega^{42}x^{48} \\ &\quad + \omega^{42}x^{50} + \omega^{21}x^{52} + \omega^{21}x^{54} + \omega^{21}x^{58} + \omega^{21}x^{60} + x^{62} \end{aligned}$$

Conversely, $\mathcal{H}_1$ is a hyperoval having a subgroup F of order 5 with $|N_G(F)| = 60$.

PROOF. By the arguments above, if $\mathcal{H}$ is irregular, then $|N_G(F)|$ divides 60. So we conclude $|N_G(F)| = 60$. Now N has only one conjugacy class of cyclic subgroups of order 12, so without loss of generality,

$$N_G(F) = F \rtimes \operatorname{Aut} GF(64^2).$$

The orbits of $N_G(F)$ on the set of orbits of F are therefore $\{i, 2i, 4i, \ldots, 2^{11}i\}$, $i \in \mathbb{Z}_{819}$. A computation shows that, $\mathcal{H}$, the only irregular hyperoval stabilised by $N_G(F)$ has $\mathcal{H} - \{P\} = \{0\} \cup \{819k \mid 1 \le k \le 4\} \cup \{51.2^j + 819k \mid 0 \le j \le 11, 0 \le k \le 4\}$, that is,

$$\mathcal{H} = \{0\} \cup \{\eta^{819k} \mid 0 \le k \le 4\} \cup \{\eta^{51.2^j + 819k} \mid 0 \le j \le 11, 0 \le k \le 4\}.$$

Also, a computation shows that $\mathcal{H}$ is equivalent to $\mathcal{H}_1$. $\square$

THEOREM 111. *If $\mathcal{H}$ is a hyperoval in $PG(2,64)$, $G = P\Gamma L(3,64)_{\mathcal{H}}$, $F \le G$, with $|F| = 5$ and 15 divides $|N_G(F)|$, then $\mathcal{H}$ is equivalent to $\mathcal{H}_1$, the regular hyperoval, or the hyperoval $\mathcal{H}_2$ equivalent to*

$$\begin{aligned} f(x) &= \omega^{42}x^2 + \omega^{21}x^4 + \omega^{42}x^6 + x^8 + \omega^{21}x^{10} + x^{12} + \omega^{21}x^{14} \\ &\quad + \omega^{21}x^{16} + x^{20} + x^{22} + \omega^{42}x^{26} + \omega^{42}x^{28} + \omega^{21}x^{30} + \omega^{42}x^{32} \\ &\quad + \omega^{42}x^{36} + \omega^{21}x^{38} + \omega^{42}x^{40} + x^{42} + \omega^{21}x^{44} + \omega^{21}x^{48} \\ &\quad + x^{52} + \omega^{21}x^{54} + \omega^{21}x^{56} + \omega^{21}x^{58} + \omega^{21}x^{60} + \omega^{21}x^{62} \end{aligned}$$

Conversely, $\mathcal{H}_2$ is a hyperoval having a subgroup F of order 5 with $|N_G(F)| = 15$.

PROOF. Similar to last proof. Without loss of generality

$$N_G(F) = F \rtimes \langle \eta \mapsto \eta^{16} \rangle.$$

Now we need one orbit of length 5, so by similar arguments, computation gives only

$$\begin{aligned} \mathcal{H} &= \{0\} \cup \{\eta^{819k} \mid 0 \le k \le 4\} \cup \{\eta^{79.16^j + 819k} \mid 0 \le j \le 2, 0 \le k \le 4\} \\ &\quad \cup \{\eta^{174.16^j + 819k} \mid 0 \le j \le 2, 0 \le k \le 4\} \cup \{\eta^{332.16^j + 819k} \mid 0 \le j \le 2, 0 \le k \le 4\} \\ &\quad \cup \{\eta^{511.16^j + 819k} \mid 0 \le j \le 2, 0 \le k \le 4\}. \end{aligned}$$

Also, a computation shows that $\mathcal{H}$ is equivalent to $\mathcal{H}_2$. $\square$

THEOREM 112. *If $\mathcal{H}$ is a hyperoval in $PG(2,64)$, $G = P\Gamma L(3,64)_{\mathcal{H}}$, 5 dividing $|G|$ then $\mathcal{H}$ is equivalent to $\mathcal{H}_1$, $\mathcal{H}_2$, or the regular hyperoval, and conversely.*

PROOF. Similar to first proof. Here we use N to assume that $1 \in \mathcal{H}$ and then to only search for hyperovals on 1 and i, for one i from each orbit of $\operatorname{Aut} GF(64^2)$. This is a long search, but nothing new has been found. $\square$

Remark on the proofs: All three proofs are proved by computer.

Of course Theorem 112, p. 61, implies Theorem 111, p. 60, which implies Theorem 110, p. 59. However, as they are computer-dependent results, with each requiring more computing time, it is of advantage to prove them independently.

Note that the fact that the two new hyperovals are hyperovals is not really computer dependent, as it can be readily verified by a trivial program. There is a computer free proof given in Chapter IV.

Now to the size of the stabilisers of our hyperovals. Let $\mathcal{C}$ be a conic in $PG(2,4)$ with nucleus P and define $\mathcal{R} = \mathcal{C} \cup \{P\}$, and let $\mathcal{H}$ be a hyperoval in $PG(2,64)$ such that $PG(2,4) \cap \mathcal{H} = \mathcal{R}$.

We know these facts from our above computations:

(i) $|G| = 60$.
(ii) G fixes $PG(2,4)$ and so fixes $\mathcal{R}$.
(iii) G fixes the line $l : x = 0$ and the point $P = (1,0,0)$.

Hence $G \leq P\Gamma L(3,64)_{\mathcal{R},l,P}$. Now

$$G_{(\mathcal{R})} \leq G_{(PG(2,4))} \leq P\Gamma L(3,64)_{(PG(2,4))} = \langle \sigma \rangle,$$

where $\sigma \in \operatorname{Aut} GF(64)$ of order 3 defined as $\sigma \colon (x,y,z) \mapsto (x^4,y^4,z^4)$. But equality occurs throughout as our o-polynomials are over $GF(4)$.

Since $P\Gamma L(3,4)_{\mathcal{R},P} \cong P\Gamma L(2,4)$ with $|P\Gamma L(2,4)| = 120$ with $P\Gamma L(3,4)_{\mathcal{R},P}$ being transitive on the six external lines to $\mathcal{R}$ (see the Note on page 23). Now

$$|P\Gamma L(3,64)^{PG(2,4)}_{\mathcal{R},l,P}| = |P\Gamma L(3,4)_{\mathcal{R},l,P}| = 20,$$

since $P\Gamma L(3,4)_{\mathcal{R},l,P}$ has index 6 in $P\Gamma L(3,4)_{\mathcal{R},P}$. Hence

$$G = P\Gamma L(3,64)_{\mathcal{R},l,P} = P\Gamma L(3,64)_{\mathcal{C},l}.$$

For q even the only subgroups of $PGL(2,q)$ of order $2(q+1)$ are dihedral and they are conjugate [**37**].

Let $H = PGL(3,64)_{\mathcal{C},l}$. Then H has index 6 in G, so $|H| = 10$, hence $H \cong D_{10}$. Now G normalises H, so by [**37**] $C_{q^3+1} \cap G = F$, so $G = F \rtimes C_{12}$. (We note that $C_5 \rtimes C_{12} \leq A\Gamma L(1,64^2)$.)

Alternatively by the method of construction it is clear that

$$F_1 \rtimes \operatorname{Aut} GF(64^2)$$

is a subgroup of the stabiliser of $\mathcal{H}_1$, and

$$F_2 \rtimes \mathrm{Gal}(GF(64^2)/GF(16))$$

is a subgroup of the stabiliser of $\mathcal{H}_2$, for some subgroups F_1 and F_2 of $P\Gamma L(3, 64)$ of order 5, conjugate to F.

To see that the groups are the full stabilisers, we used an idea introduced in Section 7, p. 54. For each quadrangle contained in a hyperoval $\mathcal{H}$, the diagonal line is either secant or external to $\mathcal{H}$. For each point P of $\mathcal{H}$, we count the number of quadrangles in $\mathcal{H}$ on P with diagonal line external to $\mathcal{H}$ and call this the height of P. The stabiliser of $\mathcal{H}$ must permute the points of $\mathcal{H}$ with the same height.

A computation shows that $\mathcal{H}_1$ has one point (P_1) of height 20700, 5 points (the orbit, $\mathcal{C}_1$, of 1 under F_1) of height 21432, and 60 points of height 21373. It follows that the stabiliser of $\mathcal{H}_1$ is contained in the stabiliser of P_1 and $\mathcal{C}_1$, which is easy to compute, and has a (small) order of 360. So by explicitly calculating with the stabiliser of P_1 and $\mathcal{C}_1$, we can see that $|P\Gamma L(3, 64)_{\mathcal{H}_1}| = 60$. In more detail, let $g_i \in P\Gamma L(3, 64)_{\mathcal{H}_i}$ so $g_i P_i = P_i$ and $g_i \mathcal{C}_i = \mathcal{C}_i$ for $i = 1$, 2. Then g_i fixes the Baer subplane containing P_i and $\mathcal{C}_i$. We can say this Baer subplane is $PG(2, 4)$ by our canonical labeling of P_i and $\mathcal{C}_i$. Hence $g_i \in (P\Gamma L(3, 4) \rtimes \mathrm{Gal}(GF(64)/GF(4)))_{P_i, \mathcal{C}_i}$. Since $\mathcal{C}_i$ is a conic in $PG(2, 4)$ with nucleus P_i we have $g_i \in P\Gamma O(3, 4) \rtimes \mathrm{Gal}(GF(64)/GF(4))$ which is $g_i \in P\Gamma L(2, 4) \rtimes \mathrm{Gal}(GF(64)/GF(4))$, by Theorem 45, p. 23. Note $|P\Gamma L(2, 4) \rtimes \mathrm{Gal}(GF(64)/GF(4))| = 120.3$. Since $\mathrm{Gal}(GF(64)/GF(4))$ fixes $\mathcal{H}_i$ we need only concern ourselves with the elements of $P\Gamma L(2, 4)$.

Similarly, a computation shows that $\mathcal{H}_2$ has one point (P_2) of height 21565, 5 points (the orbit, $\mathcal{C}_2$, of 1 under F_2) of height 21436, 15 points of height 21254, 15 points of height 21508, 15 points of height 21505, and 15 points of height 21382. So again $P\Gamma L(3, 64)_{\mathcal{H}_1}$ is a subgroup of $P\Gamma L(3, 64)_{\{P_2, \mathcal{C}_2\}}$, so we can explicitly see that we have $|P\Gamma L(3, 64)_{\mathcal{H}_2}| = 15$.

(Of course, when computing with the stabiliser of P_i and $\mathcal{C}_i$, it is best to choose a point Q_i on $\mathcal{H}_i$, not P_i, not in $\mathcal{C}_i$, and compute with the stabiliser of P_i, Q_i and $\mathcal{C}_i$ as we know the length of the orbit of Q_i under $P\Gamma L(3, 64)_{\mathcal{H}_i}$ is 60 if $i = 1$ and 15 if $i = 2$.)

9. Searching Algorithms for Hyperovals

In this section we describe the algorithms and techniques used to search for hyperovals in $PG(2, 64)$, in particular, hyperovals stabilised by F (the group of order 5 defined in Section 8.3, p. 57).

Let ω be a primitive element of $GF(64)$ satisfying $\omega^6 = \omega + 1$.

We define a k-arc to be **nice** if it is stabilised by F. Our aim is to find nice 66-arcs.

We determine the nice hyperovals by constructing graphs and finding cliques of suitable size. For each of the three theorems in Section 8.3, we determine a graph Γ_i with respect to a set of points X_i for $i = 1, 2, 3$.

By the results in Section 8.3 we can label the points of $PG(2, 64)$ not on the fixed line of F by $GF(64^2)$. Let η be a primitive element of $GF(64^2)$ satisfying $\eta^2 = \omega^{22}\eta + \omega^{10}$.

For Theorem 110, p. 59, we let X_1 be a nice 6-arc defined as

$$X_1 = \{0\} \cup \{\eta^{819k} \mid 0 \leq k \leq 4\}.$$

The vertices of the graph Γ_1 are orbits $\mathcal{O}_x$ where

$$\mathcal{O}_x = \{\eta^{x2^j+819k} \mid 0 \leq j \leq 11, 0 \leq k \leq 4\},$$

is a nice 60-arc and $X_1 \cup \mathcal{O}_x$ is a nice hyperoval. When the program is ran it finds only two vertices: $X_1 \cup \mathcal{O}_{53}$ which is equivalent to the regular hyperoval, and $X_1 \cup \mathcal{O}_{51}$ which is the hyperoval $\mathcal{H}_1$. The program took 14 seconds to run on a Sun Sparc IPC Workstation.

For Theorem 111, p. 60, we let

$$X_2 = \{0\} \cup \{\eta^{819k} \mid 0 \leq k \leq 4\},$$

with X_2 being a 6-arc. The vertices of Γ_2 are orbits $\mathcal{O}_x$ where

$$\mathcal{O}_x = \{\eta^{x16^j+819k} \mid 0 \leq j \leq 2, 0 \leq k \leq 4\},$$

is a nice 15-arc and $X_2 \cup \mathcal{O}_x$ is a nice 21-arc. Edges are defined as:

$$\mathcal{O}_x \sim \mathcal{O}_y \iff \mathcal{O}_x \cup \mathcal{O}_y \cup X_2 \text{ is a nice 36-arc.}$$

Hence a hyperoval in Γ_2 is a clique of size 4. We find that Γ_2 has very few edges (60 in total). We observe that the vertices of sufficient valency naturally fall into a few cliques by observation of the list of edges. The cliques are:

(i) $X_2 \cup \mathcal{O}_{63} \cup \mathcal{O}_{126} \cup \mathcal{O}_{252} \cup \mathcal{O}_{441}$.
(ii) $X_2 \cup \mathcal{O}_{51} \cup \mathcal{O}_{102} \cup \mathcal{O}_{204} \cup \mathcal{O}_{408}$.
(iii) $X_2 \cup \mathcal{O}_{71} \cup \mathcal{O}_{203} \cup \mathcal{O}_{348} \cup \mathcal{O}_{451}$.
(iv) $X_2 \cup \mathcal{O}_{83} \cup \mathcal{O}_{142} \cup \mathcal{O}_{406} \cup \mathcal{O}_{452}$.
(v) $X_2 \cup \mathcal{O}_{87} \cup \mathcal{O}_{166} \cup \mathcal{O}_{284} \cup \mathcal{O}_{665}$.
(vi) $X_2 \cup \mathcal{O}_{79} \cup \mathcal{O}_{174} \cup \mathcal{O}_{332} \cup \mathcal{O}_{511}$.

Hyperoval (i) is regular, (ii) is $\mathcal{H}_1$, and (iii), (iv), (v), (vi) are equivalent to $\mathcal{H}_2$. Notice (iii) $\mapsto$ (iv) $\mapsto$ (v) $\mapsto$ (vi) $\mapsto$ (iii) under the map $\eta^i \mapsto \eta^{2i}$. The program took eight and a half minutes to run on a Sun Sparc IPC Workstation.

The exhaustive search for hyperovals stabilised by an element of order 5 is slightly more complicated.

We set about trying to construct a sparsely edged graph Γ_3. We do this by noticing that any nice 21-arc must be on at least 9 nice 26-arcs for the 21-arc to complete to a nice hyperoval. We call such nice 21-arcs **live**. Now we can define Γ_3.

Let

$$X_3 = \{0\} \cup \{\eta^{819k}, \eta^{s+819k} \mid 0 \leq k \leq 4\}$$

where s is one of 516 numbers such that X_3 is a nice 11-arc. Vertices of Γ_3 are

$$\mathcal{O}_x = \{\eta^{x+819k} \mid 0 \leq k \leq 4\},$$

with $\mathcal{O}_x$ being nice 5-arcs such that $X_3 \cup \mathcal{O}_x$ is a nice 16-arc. Edges are defined as:

$$\mathcal{O}_x \sim \mathcal{O}_y \iff X_3 \cup \mathcal{O}_x \cup \mathcal{O}_y \text{ is a live 21-arc.}$$

As before, for each s, Γ_3 is graph with few edges and so by inspection the cliques of size 11 can be found. The long search of going through each s gives no new hyperovals, but does find the regular hyperovals and the hyperovals $\mathcal{H}_1$ and $\mathcal{H}_2$ as expected. For each s, the program takes 16 minutes to complete on a Sun Sparc IPC Workstation. In all it took roughly three weeks to prove Proposition 112, p. 61.

To check that the set of points of the cliques of orbits is a hyperoval we employ two methods. Firstly, we use a program that determines that the set of 66 points has no three collinear. Secondly, we use the results of Section 5.1, p. 43, to construct a permutation polynomial from the set of 66 points and then use Theorem 84, p. 42, to determine that it is an o-polynomial.

Of interest: $\mathcal{H}_1$ has 36 o-polynomials over $GF(4)$ and 6 of these have stabiliser fixing the point $(0, 0, 1)$. Similarly, $\mathcal{H}_2$ has 144 o-polynomials over $GF(4)$ with 24 of these have stabiliser fixing the point (0,0,1). The external lines to $\mathcal{H}_i \cap PG(2, 4)$ for $i = 1, 2$ of $PG(2, 4)$ are $[1, 1, \omega^{21}]$, $[1, 1, \omega^{42}]$, $[1, \omega^{21}, 1]$, $[1, \omega^{42}, 1]$, $[\omega^{21}, 1, 1]$, $[\omega^{42}, 1, 1]$.

Of particular interest is that $\mathcal{H}_1$ is equivalent to the hyperoval described by the o-polynomial

$$\begin{aligned} f = {} & \omega^{42}x^4 + \omega^{21}x^6 + \omega^{21}x^8 + \omega^{42}x^{10} + \omega^{42}x^{14} + \omega^{21}x^{16} + \omega^{21}x^{18} \\ & + \omega^{42}x^{20} + \omega^{42}x^{24} + \omega^{21}x^{26} + \omega^{21}x^{28} + \omega^{42}x^{30} + x^{32} + \omega^{42}x^{34} \\ & + \omega^{21}x^{36} + \omega^{21}x^{38} + \omega^{42}x^{40} + \omega^{42}x^{44} + \omega^{21}x^{46} + \omega^{21}x^{48} + \omega^{42}x^{50} \\ & + \omega^{42}x^{54} + \omega^{21}x^{56} + \omega^{21}x^{58} + \omega^{42}x^{60} \end{aligned}$$

This o-polynomial's coefficients are periodic except for the term $x^{1/2} = x^{32}$; this form of periodicity is referred to as "**pseudo-periodicity**." By the use of the simple ideas of geometric series we can see that $\mathcal{H}_1$ is equivalent to the hyperoval described by the o-polynomial

$$f(x) = \frac{\omega^{42}x^4 + \omega^{42}x}{(x^2 + \omega^{21}x + 1)^2} + x^{1/2},$$

under the map $(x, y, z) \mapsto (z, y + \omega^{21}z, x + \omega^{42})$.

By observing the $GF(4)$ o-polynomials of $\mathcal{H}_2$ we find that it is equivalent to the o-polynomial

$$\begin{aligned} f(x) = {} & \omega^{21}x^2 + \omega^{21}x^6 + x^8 + x^{10} + \omega^{21}x^{12} + \omega^{21}x^{16} + x^{18} \\ & + x^{20} + \omega^{21}x^{22} + \omega^{21}x^{26} + x^{28} + x^{30} + \omega^{21}x^{32} + \omega^{21}x^{36} \\ & + x^{38} + x^{40} + \omega^{21}x^{42} + \omega^{21}x^{46} + x^{48} + x^{50} + \omega^{21}x^{52} \\ & + \omega^{21}x^{56} + x^{58} + x^{60} + \omega^{21}x^{62} \end{aligned}$$

This o-polynomial shows the characteristic of "pseudo-periodicity", that is, periodicity of the coefficients except for the $x^{1/2} = x^{32}$ term. Again, we see that (from the above o-polynomial) $\mathcal{H}_2$ is equivalent to

$$f(x) = \frac{x^4 + \omega^{21}x^3 + \omega^{21}x^2}{(x^2 + \omega^{21}x + 1)^2} + \omega^{42}x^{1/2},$$

under the map $(x, y, z) \mapsto (z, y + \omega^{21}z, x + \omega^{42})$.

9.1. More on Hyperovals in $PG(2, 64)$

THEOREM 113. *Any Sylow 3-subgroup, S, of the homography stabiliser of a hyperoval in $PG(2, 64)$ has order at most 9.*

PROOF. Since $3 \equiv 66 \pmod 9$, S must stabilise a triangle. Without loss of generality let the triangle be $(0, 0, 1)$, $(0, 1, 0)$ and $(1, 0, 0)$. The pointwise stabiliser T of the triangle in $PGL(3, 64)$ is just the homographies with diagonal matrices. Hence $U = T \cap S$ contains no non-identity homologies, so elements of U have the form

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & t & 0 \\ 0 & 0 & t^i \end{pmatrix}$$

for some i such that $(i, 9) = 1$ with t having order 1, 3, or 9.

Now U has index 1 or 3 in S. If U has index 3 then a homography of the form

$$\begin{pmatrix} 0 & a & 0 \\ 0 & 0 & b \\ c & 0 & 0 \end{pmatrix}$$

normalises U which forces U to be either trivial or of order 3 and equal to the set of all homographies of the form

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & u & 0 \\ 0 & 0 & u^2 \end{pmatrix}$$

where u has order 1 or 3. Hence S has order at most 9. $\square$

From now on we label the hyperoval $\mathcal{H}_1$ from the previous Section whose stabiliser is of size 60 by $\mathcal{H}_{60}$, and the hyperoval $\mathcal{H}_2$ whose stabiliser is of order 15 by $\mathcal{H}_{15}$.

The results in the rest of this section are from [111].

There are four conjugacy classes of elements of order 3 in $P\Gamma L(3,64)$, these are:

(i) A 1387'th power of a Singer cycle, g_1, represented by the matrix,

$$\begin{pmatrix} 0 & 0 & \omega \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

(ii) A triangle element, g_2, represented by the matrix,

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega^{21} & 0 \\ 0 & 0 & \omega^{42} \end{pmatrix}.$$

(iii) An element g_3, of order 3 that is in $\operatorname{Aut} GF(64)$, represented by

$$(x,y,z) \mapsto (x^4,y^4,z^4).$$

(iv) A homology, g_4, of order 3.

Since g_4 is a homology, this element can not stabilise a hyperoval, by Theorem 52, p. 27.

The element g_1 has no fixed points, so the hyperoval it stabilises is constructed by gluing together 22 orbits. The normaliser is transitive on orbits of $\langle g_1 \rangle$ so one can pick their favourite orbit first. When the search is completed no hyperovals are found.

The element g_2 has $(0,0,1)$, $(0,1,0)$, $(1,0,0)$ as the fixed points. We can have the hyperoval containing all the fixed points or containing no fixed points; hence two searches need to be made. The normaliser of $\langle g_2 \rangle$ is transitive on orbits not on the sides of the triangle. So we take the orbit of $(1,1,1)$ under $\langle g_2 \rangle$ as the first orbit, and then commence the two separate searches. Hyperovals with the three fixed points give only the regular hyperoval, and there are no hyperovals without the three fixed points.

The element $\langle g_3 \rangle$ has as $PG(2,4)$ as a fixed configuration. Every line of $PG(2,64)$ that is a line of $PG(2,4)$ meets the hyperoval in either 0 or 2 points. Hence the hyperoval is disjoint with $PG(2,4)$ or its intersection is a hyperoval of $PG(2,4)$. If the hyperoval and $PG(2,4)$ are disjoint the search finds no hyperoval. Now assume that the hyperoval meets $PG(2,4)$ in a 6-arc (a hyperoval of $PG(2,4)$), which is the regular hyperoval $\mathcal{D}(x^2)$ in $PG(2,4)$. A total of 366 hyperovals are constructed; 6 are regular, 36 isomorphic to $\mathcal{H}_{60}$, 144 isomorphic to $\mathcal{H}_{15}$, and 180 are isomorphic to a new hyperoval, Penttila-Royle, $\mathcal{D}(f)$ where

$$\begin{aligned} f(x) = {} & \omega^{42}x^2 + \omega^{42}x^4 + x^6 + \omega^{42}x^8 + x^{10} + x^{12} + \omega^{21}x^{20} + \omega^{21}x^{22} \\ & + \omega^{42}x^{24} + \omega^{42}x^{28} + x^{32} + \omega^{42}x^{36} + \omega^{42}x^{40} + \omega^{21}x^{42} \\ & + \omega^{21}x^{44} + x^{52} + x^{54} + \omega^{42}x^{56} + x^{58} + \omega^{42}x^{60} + \omega^{42}x^{62}. \end{aligned}$$

The hyperoval has a full collineation stabiliser of order 12 and we denote it by $\mathcal{H}_{12}$.

For elements of order 2 of $P\Gamma L(3,64)$ we use Theorem 56, p. 28 to determine that we have either:

(i) An elation g_1 represented by

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix},$$

or,

(ii) the field automorphism g_2 represented by

$$(x, y, z) \mapsto (x^8, y^8, z^8).$$

By Theorem 58, p. 28, the fixed line $x = 0$ of the elation g_1 is secant to the hyperoval and the centre is not on the hyperoval. The normaliser N of $\langle g_1 \rangle$ acts doubly transitively on the points on the axis not equal to the centre so we can select the two points $(0,0,1)$ and $(0,1,0)$ to be in the hyperoval. The stabiliser of these two points in N is still transitive on all the points off the axis and therefore a further orbit of length two can be chosen, in this case, $(1,0,0)$ and $(1,1,1)$. From this initial configuration the search found 2 regular hyperovals, 64 hyperovals isomorphic to $\mathcal{H}_{12}$, and 64 hyperovals isomorphic to $\mathcal{H}_{60}$.

The element g_2 has fixed configuration $PG(2,8)$. As before, we do searches when the hyperoval is disjoint from $PG(2,8)$ and searches where they intersect; the intersection being a 10-arc of $PG(2,8)$ (without loss of generality, $\mathcal{D}(2)$). When the hyperoval and $PG(2,8)$ are disjoint the search found nothing; when they intersect the 10-arc completes to a regular hyperoval.

Theorem 114 ([**111**]). *There are precisely four isomorphism classes of hyperovals in $PG(2,64)$ stabilised by any non-trivial automorphism. They are the regular hyperoval $\mathcal{D}(x^2)$ and the three hyperovals $\mathcal{H}_{12}$, $\mathcal{H}_{15}$ and $\mathcal{H}_{60}$.*

With current computing power under a no symmetry hypothesis (that is, trivial stabiliser) the search is infeasible.

10. A Quick Look in $PG(2,q)$, $q > 64$

Searches for hyperovals (or related structures implying the existence of hyperovals) have been made in $PG(2,q)$, for some values of $q > 64$.

For $q = 128$ we have

$$|P\Gamma L(3,128)| = 337 \cdot 127^2 \cdot 43 \cdot 7^3 \cdot 3 \cdot 2^{21}.$$

By using the "prime at a time" techniques one can immediately rule out the prime 337.

Due to the large orbits obtained from the groups of order 127 and 43, naive exhaustive searches are possible. Only the regular hyperovals are found stabilised by a group divisible by 127 or by a group divisible by 43.

Searches for hyperovals in $PG(2,128)$ and $PG(2,256)$ stabilised by the element

$$(x,y,z) \mapsto (x^2,y^2,y^2)$$

that is, o-polynomials with coefficients over $GF(2)$, have been made in [**111**]. There are no new $GF(2)$ o-polynomials in $PG(2,128)$ and $PG(2,256)$. The authors speculate that $GF(2)$ o-polynomials are rare in planes of square order (the o-polynomials belonging to the regular, translation or the Subiaco hyperovals as described in Chapters III and IV).

Further searches have been done by Penttila and Royle (see [**111**] and [**101**]). As of the writing of this work (September 1995), new hyperovals have been found in $PG(2,256)$, $PG(2,1024)$, $PG(2,4096)$, and $PG(2,16384)$. These are associated with cyclic q–clans and we shall talk about these in Chapter III, Section 15.1, p. 121.

The new hyperoval found in $PG(2,256)$ has o-polynomial of the form

$$\begin{aligned}
f_2 =\!:\ & \omega^{112}x^2+\omega^{211}x^4+\omega^{130}x^6+\omega^{80}x^8+\omega^{84}x^{10}+\omega^{57}x^{12}+\omega^{250}x^{14}+\omega^{144}x^{16}+\\
& \omega^{27}x^{18}+\omega^{47}x^{20}+\omega^{135}x^{22}+\omega^{194}x^{24}+\omega^{143}x^{26}+\omega^{111}x^{28}+\omega^{214}x^{30}+\omega^{107}x^{32}+\\
& \omega^{95}x^{34}+\omega^{83}x^{36}+\omega^{79}x^{38}+\omega^{51}x^{40}+\omega^{155}x^{42}+\omega^{45}x^{44}+\omega^{200}x^{46}+\omega^{185}x^{48}+\\
& \omega^{55}x^{50}+\omega^{115}x^{52}+\omega^{209}x^{54}+\omega^{124}x^{56}+\omega^{85}x^{58}+\omega^{64}x^{60}+\omega^{94}x^{62}+\omega^{35}x^{64}+\\
& \omega^{153}x^{66}+\omega^{181}x^{68}+\omega^{54}x^{70}+\omega^{106}x^{72}+\omega^{82}x^{74}+x^{76}+\omega^{164}x^{78}+\omega^{206}x^{80}+\omega^{32}x^{82}+\\
& \omega^{69}x^{84}+\omega^{183}x^{86}+\omega^{200}x^{88}+\omega^{21}x^{90}+\omega^{22}x^{92}+\omega^{239}x^{94}+\omega^{228}x^{96}+\omega^{53}x^{98}+\\
& \omega^{31}x^{100}+\omega^{206}x^{102}+\omega^{62}x^{104}+\omega^{171}x^{106}+\omega^{122}x^{108}+\omega^{190}x^{110}+\omega^{18}x^{112}+\\
& \omega^{204}x^{114}+\omega^{66}x^{116}+\omega^{172}x^{118}+\omega^{169}x^{120}+\omega^{177}x^{122}+\omega^{9}x^{124}+\omega^{254}x^{126}+\\
& x^{128}+\omega^{254}x^{130}+\omega^{9}x^{132}+\omega^{177}x^{134}+\omega^{169}x^{136}+\omega^{172}x^{138}+\omega^{66}x^{140}+\omega^{204}x^{142}+\\
& \omega^{18}x^{144}+\omega^{190}x^{146}+\omega^{122}x^{148}+\omega^{171}x^{150}+\omega^{62}x^{152}+\omega^{206}x^{154}+\omega^{31}x^{156}+\omega^{53}x^{158}+\\
& \omega^{228}x^{160}+\omega^{239}x^{162}+\omega^{22}x^{164}+\omega^{21}x^{166}+\omega^{200}x^{168}+\omega^{183}x^{170}+\omega^{69}x^{172}+\omega^{32}x^{174}+\\
& \omega^{206}x^{176}+\omega^{164}x^{178}+x^{180}+\omega^{82}x^{182}+\omega^{106}x^{184}+\omega^{54}x^{186}+\omega^{181}x^{188}+\omega^{153}x^{190}+\\
& \omega^{35}x^{192}+\omega^{94}x^{194}+\omega^{64}x^{196}+\omega^{85}x^{198}+\omega^{124}x^{200}+\omega^{209}x^{202}+\omega^{115}x^{204}+\omega^{55}x^{206}+\\
& \omega^{185}x^{208}+\omega^{200}x^{210}+\omega^{45}x^{212}+\omega^{155}x^{214}+\omega^{51}x^{216}+\omega^{79}x^{218}+\omega^{83}x^{220}+\omega^{95}x^{222}+\\
& \omega^{107}x^{224}+\omega^{214}x^{226}+\omega^{111}x^{228}+\omega^{143}x^{230}+\omega^{194}x^{232}+\omega^{135}x^{234}+\omega^{47}x^{236}+
\end{aligned}$$

$\omega^{27}x^{238}+\omega^{144}x^{240}+\omega^{250}x^{242}+\omega^{57}x^{244}+\omega^{84}x^{246}+\omega^{80}x^{248}+\omega^{130}x^{250}+\omega^{211}x^{252}+\omega^{112}x^{254}$

where ω is a primitive element of $GF(256)$ satisfying $\omega^8+\omega^4+\omega^3+\omega^2+1=0$.

11. Applications of Hyperovals

11.1. Generalised Quadrangles

A large portion of Chapter III, p. 81, is dedicated to the connections between generalised quadrangles (see Section 9, p. 11 for the definition of a generalised quadrangle) and hyperovals.

11.2. Codes

In a point line geometry if we let A be the line-point incidence matrix of the geometry then the **code** is the span of the rows over $\mathbb{Z}_p$ for some prime p.

Usually the code is either the whole space of the geometry or a hyperplane. Only if p is well-chosen is the code interesting. For instance, in a projective plane of order q, the code is interesting if and only if p divides q [**71**][**48**].

We define the **extended code**, C, of projective plane of even order to be the code generated by

$$\begin{pmatrix} & 1 \\ A & \vdots \\ & 1 \end{pmatrix},$$

where A is the line-point incidence matrix.

Let q be even, so $p=2$. Let r_1, r_2 be rows of A. Since any two distinct lines meet in a unique point then $r_1 \cdot r_2 = 1$ so

$$(r_1,1)\cdot(r_2,1) \equiv 0 \pmod 2.$$

Also in a projective plane of order q, $r_1 \cdot r_1 = q+1$, so

$$(r_1,1)\cdot(r_1,1) = q+2 \equiv 0 \pmod 2.$$

So the rows of the extended matrix are orthogonal, that is, $C \subseteq C^{\perp}$, where C is the extended code of the extended matrix A. Studying C is equivalent to studying $C^{\perp}$ (since $C = C^{\perp\perp}$). We call $C^{\perp}$ the **dual** of the extended binary code of the plane. We define the **weight** of a codeword, r, of the extended code as the number of ones in r. Let w_i be the number of words of weight i. The weight enumerator of $C^{\perp}$ is the polynomial

$$w(x,y) = \sum_{i=0}^{q^2+q+2} w_i x^i y^{q^2+q+2-i}.$$

We will try to give some geometric interpretations of $C^\perp$, q even:

Let $(u,0) \in C^\perp$. Then we define the **support** of u to be

$$\mathrm{support}(u) = \{ \text{ points } P \mid \text{ the component of } u \text{ corresponding to } P = 1\}.$$

It will also be convenient to identify a line l with the row vector corresponding to it.

Let $U = \mathrm{support}(u)$. Then U has **even type**, that is, class $[0,2,4,\dots,q^2+q]$, (see Section 1, p. 15, Chapter I). (Since for any line l, $|l \cap U| = (l,1)\cdot(u,0) \equiv 0 \pmod 2$, as $(u,0) \in C^\perp$ with $C^\perp = \langle (l,1) \mid l\rangle^\perp$. So $|l\cap U|$ is even.)

Let $(u,1) \in C^\perp$. Let $U = \mathrm{support}(u)$. Then U has **odd type**, that is, class $[1,3,5,\dots,q^2+q+1]$. (Since for a line l, $|l\cap U| = (l,1)\cdot(u,1) \equiv 1 \pmod 2$ as $(u,1)\in C^\perp$. So $|l \cap U|$ is odd.)

So studying $C^\perp$ is equivalent to studying all sets of even type and all sets of odd type in the plane.

The **minimum weight** of $C^\perp$ is the minimum weight of the nonzero code words in $C^\perp$.

THEOREM 115 ([**3**]). *A word, w, of $C^\perp$ has weight $q+2$ if and only if the word is $w=(l,1)$, for a line l, or* support(w) *is a hyperoval.*

PROOF. Recall that a nonempty set of even type has greater than or equal to $q+2$ points with equality if and only if it is a hyperoval.

By the results of Theorem 27, p. 15 (and the notation used there); for a k-set of even type we have

$$t_0 + t_2 + \cdots + t_q = q^2+q+1,$$
$$2t_2 + 4t_4 + \cdots + qt_q = k(q+1), \text{ and}$$
$$2t_2 + 4.3t_4 + \cdots + q(q-1)t_q = k(k-1).$$

Hence we have (via the last two equations)

$$4.2t_4 + \cdots + q(q-2)t_q = k(k-(q+2)).$$

If $0 < k \le q+2$ then we have the right hand side of the above equation being less than zero while the left hand side is always positive. So $k \ge q+2$, with equality if and only if $t_4 = t_6 = \cdots = t_q = 0$. Hence if the k-set has class $[0,2]$ and is non-empty then it must be that the k-set is a hyperoval.

Let $\mathcal{K}$ be a set of odd type. Let $P \notin \mathcal{K}$, then for each of the $q+1$ lines on P they must meet $\mathcal{K}$ in at least one point. Hence $|\mathcal{K}| \ge q+1$. Now a line is a set of type $(1,q+1)$, so is of odd type. Suppose $|\mathrm{support}(u)| = q+1 = |\mathcal{K}|$ for some k-set $\mathcal{K}$ but is not a line. Let l be a secant line to $\mathcal{K}$. Let $Q \notin \mathcal{K}$ be a point on l. Then by the previous result every line on Q meets $\mathcal{K}$ in at least one point, implying $|\mathcal{K}| > q+1$. Hence support(u) is a line for $(u, 1) \in C^\perp$. Thus a set of odd type has greater than or equal to $q+1$ points with equality if and only if it is a line. □

Thus the minimum weight of $C^\perp$ is $q+2$ and

$$w_{q+2} = (q^2+q+1) + \text{ the number of hyperovals in the plane.}$$

A binary code C is **self-orthogonal** if and only if $C \subseteq C^\perp$, and is **self-dual** if and only $C = C^\perp$. The extended binary code of a projective plane of even order q is self-dual if and only if $q \equiv 2 \pmod 4$. We know only one such plane: $PG(2,2)$.

The above results have been used by Lam et al. [**70**] to show that if a **projective plane of order 10** existed it would have no hyperovals and by investigating the code (amongst other things!) Lam et al. [**69**] proved the non-existence of a projective plane of order 10.

11.3. Ovoids

A ***k*-cap** in $PG(3,q)$ is a set of k points no three collinear.

An **ovoid** is a (q^2+1)-cap of $PG(3,q)$ if $q > 2$; an ovoid of $PG(3,2)$ is a set of 5 points, no 4 coplanar.

An excellent introduction to the relationship between ovoids and ovals is [**108**].

There are only two known classes of ovoids in $PG(3,q)$ up to equivalence:

(i) Elliptic Quadric: This is the set of all totally singular one-dimensional subspaces of $GF(q)^4$ with respect to a non-singular quadratic form of Witt index one.

(ii) Tits Ovoid: This is the set of all absolute points of a polarity of $W(q)$ (see Chapter III) where $q = 2^e$ and e is odd, $e > 1$.

By the action of $P\Gamma L(4,q)$ on the ovoids we can describe the set of points of the ovoids by our favourite canonical form:

Elliptic Quadric: Let $a \in GF(q)$ with x^2+x+a being irreducible over $GF(q)$, then we can describe the elliptic quadric as:

$$\{(t^2+st+as^2, 1, s, t) \mid s, t \in GF(q)\} \cup \{(1,0,0,0)\}.$$

The stabiliser in $PGL(4,q)$ of an elliptic quadric, namely $PO^-(4,q)$, acts 3–transitively on the points of the elliptic quadric.

Tits Ovoid: Let $q = 2^e$ with e odd, $e > 1$, and let $\sigma \in \operatorname{Aut} GF(q)$ such that $\sigma^2 \equiv 2 \pmod{q-1}$ then the Tits ovoid can be described as:

$$\{(t^\sigma+st+s^{\sigma+2}, 1, s, t) \mid s, t \in GF(q)\} \cup \{(1,0,0,0)\}.$$

> The stabiliser in $PGL(4,q)$ of a Tits ovoid, namely the **Suzuki group** $Sz(q)$, acts 2-transitively on the points of the Tits ovoid.

For a Tits ovoid, as defined above with σ, we can define a **Tits oval** as an oval equivalent to $\mathcal{D}(\sigma) - \{(0,1,0)\}$ and a **Tits hyperoval** as a hyperoval equivalent to $\mathcal{D}(\sigma)$.

THEOREM 116. *Every plane meets an ovoid in either* 1 *point (**tangent plane**) or* $q+1$ *points (**secant plane**).*

A plane section of an ovoid in $PG(3,q)$ is an oval in $PG(2,q)$.

Every plane section of an elliptic quadric is a conic. Every plane section of a Tits ovoid is a Tits oval. (The Tits oval is a translation oval and so has a unique axis; these axes form the Lüneburg spread [**133**] [**74**].)

THEOREM 117 (External Lines Lemma). *Let $\mathcal{O}$ be a translation oval of $PG(2,q)$, q even, with nucleus N, and let l be an axis of $\mathcal{O}$. Let P be a point of $\mathcal{O}$ on l and let Q be another point of l, distinct from P and N. Suppose that $\mathcal{O}'$ is a translation oval containing P such that its nucleus N' is a point on l distinct from Q. If every line on Q external to $\mathcal{O}$ is also external to $\mathcal{O}'$ then l is an axis of $\mathcal{O}'$.*

For $\alpha \in \operatorname{Aut} GF(q)$ and a function $d\colon GF(q) \to GF(q)$, let $\Omega(\alpha, d)$ denote the set

$$\Omega(\alpha,d) = \{t^\alpha + st + d(s), 1, s, t) \mid s,t \in GF(q)\} \cup \{(1,0,0,0)\}.$$

With this definition we can say the elliptic quadric is the ovoid $\Omega(2, s \mapsto as^2)$ where $\operatorname{trace}(a) = 1$, and $\Omega(\sigma, \sigma+2)$ with $\sigma^2 = 2$ describes the Tits ovoid.

LEMMA 118 ([**108**]). *Suppose that Ω is an ovoid in $PG(3,q)$, where $q = 2^e > 2$, and that π is a secant plane such that $\pi \cap \Omega$ is a translation oval with associated automorphism α. Let l be an axis of $\pi \cap \Omega$. Suppose that each secant plane to Ω on l meets Ω in a translation oval. Then there is a collineation of $PG(3,q)$ mapping Ω to $\Omega(\alpha, d)$ where $d\colon GF(q) \to GF(q)$ satisfies $d(0) = 0$ and*

$$d(a) + d(b) \notin (a+b)^{\alpha/(\alpha-1)} K \tag{2}$$

for all a, $b \in GF(q)$ with $a \neq b$, where K is the kernel of the trace map. Conversely, if α is a generator of $\operatorname{Aut} GF(q)$ and $d \in GF(q) \to GF(q)$ has $d(0) = 0$ and satisfies Eq. 2 for all $a \neq b$, then $\Omega(\alpha, d)$ is an ovoid.

THEOREM 119 ([**108**]). *Suppose that Ω is an ovoid in $PG(3,q)$, where q is even, $q > 2$, and that π is a secant plane such that $\pi \cap \Omega$ is a translation oval. Let l be an axis of $\pi \cap \Omega$. Then all secant planes to Ω on l meet Ω in translation ovals if and only if Ω is an elliptic quadric or a Tits ovoid.*

PROOF. By Lemma 118, p. 72, there is a generator α of $\operatorname{Aut} GF(q)$ and a function d such that $\Omega = \Omega(\alpha, d)$:

Let

$$M_u = \begin{pmatrix} 1 & u^\alpha & u & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & u & 0 & 1 \end{pmatrix},$$

for $u \in GF(q)$. Then

$$M_u \begin{pmatrix} t^\alpha + st + d(s) \\ 1 \\ s \\ t \end{pmatrix} = \begin{pmatrix} (t+u)^\alpha + s(t+u) + d(s) \\ 1 \\ s \\ t+u \end{pmatrix},$$

so $M_u \Omega = \Omega$. Also, M_u is a translation of the inversive plane $\mathcal{I}$ (see below) associated with Ω. Moreover, $M = \{M_u \mid u \in GF(q)\}$ is transitive on the points other than $(0,0,0,1)$ of the oval $\pi_s \cap \Omega$ of the secant plane $\pi_s\colon x_3 = sx_2$ to Ω on l for each $s \in GF(q)$. Hence $\mathcal{I}$ does not have Hering type I.1. So, by the results of Glynn [**43**], Ω is an elliptic quadric or a Tits ovoid. □

Corollary 120 ([**108**]). *Since the only ovals of $PG(2,8)$ are translation ovals (see page 46) the only ovoids of $PG(3,8)$ are the elliptic quadric and the Tits ovoid.*

Theorem 121 ([**56**]). *The only ovoids of $PG(3,2)$ and $PG(3,4)$ are the elliptic quadrics.*

Let $\mathcal{O}_1$ and $\mathcal{O}_2$ be ovals of $PG(2,q)$ and let P be a point of $PG(2,q)$ not on either of the ovals and distinct from their nuclei. Then $\mathcal{O}_1$ and $\mathcal{O}_2$ are **compatible** at P if:

(i) they have the same nucleus,
(ii) they have a point Q in common,
(iii) the line PQ is a tangent line to each oval, and
(iv) every secant line to $\mathcal{O}_1$ on P is external to $\mathcal{O}_2$.

Hence we have that every external line to $\mathcal{O}_1$ on P is a secant line to $\mathcal{O}_2$.

A **pencil** of an ovoid Ω is the set of secant plane sections to Ω for planes on a fixed tangent line.

The following theorem was found independently by D. Glynn and T. Penttila [**105**].

Theorem 122 (The Plane Equivalence Theorem). *An ovoid of $PG(3,q)$ is equivalent to a set of q ovals $\mathcal{O}_s$, $s \in GF(q)$, of $PG(2,q)$ all with nucleus $(0,1,0)$ satisfying*

$$\mathcal{O}_s \cap \mathcal{O}_t = \{(0,0,1)\} \text{ for all } s \neq t \text{ in } GF(q),$$

and such that $\mathcal{O}_s$ and $\mathcal{O}_t$ are compatible at $(0,1,s+t)$. Moreover, each pencil of the ovoid Ω gives rise to such a set, and for each plane π of the pencil there is a parameterisation of the planes π_s of the pencil, $s \in GF(q)$, such that $\pi_0 = \pi$ and there is a homography M_s taking $\pi_s \cap \Omega$ to $\mathcal{O}_s$ and the tangent line of the pencil to the line $[1,0,0]$.

The image under a collineation of such a set of ovals is called a **fan** of ovals and the image of the line $[1,0,0]$ is called the **common tangent**.

Let $\mathcal{O}_1$ and $\mathcal{O}_2$ be ovals and P_1 and P_2 be points of $PG(2,q)$. We say that $(P_1, \mathcal{O}_1)$ **matches** with $(P_2, \mathcal{O}_2)$ if there is a collineation g such that $g\mathcal{O}_1$ and $\mathcal{O}_2$ are compatible at P_2 and $gP_1 = P_2$.

The Plane Equivalence Theorem leads us to study compatible ovals and therefore matching point-oval pairs. Hence a classification of hyperovals in $PG(2,q)$ will result in a classification of ovoids in $PG(3,q)$.

As all hyperovals are classified in $PG(2,q)$ for $q \leq 32$ (see Section 6, p. 46) then all matching point-oval pairs can be determined. Penttila and O'Keefe [**79**] [**83**] have shown that the only fans in $PG(2,16)$ are with conics and so every plane section of an ovoid in $PG(3,16)$ is a conic, hence all ovoids of $PG(3,16)$ are elliptic quadrics. O'Keefe, Penttila and Royle [**86**] have shown that in $PG(3,32)$ all matches are with translation ovals, hence by Theorem 119, p. 72, the only ovoids are Tits ovoids or elliptic quadrics.

11.4. Inversive Planes

An **inversive plane** is an incidence structure $\mathscr{I} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ with elements of $\mathcal{B}$ called **circles**, satisfying,

(i) any three distinct points of $\mathcal{P}$ lie on exactly one circle,
(ii) if P is a point and C_1, C_2, C_3 are distinct circles such that $C_1 \cap C_2 = C_2 \cap C_3 = \{P\}$ then $C_1 \cap C_3 = \{P\}$.

It is interesting to note that given a point $P \in \mathcal{P}$, the points different from P and the circles incident with P form an affine plane [**36**]. The **order** of the inversive plane, if it is finite, is the order of the constructed affine plane (which is independent of the choice of P).

Let $\mathcal{I} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ be an incidence structure such that

(i) $\mathcal{P} =$ points of an ovoid $\mathcal{O}$,
(ii) $\mathcal{B} =$ secant planes to $\mathcal{O}$,
(iii) I is the natural incidence.

Then $\mathcal{I}$ is an inversive plane.

A **bundle** is a set of circles through two distinct points. The two distinct points associated with a bundle are called the **carriers** of a bundle.

A **pencil** is any maximal set of mutually tangent circles (that is, meeting in exactly one point) through a common point P, called the **carrier** of the pencil.

A **flock** is a set F of mutually disjoint circles of an inversive plane such that, with exception of precisely two points, the **carriers** of the flock, every point of the inversive plane is on a unique circle of F.

An inversive plane arising from an ovoid is called **egglike**, and any inversive plane of even order is egglike [**36**, 6.2.14]. From this we have:

THEOREM 123. *If two inversive planes of even order are isomorphic then their corresponding ovoids are isomorphic.*

PROOF. By Theorem 200, p. 143, Chapter IV, all flocks of ovoids in $PG(3,q)$ are linear. Hence the incidence structure with points the points and circles of the inversive plane and lines the bundles, pencils and flocks of the inversive planes is isomorphic to the point-line structure of a projective plane. (The incidence here is natural: a circle is incident with a bundle, pencil or flock if it is in the bundle, pencil or flock, respectively; a point is incident with no flock and with only those bundles and pencils for which it is a carrier). Thus an isomorphism between two inversive planes of even order induces an isomorphism between the two associated projective spaces, carrying points of the first inversive plane to points of the second. Thus if the inversive planes are isomorphic so are the underlying ovoids. □

From this theorem and the results in Section 11.3, p. 71, we can now say that there is exactly one inversive plane of each order 2, 4, 16. There are exactly two inversive planes of order 8 and 32.

11.5. Partial Geometries and Strongly Regular Graphs

A **partial geometry** is an incidence structure $pg = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ such that:

(i) Each point is incident with $t+1$ lines ($t \geq 1$) and two distinct points are incident with at most one line.

(ii) Each line is incident with $s+1$ points ($s \geq 1$) and two distinct lines are incident with at most one point.

(iii) If P is a point and l is a line not incident with P, then there are exactly α ($\alpha \geq 1$) points $P_1, \dots, P_\alpha$ and α lines $l_1, \dots, l_\alpha$ such that $P \ \mathrm{I}\ l_i$, $P_i \ \mathrm{I}\ l_i$, and $P_i \ \mathrm{I}\ l$, for all $i = 1, \dots, \alpha$

If $|\mathcal{P}| = v$ and $|\mathcal{B}| = b$ then $v = \frac{1}{\alpha}(1+s)(st+\alpha)$ and $b = \frac{1}{\alpha}(1+t)(st+\alpha)$ and we denote $pg = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ by $pg(s,t,\alpha)$.

Let $\mathscr{I} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ be an incidence structure such that

(i) $\mathcal{P} =$ points of a hyperoval $\mathcal{H}$,

(ii) $\mathcal{B} =$ secant lines to $\mathcal{H}$,

(iii) I in the natural incidence.

Then $\mathscr{I}$ is a partial geometry $pg(q-2, q/2, (q/2)-1)$.

Now every partial geometry defines a strongly regular graph. Let Γ be the **point graph** of the partial geometry $pg(s,t,\alpha) = (\mathcal{P}, \mathcal{B}, \mathrm{I})$. That is, the vertices of Γ are $\mathcal{P}$ and $x \sim y$ (adjacency) whenever x and y are collinear in pg. The graph Γ is **regular** since every point of pg is collinear with $s(t+1)$ points (not including itself). The adjacency graph of the partial geometry has:

(i) any two adjacent vertices have $\lambda = s - 1 + t(\alpha - 1)$ common neighbours,
(ii) any two nonadjacent vertices have $\mu = \alpha(t+1)$ common neighbours.

Hence Γ is a **strongly regular graph**, with parameters

$$\mathrm{srg}(\nu, k, \lambda, \mu) = \mathrm{srg}(\frac{1}{\alpha}(1+s)(st+\alpha), s(t+1), s-1+t(\alpha-1), \alpha(t+1)).$$

11.6. B-ovals

A **Buekenhout oval** [**21**], or B**-oval**, of order q is a set M of $q+1 \geq 3$ points and a set F of permutations of M such that

(i) each $f \in F$ has order at most 2;
(ii) F is quasi sharply 2-transitive in the sense that for any (a_1, a_2) and $(b_1, b_2) \in M \times M$, with $a_i \neq b_j$ for i, $j = 1$, 2, there is a unique $f \in F$ such that $f(a_1) = a_2$ and $f(b_1) = b_2$

The identity permutation belongs to F if and only if q is even [**21**].

Every oval, $\mathcal{O}$, of a projective plane, π, gives rise to a B-oval, whose points are those of the oval, $\mathcal{O}$. The permutations, ϕ_P, are associated with each point, P, not on the oval, ϕ_P fixes the point X when $|PX \cap \mathcal{O}| = 1$, and maps X to X' where $|PX \cap \mathcal{O}| = 2$ with $PX \cap \mathcal{O} = \{X, X'\}$. We call such a B-oval obtained from an oval in a projective plane a projective B-oval. Thus we have B-conics, a projective B-oval obtained from a conic.

Faina [**39**] has classified all B-ovals of order $q \leq 8$ using some results of Mathon [**76**]. There are nine isomorphism classes.

11.7. Howell Designs

Let Γ be a graph with edges $E(\Gamma)$ and vertices $V(\Gamma)$. A graph Γ_1 is a **spanning** subgraph of Γ if $V(\Gamma_1) = V(\Gamma)$. A **factorisation** $\mathcal{F} = \{F_1, \ldots, F_t\}$ of the graph Γ is a partition of $E(\Gamma)$ into edge-disjoint spanning subgraphs, called **factors**. A subgraph Δ of Γ is **suborthogonal** to $\mathcal{F}$ if $|E(\Delta) \cap E(F_i)| \leq 1$ for $1 \leq i \leq t$ and **orthogonal** to $\mathcal{F}$ if $|E(\Delta) \cap E(F_i)| = 1$ for $1 \leq i \leq t$.

A k**-factor**, Δ, of Γ is a spanning subgraph of Γ with each vertex of Δ having valency k, that is, Δ is a k**-regular** spanning subgraph of Γ. (Note one-factors are sometimes called **perfect matchings**.) A partition of the edges of a k-regular graph into one-factors is called a **one-factorisation**.

Let K_{2n} be the **complete graph** on $2n$ vertices.

A **Howell design** $H(s,2n)$ is an $s\times s$ array, $n\le s\le 2n-1$, in which cells are empty or contain an edge of K_{2n}, no edge occurs in more than one cell, and each row and column is a 1-factor of K_{2n}. Or, more conventionally [**60**], a Howell design $H(s,2n)$ is a square of side s, $n\le s\le 2n-1$, such that each cell is empty or contains an unordered pair of integers from $\{1,2,\dots,2n\}$ such that each integer from 1 to $2n$ appears exactly once in every row and column and every unordered pair of integers appears at most once in a cell of the square. A Howell design where $s=2n-1$ is sometimes called a **Room design**.

EXAMPLE. Let $\mathcal{H}$ be a hyperoval. Define Γ to be a graph with $V(\Gamma)=\{\text{points of }\mathcal{H}\}$. Let l and m be external lines to $\mathcal{H}$ with $P=l\cap m$. Then the edges of Γ are the secants to $\mathcal{H}$ meeting l and m not on P. The vertices of Γ become the symbols for the Howell design. The edges of Γ become the pairs which occur together in the Howell design. A pair of orthogonal one-factorisations become the rows and columns of the Howell design.

THEOREM 124 ([**1**]). *Let $\mathcal{H}$ be a hyperoval in a projective plane, π, of order q. Then there is a Howell design $H(q,q+2)$.*

PROOF. Let X be a point of π not on $\mathcal{H}$. Let Γ be the complete graph on $q+2$ vertices minus a 1-factor where $V(\Gamma)=\{\text{points of }\mathcal{H}\}$ and adjacency is defined as

$$P\sim Q \iff PQ \text{ is not a line on } X.$$

Any external line l on X gives a 1-factorisation of Γ with 1-factors being the lines on Y where Y I l and distinct from X.

Any two external lines on X give an orthogonal 1-factorisation. So from the above Example we get a Howell design $H(q,q+2)$. □

COROLLARY 125. *If $e\ge 2$ then there is a Howell design of type $H(2^e,2^e+2)$.*

12. End Notes

NOTES ON SECTION 1, P. 15. The results in this Section are well known.

NOTES ON SECTION 2, P. 18. For Theorem 45, p. 23, we use the easy fact that all sharply 4-transitive groups on a set of size six are classified (being A_6 and S_6).

The results in this Section are well known. The proof to Theorem 36, p. 19,

The theorems and proofs in this section are well-known.

is nonclassical.

NOTES ON SECTION 3, P. 23. The definition of collineation here is the same as that of page 23 by Theorem 5, p. 4.

The results in this Section are well known. Work on generalised homologies and elations is new but not original; work by the author and Penttila (see [**106**]). Section 3.4, p. 38, is known though unpublished (proofs communicated by Penttila).

Notes on Section 3.1, p. 24. The results in this Section are classical.

Let g be a collineation of a linear space $\mathscr{I}$ (page 14). The incidence structure (Fixed points of g, Fixed lines of g, $\mathrm{I}\ |_{\text{restricted}}$) is a linear space. Bruijn and Erdös [**34**] has shown that for a linear space (generalised to other structures by Buekenhout [**23**] and Dembowski [**36**]) the number of lines is equal to or greater than the number of points. Hence for an automorphism of a linear space the number of fixed lines is equal to or greater than the number of fixed points.

Theorem 60, p. 29, was proved in [**15**] but may have been proved in an earlier paper. In [**15**] theorems stronger than Theorem 65, p. 30 and Theorem 66, p. 31 are proved from which they follow (with difficulty).

Notes on Section 3.5, p. 40. The study of a set of points no three collinear, especially when the set had size $q+1$, may have originated via Theorem 82, p. 40.

A **correlation**, g, of a projective space is a permutation g of the subspaces of $PG(d,q)$ which preserves equality of dimension (that is, $\dim x_1 = \dim x_2$ if and only if $\dim gx_1 = \dim gx_2$) and incidence (with incidence being symmetrised inclusion).

A correlation either preserves or reverses the usual ordering $\leq$ on the dimensions on a flag (that is, if $X \mathrm{\ I\ } x$ and $\dim X \leq \dim x$ then either we have $\dim gX \leq \dim gx$ or $\dim gx \leq \dim gX$). If g preserves $\leq$ then g is a collineation, else g is a **duality**. A duality of order two is a **polarity**.

Notes on Section 4, p. 41. The results in this Section are well known.

Notes on Section 5, p. 43. The results in this Section are well known.

Notes on Section 6, p. 46. The Lunelli-Sce hyperoval is sometimes referred to as the **Hall hyperoval** as it was rediscovered by Hall [**47**].

The results on the Lunelli-Sce hyperoval after Theorem 100, p. 48, have been calculated using the algebraic package CAYLEY [**26**].

The author would like to thank Bill Cherowitzo for working out the inverse of the Cherowitzo o-polynomial.

Theorem 102, p. 48, and Theorem 107, p. 51, are new and appear in [**106**] and are a collaborative effort between the author and Penttila. Theorem 103, p. 49, and Theorem 104, p. 50, take advantage of the herd model to be introduced in Chapter III. The rest of the Section is well known.

NOTES ON SECTION 6.8, P. 53. A rational form of the O'Keefe-Penttila o-polynomial is

$$\frac{\eta^{11}x^{12}+\eta^{8}x^{10}+x^{9}+\eta^{6}x^{8}+\eta^{19}x^{7}+\eta^{19}x^{6}\eta^{20}x^{6}+\eta^{20}x^{5}+x^{4}+\eta^{27}x^{3}+\eta^{11}x}{x^{12}+x^{10}+x^{8}+x^{6}+x^{4}+x^{2}}$$

where η is a primitive element of $GF(32)$ satisfying $\eta^5=\eta^2+1$.

NOTES ON SECTION 7, P. 54. This Section is from [**110**].

NOTES ON SECTION 8, P. 55. This Section has been published in [**107**]. The work is a collaborative effort between the author and Penttila.

NOTES ON SECTION 8.1, P. 55. Elements of $GF(q^2)$ satisfying $x^2+\omega^{58}x+1=0$ are of order 13. Hence T is the group generated by the companion matrix of this polynomial.

NOTES ON SECTION 8.2, P. 56. Let ω be a primitive element of $GF(q)$, $q=2^e$, with $\langle\omega\rangle=GF(q)^*$. For

$$G_{p,n}=\left\langle\begin{pmatrix}1&0&0\\0&\omega^i&0\\0&0&\omega^{ni}\end{pmatrix}\right\rangle$$

where $|\omega^i|=p$, $p\mid q-1$, to stabilise a hyperoval, it is necessary that the orbit of $(1,1,1)$ is an arc, since the centraliser of $G_{p,n}$ in $PGL(3,q)$ is transitive on points with all coordinates non-zero; thus all orbits on these points are equivalent.

If the prime $p=2^j-1$, that is, a Mersenne prime (so j is necessarily a prime) then the orbit $\{(1,\omega^i,\omega^{ni})\mid|\omega^i| \text{ divides } p\}$ is contained in $PG(2,2^j)$. Thus the orbit of $(1,1,1)$ is an arc if and only if $\mathcal{D}(n)$ is a hyperoval in $PG(2,2^j)$.

Unfortunately this result only seems useful when all the monomial hyperovals are known in $PG(2,2^j)$.

NOTES ON SECTION 8.3, P. 57. Recall the Samosa Lemma 7, Chapter I.

The centraliser of an element g of order a q-primitive prime divisor of q^n-1 can be bigger than just a Singer cycle: when the prime is not a p-primitive prime divisor, but rather divides $p^{ni}-1$ for some divisor i of h, when $q=2^h$, then the

$$\mathrm{Gal}\left(\frac{GF(q^n)}{GF(2^{ni})}\right)$$

part of the normaliser of the Singer cycle in question centralises g. Hence we can not always assume that from Theorem 20, p. 7 that $GF(q^d)^*$ part of the normaliser is the centraliser of the group G in $P\Gamma L(3,q)$. In particular:

For $q=4^e$, e odd, g is of order 5, we have $i=2$, as the centraliser of an element of order 5 in $P\Gamma L(2,q)$ has order $(q+1)e$ and thus the centraliser of an element of order 5 in $P\Gamma L(3,q)$ has order $(q^2-1)e$. From this we have $C_{P\Gamma L(3,64)}(C_5)$ has an element of order 3 that is not in $C_{PGL(3,64)}(C_5)$. This is the reason why we concentrate on calculating in $C_{PGL(3,64)}(C_5)$.

This is also of relevance to Theorem 186, p. 118, Chapter III.

NOTES ON SECTION 9, P. 62. The algorithms in this Section were implemented by the author and Penttila. Section 9.1, p. 65, is from [**111**].

NOTES ON SECTION 10, P. 68. The work in $PG(2,128)$ on the primes is by the author. The other searches are by Penttila and Royle ([**111**]).

NOTES ON SECTION 11, P. 69. The results in this Section are well known.

NOTES ON SECTION 11.6, P. 76. Pascal's theorem states that the three points of intersection of opposite sides of any hexagon inscribed in a nondegenerate conic are collinear. Buekenhout in [**22**] proved that if Pascal's theorem holds for any oval in a projective plane (not necessarily finite) then the plane is Pappian (equivalent to a plane constructed from a three dimensional vector space defined over a field) and the oval is a conic. This theorem shows how a local property of the plane can determine what type of plane it is. Buekenhout's results relied on the improved classification of 3-transitive groups by Zassenhaus' [**137**] work on 2-transitive groups.

The concept of B-oval arose from this work of Buekenhout.

CHAPTER III

Generalised Quadrangles

Recall the definitions of generalised quadrangles in Section 9, p. 11, Chapter I. We usually label $\mathscr{S} = (\mathscr{P}, \mathscr{B}, \mathrm{I})$ to be a GQ with points $\mathscr{P}$ and lines $\mathscr{B}$. We say GQ(s,t) or $\mathscr{S}(s,t)$ to mean a GQ of order (s,t). The reference [**103**] will be referred to as Payne and Thas. Note in this Chapter our groups are acting on the right!

1. Parameters and Regularity

THEOREM 126 (Payne and Thas, 1.2.1). *A finite generalised quadrangle of order (s,t) has $(s+1)(st+1)$ points and $(t+1)(st+1)$ lines.*

Let $\mathscr{S} = (\mathscr{P}, \mathscr{B}, \mathrm{I})$ be a generalised quadrangle of order (s,t). Let

$$E = \{\{x,y\} \mid x,y \in \mathscr{P}, x \sim y, \text{ and } x \neq y\},$$

then $(\mathscr{P}, E)$ is a graph, the point graph (see page 75) of $\mathscr{S}$.

Recall the definition and parameters of a strongly regular graph (SRG) in Section 11.5, p. 75.

LEMMA 127 (Payne and Thas, 1.2.2). *$(\mathscr{P}, E)$ is a strongly regular graph with parameters $v = (s+1)(st+1)$, where $|\mathscr{P}| = v$, $k = s(t+1)$, $\lambda = s-1$, and $\mu = t+1$.*

THEOREM 128 (Payne and Thas, 1.2.2). *A generalised quadrangle of order (s,t) has*

$$(s+t) \,\big|\, st(t+1)(s+1) \text{ and } (s+t) \,\big|\, s^2(st+1)$$

Let $\mathscr{S} = (\mathscr{P}, \mathscr{B}, \mathrm{I})$ be a generalised quadrangle. For $x \in \mathscr{P}$ we define x **perp** to be

$$x^{\perp} = \{y \in \mathscr{P} \mid y \sim x\}.$$

We note that $x \in x^\perp$ for all $x \in \mathscr{P}$. For a set $A \subseteq \mathscr{P}$ we define

$$A^\perp = \bigcap_{x \in A} \{x^\perp\},$$

that is, $A^\perp$, is the set of points collinear with *all* points of A.

The **trace** of a pair of distinct points x and y is

$$\text{trace}(x,y) = \{x,y\}^\perp = x^\perp \cap y^\perp = \{z \in \mathscr{P} \mid z \sim x \text{ and } z \sim y\}.$$

LEMMA 129. *If $x \sim y$, $x \neq y$, then $|\{x,y\}^\perp| = s+1$. If $x \nsim y$ then $|\{x,y\}^\perp| = t+1$.*

We define the **span** of a pair of distinct points x and y to be

$$\text{span}(x,y) = \{x,y\}^{\perp\perp} = \{u \in \mathscr{P} \mid u \sim z \text{ for all } z \in \{x,y\}^\perp\},$$

that is, points collinear with *all* points of $\{x,y\}^\perp$. If $x \nsim y$ then we call $\{x,y\}^{\perp\perp}$ the **hyperbolic line** determined by x and y.

LEMMA 130. *If $x \sim y$, $x \neq y$, then $|\{x,y\}^{\perp\perp}| = s+1$. If $x \nsim y$ then $2 \leq |\{x,y\}^{\perp\perp}| \leq t+1$.*

PROOF. If $x \sim y$ then $\{x,y\}^{\perp\perp}$ equals the line incident with x and y (there can be no other points by **GQ2** (page 11)).

Let $x \nsim y$. Now x and y are collinear with all points of $\{x,y\}^\perp$ so we have $x,y \in \{x,y\}^{\perp\perp}$, hence we have the lower bound. Let $u,v \in \{x,y\}^\perp$. Any point in $\{x,y\}^{\perp\perp}$ must be collinear with u and v hence $\{x,y\}^{\perp\perp} \subseteq \{u,v\}^\perp$. As $u \nsim v$ Lemma 129 implies $|\{u,v\}^\perp| = t+1$. $\square$

THEOREM 131 (Payne and Thas, 1.2.3). *A finite generalised quadrangle of order (s,t) has $t \leq s^2$.*

COROLLARY 132. *A finite generalised quadrangle of order $(2,t)$ has $t = 2$ or 4.*

PROOF. From above $t \leq 4$, the divisiblility condition disallows $t = 3$ and thickness implies $t \geq 2$. $\square$

We denote a generalised quadrangle of order $(2,2)$ by $Q(4,2)$ and denote a generalised quadrangle of order $(2,4)$ by $Q(5,2)$ (following Payne and Thas). These generalised quadrangles correspond to a parabolic and elliptic orthogonal space of rank 2 over $GF(2)$ denoted $O(5,2)$ and $O^-(6,2)$, respectively. A grid of type $(2,2)$ corresponds to a hyperbolic orthogonal polar space $O^+(4,2)$, which is a Payne and Thas generalised quadrangle of order $(2,1)$ (Q(3,2) in Payne and Thas notation).

THEOREM 133 ([**52**][**53**]). *In a generalised quadrangle of order (s,t) if $t \neq s^2$ then $t \leq s^2 - s$.*

The pair (x, y) of distinct points is called **regular** if $x \sim y$ or if $x \not\sim y$ then $|\{x, y\}^{\perp\perp}| = t + 1$. A point x is **regular** if all distinct pairs (x, y) are regular. Hence for $x \not\sim y$, this implies that $\{x, y\}^{\perp\perp} = \{v, w\}^{\perp}$ for all v, $w \in \{x, y\}^{\perp}$. (The above definitions are easier to visualise in the dual setting.)

A **triad** of points is a triple of pairwise non-collinear points. Given a triad $T = \{x, y, z\}$, a **centre** of T is a point collinear to x, y and z, that is, a point of $T^{\perp}$. We say the triad T is **acentric** if $|T^{\perp}| = 0$, **centric** if $|T^{\perp}| > 0$ and **unicentric** if $|T^{\perp}| = 1$.

THEOREM 134 (Bose-Shrikhande [**17**]). *In a generalised quadrangle of order (s, t) we have:*

$$t = s^2 \text{ if and only if each triad has } s+1 \text{ centres}$$

That is, any three pairwise non-collinear points has exactly $s + 1$ neighbours.

A point x is **coregular** provided each line incident with x is itself regular. The noncollinear pair (x, y) is **antiregular** provided $|z^{\perp} \cap \{x, y\}^{\perp}| \leq 2$ for all $z \in \mathscr{P} - \{x, y\}$. A point x is **antiregular** provided (x, y) is antiregular for all $y \in \mathscr{P} - \{x\}$.

Let $s^2 = t$, so by Theorem 134, p. 83, for any triad (x, y, z) we have $|\{x, y, z\}^{\perp}| = s+1$. So we have $|\{x, y, z\}^{\perp\perp}| \leq s+1$. We say (x, y, z) is **3-regular** if $|\{x, y, z\}^{\perp\perp}| = s + 1$. The point x is 3-regular if each triad containing x is 3-regular.

An interesting property of 3-regular points is:

THEOREM 135 (Payne and Thas, 1.3.3). *Let $\mathscr{S}$ be a $GQ(s, s^2)$ and suppose that any triad contained in $\{x, y\}^{\perp}$, $x \not\sim y$, is 3-regular. The incidence structure with pointset $\{x, y\}^{\perp}$, with lineset the set of elements $\{u, v, w\}^{\perp\perp}$, where u, v, w are distinct points in $\{x, y\}^{\perp}$, and with the natural incidence, is an inversive plane of order s (see Section 11.4, p. 74).*

By Theorem 1.3.6 in Payne and Thas if $s = t$ and each point in $x^{\perp} - \{x\}$ is regular, then every point is regular.

2. Some examples of generalised quadrangles

2.1. Sylvester's Syntheme-Duad geometry

The following construction was first discovered by Sylvester [**123**].

Let $X = \{1, 2, 3, 4, 5, 6\}$. Let

$$\mathscr{P} = \{x \mid x \subseteq X, |x| = 2\}$$

$$\mathscr{B} = \{L \mid L \text{ is a partition of } X \text{ into 3 disjoint subsets of size } 2\}$$

and I is membership. Then $\mathscr{S} = (\mathscr{P}, \mathscr{B}, \mathrm{I})$ is a generalised quadrangle of order 2.

2.2. $T_2^*(\mathcal{H})$

Let $\mathcal{H}$ be a hyperoval in $PG(2,q)$, $q = 2^e$, $q > 2$. Embed $PG(2,q)$ in $PG(3,q)$. Define:

The set of POINTS, $\mathscr{P}$ = points of $PG(3,q) - PG(2,q)$.

The set of LINES, $\mathscr{B}$ = lines of $PG(3,q) - PG(2,q)$ meeting $\mathcal{H}$ (uniquely).

INCIDENCE = incidence of $PG(3,q)$.

THEOREM 136 ([**36**]). *For $q > 2$ we have $T_2^*(\mathcal{H}) = (\mathscr{P}, \mathscr{B}, \text{INCIDENCE})$ is a generalised quadrangle of order $(q-1, q+1)$.*

PROOF. Any two POINTS are on exactly one line of $PG(3,q)$, (this line may meet $\mathcal{H}$). So **GQ1** is satisfied.

Any POINT is COLLINEAR with exactly $(q+2)q$ other POINTS. When $q > 2$ the incidence of $PG(3,q)$ shows that there are no POINTS COLLINEAR with all other POINTS so axiom **ptGQ** (page 11) is satisfied.

For $q > 2$ every LINE has q POINTS on it, and every POINT has $q+2$ LINES on it, so we have thickness.

Let x be a POINT and L be a LINE not incident with x. So L is a line not incident with the point x. Let L meet $\mathcal{H}$ at a point y. The plane $\langle x, L\rangle$ will be a secant plane to $\mathcal{H}$. Let the plane meet $\mathcal{H}$ at point y and another point z. There is a unique line M through z and x, which also meets the line L at a point w. So we have $x \mathrm{~I~} M \mathrm{~I~} w \mathrm{~I~} L$. □

REMARK. For $q = 2$, $T_2^*(\mathcal{H})$ is a firm GQ, in fact, it is a grid of type $(3,3)$.

$T_2^*(\mathcal{H}_1) \cong T_2^*(\mathcal{H}_2)$ if and only if there exists an automorphism, g, of the space taking the plane $\pi_1 \supseteq \mathcal{H}_1$ onto the plane $\pi_2 \supseteq \mathcal{H}_2$ for which $g\colon \mathcal{H}_1 \mapsto \mathcal{H}_2$.

2.3. $T_2(\mathcal{O})$

Let $\mathcal{O}$ be an oval of $PG(2,q)$. Embed $PG(2,q)$ in $PG(3,q)$. Define:

the set of POINTS, $\mathscr{P}$ =

(i): points of $PG(3,q) - PG(2,q)$,
(ii): hyperplanes of $PG(3,q)$ meeting $\mathcal{O}$ in one point, and
(iii): a new symbol (∞),

the set of LINES, $\mathscr{B}$ =

(a): lines of $PG(3,q) - PG(2,q)$ meeting $\mathcal{O}$, and
(b): points of $\mathcal{O}$,

and INCIDENCE as:

POINTS (i) are INCIDENT only with LINES (a), defined by the incidence of $PG(3,q)$.

POINTS (ii) are INCIDENT with all LINES (a) contained in it and meeting the same point of $\mathcal{O}$.

(∞) is INCIDENT with no LINES (a) and all LINES (b).

Let $T_2(\mathcal{O}) = (\mathscr{P}, \mathscr{B}, \text{INCIDENCE})$.

THEOREM 137 ([**36**]). *We have $T_2(\mathcal{O})$ is a generalised quadrangle of order q.*

PROOF. The point (∞) is not COLLINEAR with any POINTS of type (a). There exists POINTS of type (i) not INCIDENT with POINTS of type (ii). So **ptGQ** axiom is satisfied.

Let x, y be POINTS of type (ii). The planes x and y will lie on two lines if the planes are secant to $\mathcal{O}$, contradiction. Let x, y be POINTS of type (i). These POINTS are incident with LINES of type (a) which is a line of $PG(3,q)$ hence **GQ1** is satisfied. Let y be a POINT of type (i), these points are never incident with the POINT (∞). Let y be a POINT of type (ii), then the plane y must be secant to $\mathcal{O}$ to lie on two lines with (∞), contradiction. Let x be a POINT of type (i) and y be a POINT of type (ii). There is only one LINE (line of $PG(3,q)$) incident with x and y else there will be two lines on x and the point of $\mathcal{O}$ which y is tangent to, contradiction. Hence **GQ1** is satisfied.

A LINE of type (a) has q affine points (POINTS of type (i)) on it and a POINT of type (ii) on it, so a total of $q+1$ points. A LINE of type (b) has q POINTS of type (ii) on it and is also incident with the POINT (∞). A POINT of type (i) has $q+1$ LINES on it (the cone with vertex the POINT and the base being $\mathcal{O}$). A POINT of type (ii) has q lines (LINES) on it from the tangent point and the tangent point itself (a LINE of type (b)). The POINT (∞) has the $q+1$ lines of $\mathcal{O}$. Hence for $q \geq 2$ we have thickness.

Now we will prove that the **GQ2** axiom is satisfied. We will split up the proof into the different types of anti-flags.

The POINT is (∞):

(i) Every LINE of type (b) is INCIDENT with (∞).
(ii) Every LINE, L, of type (a) is not INCIDENT with (∞). The line L is incident with a unique point, M, of $\mathcal{O}$, a LINE of the GQ. There is a unique tangent plane, y, on M and the line L, this is a POINT of the GQ. Hence $(\infty)\ \mathrm{I}\ M\ \mathrm{I}\ y\ \mathrm{I}\ L$.

Let x be a POINT of type (ii), which intersects $\mathcal{O}$ at the point M:

(i) Let L be a LINE of type (a), that is a line of $PG(3,q)$:
    (a) L intersects $\mathcal{O}$ at M, but not in x: Then there is a unique plane, y, through M and L. So we have $x\ \mathrm{I}\ M\ \mathrm{I}\ y\ \mathrm{I}\ L$.
    (b) L does not intersect $\mathcal{O}$ at M: Then L intersects the plane x at a point y. There is a unique line (LINE), N, through M and y. Then $x\ \mathrm{I}\ N\ \mathrm{I}\ y\ \mathrm{I}\ L$.
(ii) Let L be a LINE of type (b), that is point of $\mathcal{O}$ distinct from M: The point (∞) is COLLINEAR with M and L, so $x\ \mathrm{I}\ M\ \mathrm{I}\ (\infty)\ \mathrm{I}\ L$.

Let x be a POINT of type (i):

(i) Let L be a LINE of type (a), that is not incident with x, L intersecting $\mathcal{O}$ at R:

(a) We have $\langle x, L\rangle$ generating a secant plane, z to $\mathcal{O}$, meeting it at the points R and S. The line M through x and S on the plane z meets L at a point (POINT) y. Hence $x \mathrm{~I~} M \mathrm{~I~} y \mathrm{~I~} L$.

(b) We have $\langle x, L\rangle$ generating a tangent plane z to $\mathcal{O}$, meeting at the point R. Then there is a line M from x to R, so $x \mathrm{~I~} M \mathrm{~I~} z \mathrm{~I~} L$.

(ii) L is a LINE of type (b): Let y be the unique tangent plane on x and L. Let M be the unique line on x and L, then $x \mathrm{~I~} M \mathrm{~I~} y \mathrm{~I~} L$. □

THEOREM 138. *If q is even then the* POINT (∞) *in $T_2(\mathcal{O})$ is regular.*

PROOF. We need to show that all distinct pairs of POINTS $(x, (\infty))$ are regular. If $x \sim (\infty)$ then those pairs are regular. We now assume $x \not\sim (\infty)$. Let x be a POINT of type (i). Then $\{x, (\infty)\}^{\perp}$ is the set of planes on x meeting $\mathcal{O}$ at a tangent, that is, POINTS of type (ii). There are $q+1$ such planes. Since q is even all tangent planes meet in a line (with the line meeting $PG(2,q)$ in the nucleus of $\mathcal{O}$). So we can say $\{x, (\infty)\}^{\perp\perp}$ is the set of POINTS on the line that is the intersection of the planes and the POINT (∞), which makes a total of $q+1$ points. So $(x, (\infty))$ is regular. □

2.4. $P(\mathcal{S}, x)$

To each regular point x of the GQ(s), $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$, there is associated a GQ $P(\mathcal{S}, x) = (\mathcal{P}', \mathcal{B}', \mathrm{I}')$ of order $(s-1, s+1)$. The pointset is the set $\mathcal{P} - x^{\perp}$, the lineset is made from (a) lines not incident with x and (b) hyperbolic lines $\{x, y\}^{\perp\perp}$ for $x \not\sim y$. Incidence is defined as: If $y \in \mathcal{P}'$ and $L \in \mathcal{B}'$ of type (a) then $y \mathrm{~I}' L$ if and only if $y \mathrm{~I~} L$ and if $y \in \mathcal{P}'$ and $L \in \mathcal{B}'$ of type (b) then $y \mathrm{~I}' L$ if and only if $y \in L$. (Theorem 3.1.4 Payne and Thas.)

THEOREM 139 ([**91**]). *$T_2^*(\mathcal{H})$ is isomorphic to $P(T_2(\mathcal{O}), (\infty))$ with $\mathcal{O} = \mathcal{H} - \{x\}$ and $x \in \mathcal{H}$ (hence $\mathcal{O}$ is an oval with nucleus x). But $P(T_2(\mathcal{O}), x)$ is not isomorphic to any $T_2^*(\mathcal{H})$ for any $x \neq (\infty)$.*

2.5. $T_3(\Omega)$

Let Ω be an ovoid of $PG(3,q)$. Embed $PG(3,q)$ in $PG(4,q)$. Define:

the set of POINTS, $\mathcal{P} =$,

(i): points of $PG(4,q) - PG(3,q)$,

(ii): hyperplanes of $PG(4,q)$ meeting Ω in one point, and

(iii): a new symbol (∞),

the set of LINES, $\mathcal{B} =$,

(a): lines of $PG(4,q) - PG(3,q)$ meeting Ω, and

(b): points of Ω, and

INCIDENCE is the incidence of $T_2(\mathcal{O})$ with $PG(3,q)$ replaced with $PG(4,q)$

THEOREM 140 ([**36**]). *Let Ω be an ovoid in $PG(3,q)$, then $T_3(\Omega)$ is a $GQ(q,q^2)$.*

THEOREM 141 (Payne and Thas, 3.3.1, 3.3.2). (i) *Properties of $T_2(\mathcal{O})$: all type (b) lines are regular; the point (∞) is regular or antiregular according as q is even or odd.*

(ii) *Properties of $T_3(\Omega)$: all type (b) lines are regular; the point (∞) is 3-regular.*

2.6. Other GQs from arcs

Let $q = 2^e$, $H = PG(2,q)$ and $\Sigma = PG(3,q)$.

We can give two other constructions of GQs from $\mathcal{H}$. We have H embedded in Σ as before, and define $\mathcal{O}_x = \mathcal{H} - \{x\}$ for $x \in \mathcal{H}$. The GQ $T_2^*(\mathcal{O}_x)$ is defined as POINTS being points of $\Sigma - H$ and planes containing x, with H given a special treatment by being labelled by (∞), LINES being tangent lines to $\mathcal{O}_x$, and INCIDENCE being carried over from Σ. This GQ is in fact the GQ $T_2(\mathcal{O})$ where $\mathcal{O} = \mathcal{O}_x$.

Let $\mathcal{O}_{xy} = \mathcal{H} - \{x, y\}$ for distinct points x, $y \in \mathcal{H}$. Let the POINTS be (i) points of $\Sigma - H$, (ii) planes that contain x but not y, and (iii) planes that contain y but not x, and let the LINES be all the lines of $\Sigma - H$ meeting H at a point of $\mathcal{O}_{xy}$. INCIDENCE is that of Σ. We denote this GQ of order $(q+1, q-1)$ by $T_2(\mathcal{O}_{xy})$.

REMARK. Orbits of the stabilisers of $\mathcal{H}$ on pairs of points $\{x, y\}$ of $\mathcal{H}$ correspond to isomorphism classes of $T_2(\mathcal{O}_{xy})$.

3. Classical Generalised Quadrangles

Classical generalised quadrangles are generalised quadrangles from polar spaces of rank two. We define $W(q)$ to be the space of $Sp(4,q)$, that is, the polar space with respect to a symplectic polarity of $PG(3,q)$. We define $Q(4,q)$ to be the space of $O(5,q)$ and define $Q(5,q)$ to be the space of $O^-(6,q)$. We define $H(d,q^2)$ to be the polar space $U(d+1,q^2)$, the polar space from a nonsingular hermitian variety of $PG(d,q^2)$ for $d=3$ or $d=4$.

For the classical generalised quadrangles $W(q)$, $Q(4,q)$ and $Q(5,q)$ we have $s = q$ and for $H(3,q^2)$ and $H(4,q^2)$ we have $s = q^2$. The values of t for these GQs are calculated below:

Let x be an absolute point with respect to the polarity Δ. Then the quotient space $\Delta(x)/x$ will replace the form $\langle\ ,\ \rangle$ with $\langle\ ,\ \rangle'$ where

$$\langle u+x, u+x\rangle' = \langle u, v\rangle,$$

similarly for the quadratic case. This form $\langle\ ,\ \rangle'$ is nondegenerate and of the same type as $\langle\ ,\ \rangle$.

For $W(q)$: $\Delta(x)/x \cong GF(q)^2$ with every point absolute (as the form is alternating), so $q+1$ absolute points. So $t = q$.

For $H(3,q^2)$: $\Delta(x)/x \cong GF(q^2)^2$ form is, without loss of generality, $x_1\bar{x}_2 - x_3\bar{x}_4$, where $x \mapsto \bar{x}$ is conjugation. So $q+1$ absolute points (in subfield, $PG(1,q) \subseteq PG(1,q^2)$). So $t = q$.

For $H(4,q^2)$: $\Delta(x)/x \cong GF(q^2)^3$. The form gives a classical unital in $PG(2,q^2)$ with q^3+1 points. So $t = q^3$.

For $Q(4,q)$: $\Delta(x)/x \cong GF(q)^3$. We have a conic in $PG(2,q)$ with $q+1$ points. So $t = q$.

For $Q(5,q)$: $\Delta(x)/x \cong GF(q)^4$. We have an elliptic quadric in $PG(3,q^2)$ with q^2+1 points. So $t = q^2$.

Note: $Q(3,q)$ (see Section 9, p. 11) is a Payne and Thas generalised quadrangle, it has $s = q$. We have $\Delta(x)/x \cong GF(q)^2$ which has two points so $t = 1$.

3.1. Trace and span in $W(q)$

Generally, $x^\perp = \Delta(x) \cap \{\text{absolute points}\}$. Since all points are absolute for $W(q)$ we have $x^\perp = \Delta(x)$.

Now

$$\operatorname{trace}(x,y) = \{x,y\}^\perp = x^\perp \cap y^\perp = \Delta(x) \cap \Delta(y) = \Delta(\langle x,y\rangle).$$

For $x \not\sim y$ we have

$$\operatorname{span}(x,y) = \{x,y\}^{\perp\perp} = \Delta^2(\langle x,y\rangle) = \langle x,y\rangle$$

Hence for $x \not\sim y$ a hyperbolic line $\langle x,y\rangle$ in $W(q)$ is a line of $PG(3,q)$.

3.2. Regularity of $W(q)$

In $W(q)$ we have $\Delta(\langle x,y\rangle) = \Delta(x) \cap \Delta(y)$. All points of $W(q)$ are regular if and only if all non-collinear pairs of points are regular. So we let $x \not\sim y$. Then $\langle x,y\rangle$ is a line of $PG(3,q)$ as all points of $PG(3,q)$ are absolute under Δ. So we have the size of $\langle x,y\rangle$ being equal to $q+1$. But $|\{x,y\}^{\perp\perp}| = |\langle x,y\rangle| = q+1 = t+1$. Hence the pair (x,y) is regular. Hence all points of $W(q)$ are regular.

In fact by theorem 3.3.3 in Payne and Thas all lines of $W(q)$ are regular if and only if q is even

THEOREM 142 (Payne and Thas, 5.2.1). *A generalised quadrangle of order q is isomorphic to $W(q)$ if and only if all its points are regular.*

4. Ovoids and Spreads

Let $\mathscr{S} = (\mathscr{P}, \mathscr{B}, \mathrm{I})$ be a generalised quadrangle. Then the set $\mathscr{O} \subseteq \mathscr{P}$ of $\mathscr{S}$ is an **ovoid** if every line of $\mathscr{S}$ meets $\mathscr{O}$ in exactly one point. A set $\mathscr{D} \subseteq \mathscr{B}$ of $\mathscr{S}$ is a **spread** if every point of $\mathscr{S}$ is on exactly one line of the set $\mathscr{D}$.

Theorem 143 (Payne and Thas, 1.8.1). *If $\mathscr{O}$ is an ovoid of a generalised quadrangle of order (s,t) then $|\mathscr{O}| = st+1$. Dually, if $\mathscr{D}$ is a spread of a generalised quadrangle of order (s,t) then $|\mathscr{D}| = st+1$.*

A polarity of a $\mathrm{GQ}(s) = (\mathscr{P}, \mathscr{B}, \mathrm{I})$ is an automorphism of the GQ of order two that maps $\Delta\colon \mathscr{P} \mapsto \mathscr{B}$ and $\Delta\colon \mathscr{B} \mapsto \mathscr{P}$.

Let Δ be a polarity of the generalised quadrangle $\mathscr{S}$. We have absolute points if and only if $s = t$.

Theorem 144 (Payne and Thas, 1.8.2). *The set of absolute points (lines) of a polarity of a generalised quadrangle of order s is an ovoid (spread) of the generalised quadrangle.*

Proof. Let Δ be a polarity of the generalised quadrangle $\mathscr{S}$. We will first show that each line is incident with at most one absolute point. Suppose not, that is, let x and y be distinct absolute points on a line L. Since $x \sim y$ we have $\Delta(x) \sim \Delta(y)$. Now $\Delta(x)$, $\Delta(y)$ and L can not be all distinct else we will get a triangle (since $x \mathrel{\mathrm{I}} \Delta(x)$ etc.) So without loss of generality we let $L = \Delta(x)$. Then $y \mathrel{\mathrm{I}} L$ implies $y \mathrel{\mathrm{I}} \Delta(x)$ which implies $x \mathrel{\mathrm{I}} \Delta(y)$. Since $y \mathrel{\mathrm{I}} \Delta(y)$ and $x \mathrel{\mathrm{I}} \Delta(y)$ we have $L = \Delta(x) = \Delta(y)$ by **GQ1**. But this implies $x = y$. Contradiction.

Now we show that every line has at least one absolute point. Let L be a line of the generalised quadrangle. First, suppose L is absolute. Then $\Delta(L) \mathrel{\mathrm{I}} L$ hence $\Delta(L)$ is an absolute point (on L). Now suppose L is not absolute. Then $\Delta(L) \not\mathrel{\mathrm{I}} L$ so by **GQ2** we have a unique point-line pair (x, M) with $\Delta(L) \mathrel{\mathrm{I}} M \mathrel{\mathrm{I}} x \mathrel{\mathrm{I}} L$. As $x \mathrel{\mathrm{I}} M$ we have $\Delta(M) \mathrel{\mathrm{I}} \Delta(x)$, so by uniqueness of x and M we have $\Delta(x) = M$ and $\Delta(M) = x$. Hence $x \mathrel{\mathrm{I}} \Delta(x)$ so x is absolute. ∎

Theorem 145 (Payne and Thas, 1.8.4). *Let $\mathscr{S}$ be a generalised quadrangle of order s and having a regular pair (x,y) with $x \not\sim y$. If $\mathscr{O}$ is an ovoid of $\mathscr{S}$ then*

$$\left|\mathscr{O} \cap \{x,y\}^{\perp}\right|,\ \left|\mathscr{O} \cap \{x,y\}^{\perp\perp}\right| \in \{0,\ 2\},$$
$$\textit{and}\ \left|\mathscr{O} \cap \left(\{x,y\}^{\perp} \cup \{x,y\}^{\perp\perp}\right)\right| = 2.$$

Theorem 146 (Payne and Thas, 1.8.4). *If a generalised quadrangle of order s contains an ovoid $\mathscr{O}$ and a regular point $z \notin \mathscr{O}$ then s is even.*

Corollary 147. *$W(q)$ has ovoids only if q is even.*

Proof. Use Theorem 146 and Theorem 142, p. 88. ∎

THEOREM 148 (Payne and Thas, 1.8.3). *A generalised quadrangle of order* (s,t) *with* $t > s^2 - s$ *has no ovoids.*

COROLLARY 149. *A generalised quadrangle of order* (s, s^2) *has no ovoids.*

In particular, $T_3(\Omega)$ has no ovoids.

THEOREM 150 (Payne and Thas, 3.4.2). $T_2(\mathcal{O})$ *always has ovoids.*

PROOF. We give two constructions of ovoids of $T_2(\mathcal{O})$, one of which works if $\mathcal{O}$ is a secant plane section of an ovoid Ω.

Let π be a plane with no point in common with $\mathcal{O}$. There are q^2 points of type (i) in π. These affine points of π and the POINT (∞) form an ovoid. Every line of type (b) is on (∞) only. Every line of type (a) meets π exactly once.

Suppose $\mathcal{O}$ is contained in an ovoid Ω of $PG(3,q)$. Let $\mathcal{O} = \{x_0, \dots, x_q\}$. Let π_i be the tangent plane of $\mathcal{O}$ at x_i, $i = 0, \dots, q$. The set $(\Omega - \mathcal{O}) \cup \{\pi_0, \dots, \pi_q\}$ is an ovoid of $T_2(\mathcal{O})$. Every point x_i of $\mathcal{O}$ as a LINE meets only one POINT (∞) of the generalised quadrangle ovoid. So every LINE of type (b) meets the ovoid exactly once. Each q lines (LINES) contained in π_i are tangent to Ω, so each of the q LINES on x_i contains only the POINT π_i. Each of the $q^2 - q$ other lines on x_i but not in π_i meets Ω at two points, the point x_i and an affine point of Ω. So each LINE meets the ovoid in precisely one point. □

THEOREM 151 ([**125**]). *An ovoid of* $W(q)$*,* q *even, is an ovoid of* $PG(3,q)$*.*

PROOF. Let $\mathscr{O}$ be an ovoid of $W(q)$. All points of $W(q)$ are points of $PG(3,q)$. Let x, y be points of $W(q)$. If $\langle x,y\rangle$ is an absolute line, then it is a line of $W(q)$ so meets $\mathscr{O}$ at one point. Then $\langle x,y\rangle$ is a line of $PG(3,q)$ that meets these points of $\mathscr{O}$ in one point. Then $\langle x,y\rangle$ is a line of $PG(3,q)$ that meets $\mathscr{O}$ at one point.

If $\langle x,y\rangle$ is not an absolute line, then $\langle x,y\rangle$ is a hyperbolic line $\{x,y\}^{\perp\perp}$. But we have shown that $|\mathscr{O} \cap \{x,y\}^{\perp\perp}| = 0$ or 2. Hence the nonabsolute line $\langle x,y\rangle$ meets the set $\mathscr{O}$ in $PG(3,q)$ in 0 or 2 points. Since $\mathscr{O}$ has size q^2+1 then we have $\mathscr{O}$ being an ovoid of $PG(3,q)$. □

THEOREM 152 ([**119**]). *An ovoid* Ω *of* $PG(3,q)$*,* q *even, is an ovoid of a generalised quadrangle isomorphic to* $W(q)$*.*

REMARK. The above theorem uses the fact that an ovoid determines a nondegenerate alternating form (up to similiarity) for q even. Hence the tangent lines of an ovoid are absolute with respect to the polarity induced by this form, (these lines form a **linear complex** of $PG(3,q)$).

For q even and a square only one type of ovoid of $Q(4,q)$ is known. But for q even and not a square, two types of ovoids of $Q(4,q)$ are known. Their projection from the nucleus of Q onto a $PG(3,q)$ are the elliptic quadric and the Tits ovoid of $PG(3,q)$ (see Section 11.3, p. 71). The corresponding spreads in $W(q)$ are the regular spread and the Lüneburg spread of $PG(3,q)$ [**125**]. W. M. Kantor [**66**] has constructed, for odd non-prime values of q, ovoids of $Q(4,q)$ that are not contained in $PG(3,q)$. These ovoids arise from flocks of the quadratic cone in $PG(3,q)$. (Since the planes of the flock have a common point, an ovoid of $O(5,q)$ arises, rather than just one of $O^+(6,q)$.)

5. Isomorphisms of some GQs

We list some isomorphisms between the known GQs.

THEOREM 153 (Payne and Thas, 3.2.1, 3.2.2, 3.3.3). (i) *If $T_2(\mathcal{O})$ has at least one regular pair of nonconcurrent type (a) lines on distinct points of $\mathcal{O}$, then $\mathcal{O}$ is a conic and $T_2(\mathcal{O}) \cong Q(4,q)$.*

(ii) *$Q(4,q)$ is isomorphic to the dual of $W(q)$. Moreover, $Q(4,q)$ or $W(q)$, is self-dual if and only if q is even.*

(iii) *The GQ $T_2(\mathcal{O})$ is isomorphic to $Q(4,q)$ if and only if $\mathcal{O}$ is an irreducible conic; it is isomorphic to $W(q)$ if and only if q is even and $\mathcal{O}$ is a conic.*

(iv) *If $T_2(\mathcal{O})$ has a regular type (ii) point, then q is even, $\mathcal{O}$ is a conic and $T_2(\mathcal{O})$ is isomorphic to $Q(4,q)$.*

(v) *If $T_3(\Omega)$ has a regular type (a) line, then Ω is an elliptic quadric and $T_3(\Omega)$ is isomorphic to $Q(5,q)$.*

(vi) *If $T_3(\Omega)$ has a 3-regular point other than (∞), then Ω is an elliptic quadric and $T_3(\Omega)$ is isomorphic to $Q(5,q)$.*

For q odd any oval is a conic and any ovoid is an elliptic quadric, so that $T_2(\mathcal{O}) \cong Q(4,q)$ and $T_3(\Omega) \cong Q(5,q)$. For q even, $q > 4$, there are always ovals $\mathcal{O}$ for which $T_2(\mathcal{O})$ has a unique line of regular points. Also for $q = 2^e$, e odd and $e > 2$, the Tits ovoid, Ω, provides examples of $T_3(\Omega)$ not isomorphic to $Q(5,q)$.

6. Subquadrangles

Let $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ be a generalised quadrangle of order (s,t). We say $\mathcal{S}' = (\mathcal{P}', \mathcal{B}', \mathrm{I}')$ is a **subquadrangle** (or **subGQ**) of order (s',t') of $\mathcal{S}$ if $\mathcal{S}'$ is a generalised quadrangle and $\mathcal{P} \subseteq \mathcal{P}'$, $\mathcal{B} \subseteq \mathcal{B}'$ and I' is a restriction of I to $\mathcal{P}' \times \mathcal{B}'$. If $\mathcal{S} \neq \mathcal{S}'$ then $\mathcal{S}'$ is a **proper** subGQ of $\mathcal{S}$, so we have $\mathcal{P}' \neq \mathcal{P}$ or $\mathcal{B}' \neq \mathcal{B}$, hence $s \neq s'$ or $t \neq t'$. For convenience we will denote by $\mathcal{S}'(s',t') \subseteq \mathcal{S}(s,t)$ to mean that the generalised quadrangle $\mathcal{S}'$ of order (s',t') is a subGQ of the generalised quadrangle $\mathcal{S}$ of order (s,t) and that $\mathcal{P}$, $\mathcal{P}'$ belong to the appropriate generalised quadrangle. We denote collinearity in $\mathcal{S}'$ by $\sim_{\text{sub}}$.

If two points x and y are non-collinear in the subGQ then they are non-collinear in the generalised quadrangle, (since, points and lines of $\mathscr{S}'$ are subsets of $\mathscr{S}$, so if we have $x \sim y$ but $x \nsim_{\text{sub}} y$ then we will contradict **GQ2** in $\mathscr{S}$).

Let $L \in \mathscr{B}$. Then we have

(i) $L \in \mathscr{B}'$ is a **internal line** of $\mathscr{S}'$ or
(ii) $L \notin \mathscr{B}'$ and L is incident with a unique point $x \in \mathscr{P}'$. We call L a **tangent line** of $\mathscr{S}'$ at x, or
(iii) $L \notin \mathscr{B}'$ and L is incident with no points of $\mathscr{P}'$. We call L an **external line** of $\mathscr{S}'$.

Notice that L meets $\mathscr{S}'$ in either 0, 1 or all points and in no other number. Say L meet $\mathscr{S}'$ in two points x and y, so $L \notin \mathscr{S}'$. Then x and y are not collinear in $\mathscr{S}'$ but are collinear in $\mathscr{S}$. Contradiction.

Dually, we can define a point x as a **internal point**, **tangent point** and **external point**.

LEMMA 154. *No tangent point of a subGQ $\mathscr{S}' = (\mathscr{P}', \mathscr{B}', \mathrm{I}') \subseteq \mathscr{S} = (\mathscr{P}, \mathscr{B}, \mathrm{I})$ is on a tangent line of a subGQ.*

PROOF. Suppose so. Let L be a tangent line of $\mathscr{S}'$ and y be a tangent point of $\mathscr{S}'$ with $y \mathrm{~I~} L$, $y \notin \mathscr{P}'$, $L \notin \mathscr{B}'$. Let x be the point that L meets $\mathscr{S}'$ in, as $x \in \mathscr{P}'$ we have $x \neq y$. Let M be the line on the point y, $M \in \mathscr{B}'$, $M \neq L$, so $x \not\mathrm{I}\, M$. By **GQ2** we have a unique pair $(z, N) \in \mathscr{P} \times \mathscr{B}$ such that $x \mathrm{~I}' N \mathrm{~I}' z \mathrm{~I}' M$ in $\mathscr{S}'$. As $\mathscr{B}' \subseteq \mathscr{B}$ and $\mathscr{P}' \subseteq \mathscr{P}$ we have a triangle. □

LEMMA 155. *Let $\mathscr{S}'(s', t') \subseteq \mathscr{S}(s, t)$ with $t > t'$. Then there are no external lines of $\mathscr{S}'$ if and only if $t = st'$.*

PROOF. Simply count the number of lines in $\mathscr{S}'$ and compare with the number of lines in $\mathscr{S}$. □

THEOREM 156 (Payne and Thas, 2.3.1). *Let $\mathscr{S}(s', t')$ be a proper subGQ of $\mathscr{S}(s, t)$. Then either $s = s'$ or $s \geq s't'$ (or dually, $t = t'$ or $t \geq s't'$).*

If $s = s'$ then each external point is collinear with $1 + s't'$ points of an ovoid of $\mathscr{S}'$ and dually.

If $s = s't'$ then each external point is collinear with exactly $1 + s'$ points of $\mathscr{S}'$ and dually.

COROLLARY 157. *If $\mathscr{S}'(s, t') \subseteq \mathscr{S}(s, t)$, with $t' < t$, then $\mathscr{S}'$ has ovoids. In fact, every pair of non-collinear points in $\mathscr{S}'$ lies on an ovoid.*

THEOREM 158 (Payne and Thas, 2.2.2). *Let $\mathscr{S}'(s, t') \subseteq \mathscr{S}(s, t)$ with $t' < t$. Then we have*

(i) *$t' \leq s$ and if $t' = s$ then $t = s^2$.*
(ii) *$\sqrt{s} \leq t' \leq s$ and $s^{3/2} \leq t \leq s^2$.*

(iii) *If* $t = s^{3/2}$ *then* $t' = \sqrt{s}$.

COROLLARY 159. *If* $\mathscr{S}'(s,t') \subseteq \mathscr{S}(s,t)$, *with* $t' < t$, *then* $t > s$.

COROLLARY 160 (Payne and Thas, 2.2.2). *Let* $\mathscr{S}'(s,t') \subseteq \mathscr{S}(s,t)$ *with* $t' < t$. *There can be no proper subGQ* $\mathscr{S}''(s,t'')$ *of* $\mathscr{S}'$.

REMARK. Though $\mathscr{S}''(s,t'')$ is a grid of type $(s,1)$, if $t''=1$, and this can arise.

6.1. Rosette of ovoids

A **rosette of ovoids**, or a **rosette**, based at x in a generalised quadrangle $\mathscr{S}(s,t)$ is a set $\mathscr{R}$ of ovoids pairwise meeting at x such that

$$\{\mathscr{O} - \{x\} \mid \mathscr{O} \in \mathscr{R}\},$$

partition the points of the generalised quadrangle not collinear with x. There are s^2t points not collinear with x, so $|\mathscr{R}| = s$.

THEOREM 161. *Let* $\mathscr{S}'(s,t') \subseteq \mathscr{S}(s,t)$ *with* $t' < t$. *Each tangent line of* $\mathscr{S}'$ *meeting at a point* x *gives rise to* $(t-t')$ *rosettes based at* x *in* $\mathscr{S}'$. *Also each external line of* $\mathscr{S}'$ *gives a partition of* $\mathscr{S}'$ *into ovoids.*

EXAMPLE. For q even,

$$W(q) \cong Q(4,q) \subseteq Q(5,q).$$

Now $O^-(6,q) = O^-(4,q) \perp O^+(2,q)$ where $O^+(2,q)$ is a secant line. Now each ovoid of $Q(4,q)$ is an ovoid of $W(q)$ which is an ovoid of $PG(3,q)$.

A point of $Q(5,q)$ not in $Q(4,q)$ gives rise to an elliptic quadric in $Q(4,q)$. (Let H be a hyperplane containing the given $Q(4,q)$, let x be an external point of $Q(4,q)$ not on H. The set of points of $Q(5,q)$ collinear with x form an elliptic quadric cone with vertex x, which meets H in an elliptic quadric). Conversely, let $\mathscr{O}$ be an ovoid (elliptic quadric) in H. Let S be the span of the ovoid. The totally singular points are perpendicular to S, so the perp of S is a secant line to the ovoid. Hence each ovoid appears twice.

There are $q^2(q^2-1)/2$ elliptic quadrics in $Q(4,q)$, each of which has q^2+1 tangent planes. The number of tangent planes in $Q(4,q)$ is $(q^2+1)(q+1)q(q-1)/2$. So there are q elliptic quadrics on a given tangent plane. Clearly these form a rosette (as the solids they span pairwise intersect in the tangent plane). So the number of rosettes is the number of tangent planes.

Each rosette appears twice. For a line gives rise to a rosette if and only if it is perpendicular to the tangent plane. The perp of a tangent plane is a plane containing a pair of intersecting lines. Hence we have a model of generalised quadrangle $Q(5,q)$ as follows:

Points are of two types:

(i) Points of $Q(4,q)$, and
(ii) (elliptic quadric of $Q(4,q)$, $\pm$).

Lines are of two types:

(i) Lines of $Q(4,q)$, and
(ii) (elliptic quadric rosettes of $Q(4,q)$, $\pm$).

and incidence is natural except for the highly nontrivial complication of the signs.

6.2. Automorphisms

THEOREM 162. *Let $\mathscr{S}_\theta = (\mathscr{P}_\theta, \mathscr{B}_\theta, \mathrm{I}_\theta)$ be the fixed substructure of an automorphism, θ, of a GQ of order (s,t). Then the substructure will be one of the following:*

(i) *$B_\theta = \emptyset$ and P_θ is a set of pairwise noncollinear points.*
(ii) *$P_\theta = \emptyset$ and B_θ is a set of pairwise noncollinear lines.*
(iii) *P_θ contains a point x such that every point of P_θ is collinear with x, and each line of B_θ is incident with x.*
(iv) *B_θ contains a line L such that every line of B_θ is concurrent with L, and each point of P_θ is incident with L.*
(v) *$\mathscr{S}_\theta$ is a grid.*
(vi) *$\mathscr{S}_\theta$ is a dual grid.*
(vii) *$\mathscr{S}_\theta$ is a subquadrangle.*

7. 4-gonal families and EGQs

The material in this section is the reason why groups act on the right in this chapter. It seemed to be ridiculous to rewrite all of this on the left, or to convert the rest of the thesis to the right.

Let $\mathscr{S} = (\mathscr{P}, \mathscr{B}, \mathrm{I})$ be a GQ(s,t). A collineation g of $\mathscr{S}$ is a **whorl** about a point x provided g fixes setwise each line incident with x.

THEOREM 163 (Payne and Thas, 8.1.1). *Let g be a nonidentity whorl about a point x. Then one of the following must occur:*

(i) *g fixes no point of $\mathscr{P} - x^\perp$.*
(ii) *There is a point, $y \not\sim x$ that is fixed by g. Let $T = \{x,y\}^\perp$ and $U = \{x,y\}^{\perp\perp}$. Then, in the notation of Section 6.2, $T \cup \{x,y\} \subseteq \mathscr{P}_g \subseteq T \cup U$ and $L \in \mathscr{B}_g$ if and only if L is incident with a point of T and a point of $U \cap \mathscr{P}_g$.*
(iii) *The substructure of fixed elements of g is a subquadrangle $\mathscr{S}_g$ of order (s',t) where $t \geq s/t \geq s'$ implying $s > t$. This is a more general case of* (ii).

If a whorl, g, about x is either the identity element or fixes no point of $\mathscr{P} - x^\perp$ then g is an **elation** about x. If g fixes each point of $x^\perp$, that is, fixing each line on x pointwise, then g is a **symmetry** about x. From Theorem 163 any symmetry about x is also an elation about x.

The symmetries about x form a group. For each $y \sim x$ and $y \neq x$, the group of symmetries about x acts semiregularly on the set $\{L \in \mathscr{B} \mid y \text{ I } L, x \not\text{I} L\}$, and so this group has order dividing t. The point x is called the **centre of symmetry**, (dually, **axis of symmetry**), provided its group of symmetries has order t, hence any such group acts regularly.

If there is a group, G, of elations about x acting regularly on $\mathscr{P} - x^\perp$, then we say the GQ is an **elation generalised quadrangle** (**EGQ**) with **elation group** G and **base point** x. If $\mathscr{S}$ is an EGQ(s,t) with base point x and elation group G and if G contains a full group of s symmetries about each line through x, then $\mathscr{S}$ is called a **translation generalised quadrangle** (**TGQ**) with **base point** x and **translation group** G.

Let $\mathscr{S}$ be an EGQ(s,t) with base point x and elation group G. Let y be a fixed point of $\mathscr{P} - x^\perp$ and $L_0, \dots, L_t$ be the lines incident with x. Define the points z_i and the lines M_i by $L_i \text{ I } z_i \text{ I } M_i \text{ I } y$ for all $i = 0, \dots, t$. Put $A(i) = \{g \in G \mid M_i^g = M_i\}$, $A^*(i) = \{g \in G \mid z_i^g = z_i\}$ and $\mathscr{F} = \{A(i) \mid 0 \leq i \leq t\}$. Then $|G| = s^2t$, $\mathscr{F}$ is a collection of $1+t$ sugroups of G, each of order s, and each $A^*(i)$ is a subgroup of order st containing, as a subgroup, $A(i)$. Importantly they satisfy two conditions:

K1: $A(i)A(j) \cap A(k) = \{1\}$ for distinct i, j, k.
K2: $A^*(i) \cap A(j) = \{1\}$ for distinct i, j.

Conversely, let G be a group of size s^2t with $1+t$ subgroups, $A(i)$, each of order s and $1+t$ subgroups, $A^*(i)$, of order st with $A(i) \leq A^*(i)$ satisfying **K1** and **K2**, then we can describe an EGQ(s,t) with base point (∞) as follows.
Points are of three kinds:

(i) elements of G,
(ii) right cosets $A^*(i)g$, $g \in G$, $i = 0, \dots, t$,
(iii) a symbol (∞).

Lines are of two kinds:

(a) right cosets $A(i)g$, $g \in G$, $i = 0, \dots, t$,
(b) symbols $[A(i)]$, $i = 0, \dots, t$.

Incidence is: a point of type (i), g, is incident with each line $A(i)g$, $i = 0, \dots, t$. A point of type (ii), $A^*(i)g$ is incident with $[A(i)]$ and with each line $A(i)h$ contained in $A^*(i)g$. The point (∞) is incident with each line of type (b), $[A(i)]$. These are the only incidences.

Note that $A^*(i) = A(i) \cup \{g \in G \mid A(i)g \cap A(j) = \emptyset \text{ for } 0 \leq j \leq t\}$ and we sometimes say $A^*(i)$ is a **tangent space** to $A(i)$ (see Payne and Thas p. 167).

THEOREM 164 (Payne and Thas, 8.2.1). *An EGQ $\mathscr{S}$ with base point x and elation group G is isomorphic to some EGQ with $A(i)$ and $A^*(i)$ being subgroups of the elation group G.*

Let G be a group of order s^2t. Let $\mathscr{F} = \{A(i) \leq G \mid 0 \leq i \leq t\}$ with $A(i)$ having order s satisfy **K1** and let $\mathscr{F}^* = \{A^*(i) \leq G \mid 0 \leq i \leq t\}$ with $A^*(i)$ having order st satisfy **K2** with $A(i) \leq A^*(i)$, then we say $\mathscr{F}$ is a **4-gonal family** for G. From above we see that each 4-gonal family produces an EGQ(s,t) denoted $\mathscr{S}(G,\mathscr{F})$.

THEOREM 165 (Payne and Thas, 8.2.2). (i) *G acts by right multiplication as a (maximal) group of elations about (∞).*

(ii) *$A(i)$ is the subgroup of G fixing the line $A(i)$ of the EGQ.*

(iii) *Any automorphism of G leaving $\mathscr{F}$ invariant induces a collineation of the EGQ fixing (∞).*

THEOREM 166. *Let $\mathcal{O}$ be an oval. Then $T_2(\mathcal{O})$ is self-dual if and only if $\mathcal{O}$ is a translation oval.*

PROOF. Let $\mathcal{O}$ be an oval in a hyperplane, H, of $PG(3,q)$. Now if $\mathcal{O}$ is a conic it is also a translation oval for q even (but not for q odd). If $\mathcal{O}$ is a conic then $T_2(\mathcal{O})$ is isomorphic to $Q(4,q)$ which is self-dual for q even. Since all ovals are conics for q odd by Segre's Theorem (page 20), we may assume q is even.

For q even and $\mathcal{O}$ is not a conic (∞) is regular and all type (b) LINES are regular, but no type (a) LINES are, so any duality of $T_2(\mathcal{O})$ must take (∞) to a type (b) LINE. Now $T_2(\mathcal{O})$ is a TGQ with base point (∞) hence there is an elation group with axis H. So if there is a duality $\wedge$ taking (∞) to P, then $T_2(\mathcal{O})^\wedge$ is a TGQ with base point P, that is, there is a group, G, of automorphisms of $T_2(\mathcal{O})$ fixing P, (∞) and all POINTS of type (ii) on P and is regular on the lines of $PG(3,q)$ meeting H in a point of $\mathcal{O} - \{P\}$.

Now by Theorem 141, p. 87, it follows that $\mathrm{Aut}\, T_2(\mathcal{O})$ fixes (∞) and so permutes the POINTS and LINES of a given type. We also have that the stabiliser of (∞) in $\mathrm{Aut}\, T_2(\mathcal{O})$ is the stabiliser of $\mathcal{O}$ in $P\Gamma L(4,q)$. Hence G is a subgroup of $P\Gamma L(4,q)$. Let l be the tangent line to P in H. Since G fixes l planewise, we have G being a subgroup of $PGL(4,q)$ and as G is transitive on the lines meeting H in a point of $\mathcal{O}-\{P\}$, we have G being transitive on $\mathcal{O}-\{P\}$. So by Corollary 98, p. 47, it follows that $\mathcal{O}-\{P\}$ is a translation q-arc, and so $\mathcal{O}$ is a translation oval.

For the converse see the original proofs in Chapter 12 of Payne and Thas. □

THEOREM 167 (T. Penttila, personal communication). *We have $T_3(\Omega)^\wedge$ is an EGQ if and only if Ω is an elliptic quadric or a Tits ovoid.*

8. Constructing GQs of order (q^2, q)

We now explicitly construct some EGQs of order (q^2, q), for q a prime power.

Let q be either odd or even. Let $f\colon GF(q)^2 \times GF(q)^2 \to GF(q)$ be a given biadditive map. Let $G = \{(\boldsymbol{a}, c, \boldsymbol{b}) \mid a, b \in GF(q)^2, c \in GF(q)\}$ with multiplication on G defined as

$$(\boldsymbol{a}, c, \boldsymbol{b}) \cdot (\boldsymbol{a}', c', \boldsymbol{b}') = (\boldsymbol{a} + \boldsymbol{a}', c + c' + f(\boldsymbol{b}, \boldsymbol{a}'), \boldsymbol{b} + \boldsymbol{b}').$$

If f is nonsingular then the centre of G is

$$Z = \{(0, c, 0) \mid c \in GF(q)\}.$$

Under this multiplication

$$(\boldsymbol{a}, c, \boldsymbol{b})^{-1} = (-\boldsymbol{a}, -c + f(\boldsymbol{b}, \boldsymbol{a}), -\boldsymbol{b}).$$

Suppose that for each $t \in GF(q)$ there is an additive map $d_t\colon GF(q)^2 \to GF(q)^2$ and a map $g_t\colon GF(q)^2 \to GF(q)$. Then we can let

$$A(\infty) = \{(0, 0, \boldsymbol{b}) \in G \mid \boldsymbol{b} \in GF(q)^2\}$$

and, for $t \in GF(q)$,

$$A(t) = \{(\boldsymbol{a}, g_t(\boldsymbol{a}), d_t(\boldsymbol{a})) \in G \mid \boldsymbol{a} \in GF(q)^2\}.$$

Now for each $t \in GF(q) \cup \{\infty\}$ we have $A(t)$ being a subgroup of G if and only if

$$g_t(\boldsymbol{a} + \boldsymbol{b}) - g_t(\boldsymbol{a}) - g_t(\boldsymbol{b}) = f(d_t(\boldsymbol{a}), \boldsymbol{b}) \tag{3}$$

for all $\boldsymbol{a}$, $\boldsymbol{b} \in GF(q)^2$, $t \in GF(q)$. Let $A^*(t) = A(t)Z$ for all $t \in GF(q) \cup \{\infty\}$ and let $\mathscr{F} = \{A(t) \mid t \in GF(q) \cup \{\infty\}\}$. We would like to know when $\mathscr{F}$ is a 4-gonal family.

THEOREM 168 (Payne and Thas, 10.4.1). *We have $\mathscr{F}$ being a 4-gonal family for G providing the following hold:*

(i) *Equation* (3) *holds,*
(ii) *The function $d(t, u)\colon \boldsymbol{a} \mapsto d_t(\boldsymbol{a}) - d_u(\boldsymbol{a})$ is nonsingular for all $t \neq u$,*
(iii) *$g_t(\boldsymbol{a}) = g_u(\boldsymbol{a})$ for $t \neq u$ implies $\boldsymbol{a} = \boldsymbol{0}$, and*
(iv)

$$g_t(d^{-1}(t, v)(\boldsymbol{a})) - g_v(d^{-1}(t, v)(\boldsymbol{a})) + g_v(d^{-1}(v, u)(-\boldsymbol{a})) - g_u(d^{-1}(v, u)(-\boldsymbol{a})) = 0$$

implies $\boldsymbol{a} = 0$ for distinct t, u, v is true.

Then $\mathscr{F}$ and G yield a GQ of order (q^2, q) denoted (as in the previous section) $\mathscr{S}(G, \mathscr{F})$.

Suppose G_1 and G_2 are groups and $\mathscr{F}$ a 4-gonal family of G_1. If $\theta\colon G_1 \to G_2$ is a group isomorphism or group anti-isomorphism then $\mathscr{S}(G_1, \mathscr{F})$ and $\mathscr{S}(G_2, \mathscr{F}^\theta)$ are isomorphic generalised quadrangles.

Note we have not explicitly stated what d_t, g_t and f are! We will need to develop some more machinery before we can do this. The next two Sections will help construct some $\mathscr{S}(G,\mathscr{F})$ and in doing so develop a connection between these GQs and ovals. In particular in Section 10, p. 102, we will look at specific forms for d_t, g_t and f when q is even.

8.1. Incidence of $\mathscr{S}(G,\mathscr{F})$ of order (q^2,q)

We shall now take a closer look at the incidence of $\mathscr{S}(G,\mathscr{F})$. This section is mostly for fun, but determining the coset representatives for the lines of $\mathscr{S}(G,\mathscr{F})$ is used in Section 17.2, p. 127.

It will be of benefit to write the coset representatives of $A(t)(\boldsymbol{a},c,\boldsymbol{b})$ and $A^*(t)(\boldsymbol{a},c,\boldsymbol{b})$ for $t \in GF(q)\cup\{\infty\}$, $c \in GF(q)$ and $\boldsymbol{a}$, $\boldsymbol{b} \in GF(q)^2$. It is easy to check that they are:

$$\begin{aligned}
&A(t)(0,c,\boldsymbol{b}) \text{ for } t \in GF(q),\ c \in GF(q) \text{ and } \boldsymbol{b} \in GF(q)^2,\\
&A(\infty)(\boldsymbol{a},c,0) \text{ for } c \in GF(q) \text{ and } \boldsymbol{a} \in GF(q)^2,\\
&A^*(t)(0,0,\boldsymbol{b}) \text{ for } t \in GF(q) \text{ and } \boldsymbol{b} \in GF(q)^2, \text{ and}\\
&A^*(\infty)(\boldsymbol{a},0,0) \text{ for } \boldsymbol{a} \in GF(q)^2.
\end{aligned}$$

Each line has q^2+1 points incident with it. Below we denote the lines of $\mathscr{S}(G,\mathscr{F})$ as the set of point incident with them:

$$\begin{aligned}
[A(\infty)] &= \{A^*(\infty)(\boldsymbol{a},0,\boldsymbol{0}) \mid \boldsymbol{a} \in GF(q)^2\}\cup\{(\infty)\}.\\
[A(t)] &= \{A^*(t)(\boldsymbol{0},0,\boldsymbol{b}) \mid b \in GF(q)^2\}\cup\{(\infty)\},\ \text{for each } t \in GF(q).\\
A((\infty))(\boldsymbol{a},c,\boldsymbol{0}) &= \{A^*(\infty)(\boldsymbol{a},0,\boldsymbol{0})\}\cup\{(\boldsymbol{a},c+f(\boldsymbol{b},\boldsymbol{a}),\boldsymbol{b}) \mid \boldsymbol{b} \in GF(q)^2\},\\
&\qquad \text{for } \boldsymbol{a} \in GF(q)^2,\ c \in GF(q).\\
A(t)(\boldsymbol{0},c,\boldsymbol{b}) &= \{A^*(t)(\boldsymbol{0},0,\boldsymbol{b})\}\cup\{(\boldsymbol{a},g_t(\boldsymbol{a})+c,d_t(\boldsymbol{a})+\boldsymbol{b}) \mid \boldsymbol{a} \in GF(q)^2\},\\
&\qquad \text{for } t,\ c \in GF(q),\ \boldsymbol{b} \in GF(q)^2.
\end{aligned}$$

The collinearity on points of $\mathscr{S}(G,\mathscr{F})$ is:

$$\begin{aligned}
\{A^*(\infty)\}^\perp &= \{(\boldsymbol{0},c,\boldsymbol{b}) \mid c \in GF(q),\ \boldsymbol{b} \in GF(q)^2\}\\
&\quad \cup\{A^*(\infty)(\boldsymbol{a},0,\boldsymbol{0}) \mid \boldsymbol{a} \in GF(q)^2\}\cup\{(\infty)\}.\\
\{A^*(t)\}^\perp &= \{(\boldsymbol{a},g_t(\boldsymbol{a})+c,d_t(\boldsymbol{a})) \mid c \in GF(q),\ \boldsymbol{a} \in GF(q)^2\}\\
&\quad \cup\{A^*(t)(0,0,\boldsymbol{b}) \mid \boldsymbol{b} \in GF(q)^2\}\cup\{(\infty)\},\ \text{for all } t \in GF(q).\\
\{(\boldsymbol{a},c,\boldsymbol{b})\}^\perp &= \{A^*(t)(\boldsymbol{0},0,\boldsymbol{b}-d_t(\boldsymbol{a})) \mid t \in GF(q)\}\cup\{A^*(\infty)(\boldsymbol{a},0,\boldsymbol{0})\}\\
&\quad \cup\{(\boldsymbol{d},c-g_t(\boldsymbol{a})+g_t(\boldsymbol{d}),d_t(\boldsymbol{d})+\boldsymbol{b}+d_t(\boldsymbol{a}) \mid\\
&\qquad \boldsymbol{a}\neq\boldsymbol{d} \in GF(q)^2,\ t \in GF(q)\}\cup\{(\boldsymbol{a},+f(\boldsymbol{d},\boldsymbol{a}),\boldsymbol{d}) \mid \boldsymbol{d} \in GF(q)^2\}.
\end{aligned}$$

$$
\begin{aligned}
\{A^*(\infty)(\boldsymbol{a},0,\boldsymbol{0})\}^{\perp} &= \{(\boldsymbol{a},c+f(\boldsymbol{b},\boldsymbol{a}),\boldsymbol{b}) \mid c \in GF(q),\ \boldsymbol{b} \in GF(q)^2\} \\
&\quad \cup \{A^*(\infty)(\boldsymbol{d},0,\boldsymbol{0}) \mid \boldsymbol{d} \in GF(q)^2\} \cup \{(\infty)\}. \\
\{A^*(t)(\boldsymbol{0},0,\boldsymbol{b})\}^{\perp} &= \{(\boldsymbol{a},g_t(\boldsymbol{a})+d,d_t(\boldsymbol{a})+\boldsymbol{b}) \mid d \in GF(q),\ \boldsymbol{a} \in GF(q)^2\} \\
&\quad \cup \{A^*(t)(\boldsymbol{0},0,\boldsymbol{d}) \mid d \in GF(q)^2\} \cup \{(\infty)\}.
\end{aligned}
$$

9. q–clan geometry

Following Payne [**96**][**95**][**6**], we investigate collections of 2×2 matrices over $GF(q)$ that will later on be used to construct 4-gonal families yielding a GQ(q^2, q). We also see the use of the trace equation defined in Section 6, p. 9, Chapter I.

Let $\boldsymbol{C} = \{A_t \mid t \in GF(q)\}$ be a family of 2×2 matrices with entries in $GF(q)$. We define the quadratic form Q_{st} as

$$Q_{st}(x,y) = \begin{pmatrix} x & y \end{pmatrix} (A_s - A_t) \begin{pmatrix} x \\ y \end{pmatrix}.$$

If Q_{st} is anisotropic for all $s \neq t$ we call $\boldsymbol{C}$ a ***q*–clan**.

If $\boldsymbol{C} = \{A_t \mid t \in GF(q)\}$ is a q–clan so is $\boldsymbol{C}' = \{A_t - A_0 \mid t \in GF(q)\}$, so without loss of generality we let A_0 equal the zero matrix $\boldsymbol{0}$. Also if $\{A_t = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid t \in GF(q)\}$ is a q–clan then so is $\{A_t' = \begin{pmatrix} a & b+c \\ 0 & d \end{pmatrix} \mid t \in GF(q)\}$, hence without loss of generality each A_t is upper triangular. (We say two matrices $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ are **equivalent**, denoted $A \equiv B$, if $\begin{pmatrix} a & b+c \\ 0 & d \end{pmatrix} = \begin{pmatrix} e & f+g \\ 0 & h \end{pmatrix}$.) If $A_t = \begin{pmatrix} a_t & b_t \\ 0 & c_t \end{pmatrix}$ then

$$Q_{st}(x,y) = (a_s - a_t)x^2 + (b_s - b_t)xy + (c_s - c_t)y^2.$$

As we shall only be concerned with fields of characteristic two Q_{st} is anisotropic if and only if

$$\operatorname{trace}\left(\frac{(a_s + a_t)(c_s + c_t)}{(b_s + b_t)^2}\right) = 1.$$

We will show how q–clans are related to other structures, for instance: elation generalised quadrangles from q–clans (Section 10, p. 102), flocks of quadratic cones from q–clans (Chapter IV), translation planes from flocks (Chapter IV, Section 2, p. 141).

The known q–clans for q even are presented in Chapter IV, Section 8, p. 147.

We now investigate further the entries of the matrices A_t for q even, and in doing so develop the theory of q–clans and ovals.

9.1. Herds and q–clans

If $\boldsymbol{C}$ is a q–clan we have $b_s \neq b_t$ for all $s \neq t$. So $t \mapsto b_t$ is a permutation; we may relabel the subscript so that $b_t = t^{1/2}$. We have

$$\boldsymbol{C}' = \left\{ A'_t = \begin{pmatrix} a_1^{-1/2} & 0 \\ 0 & a_1^{1/2} \end{pmatrix} A_t \begin{pmatrix} a_1^{-1/2} & 0 \\ 0 & a_1^{1/2} \end{pmatrix} \;\middle|\; t \in GF(q) \right\},$$

is also a q–clan with $A'_0 = \boldsymbol{0}$, $A'_t = \begin{pmatrix} a'_t & t^{1/2} \\ 0 & c'_t \end{pmatrix}$ with $A'_1 = \begin{pmatrix} 1 & 1 \\ 0 & c'_1 \end{pmatrix}$. So without loss of generality $a_1 = 1$.

Let $a = c'_1$ (since Q_{01} is anisotropic, trace$(a) = 1$). Define $f\colon GF(q) \to GF(q)$ by $f(t) = a_t$ and $g\colon GF(q) \to GF(q)$ by $g(t) = c_t/a$. Then $f(0) = g(0) = 0$ and $f(1) = g(1) = 1$. Since Q_{st} is anisotropic for all $s \neq t$, we have, with $f(0) = g(0) = 0$ and $f(1) = g(1) = 1$,

$$\mathcal{T}_a(f,g): \qquad \operatorname{trace}\left(\frac{a(f(s)+f(t))(g(s)+g(t))}{s+t} \right) = 1, \text{ for all } s \neq t.$$

Conversely, if f and g satisfy $\mathcal{T}_a(f,g)$ and if $A_t = \begin{pmatrix} f(t) & t^{1/2} \\ 0 & ag(t) \end{pmatrix}$, then $\boldsymbol{C} = \{A_t \mid t \in GF(q)\}$ is a q–clan with $A_0 = \boldsymbol{0}$ and $A_1 = \begin{pmatrix} 1 & 1 \\ 0 & a \end{pmatrix}$ where trace$(a) = 1$.

We now show that the permutation polynomials f and g of a q–clan

$$\boldsymbol{C} = \left\{ \begin{pmatrix} f(t) & t^{1/2} \\ 0 & ag(t) \end{pmatrix} \mid t \in GF(q) \right\}$$

are in fact o-polynomials (see Section 4, p. 41, Chapter II). Moreover, given f and g $q-1$ other o-polynomials can be constructed.

Theorem 169. *Let q be even. Let f, $g\colon GF(q) \to GF(q)$ with $f(0) = g(0) = 0$ and $f(1) = g(1) = 1$. Then $\mathcal{T}_a(f,g)$ is true if and only if g is an o-polynomial, f_s is an o-polynomial for all $s \in GF(q)$ where*

$$f_s(x) = \frac{f(x) + asg(x) + s^{1/2}x^{1/2}}{1 + as + s^{1/2}}$$

and trace$(a) = 1$.

Proof.
($\Rightarrow$) Suppose $\mathcal{T}_a(f,g)$ is true. We also suppose that $f(0) = 0$ and $f(1) = 1$. The function f is one-to-one since if $x \neq y$ and $f(x) = f(y)$ then $a(f(x)+f(y))(g(x)+g(y))/(x+y) = 0$, contradicting $\mathcal{T}_a(f,g)$. Let $\mathcal{H}$ be the set of points $\{(1, t, f(t)) \mid$

$t \in GF(q)\} \cup \{(0,1,0),(0,0,1)\}$. Since f is one-to-one no line on $(0,1,0)$ meets $\mathcal{H}$ in more than two points. Clearly no line on $(0,0,1)$ meets $\mathcal{H}$ in more than two points. We show that no three points of $\{(1,t,f(t)) \mid t \in GF(q)\}$ are collinear.

Suppose x, y, $z \in GF(q)$ are distinct and that the points $(1,x,f(x))$, $(1,y,f(y))$ and $(1,z,f(z))$ are collinear. Then

$$\frac{f(x)+f(y)}{x+y} = \frac{f(x)+f(z)}{x+z} = \frac{f(y)+f(z)}{y+z} = b, \text{ say.}$$

Since trace is additive we have

$$\mathrm{trace}(ab(g(x)+g(y))) + \mathrm{trace}(ab(g(x)+g(z))) = \mathrm{trace}(ab(g(y)+g(z))).$$

But this is contrary to $\mathcal{T}_a(f,g)$. So $\mathcal{H}$ is a hyperoval. As $f(0)=0$ and $f(1)=1$, f is an o-polynomial.

Since $\mathcal{T}_a(f,g)$ is true if and only if $\mathcal{T}_a(g,f)$ is true, g is also an o-polynomial.

We now look at $\mathrm{trace}(b(f(x)+f(y))(f_s(x)+f_s(y))/(x+y))$ where $b = a + s^{-1} + s^{-1/2}$.

$$\begin{aligned}
&\mathrm{trace}\left(\frac{b(f(x)+f(y))(\frac{f(x)+asg(x)+s^{1/2}x^{1/2}}{1+as+s^{1/2}} + \frac{f(y)+asg(y)+s^{1/2}y^{1/2}}{1+as+s^{1/2}})}{x+y}\right), \ x \neq y \\
&\quad = \mathrm{trace}\left(\frac{a(f(x)+f(y))(g(x)+g(y))}{x+y}\right) \\
&\qquad + \mathrm{trace}\left(\frac{1}{s}\frac{(f(x)+f(y))^2}{x+y} + \frac{1}{s^{1/2}}\frac{f(x)+f(y)}{(x+y)^{1/2}}\right), \ x \neq y \\
&\quad = \mathrm{trace}\left(\frac{a(f(x)+f(y))(g(x)+g(y))}{x+y}\right), \ x \neq y, \text{ since } \mathrm{trace}(X^2+X)=0.
\end{aligned}$$

So $\mathcal{T}_b(f,f_s)$ is true if and only if $\mathcal{T}_a(f,g)$ is true. Since $f_s(0)=0$ and $f_s(1)=1$ for all $s \in GF(q)$, f_s is an o-polynomial. Putting $x=0$ and $y=1$ in $\mathcal{T}_a(f,g)$, we see that $\mathrm{trace}(a)=1$.

($\Leftarrow$) Let

$$f_s(x) = \frac{f(x)+asg(x)+s^{1/2}x^{1/2}}{1+as+s^{1/2}}$$

for some a with $\mathrm{trace}(a)=1$. Suppose that f_s is an o-polynomial for all $s \in GF(q)$.

Fix $x \neq y$. Then $(1,x,f_s(x))$, $(1,y,f_s(y))$ and $(0,1,0)$ are not collinear for all $s \in GF(q)$. So $f_s(x) \neq f_s(y)$, giving $f_s(x)+f_s(y) \neq 0$, that is,

$$f(x)+f(y)+s(ag(x)+ag(y))+s^{1/2}(x^{1/2}+y^{1/2}) \neq 0 \text{ for all } s \in GF(q).$$

The above equation is a quadratic in $s^{1/2}$. Hence this implies that

$$\mathrm{trace}\left(\frac{(f(x)+f(y))(ag(x)+ag(y))}{x+y}\right) = 1.$$

Thus $\mathcal{T}_a(f,g)$ holds. $\square$

Hence for q even every q–clan in our particular form yields $q+1$ ovals; this naturally leads to the following definition.

A **herd** of ovals in $PG(2,q)$, q even, is a family of $q+1$ ovals $\{\mathcal{O}_s \mid s \in GF(q) \cup \{\infty\}\}$, each containing $(1,0,0)$, $(0,1,0)$ and $(1,1,1)$ and with nucleus $(0,0,1)$, with

$$\begin{aligned}
\mathcal{O}_\infty &= \{(1,t,g(t)) \mid t \in GF(q)\} \cup \{(0,1,0)\},\\
\mathcal{O}_s &= \{(1,t,f_s(t)) \mid t \in GF(q)\} \cup \{(0,1,0)\},\ \ s \in GF(q), \text{ where}\\
f_s(t) &= \frac{f(x) + asg(x) + s^{1/2}x^{1/2}}{1 + as + s^{1/2}},
\end{aligned}$$

for some a where $\text{trace}(a) = 1$.

Thus the last theorem says that, for q even, a q–clan, $\boldsymbol{C}$, gives rise to a herd of ovals of $PG(2,q)$, which we shall denote by $H(\boldsymbol{C})$, and conversely.

REMARKS. 1. The only if part of the theorem is due to Payne [**93**], although not explicitly stated there. The proof given here is from [**30**], and, in particular, does not involve generalised quadrangles.

2. We have provided a proof of the existence of Payne's [**93**] hyperovals that does not involve the use of generalised quadrangles, as desired by Cherowitzo [**28**].

3. This theorem is used by Penttila and Royle to classify 32-clans by computer [**111**]. Results are also obtained for q–clans, q even, q small.

4. The sufficiency half of the proof needs only the hypothesis that each f_s is a permutation.

10. Elation Generalised Quadrangles from q–clans

Let q be even and recall the definition of 4-gonal family in Section 7, p. 94, and the construction of a generalised quadrangle from a group G and a 4-gonal family $\mathscr{F}$ in Section 8, p. 97. We are now ready to define f, g_t and d_t.

Let

$$G = \{(\boldsymbol{a}, c, \boldsymbol{b}) \mid \boldsymbol{a}, \boldsymbol{b} \in GF(q)^2, c \in GF(q)\}$$

with muliplication defined as

$$(\boldsymbol{a}, c, \boldsymbol{b})(\boldsymbol{a}', c', \boldsymbol{b}') = (\boldsymbol{a} + \boldsymbol{a}', c + c' + \boldsymbol{b} \circ \boldsymbol{a}', \boldsymbol{b} + \boldsymbol{b}'),$$

where

$$\boldsymbol{b} \circ \boldsymbol{a} = \sqrt{\boldsymbol{b} P \boldsymbol{a}^T} \text{ with } P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Let $\boldsymbol{C} = \{A_t \mid t \in GF(q)\}$ be a q–clan where $A_t = \begin{pmatrix} a_t & b_t \\ 0 & c_t \end{pmatrix}$, $a_t, b_t, c_t \in GF(q)$.

By taking $g_t(\boldsymbol{a}) = \sqrt{\boldsymbol{a}A_t\boldsymbol{a}^T}$ and $d_t(\boldsymbol{a}) = b_t\boldsymbol{a}$ then g_t, d_t satisfy the conditions of Theorem 168, p. 97, yielding a 4-gonal family $\mathscr{F} = \{A(t) \mid t \in GF(q) \cup \{\infty\}\}$ where

$$\begin{aligned} A(\infty) &= \{(\mathbf{0}, 0, \boldsymbol{b}) \in G \mid \boldsymbol{b} \in GF(q)^2\}, \\ A(t) &= \{(\boldsymbol{a}, \sqrt{\boldsymbol{a}A_t\boldsymbol{a}^T}, b_t\boldsymbol{a}) \mid \boldsymbol{a} \in GF(q)^2\},\ t \in GF(q). \end{aligned}$$

The centre of G is

$$Z = \{(0, c, 0) \mid c \in GF(q)\}.$$

For $t \in GF(q) \cup \{\infty\}$ the tangent space at $A(t)$ is

$$A^*(t) = A(t)Z.$$

If q is even and $\boldsymbol{C}$ is a q–clan then the 4-gonal family $\mathscr{F}$ yields an elation generalised quadrangle, $\mathrm{GQ}(\boldsymbol{C}) = \mathscr{S}(G, \mathscr{F})$, of order (q^2, q).

10.1. Ovoids from q–clans

We show that every $\mathrm{GQ}(\boldsymbol{C})$ for q even has ovoids.

We recall that for q even $(\boldsymbol{a}, c, \boldsymbol{b})^{-1} = (\boldsymbol{a}, c + \boldsymbol{b} \circ \boldsymbol{a}, \boldsymbol{b})$. Let $H = \begin{pmatrix} 1 & 1 \\ 0 & d \end{pmatrix}$ with trace$(d) = 1$, hence H has no eigenvalues in $GF(q)$. Let

$$\mathscr{O} = \{(\boldsymbol{a}, c, \boldsymbol{a}H) \mid \boldsymbol{a} \in GF(q)^2,\ c \in GF(q)\} \cup \{(\infty)\}.$$

Then $\mathscr{O}$ is an ovoid of $\mathrm{GQ}(\boldsymbol{C})$.

Proof. Since $|\mathscr{O}| = q^3 + 1$ we only need to show that any two points of $\mathscr{O}$ are not collinear. That is, $g = (\boldsymbol{a}, c, \boldsymbol{a}H)(\boldsymbol{a}', c', \boldsymbol{a}'H)^{-1} \notin A(t)$ for all $t \in GF(q) \cup \{\infty\}$ unless $\boldsymbol{a} = \boldsymbol{a}'$ and $c = c'$.

Now suppose, for $t \in GF(q) \cup \{\infty\}$,

$$\begin{aligned} g &= (\boldsymbol{a}, c, \boldsymbol{a}H)(\boldsymbol{a}', c' + (\boldsymbol{a}'H) \circ \boldsymbol{a}', \boldsymbol{a}'H) \\ &= (\boldsymbol{a} + \boldsymbol{a}', c + c' + (\boldsymbol{a}'H) \circ \boldsymbol{a}' + (\boldsymbol{a}H) \circ \boldsymbol{a}', \boldsymbol{a}H + \boldsymbol{a}'H) \in A(t). \end{aligned}$$

Then $g \in A(\infty)$ if and only if $\boldsymbol{a} = \boldsymbol{a}'$ and $c = c'$. For $t \in GF(q)$ we have $g \in A(t)$ if and only if

$$c + c' + (\boldsymbol{a}'H) \circ \boldsymbol{a}' + (\boldsymbol{a}H) \circ \boldsymbol{a}' = \sqrt{(\boldsymbol{a} + \boldsymbol{a}')A_t(\boldsymbol{a} + \boldsymbol{a}')^T}$$

and

$$(\boldsymbol{a} + \boldsymbol{a}')H = t^{1/2}(\boldsymbol{a} + \boldsymbol{a}').$$

But since H has no eigenvalues in $GF(q)$ this implies that $\boldsymbol{a} = \boldsymbol{a}'$ which implies that $c = c'$. $\square$

11. Subquadrangles of EGQs

We now show that there are $q+1$ subquadrangles of $\mathrm{GQ}(\boldsymbol{C})$. With each of the $q+1$ subquadrangles being associated with an oval.

Let q be even and let G the group of order q^5 with multiplication defined as in the previous section and let $\mathscr{F}$ be the 4-gonal family associated with G under this multiplication.

Let $\boldsymbol{C} = \left\{ \begin{pmatrix} x_t & y_t \\ 0 & z_t \end{pmatrix} \mid t \in GF(q) \right\}$ be a q–clan. Let $\mathscr{S} = \mathscr{S}(G, \mathscr{F}) = \mathrm{GQ}(\boldsymbol{C})$. For $\boldsymbol{a} \neq 0$ put $G(\boldsymbol{a}) = \{(a\boldsymbol{a}, c, b\boldsymbol{a}) \mid a, b, c \in GF(q)\}$ so

$$(a\boldsymbol{a}, c, b\boldsymbol{a}) \cdot (a'\boldsymbol{a}, c', b'\boldsymbol{a}) = ((a+a')\boldsymbol{a}, c+c', (b+b')\boldsymbol{a}).$$

Notice $G(\boldsymbol{a})$ is a elementary abelian group of order q^3. If we define

$$A_{\boldsymbol{a}}(\infty) = A(\infty) \cap G(\boldsymbol{a}) \quad A^*_{\boldsymbol{a}}(\infty) = A^*(\infty) \cap G(\boldsymbol{a})$$
$$A_{\boldsymbol{a}}(t) = A(t) \cap G(\boldsymbol{a}) \quad A^*_{\boldsymbol{a}}(t) = A^*(t) \cap G(\boldsymbol{a}).$$

Then $\mathrm{GQ}(\boldsymbol{a}) = \mathscr{F}(\boldsymbol{a}) = \{A_{\boldsymbol{a}}(t) \mid t \in GF(q) \cup \{\infty\}\}$ is a 4-gonal family for $G(\boldsymbol{a})$ and we denote the associated GQ as $\mathrm{GQ}(\boldsymbol{a})$.

By [**99**] $\mathscr{S}(\boldsymbol{a}) = \mathscr{S}(G(\boldsymbol{a}), \mathscr{F}(\boldsymbol{a}))$ can be thought of as a subquadrangle of order q of $\mathscr{S}$. Also they showed that there are exactly $q+1$ such subquadrangles since $\mathrm{GQ}(\boldsymbol{a}) = \mathrm{GQ}(\boldsymbol{b})$ if and only if $\langle \boldsymbol{a} \rangle = \langle \boldsymbol{b} \rangle$. Most importantly it can be shown that each $\mathrm{GQ}(\boldsymbol{a})$ is isomorphic to the GQ $T_2(\mathcal{O})$ for some oval $\mathcal{O}$. We now determine what the oval is.

Since $G(\boldsymbol{a})$ is elementary abelian it is isomorphic to $GF(q)^3$ under componentwise addition. We define scalar multiplication as

$$d(a\boldsymbol{a}, c, b\boldsymbol{a}) = (da\boldsymbol{a}, dc, db\boldsymbol{a}) \text{ for } a,\ b,\ c,\ d \in GF(q).$$

It is important to note that $\theta\colon (\boldsymbol{a}, c, \boldsymbol{b}) \mapsto (d\boldsymbol{a}, dc, d\boldsymbol{b})$ for $0 \neq d \in GF(q)$ is an automorphism of G fixing each $A(t)$ of $\mathscr{F}$. There is an isomorphism between $G(\boldsymbol{a})$ and points of $PG(2,q)$ by

$$(\boldsymbol{a}, 0, \boldsymbol{0}) \mapsto (1,0,0)$$
$$(0,1,0) \mapsto (0,1,0)$$
$$(\boldsymbol{0}, 0, \boldsymbol{a}) \mapsto (0,0,1).$$

We have $\mathscr{F}(\boldsymbol{a})$ being a set of $q+1$ points of $PG(2,q)$ no three collinear. So

$$\mathcal{O}_{\boldsymbol{a}} = \{(1, \sqrt{\boldsymbol{a}A_t\boldsymbol{a}^T}, y_t) \mid t \in GF(q)\} \cup \{(0,0,1)\}$$

is an oval of $PG(2,q)$ with nucleus $(0,1,0)$.

Hence $\mathrm{GQ}(\boldsymbol{a})$ is isomorphic to $T_2(\mathcal{O}_{\boldsymbol{a}})$ where $\mathcal{O}_{\boldsymbol{a}}$ corresponds to the 4-gonal family $\mathscr{F}(\boldsymbol{a})$.

Recall that we denote the group of all collineations of a GQ($\boldsymbol{C}$) fixing (∞) and $(\mathbf{0},0,\mathbf{0})$ by $\mathcal{G}_0$. Since each GQ($\boldsymbol{a}$) contains the points (∞) and $(\mathbf{0},0,\mathbf{0})$ we can say that each element of $\mathcal{G}_0$ permutes $G(\boldsymbol{a})$ and so $\mathcal{O}_{\boldsymbol{a}}$ and GQ($\boldsymbol{a}$) among themselves. We note that no element of G can do this. Hence $\mathcal{G}_0$ is the full group of collineations of GQ($\boldsymbol{C}$) that acts on the set $\{G(\boldsymbol{a}) \mid \text{for } q+1 \text{ representatives for } \boldsymbol{a}\}$. (See [**99**] or [**97**] for details.)

12. A view of the Subiaco q–clan

We now define a q–clan, $\boldsymbol{S}$, that will be a major part of this and later chapters. Let $d \in GF(q)$, q even, such that $d^2+d+1 \neq 0$ and $\operatorname{trace}(1/d) = 1$. Let

$$\begin{aligned} a &= \frac{d^2+d^5+d^{1/2}}{d(1+d+d^2)}, \\ f(x) &= \frac{d^2(x^4+x)+d^2(1+d+d^2)(x^3+x^2)}{(x^2+dx+1)^2} + x^{1/2}, \text{ and} \\ g(x) &= \frac{d^4x^4+d^3(1+d^2+d^4)x^3+d^3(1+d^2)x}{(d^2+d^5+d^{1/2})(x^2+dx+1)^2} + \frac{d^{1/2}}{d^2+d^5+d^{1/2}}x^{1/2}. \end{aligned}$$

Then

$$\boldsymbol{S} = \boldsymbol{S}_d = \left\{ A_x = \begin{pmatrix} f(x) & x^{1/2} \\ 0 & ag(x) \end{pmatrix} \;\middle|\; x \in GF(q) \right\}$$

is a q–clan.

We call $\boldsymbol{S}$ the **Subiaco q–clan**. We prove $\boldsymbol{S}$ is a q–clan in Theorem 213, p. 154, in Chapter IV. The herd of the q–clan is related to the hyperovals $\mathcal{H}_{60}$ and $\mathcal{H}_{15}$ constructed by myself and Penttila.

Historically, the q–clan $\boldsymbol{S}$ first appeared in [**30**] and was investigated in the papers [**6**] [**97**] [**100**], mostly investigating the isomorphisms of GQ($\boldsymbol{S}$). In the following Sections we will give a summary of these results. The papers [**98**] [**101**] [**27**] are heavily influenced by the already mentioned papers.

13. Fundamental Theorem of q–clan Geometry

Let q be even. Let $G = \{(\boldsymbol{a}, c, \boldsymbol{b}) \mid \boldsymbol{a},\ \boldsymbol{b} \in GF(q)^2,\ c \in GF(q)\}$ with multiplication as defined in Section 10, p. 102. Recall that the 4-gonal family $\mathscr{F} = \{A(t) \mid t \in GF(q) \cup \{\infty\}\}$ is defined from the q–clan

$$\begin{aligned} A(t) &= \{(\boldsymbol{a}, \sqrt{\boldsymbol{a}A_t\boldsymbol{a}^T}, b_t\boldsymbol{a}) \mid \boldsymbol{a} \in GF(q)^2\} \\ A(\infty) &= \{(\mathbf{0}, 0, \boldsymbol{b}) \mid b \in GF(q)^2\}. \end{aligned}$$

We are now interested in determining the full collineation group $\mathcal{G}$ of GQ($\boldsymbol{C}$) constructed from a q–clan $\boldsymbol{C}$. In particular, we are interested in the case of the Subiaco q–clan. Of extreme importance is The Fundamental Theorem, described below, which (usually) allows the full collineation group of GQ($\boldsymbol{C}$) to be determined by knowing how a collineation of GQ($\boldsymbol{C}$) maps the line $[A(\infty)]$ to another line on the point (∞). Hence to determine the full collineation group $\mathcal{G}$ of GQ($\boldsymbol{C}$) it suffices to determine the subgroup $\mathcal{G}_0$ fixing $(\mathbf{0}, 0, \mathbf{0})$ (and $\mathcal{G}_0$ also fixes (∞)). Since the Subiaco GQ is not classical (as the ovals from the herd are not regular) we use:

THEOREM 170 ([**104**]). *Given a q–clan $\boldsymbol{C}$ then if $\mathscr{S}(\boldsymbol{C})$ is not the GQ $H(3, q^2)$ the point (∞) is fixed by the full collineation group of $\mathscr{S}(\boldsymbol{C})$.*

Right multiplication by elements of G induces a group of collineations of GQ($\boldsymbol{C}$) acting regularly on the points not collinear with (∞) and fixing each line through (∞).

Let $\boldsymbol{C} = \{A_t = \begin{pmatrix} a_t & b_t \\ 0 & c_t \end{pmatrix} \mid t \in GF(q)\}$ and $\boldsymbol{C}' = \{A'_t = \begin{pmatrix} x_t & y_t \\ 0 & z_t \end{pmatrix} \mid t \in GF(q)\}$ be q–clans with $A_0 = A'_0 = \mathbf{0}$. Now let GQ($\boldsymbol{C}$) and GQ($\boldsymbol{C}'$) be the corresponding GQs constructed from the q–clans from the same group G. Hence the points $(\boldsymbol{a}, c, \boldsymbol{b})$ and (∞) of GQ($\boldsymbol{C}$) and GQ($\boldsymbol{C}'$) are the same, but with the other points and lines labelled with $A'(t)$ instead of $A(t)$ and $A'^*(t)$ instead of $A^*(t)$. We now state the Fundamental Theorem which is used to determine the full collineation group of GQ($\boldsymbol{C}$), though we state it in the more general form.

THEOREM 171 (Fundamental Theorem of q–clan Geometry [**6, 96, 97, 100**]). *Let the map $\theta\colon GQ(\boldsymbol{C}) \to GQ(\boldsymbol{C}')$ be an isomorphism with $\theta\colon (\infty) \mapsto (\infty)$, $[A(\infty)] \mapsto [A'(\infty)]$ and $(\mathbf{0}, 0, \mathbf{0}) \mapsto (\mathbf{0}, 0, \mathbf{0})$. Then the following exist:*

(i) $D \in GL(2, q)$,

(ii) $\lambda \in GF(q)$, $\lambda \neq 0$,

(iii) $\sigma \in \operatorname{Aut} GF(q)$, *and*

(iv) *a permutation* $\pi\colon t \mapsto \bar{t}$ *of* $GF(q)$, *for which* $A'_{\bar{t}} \equiv \lambda D^T A_t^\sigma D + A'_{\bar{0}}$ *for all* $t \in GF(q)$,

and $\theta\colon GQ(\boldsymbol{C}) \to GQ(\boldsymbol{C}')$ is induced by an automorphism (also denoted by θ) of G of the following form:

$$\theta = \theta(\sigma, D, \lambda, \pi):$$

$$(\boldsymbol{a}, c, \boldsymbol{b}) \mapsto (\lambda^{-1}\boldsymbol{a}^\sigma D^{-T}, \lambda^{-1/2}c^\sigma + \lambda^{-1}\sqrt{\boldsymbol{a}^\sigma D^{-T} A'_{\bar{0}} D^{-1} (\boldsymbol{a}^\sigma)^T}, \boldsymbol{b}^\sigma P D P + \lambda^{-1}\bar{0}^{1/2}\boldsymbol{a}^\sigma D^{-T})$$

Conversely, given (i), (ii), (iii) *and* (iv) *the automorphism of G $\theta = \theta(\lambda, D, \sigma, \pi)$ induces an isomorphism from $GQ(\boldsymbol{C})$ to $GQ(\boldsymbol{C}')$ mapping (∞), $[A(\infty)]$ and $(\mathbf{0}, 0, \mathbf{0})$ to (∞), $[A'(\infty)]$ and $(\mathbf{0}, 0, \mathbf{0})$, respectively.*

Note the Fundamental Theorem is related to the collineations determining when two flocks of a quadratic cone (Chapter IV, p. 141) are equivalent.

We define three maps on G and see how they map A_t to A'_t. We have $A_t = \begin{pmatrix} f(t) & t^{1/2} \\ 0 & g(t) \end{pmatrix}$.

Shift by s. *For $s \in GF(q)$ defined by*

$$\tau_s \colon (\boldsymbol{a}, c, \boldsymbol{b}) \mapsto (\boldsymbol{a}, c + \sqrt{\boldsymbol{a} A_s \boldsymbol{a}^T}, \boldsymbol{b} + s^{1/2}\boldsymbol{a}).$$

In the Fundamental Theorem we have $\bar{t} = t + s$, $\lambda = 1$, $D = I$, $A'_{\bar{0}} = A_s$, $\sigma =$ id.

Scale by a. *For $a \neq 0 \in GF(q)$.*

$$\sigma_a \colon (\boldsymbol{a}, c, \boldsymbol{b}) \mapsto (\boldsymbol{a}, a^{1/4}c, a^{1/2}\boldsymbol{b}).$$

Now σ_a leaves $A(\infty)$ and $A(0)$ invariant and for $t \in GF(q)$ we have $A_t \mapsto A'_{at} = a^{1/2}A_t$. In the Fundamental Theorem it is $\lambda = a^{-1/2}$, $D = a^{-1/2}I$, $\sigma =$ id, $A'_{\bar{0}} = \mathbf{0}$ and $\bar{t} = at$.

Flip.

$$\varphi \colon (\boldsymbol{a}, c, \boldsymbol{b}) \mapsto (\boldsymbol{b}, c + \boldsymbol{a} \circ \boldsymbol{b}, \boldsymbol{a}).$$

We have φ interchanging $A(0)$ and $A(\infty)$ and for $t \neq 0$ then $A_t \mapsto t^{-1}A_t = A'_{t^{-1}}$.

Note that the above maps, for $t \in GF(q) \cup \{\infty\}$, map

$$\tau_s \colon t \mapsto t + s$$
$$\sigma_a \colon t \mapsto at$$
$$\varphi \colon t \mapsto t^{-1}$$

(With infinity being treated conventionally.)

These maps provide all the possible Möbius transformations. Hence we can say $PGL(2,q)$ is acting on $PG(1,q) \cong GF(q) \cup \{\infty\}$. (Since $PGL(2,q)$ acts 3-transitively, and so, primitively, on $PGL(1,q)$. So $PGL(2,q)_{(\infty)} = AGL(1,q)$ is a maximal subgroup of $PGL(2,q)$. So

$$\langle \tau_s, \sigma_a \mid s,\ a \in GF(q) \rangle = AGL(1,q).$$

Since $\varphi \notin AGL(1,q)$ we have

$$\langle \tau_s, \sigma_s, \varphi \mid s,\ a \in GF(q) \rangle = PGL(2,q).)$$

Now we have:

Theorem 172 ([**6**], 2.3). *Let $\theta \colon G \to G$ be an automorphism of G obtained as a finite sequence of shifts, flips and scales. Moreover, suppose $\boldsymbol{C}$ and $\boldsymbol{C}'$ are two normalised q–clans for which θ maps the 4-gonal family $\mathscr{F}$ of $\boldsymbol{C}$ to the 4-gonal family $\mathscr{F}'$ of $\boldsymbol{C}'$ in such a way that it effects the identity permutation on $GF(q) \cup \{\infty\}$. Then θ must have the form*

$$\theta \colon (\boldsymbol{a}, c, \boldsymbol{b}) \mapsto (a\boldsymbol{a}, ac, a\boldsymbol{b})$$

for some $a \in GF(q)$ $a \neq 0$ so $\mathscr{F} = \mathscr{F}'$.

14. Subiaco q–clans

In this section we will deal with the Subiaco q–clans which first appeared in [**30**] and were explicitly studied in Chapter IV. We will use the Subiaco q–clans as (re)defined by Payne.

14.1. Collineations of the Subiaco q–clan

We (re)define the Subiaco q–clan in the version that Payne constructed [**6**]. Let $d \in GF(q)$ such that trace$(d^{-1}) = 1$. Define

$$\begin{aligned} f'(t) &= d^2t^4 + d^3t^3 + (d^2 + d^4)t^2 \\ g'(t) &= (d^2 + d^4)t^3 + d^3t^2 + d^2t \\ k(t) &= (v(t))^2 = t^4 + d^2t^2 + 1 \end{aligned}$$

so we can define

$$\begin{aligned} f(t) &= \frac{f'(t)}{k(t)} + d^{-1/2}t^{1/2}, \text{ and} \\ g(t) &= \frac{g'(t)}{k(t)} + d^{-1/2}t^{1/2}. \end{aligned}$$

In Chapter IV we define the q–clans

$$\begin{aligned} \boldsymbol{S}_d &= \{A_t^{(d)} \mid t \in GF(q)\} \text{ for all } q \text{ even} \\ \boldsymbol{S}' &= \{A'_t \mid t \in GF(q)\} \text{ for } q = 4^e \ e \text{ odd} \\ \boldsymbol{S}'' &= \{A''_t \mid t \in GF(q)\} \text{ for } q = 2^e \ e \text{ odd} \end{aligned}$$

For $B \in GL(2,q)$, $\boldsymbol{C}' = \{B^TA_tB \mid t \in GF(q)\}$ is a q–clan whenever $\boldsymbol{C} = \{A_t \mid t \in GF(q)\}$ is (see [**102**]).

Now we show that the q–clans $\boldsymbol{S}_d$, $\boldsymbol{S}'$ and $\boldsymbol{S}''$ are equivalent to the q–clan

$$\boldsymbol{C}_d = \left\{ A_t = \begin{pmatrix} f(t) & t^{1/2} \\ 0 & g(t) \end{pmatrix} \mid t \in GF(q) \right\},$$

with f and g as defined above with trace$(d^{-1}) = 1$.

Now for all q even A_t is equivalent to

$$\begin{pmatrix} 1 & 1 \\ \left(\frac{d}{1+d+d^2}\right)^{1/2} & \left(\frac{d}{1+d+d^2}\right)^{1/2} + 1 \end{pmatrix} A_t^{(d)} \begin{pmatrix} 1 & \left(\frac{d}{1+d+d^2}\right)^{1/2} \\ 1 & \left(\frac{d}{1+d+d^2}\right)^{1/2} + 1 \end{pmatrix}.$$

For $q = 4^e$, e odd, let $d = \omega$ where $\omega \in GF(4)$ satisfying $\omega^2 + \omega + 1 = 0$, then A_t is equivalent to

$$\begin{pmatrix} \omega^2 & 0 \\ 0 & \omega \end{pmatrix} A'_t \begin{pmatrix} \omega^2 & 0 \\ 0 & \omega \end{pmatrix}.$$

For $q = 2^e$, e odd, let $d = 1$ then A_t is equivalent to

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} A''_t \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Let $\boldsymbol{C}$ be a Subiaco q–clan. In [**6**] it is shown that for $\theta(\sigma, D, \lambda, \pi)$ we can uniquely determine π from σ, D and λ. So we can now label θ by $\theta(\sigma, D, \lambda)$.

Recall that the subgroup $\mathcal{G}_0$ of the full collineation group $\mathcal{G}$ of GQ($\boldsymbol{C}$) is the subgroup that fixes (∞) and $(\mathbf{0}, 0, \mathbf{0})$. Let H be the subgroup of $\mathcal{G}$ that fixes the line $[A(\infty)]$. Let M be the subgroup of H that fixes $[A(\infty)]$ and $[A(0)]$. Then we have a theorem from [**6**].

Theorem 173 ([**6**], 6.4). *Let $\boldsymbol{C}$ be a Subiaco q–clan and let $GF(q_0)$ be the smallest subfield of $GF(q)$ containing d. Let $r = [GF(q) : GF(q_0)]$ so r is odd. Then the subgroup M is given by*

$$\begin{aligned} M = \{\theta(\sigma, aI, a^{-2})\colon (\boldsymbol{a}, c, \boldsymbol{b}) &\mapsto (a\boldsymbol{a}^\sigma, ac^\sigma, a\boldsymbol{b}^\sigma) \mid \\ & 0 \neq a \in GF(q),\ \sigma \in \mathrm{Gal}\left(\frac{GF(q)}{GF(q_0)}\right)\}. \end{aligned}$$

So $|M| = (q-1)r$.

We will now quote extensively from [**100**].

The results in Section 5 of [**100**] are used to show that:

Theorem 174 ([**100**], 5.1, 5.2). *We have*

$$|H| = 2e(q-1) \text{ and } |\mathcal{G}_0| = 2e(q^2-1).$$

We now investigate the action of the involutions (of lines on (∞)) where one fixes $[A(0)]$ and one fixes $[A(d)]$ where trace$(1/d) = 1$.

Let $I_0 = \theta(1, B_0, \mathrm{id})$ with

$$B_0 = \begin{pmatrix} 1+d+d^2 & d^{1/2}+d^{5/2} \\ d^{3/2} & 1+d+d^2 \end{pmatrix}$$

and $t \mapsto t/(dt+1)$, be the involution fixing $[A(0)]$.

Let $I_d = \theta(1, B_d, \mathrm{id})$ with

$$B_d = \begin{pmatrix} 1+d^4+d^6+d^7 & d^{1/2}+d^{9/2}+d^{13/2} \\ d^{15/2} & 1+d^4+d^6+d^7 \end{pmatrix}$$

and $t \mapsto (t(d^2+1)+d^3)/(dt+d^2+1)$ be the involution fixing $[A(d)]$. Now if $(I_0 \circ I_d)^j = 1$ then $I_0 \circ I_d$ permutes the lines $[A(t)]$ in a cycle of length $q+1$ [**100**]. Importantly the action of $I_0 \circ I_d$ on the $q+1$ lines $[A(t)]$ can be restricted to $GF(q) \cup \{\infty\} \cong PG(1,q)$ so the action is on points of $PG(1,q)$. This action of $I_0 \circ I_d$ on $PG(1,q)$ is determined by the matrix $B_0 \circ B_d$.

Now $I_0 \circ I_d$ maps $G(\boldsymbol{a})$ to $G(\boldsymbol{a}B_0B_d)$ and we have in general, (using the notation introduced in [**100**] and explored in further detail in [**98**]),

$$(B_0 \circ B_d)^j = \frac{1}{d^{1/2}} \begin{pmatrix} [10j + \frac{1}{2}] & [10j] \\ [10j] & [10j - \frac{1}{2}] \end{pmatrix}$$

where $[x] = \lambda^x + \lambda^{-x}$ with $\lambda \in GF(q^2) \setminus GF(q)$ such that $\lambda^{q+1} = 1$. Since $\lambda^{q+1} = 1$ is equivalent to $\lambda = \eta^j$ for some j where η is a primitive element of $GF(q^2)$, then $\lambda \notin GF(q)$ if and only if $j \equiv 0 \pmod{q+1}$. Hence $\lambda^{q+1} = 1$ is equivalent to $j \equiv 0 \pmod{q-1}$.

We have $(B_0 \circ B_d)^j$ leaving invariant some $G(\boldsymbol{a})$ if and only if $(\lambda^{10})^j \in GF(q)$. So if $\lambda = \eta^{q-1}$, $(\lambda^{10})^j \in GF(q)$ if and only if $5j \equiv 0 \pmod{q+1}$.

THEOREM 175 ([**100**], 5.3). *Let $d = \lambda + \lambda^{-1}$ where $\lambda = \eta^{q-1}$, η a primitive element of $GF(q^2)$. Then*

(i) *$I_0 \circ I_d$ permutes the lines through (∞) in a cycle of length $q+1$.*
(ii) *If $q+1 \not\equiv 0 \pmod 5$ then $I_0 \circ I_d$ permutes the $G(\boldsymbol{a})$ in a cycle of length $q+1$.*
(iii) *If $q+1 \equiv \pmod 5$ then $I_0 \circ I_d$ permutes the $G(\boldsymbol{a})$ in five cycles of length $(q+1)/5$.*

COROLLARY 176 ([**100**], 5.4). *If $q = 2^e$ and $q+1 \not\equiv 0 \pmod 5$ there is a unique Subiaco oval. It has stabiliser of order $2e$ inherited from $\mathcal{G}_0$.*

PROOF. Uniqueness follows from Theorem 4.4 of [**100**] and Theorem 175 (ii). Since $|\mathcal{G}_0| = 2e(q^2-1)$, $\mathcal{G}_0$ is transitive on all $q+1$ $G(\boldsymbol{a})$'s and the kernel induces the identity map on the plane of the oval $\mathcal{O}_{\boldsymbol{a}}$. □

We now concentrate our energies on the case $q+1 \equiv 0 \pmod 5$; that is for $q = 4^e$, e odd.

14.2. Subiaco q–clans, for $q = 4^e$, e odd

Let $\boldsymbol{C}$ be the Subiaco q–clan for $q = 4^e$, e odd. Then the 64–clan has $\mathcal{H}_{60}$ and $\mathcal{H}_{15}$ as elements of its herd. Since $\boldsymbol{C}$ is an infinite family q–clan we have generalised these hyperovals. But these hyperovals are inequivalent in $PG(2,64)$. The next question is are there two inequivalent ovals in $H(\boldsymbol{C})$? We (slowly) answer this question.

Let $q = 2^e = 4^r$ r odd so $e = 2r$. Let $d = \omega$ and $\omega \in GF(q)$ such that $\omega^2 + \omega + 1 = 0$. Recall that

$$g_t(\boldsymbol{a}) = \sqrt{\boldsymbol{a}A_t\boldsymbol{a}^T}.$$

From [**100**] we define two involutions on the lines of (∞) by

$$(4)\qquad \begin{aligned} I_\infty &: (\boldsymbol{a}, c, \boldsymbol{b}) \mapsto (\boldsymbol{a}P, g_\omega(\boldsymbol{a}) + c, (\boldsymbol{b} + \omega^2\boldsymbol{a})P), \\ I_1 &: (\boldsymbol{a}, c, \boldsymbol{b}) \mapsto (\boldsymbol{b}P, c + \boldsymbol{a} \circ \boldsymbol{b}, \boldsymbol{a}P), \end{aligned}$$

and their compositions

$$\begin{aligned} I_\infty \circ I_1 &: (\boldsymbol{a}, c, \boldsymbol{b}) \mapsto (\boldsymbol{b} + \omega^2\boldsymbol{a}, c + g_\omega(\boldsymbol{a}) + \boldsymbol{a} \circ \boldsymbol{b}, \boldsymbol{a}), \\ I_\infty \circ I_1 &: (a\boldsymbol{a}, c, b\boldsymbol{a}) \mapsto ((b + \omega^2 a)\boldsymbol{a}, c + a g_\omega(\boldsymbol{a}), a\boldsymbol{a}). \end{aligned}$$

Now $I_\infty \circ I_1$ leaves invariant each $G(\boldsymbol{a})$, $\boldsymbol{a} \in PG(1, q)$, and has order 5.

LEMMA 177 ([**100**], 6.3). *$\mathcal{G}_0$ has exactly $q + 1$ involutions each fixing a unique $G(\boldsymbol{a})$.*

In [**100**] we also show that the orbit containing $G(\boldsymbol{a})$ has length at most $4(q+1)/5$. Let Ω_1 be the $\mathcal{G}_0$-orbit containing $G((1,1))$. Then by lemma 6.2 in [**100**] this orbit has length $(q + 1)/5$.

Note that I_∞ fixes only $G((1,1))$. For $s \in GF(q)$ I_s fixes a unique $G(\boldsymbol{a})$. Now (from [**100**]) I_s fixes $G((0,1))$ if and only if $s^5 + s^4 + \omega^2 s + 1 = 0$ and I_s fixes

$$G((c(s), a(s) + 1)) \text{ if and only if } c(s) \neq 0,$$

where

$$\begin{aligned} a(s) &= \frac{(s^5+1)(1+\omega+\omega^2) + (s^4+s)(1+\omega)}{(1+\omega s+s^2)^{5/2}}, \text{ and} \\ c(s) &= \frac{(\omega^{1/2}+\omega^{5/2})s^5 + \omega^{3/2}s + \omega^{1/2}s + \omega^{3/2}}{(1+\omega s+s^2)^{5/2}}. \end{aligned}$$

THEOREM 178 ([**100**], 6.4 also cf Theorem 7.6 of [**6**]). *$\mathcal{G}_0$ has two orbits on the $G(\boldsymbol{a})$, the short orbit Ω_1 of length $(q+1)/5$ and containing $G((1,1))$ and a long orbit Ω_2 of length $4(q+1)/5$.*

PROOF. Since $\mathcal{G}_0$ acts on Ω_1 and $|\Omega_1| = (q+1)/5$ is odd, each of the $q+1$ involutions $I_s \in \mathcal{G}_0$ must fix some $G(\boldsymbol{a}) \in \Omega_1$. Hence by Lemma 177 no I_s can fix any $G(\boldsymbol{b})$ not in Ω_1. Suppose Ω_2 is any $\mathcal{G}_0$-orbit on the $G(\boldsymbol{a})$'s other than Ω_1. The stabiliser of any $G(\boldsymbol{b}) \in \Omega_2$ must have odd order, implying that 4, the highest power of 2 dividing $|\mathcal{G}_0|$, must divide $|\Omega_2|$. By Theorems 4.4 of [**100**] and Theorem 175, p. 110, $|\Omega_2| = k(q+1)/5$, with $1 \leq k \leq 4$. Since $(q+1)/5$ is odd, it must be that $k = 4$. □

14.3. Ovals for $q = 4^e$, e odd

For a given $\boldsymbol{a}$ the oval $\mathcal{O}_{\boldsymbol{a}}$ obtained directly from $G(\boldsymbol{a})$ is

$$\mathcal{O}_{\boldsymbol{a}} = \{(1, g_t(\boldsymbol{a}), t^{1/2}) \in PG(2,q) \mid t \in GF(q)\} \cup \{(0,0,1)\}.$$

The map $(x,y,z)\mapsto(x^2,z^2,y^2)$ on $PG(2,q)$ replaces $\mathcal{O}_{\boldsymbol{a}}$ with

$$\mathcal{D}_{q+1}(h_{\boldsymbol{a}}(t))=\mathcal{D}(h_{\boldsymbol{a}}(t))-\{(0,0,1)\}\text{ where }h_{\boldsymbol{a}}(t)=\boldsymbol{a}A_t\boldsymbol{a}^T.$$

(Using the o-polynomial notation of Chapter II, Section 4, p. 41.)

$$\text{For }\boldsymbol{a}=(1,1),\ h_{\boldsymbol{a}}(t)=\frac{\omega^2(t^4+t)}{t^4+\omega^2t^2+1}+t^{1/2},$$

in $PG(2,64)$ this o-polynomial is equivalent to the hyperoval $\mathcal{H}_{60}$.

$$\text{For }\boldsymbol{a}=(0,1),\ h_{\boldsymbol{a}}(t)=\frac{t^3+t^2+\omega^2t}{t^4+\omega^2t^2+1}+\omega t^{1/2},$$

in $PG(2,64)$ this o-polynomial is equivalent to the hyperoval $\mathcal{H}_{15}$.

For $\boldsymbol{a}=(1,1)$, $\mathcal{O}_{\boldsymbol{a}}$ belongs to the short $\mathcal{G}_0$-orbit Ω_1 with length $(q+1)/5$. For $\boldsymbol{a}=(0,1)$, if $5\not|\,(e/2)$, $\mathcal{O}_{\boldsymbol{a}}$ belongs to the long $\mathcal{G}_0$-orbit Ω_2. But if $5\,|\,(e/2)$, it follows from computations in [**6**] that $\mathcal{O}_{\boldsymbol{a}}$ also belongs to the short orbit Ω_1.

So $\mathcal{O}_{(1,1)}$ and $\mathcal{O}_{(0,1)}$ are inequivalent if and only if $5\not|\,(e/2)$. Below we give a more detailed picture of the induced groups for the ovals.

THEOREM 179 ([**100**], 6.6). *For $e\equiv 2\pmod 4$, $d=\omega$ and $\boldsymbol{a}=(1,1)$, the complete group induced by $\mathcal{G}_0$ on $PG(2,q)$ and stabilising*

$$\mathcal{D}_{q+1}(h_{(1,1)}(t))=\left\{(1,t,\frac{\omega^2(t^4+t)}{t^4+\omega^2t^2+1}+t^{1/2})\mid t\in GF(q)\right\}\cup\{(0,1,0)\},$$

has order $10e$ and is generated by the following three collineations:

(i) $\varphi\colon(x,y,z)\mapsto(y,x,z)$,
(ii) $\theta\colon(x,y,z)\mapsto(x,y+\omega x,z+\omega^2x)$, *and*
(iii) $\psi\colon(x,y,z)\mapsto(x^2,x^2+\omega^2y^2,x^2+\omega z^2)$.

PROOF. See pages 213–4 in [**100**]. We note that I_∞ stabilises $\mathcal{D}_{q+1}(h_{\boldsymbol{a}}(t))$ for $\boldsymbol{a}=(1,1)$ and acts on the oval as

$$I_\infty\colon(x,y,z)\mapsto(x,y+\omega x,z+\omega^2x).\quad\square$$

NOTE. (i) φ leaves $\mathcal{D}_{q+1}(h_{\boldsymbol{a}}(t)))$ invariant for $\boldsymbol{a}=(1,1)$ but not for $\boldsymbol{a}=(0,1)$.
(ii) $\theta\circ\varphi\colon(x,y,z)\mapsto(y+\omega x,x,z+\omega^2x)$ has order 5.

THEOREM 180 ([**100**], 6.7). *For $e\equiv 2\pmod 4$, $5\not|\,e$, $d=\omega$, and $\boldsymbol{a}=(0,1)$, the complete group induced by $\mathcal{G}_0$ on $PG(2,q)$ and stabilising*

$$\mathcal{D}_{q+1}(h_{(0,1)}(t))=\left\{(1,t,\frac{t^3+t^2+\omega^2t}{t^4+\omega^2t^2+1}+\omega t^{1/2})\mid t\in GF(q)\right\}\cup\{(0,1,0)\},$$

has order $5e/2$ and is generated by the following collineations:

(i) $\theta_\sigma\colon(x,y,z)\mapsto(x^\sigma,y^\sigma,z^\sigma)$, $\sigma\in\operatorname{Aut}F$ *with* $\omega^\sigma=\omega$,
(ii) $\theta\circ\varphi\colon(x,y,z)\mapsto(y+\omega x,x,z+\omega x)$.

14.4. Ovals for $q = 4^e$, e odd, $5 \mid (e/2)$

Now we want to prove that there are two inequivalent ovals in the herd of the Subiaco q–clan. We have shown this is true except for the case when $5 \mid (e/2)$.

From the proof of Theorem 178, p. 111, we know that $\boldsymbol{a}$ (that is, $G(\boldsymbol{a})$) is in the long orbit Ω_2 precisely if it is fixed by no involution I_s. So we may use Eq.(11) of [**100**] (determining the unique involution I_s fixing $[A(s)]$) to recognize members of Ω_2. Moreover, each oval $\mathcal{D}_{q+1}(h_{\boldsymbol{a}}(t))$ may be associated with an irreducible algebraic curve in $PG(2,q)$ of degree 10 (see below).

There will be some manipulations made on the elements of the herd of the Subiaco q–clan (Payne version) so they correspond with the herd of the Subiaco q–clan in [**30**] (which corresponds to the rational function forms of the hyperovals $\mathcal{H}_{60}$ and $\mathcal{H}_{15}$ in $PG(2,64)$).

We want to reindex the $\boldsymbol{a} \in PG(1,q)$ by $c \in GF(q) \cup \{\infty\}$ in the following way. For $c \in GF(q) \cup \{\infty\}$, put $\boldsymbol{a}_c = \left(\frac{\omega^2+\omega c}{1+c^{1/2}+\omega c}, \frac{\omega c}{1+c^{1/2}+\omega c}\right)$. Clearly $1 + c^{1/2} + \omega c \neq 0$ for all $c \in GF(q)$. Then $\boldsymbol{a}_c = (1,1)$ if and only if $c = \infty$, and for c, $d \in GF(q)$, $\boldsymbol{a}_c \equiv \boldsymbol{a}_d$ if and only if $c = d$. For $c = \omega$, $\boldsymbol{a}_c = (0, \omega^2) \equiv (0,1)$. For $c \in GF(q) \cup \{\infty\} \setminus \{\infty, \omega\}$, $\boldsymbol{a}_c \equiv (1, c/(c+\omega))$. Index the ovals $\mathcal{D}_{q+1}(h_{\boldsymbol{a}}(t))$ for $\boldsymbol{a} \in PG(1,q)$ so that $\mathcal{O}_c = \mathcal{D}_{q+1}(h_{\boldsymbol{a}_c}(t))$, $c \in GF(q) \cup \{\infty\}$. Hence we have the following:

$$\mathcal{O}_\infty = \{(1, t, f_\infty(t)) \mid t \in F\} \cup \{(0,1,0)\}, \tag{5}$$

where

$$f_\infty(t) = \frac{\omega^2 t^4 + \omega^2 t}{t^4 + \omega^2 t^2 + 1} + t^{1/2}.$$

Then for $c \in GF(q)$, using Payne's version of the Subiaco q–clan, obtaining $\mathcal{D}_{q+1}(h_{\boldsymbol{a}}(t))$ from $\mathcal{O}_{\boldsymbol{a}}$ and the Subiaco herd we obtain

$$\mathcal{O}_c = \{(1, t, f_c(t)) \mid t \in GF(q)\} \cup \{(0,1,0)\}$$

where

$$\begin{aligned} f_c(t) &= \left(\frac{\omega^2+\omega c}{1+c^{1/2}+\omega c}\right)^2 \left(\frac{\omega^2 t^4 + t^3 + t^2}{t^4+\omega^2 t^2+1} + \omega t^{1/2}\right) \\ &\quad + \left(\frac{(\omega^2+\omega c)\omega c}{1+c+\omega^2 c^2}\right) t^{1/2} + \frac{\omega^2 c^2}{1+c+\omega^2 c^2} \left(\frac{t^3+t^2+\omega^2 t}{t^4+\omega^2 t^2+1} + \omega t^{1/2}\right) \\ &= \frac{1}{1+c+\omega^2 c^2} \left(\frac{(1+\omega c^2)t^4 + \omega t^3 + \omega t^2 + \omega c^2 t}{t^4+\omega^2 t^2+1} + (\omega^2 + c + \omega^2 c^2) t^{1/2}\right). \end{aligned}$$

Lemma 181 ([**100**], 6.8). *Let $g \in PGL(3,q)$ be defined by*

$$g\colon (x,y,z) \mapsto (y, x+\omega y, \omega^2 y + z).$$

Then g is a collineation of order 5 stabilising $\mathcal{O}_c$ for every $c \in GF(q) \cup \{\infty\}$.

Proof. Using Eq.(4) we see that $I_1 \circ I_\infty \colon (\boldsymbol{a}, c, \boldsymbol{b}) \mapsto (\boldsymbol{b}, c+\boldsymbol{a}\circ\boldsymbol{b}+g_\omega(\boldsymbol{b}P), \boldsymbol{a}+\omega^2\boldsymbol{b})$, and in particular, $I_1 \circ I_\infty \colon (a\boldsymbol{a}, c, b\boldsymbol{a}) \mapsto (b\boldsymbol{a}, c + g_\omega(b\boldsymbol{a}P), (a+\omega^2 b)\boldsymbol{a})$. Hence $I_1 \circ I_\infty$ is a collineation of order 5 leaving $G(\boldsymbol{a})$ invariant for each $\boldsymbol{a} \in PG(1,q)$. Use the semilinear map $T\colon (x,y,z) \mapsto (x^2, y^2, z^2)$ mapping $\mathcal{O}_{\boldsymbol{a}}$ to $\mathcal{D}_{q+1}(h_{\boldsymbol{a}}(t))$ to transfer the action of $I_1 \circ I_\infty$ to the map

$$g_{\boldsymbol{a}} \colon (x,y,z) \mapsto (y, x+\omega y, z + y\boldsymbol{a}(PA_\omega P^T)\boldsymbol{a}^T)$$

which stabilises $\mathcal{O}_{\boldsymbol{a}}$. Note that $PA_\omega P^T \equiv A_\omega = \begin{pmatrix} \omega & \omega^2 \\ 0 & \omega \end{pmatrix}$. For $\boldsymbol{a} = (1,1)$, $\boldsymbol{a}A_\omega\boldsymbol{a}^T = \omega^2$. Now put $\boldsymbol{a} = \boldsymbol{a}_c$ and compute

$$\boldsymbol{a}A_\omega\boldsymbol{a}^T = \left(\frac{\omega+\omega^2c^2}{1+c+\omega^2c^2}\right)\omega + \left(\frac{(\omega^2+\omega c)\omega c}{1+c+\omega^2c^2}\right)\omega^2 + \left(\frac{\omega^2c^2}{1+c+\omega^2c^2}\right)\omega = \omega^2.$$

Hence for every $c \in GF(q) \cup \{\infty\}$, $g_{\boldsymbol{a}}$ is the map g of the Lemma. $\square$

Lemma 182 ([**100**], 6.9). (i) *$\mathcal{O}_\infty$ is always in the short orbit Ω_1.*

(ii) *For $c \in GF(q)$, $\mathcal{O}_c \in \Omega_2$ if and only if*

$$p_c(x) = x^5 + (\omega^2c^2 + \omega^2)x^4 + (\omega^2c^2+1)x + 1 = 0,$$

has no root in $GF(q)$.

(iii) *There is a $c \in GF(q) \setminus GF(4)$ for which both $p_c(x) = 0$ and*

$$p_{(\omega^2c^2+\omega^2)}(x) = x^5 + (c^4+\omega)x^4 + c^4x + 1 = 0,$$

have no root in $GF(q)$.

Define the conic $\mathcal{C}\colon xy = z^2$, that is,

$$\mathcal{C} = \{(1, t, t^{1/2}) \mid t \in GF(q)\} \cup \{(0,1,0)\}.$$

Lemma 183 ([**100**], 6.10). (i) *$\mathcal{O}_\infty \cap \mathcal{C} = PG(2,4) \cap \mathcal{C}$,*

(ii) *For c satisfying condition (iii) of Lemma 182, we have*

$$\mathcal{O}_c \in \Omega_2 \text{ and } \mathcal{O}_c \cap \mathcal{C} = PG(2,4) \cap \mathcal{C}.$$

Proof. For (i), $(\mathcal{O}_\infty \setminus \{(0,1,0)\}) \cap \mathcal{C} = \{(1,t,f_\infty(t)) \mid f_\infty(t) = t^{1/2}\}$. Clearly $f_\infty(t) = t^{1/2}$ if and only if $t \in GF(4)$. Similarly, if c satisfies condition (iii) of Lemma 182, then $\mathcal{O}_c \in \Omega_2$ and $(\mathcal{O}_c \setminus \{(0,1,0)\}) \cap \mathcal{C} = \{(1,t,f_c(t)) \mid f_c(t) = t^{1/2}\}$. Using Eq. (5) we may compute that $f_c(t) = t^{1/2}$ if and only if $\omega^2t(t^3+1)(t^5+(c^4+\omega)t^4 + c^4t + 1) = 0$, proving (ii). $\square$

For each $c \in GF(q) \cup \{\infty\}$ we may define the hyperoval $\mathcal{H}_c = \mathcal{O}_c \cup \{(0,0,1)\}$, and with a natural abuse of language refer to $\mathcal{H}_c$ belonging to Ω_1 or Ω_2. For example, $\mathcal{H}_\infty \in \Omega_1$. And for $c = c_0$ satisfying condition (iii) of Lemma 182, $\mathcal{H}_{c_0} \in \Omega_2$. From now on fix $c = c_0$ to be such an element.

From Section 8.3, p. 57, the hyperovals $\mathcal{H}_\infty$ and $\mathcal{H}_{c_0}$ are inequivalent for $q = 64$ and have full collineation stabilisers of order 60 and 15, respectively. So from now on we assume that $q \geq 1024$.

Using the ideas of [**87**] we shall show that $\mathcal{H}_\infty$ and $\mathcal{H}_{c_0}$ are the pointsets of two absolutely irreducible degree ten algebraic curves in $PG(2,q)$. We remind the reader that in this section groups act on the right.

We refer the reader to Sections 2.6 and 10.1 in [**55**] for the algebraic geometric definitions used here.

LEMMA 184 ([**100**], 6.11). *For both $c=\infty$ and $c=c_0$, $\mathcal{H}_c$ is the pointset of an absolutely irreducible degree ten algebraic curve $\mathscr{C}$ in $PG(2,q)$ having $(0,0,1)$ as its only singular point. The multiplicity of $(0,0,1)$ for $\mathscr{C}$ is 8, and in $PG(2,q^2)$ there are two tangent lines for $\mathscr{C}$ at $(0,0,1)$. The tangent lines are $Q=[\eta,1,0]^T:\eta x+y=0$ and $\bar{Q}=[\eta^q,1,0]^T:\eta^q x+y=0$, where $\eta\in GF(q^2)\setminus GF(q)$ satisfies $\eta^{q+1}=1$ and $\eta^q+\eta=\omega$.*

PROOF. For $c\in\{\infty,c_0\}$, write $d=c/(c+\omega)$, so $d\in\{1,c_0/(c_0+\omega)\}$. In particular, we are avoiding the case $c=\omega$ with $d=\infty$. Put $m_c=\left(\frac{\omega^2+\omega c}{1+c^{1/2}+\omega c}\right)^2$. So $m_c\neq 0$, $m_\infty=1$, and $\boldsymbol{a}_c=(m_c)^{1/2}(1,d)$. Then $\mathcal{H}_c=\{(1,t,f_c(t))\mid t\in GF(q)\}\cup\{(0,1,0),(0,0,1)\}$ is projectively equivalent to $\bar{\mathcal{H}}_c=\{(1,t,f_c(t)/m_c)\mid GF(q)\in F\}\cup\{(0,1,0),(0,0,1)\}$. Here

$$\begin{aligned}\frac{f_c(t)}{m_c}=f(t,d)&=\left(\frac{\omega^2t^4+t^3+t^2}{t^4+\omega^2t^2+1}+\omega t^{1/2}\right)+dt^{1/2}+d^2\left(\frac{t^3+t^2+\omega^2t}{t^4+\omega^2t^2+1}+\omega t^{1/2}\right)\\&=\frac{\omega^2t^4+(1+d^2)(t^3+t^2)+\omega^2d^2t}{t^4+\omega^2t^2+1}+(\omega+d+\omega d^2)t^{1/2}.\end{aligned}$$

Define $g_c\in PGL(3,q^2)$ by $g_c\colon(x,y,z)\mapsto(x,y,m_cz)$. So $g_c\colon\bar{\mathcal{H}}_c\mapsto\mathcal{H}_c$, and g_c fixes the two points $(0,1,0)$ and $(0,0,1)$. We show that $\bar{\mathcal{H}}_c$ satisfies the conclusions of the Lemma. Since g_c also fixes the lines Q, $\bar{Q}$, it will follow that $\mathcal{H}_c$ satisfies the same conclusions.

The point $(1,t,f(t,d))\equiv(1,y,z)$ satisfies

$$z=\frac{\omega^2y^4+(1+d^2)(y^3+y^2)+d^2\omega^2y}{y^4+\omega^2y^2+1}+(\omega+d+\omega d^2)y^{1/2}.$$

Multiply through by $y^4+\omega^2y^2+1$, square both sides, and then make the resulting equation homogeneous in x, y, z to get the algebraic curve $\mathscr{C}_d\colon h_d(x,y,z)=0$, where

$$\begin{aligned}h_d(x,y,z)=(z^2+(\omega^2+d^2+\omega^2d^4)xy)(y^2+\omega xy+x^2)^4\\+\omega x^2y^8+\omega d^4x^8y^2+(1+d^4)(x^4y^6+x^6y^4).\end{aligned}$$

By construction, for all $t\in GF(q)$, $(1,t,f(t,d))\in\mathscr{C}_d$. Now $h_d(0,y,z)=z^2y^8=0$ if and only if $y=0$ or $z=0$. Hence the pointset of $\mathscr{C}_d$ is exactly the hyperoval $\bar{\mathcal{H}}_c$ (always $d=c/(c+\omega)$). So $|\mathscr{C}_d|=q+2$, and we now want to prove that $h_d(x,y,z)$ is absolutely irreducible.

First compute $\frac{\partial h_d}{\partial x}=(\omega^2+d^2+\omega^2d^4)y(y^2+\omega xy+x^2)^4$, $\frac{\partial h_d}{\partial y}=(\omega^2+d^2+\omega^2d^4)x(y^2+\omega xy+x^2)^4$, and $\frac{\partial h_d}{\partial z}=0$. Since $\omega^2+x+\omega^2x^2$ is irreducible over $GF(4)$, and hence over $GF(q)$, $\omega^2+d^2+\omega^2d^4\neq 0$ for all $d\in GF(q)$. We have $(0,0,1)$

as a singular point. The point $(0,0,1)$ is incident with the lines $l = [a,b,0]$ for a, $b \in GF(q)$ (recall the definition of multiplicity in [**55**], p. 52).

$$\begin{aligned}\mathscr{C}_d \cap l &= \{(x,y,z) \mid \begin{pmatrix} a & b & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0 \text{ and } h_d(x,y,z) = 0\} \\ &= \{(x,y,z) \mid ax + by = 0 \text{ and } h_d(x,y,z) = 0\}\end{aligned}$$

now assume $a \neq 0$, so $a = 1$,

$$\begin{aligned} &= \{(x,y,z) \mid x + by = 0 \text{ and } h_d(x,y,z) = 0\} \\ &= \{(by,y,z) \mid h_d(by,y,z) = 0\}.\end{aligned}$$

Let $h'_d \in GF(q)[x,y]$ with h'_d homogeneous with $h'_d(y,z) = h_d(by,y,z)$. Then

$$\begin{aligned} h'_d(y,z) = (z^2 + (\omega^2 + d^2 + \omega^2 d^4)by^2)(y^2 + b\omega y^2 + b^2y^2)^4 \\ + \omega b^2 y^{10} + \omega d^4 b^8 y^{10} + (1+d^4)(b^4y^{10} + b^6 y^{10}).\end{aligned}$$

Now $(0,1)$ is a zero of h'_d of multiplicity m if and only if 0 is a zero of $h'_d(y,1)$ of multiplicity m if and only if y^m divides $h'_d(y,1)$ but y^{m+1} does not divide $h'_d(y,1)$. So

$$\begin{aligned} h'_d(y,1) = (1 + d^4 + b^8)y^8 + \\ (\omega^2(1+b^2+b^8) + (b^4+b^6)(1+d^4) + d^2b^8(1+d^2) + d^2 + d^6(1+\omega d^2))y^{10}.\end{aligned}$$

The line $[0,1,0]$ gives $y = 0$ and $h_d(x,0,z) = 0$ if and only if $z^2x^8 = 0$ if and only if $h'_d(x,z) = 0$ if and only if $(0,1)$ has multiplicity 8. The line $[1,0,0]$ gives $x = 0$ and $h_d(0,y,z) = 0$ if and only if $z^2y^8 = 0$ if and only if $h'_d(y,z) = 0$ if and only if $(0,1)$ has multiplicity 8. Hence $(0,0,1)$ has multiplicity 8.

Let $\mathbb{F}$ be the algebraic closure of $GF(q)$. The lines $[a,1,0]$, $a \in \mathbb{F}$ and $[1,0,0]$ are the lines on the point $(0,0,1)$. Firstly, we notice that for the line $l = [1,0,0]$, $\mathscr{C}_d \cap l$ implies that $h_d(x,y,z) = 0$ and $x = 0$, so $x = 0$ and $z^2y^8 = 0$. So the point $(0,0,1)$ still has multiplicity 8, so $[1,0,0]$ is not a tangent line to $(0,0,1)$.

Let $l = [a,1,0]$ for $a \in \mathbb{F}$. Now $h_d(x,y,z) = 0$ and $ax + y = 0$ means $ax = y$ and

$$\begin{aligned} 0 = x^{10}(\omega a^8 + \omega d^4 a^2 + (1+d^4)(a^6 + a^4)) \\ + (z^2 + (\omega^2 + d^2 + \omega^2 d^4)ax^2)x^8(a^2 + \omega a + 1)^4\end{aligned}$$

We have $[a,1,0]$ being a tangent line to $(0,0,1)$ if $(a^2 + \omega a + 1)^4 = 0$ (with $(0,0,1)$ having multiplicity 10 on $\mathscr{C}_d \cap l$). So $a^2 + \omega a + 1 = 0$ if and only if $(x + a_1)(x + a_2) = 0$ for some a_1, $a_2 \in \mathbb{F}$ with $a_1 a_2 = 1$ and $a_1 + a_2 = \omega$. Now a_1 and a_2 are conjugate in $GF(q^2)$ so we let

$$x^2 + \omega xy + y^2 = (x + \eta y)(x + \eta^q y),$$

where $\eta \in GF(q) \setminus GF(q^2)$, $\eta^{q+1} = 1$ and $\eta + \eta^q = \omega$. So the tangent lines to $(0,0,1)$ are

$$Q\colon [\eta, 1, 0] \text{ and } \bar{Q}\colon [\eta^q, 1, 0].$$

If one of Q, $\bar{Q}$ is a component of $\mathscr{C}_d$, so is the other, then $y^2 + \omega xy + x^2$ must divide $h_d(x,y,z)$. We now show that this is not the case. Put $y^2 = \omega xy + x^2$, and hence $y^4 = x^3(y + \omega x)$, $y^6 = x^5 y$, $y^8 = \omega x^8 + \omega y x^7$ into $h_d(x,y,z)$. After a little simplification, $h_d(x,y,z) = x^9(\omega^2(1 + d^4)y + x)$, which is not the zero polynomial. This proves that neither tangent to $\mathscr{C}_d$ at $(0,0,1)$ is a component of $\mathscr{C}_d$.

Now suppose that $\mathscr{C}_d$ has components $C_1, \dots, C_l$, $l > 1$, with $\deg C_i = k_i$, and suppose $(0,0,1)$ has multiplicity t_i for C_i. So $\sum k_i = 10$ and $\sum t_i = 8$. If some $t_i = k_i$, then $t_i = k_i = 1$ and C_i is a line. But in this case C_i must be tangent to C_i at $(0,0,1)$, so C_i is tangent to $\mathscr{C}_d$ at $(0,0,1)$, contradicting the previous paragraph. So the only possibility is that there are exactly two components C_1 and C_2 with $t_1 = k_1 - 1$ and $t_2 = k_2 - 1$.

First suppose C_1 and C_2 are defined over $GF(q)$, and $(0,0,1)$ is a $(k_i - 1)$-tuple point for C_i, $i = 1, 2$. Any tangent to C_i at $(0,0,1)$ is tangent to $\mathscr{C}_d$ and not defined over $GF(q)$. So any line (over $GF(q)$) through $(0,0,1)$ meets C_i in a second point, which implies $|C_i| \geq q + 2$. Since any point of $C_1 \cap C_2$ is a singular point for $\mathscr{C}_d$ clearly $|C_1 \cup C_2| \geq 2(q+2) - 1 > q + 2 = |\mathscr{C}_d|$, an impossibility.

So we may suppose C_1 and C_2 are not defined over $GF(q)$, but over some $GF(q^r)$, $r > 1$. Let $\mathrm{id} \neq \sigma \in \mathrm{Gal}(GF(q^r)/GF(q))$. Then $C_1^\sigma = C_2$, so $\deg C_1 = \deg C_2 = 5$. By Lemma 10.1.1 of [**55**], $|C_i| \leq 5^2$, so $|\mathscr{C}_d| \leq 49$. Since $q > 64$ we have a contradiction. □

For the remainder of this section write $\mathcal{H}_1 = \mathcal{H}_\infty$ and $\mathcal{H}_2 = \mathcal{H}_{c_0}$. Then for $i = 1, 2$, let $G_i = P\Gamma L(3,q)_{\mathcal{H}_i}$ be the full collineation stabiliser of the hyperoval $\mathcal{H}_i$. Note that $\mathcal{H}_1$ and $\mathcal{H}_2$ are equivalent to the hyperovals similarly named in Chapter II, Section 8.3, p. 57.

Let $g \in P\Gamma L(3,q)$ have companion automorphism $\sigma \in \mathrm{Aut}\, GF(q)$. Let $h \in GF(q)[x,y,z]$ be a homogeneous polynomial. The **image**, h^g, of h under g is defined by:

$$h^g = g \circ h \circ \sigma^{-1},$$

and for $d = 1 \in GF(q)$, write $h_1 = h_d(x,y,z)$ (since $g_\infty = \mathrm{id}$), and for $d = c_0/(c_0 + \omega)$, let h_2 be the image of $h_d(x,y,z)$ under $g_{c_0}^{-1}$. Then we have $\mathcal{H}_i = \{(x,y,z) \in PG(2,q) \mid h_i(x,y,z) = 0\}$, $i = 1, 2$.

Lemma 185 ([**100**], 6.12).

$$G_i = \{g \in P\Gamma L(3,q) \mid h_i^g = \lambda h_i, \lambda \in GF(q) \setminus \{0\}\}, \text{ for } i = 1,\ 2.$$

PROOF. ($\supseteq$) Let $g \in P\Gamma L(3,q)$ with $h_i^g = \lambda h_i$, $\lambda \in GF(q) \setminus \{0\}$ for $i = 1, 2$. Then g fixes the set of points (x,y,z) such that $h_i(x,y,z) = 0$. But these are just the points of the hyperoval $\mathcal{H}_i$ for $i = 1, 2$.

($\subseteq$) Let $g \in G_i$ and suppose $h_i^g \neq h_i$. If $\mathscr{C}_i\colon h_i(x,y,z) = 0$, $i = 1, 2$, then the pointsets of $\mathscr{C}_i$ and $\mathscr{C}_i{}^g$ coincide. By Bezout's Theorem (see [**55**] 10.1 VII), it follows that the number of points of $\mathscr{C}_i \cap \mathscr{C}_i{}^g$, counted according to multiplicity, is at most 100. This is contrary to our hypothesis that $q \geq 1024$. □

Since $(0,0,1)$ is the unique singular point of $\mathscr{C}_i$, $i = 1, 2$, G_i must fix $(0,0,1)$ and the set $\{Q, \bar{Q}\}$ of tangents. Also, since $(0,0,1)$ is on $\mathcal{H}_i$, no nontrivial element of G_i can have $(0,0,1)$ as its centre, $i = 1, 2$. Hence G_1 and G_2 fix $(0,0,1)$ but not linewise, and so act faithfully on the quotient space $PG(2,q)/(0,0,1)$.

We are now ready to prove the final theorem of this section.

THEOREM 186. *The hyperovals $\mathcal{H}_1$ and $\mathcal{H}_2$ in $PG(2,q)$, $q = 2^e$, are inequivalent for $e \equiv 2 \pmod 4$. The full collineation stabiliser of $\mathcal{H}_1$ in $P\Gamma L(3,q)$ is isomorphic to $C_5 \rtimes C_{2e}$, and the full collineation stabiliser of $\mathcal{H}_2$ in $P\Gamma L(3,q)$ is isomorphic to $C_5 \rtimes C_{e/2}$.*

PROOF. Let $h \in PGL(2,q)$ with $|h| = q+1$. Then $\langle h \rangle$ is a Singer cycle of $PG(1,q)$, so $\langle h \rangle = C_{q+1}$ acts regularly on $PG(1,q)$. Since h is induced by an invertible 2×2 matrix over F with (conjugate) eigenvalues in $GF(q^2) \setminus GF(q)$, we have $\langle h \rangle$ fixing a conjugate pair of points, say $\{P, \bar{P}\}$. As $N_{P\Gamma L(2,q)}(\langle h \rangle)$ permutes the fixed points of $\langle h \rangle$, $N_{P\Gamma L(2,q)}(\langle h \rangle)$ stabilises the conjugate pair $\{P, \bar{P}\}$. Hence $N_{P\Gamma L(2,q)}(\langle h \rangle) \leq P\Gamma L(2,q)_{\{P,\bar{P}\}}$. And since $P\Gamma L(2,q)$ acts transitively on conjugate pairs of points, then replacing h by a conjugate if necessary,

$$N_{P\Gamma L(2,q)}(\langle h \rangle) \leq P\Gamma L(2,q)_{\{Q,\bar{Q}\}},$$

where $\{Q, \bar{Q}\}$ is the pair of conjugate tangent lines (which are conjugate points in the quotient space) to the hyperovals at $(0,0,1)$ in $PG(2,q)$. By Theorem 20, p. 7, we have

$$N_{P\Gamma L(2,q)}(\langle h \rangle) = C_{q+1} \rtimes C_{2e}.$$

But the order of $P\Gamma L(2,q)_{\{Q,\bar{Q}\}}$ is $2(q+1)e$, so by comparing orders

$$C_{q+1} \rtimes C_{2e} = P\Gamma L(2,q)_{\{Q,\bar{Q}\}}.$$

Hence both G_1 and G_2 are subgroups of $C_{q+1} \rtimes C_{2e}$. From this, for the g from Lemma 181, p. 113, we have that $\langle g \rangle$ is normal in $PGL(2,q)_{\{Q,\bar{Q}\}}$, since $\langle g \rangle$ is characteristic in $\langle h \rangle$, which is normal in $PGL(2,q)_{\{Q,\bar{Q}\}}$. Since $q^2 + q + 1 \equiv 1 \pmod 5$, g has a unique fixed line, namely $x + y + \omega^2 z = 0$. Since G_1 and G_2 normalise $\langle g \rangle$, they fix $x + y + \omega^2 z = 0$.

Let $H_i = G_i \cap C_{q+1}$, for $i = 1, 2$. We have H_1 and H_2 fixing both tangent lines Q and $\bar{Q}$, so fixing their product $x^2 + \omega xy + y^2 = 0$. They also fix the line

$x + y + \omega^2 z = 0$, so fix $x^2 + y^2 + \omega z^2 = 0$. Let $\mathcal{P}$ be the pencil generated by these two. The group induced on the set of conics of $\mathcal{P}$ by the stabiliser in $PGL(3, q)$ of $\mathcal{P}$ is cyclic of order $q - 1$. Since $(q + 1, q - 1) = 1$ and H_i fixes the tangent lines then each H_i fixes every conic in $\mathcal{P}$. So for $i = 1$, 2, H_i fixes the conic $\mathcal{C}\colon xy = z^2$, so it fixes $\mathcal{H}_i \cap \mathcal{C} = \mathcal{C} \cap PG(2, 4)$, by Lemma 183, p. 114.

Now H_i acts semiregularly on $PG(2, q) \setminus \{(0, 0, 1)\}$ for $i = 1, 2$. All points (except the fixed point) have orbits of length $|H_i|$. But since H_i fixes $\mathcal{C} \cap PG(2, 4)$ and acts semiregularly on $\mathcal{C}$, we have $|H_i|$ dividing $|\mathcal{C} \cap PG(2, 4)| = 5$. Hence $|H_i| = 1$ or 5. But $\langle g \rangle \le H_i$, so $H_i = \langle g \rangle$ for $i = 1$, 2. Hence G_1 and G_2 are subgroups of $\langle g \rangle \rtimes C_{2e}$.

From Theorem 179, p. 112 we have the induced group of $\mathcal{H}_1$ having order $10e$ so we have $G_1 = \langle g \rangle \rtimes C_{2e}$.

As $q + 1 \equiv 0 \pmod 5$ with $q = 2^e$, then $e = 2r$ where r is odd, so $e/2$ is odd. We now show that $G_2 \le \langle g \rangle \rtimes C_{e/2}$. The subgroup $C_5 \rtimes C_4$ contains all the involutions of $\langle g \rangle \rtimes C_{2e}$ (five in total) since $e/2$ is odd. These five involutions are conjugate under $\langle g \rangle$. If G_2 contains an involution then it will contain the involution φ from Theorem 179, p. 112. Since

$$\varphi\colon \{(1, t, f_2(t)) \mid t \in F\} \mapsto \{(t, 1, f_2(t)) \mid t \in F\} = \{(1, u, uf_2(u^{-1})) \mid u \in F\},$$

it follows that if G_2 contains an involution, then $f_2(t) = tf_2(t^{-1})$ for all $t \in F$, but this is not so. Hence 2 does not divide $|G_2|$. That is, $G_2 \le \langle g \rangle \rtimes C_{e/2}$.

From the proof of Theorem 180, p. 112 we have the induced group of $\mathcal{H}_2$ has order $5e/2$. Hence $G_2 = \langle g \rangle \rtimes C_{e/2}$.

This completes the proof of the theorem. □

14.5. Remarks on the Subiaco hyperovals

A discussion of the Subiaco hyperovals and related structures can be found in Section 10, p. 158, Chapter IV.

15. Tensor q–clan geometries

While S. E. Payne visited The University of Western Australia in 1993 he was stimulated by a seemingly simple question. "Why is the c in the EGQ group G in the centre?" Payne's answer to resolving this question was tensor q–clan geometry.

We will only talk briefly on this subject since much of the theory and applications are still in progress. The main references are [**98**] and [**101**].

Let $q = 2^e$. We will attempt to describe the automorphisms of the Fundamental Theorem in terms of tensor products of pairs of matrices in $GL(2, q)$.

Let $P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and define $\boldsymbol{b} \circ \boldsymbol{a} = \boldsymbol{b} P \boldsymbol{a}^T$ for $\boldsymbol{a},\ \boldsymbol{b} \in GF(q)^2$. (Note this is different from the definition used previously for $\boldsymbol{b} \circ \boldsymbol{a}$.) Let

$$G = \{(\boldsymbol{a}, c, \boldsymbol{b}) \mid \boldsymbol{a},\ \boldsymbol{b} \in GF(q)^2,\ c \in GF(q)\}$$

with binary operation

$$(\boldsymbol{a}, c, \boldsymbol{b})(\boldsymbol{a}', c', \boldsymbol{b}') = (\boldsymbol{a} + \boldsymbol{a}', c + c' + \sqrt{\boldsymbol{b} \circ \boldsymbol{a}'}, \boldsymbol{b} + \boldsymbol{b}').$$

Let

$$K = \{((\boldsymbol{a}, \boldsymbol{b}), c) \mid \boldsymbol{a},\ \boldsymbol{b} \in GF(q)^2,\ c \in GF(q)\}$$

with binary operation

$$((\boldsymbol{a}, \boldsymbol{b}), c)((\boldsymbol{a}', \boldsymbol{b}'), c') = ((\boldsymbol{a} + \boldsymbol{a}', \boldsymbol{b} + \boldsymbol{b}'), c + c' + \boldsymbol{b} \circ \boldsymbol{a}').$$

The group K has centre $Z = \{((\boldsymbol{0}, \boldsymbol{0}), c) \mid c \in GF(q)\}$. Note there is an isomorphism ψ from K to G defined by $((\boldsymbol{a}, \boldsymbol{b}), c) \mapsto (\boldsymbol{a}, c^{1/2}, \boldsymbol{b})$.

For each $\boldsymbol{0} \neq \boldsymbol{a} \in GF(q)^2$ we define

$$L_{\boldsymbol{a}} = \{(\boldsymbol{a} \otimes \boldsymbol{b}, c) \mid \boldsymbol{b} \in GF(q)^2,\ c \in GF(q)\},$$

and for each $\boldsymbol{0} \neq \boldsymbol{b} \in GF(q)^2$ we define

$$R_{\boldsymbol{b}} = \{(\boldsymbol{a} \otimes \boldsymbol{b}, c) \mid \boldsymbol{a} \in GF(q)^2,\ c \in GF(q)\}.$$

We have $L_{\boldsymbol{a}}$ and $R_{\boldsymbol{b}}$ being elementary abelian subgroups of K of order q^3. For each nonzero $\boldsymbol{a},\ \boldsymbol{b} \in GF(q)^2$, $L_{\boldsymbol{a}} = L_{\boldsymbol{b}}$ if and only if $\langle \boldsymbol{a} \rangle = \langle \boldsymbol{b} \rangle$. So we can think of the $L_{\boldsymbol{a}}$ as indexed by the points of $PG(1, q)$. The scalar multiplication

$$d(\boldsymbol{a} \otimes \boldsymbol{b}, c) = (d\boldsymbol{a} \otimes \boldsymbol{b}, d^2 c) = (\boldsymbol{a} \otimes d\boldsymbol{b}, d^2 c)$$

makes each $L_{\boldsymbol{a}}$ into a 3-dimensional vector space over $GF(q)$. So there is an associated projective plane $\bar{L}_{\boldsymbol{a}} \cong PG(2, q)$. Similarly, for $R_{\boldsymbol{a}}$.

A vector $\boldsymbol{v} \in GF(q)^4$ is called **pure**, (or **decomposable**) if $\boldsymbol{v} = \boldsymbol{u} \otimes \boldsymbol{w}$ for some vectors $\boldsymbol{u},\ \boldsymbol{w} \in GF(q)^2$. (Generally, $\boldsymbol{v} = \sum \boldsymbol{u} \otimes \boldsymbol{w}$. Indeed if $V = U \otimes W$ and $\mathcal{B}$ is a basis for U and $\mathcal{C}$ is a basis for W then $\{\boldsymbol{u} \otimes \boldsymbol{w} \mid \boldsymbol{u} \in \mathcal{B},\ \boldsymbol{w} \in \mathcal{C}\}$ is a basis for V.) We have

$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c & d \end{pmatrix} = \begin{pmatrix} ac & ad \\ bc & bd \end{pmatrix} \cong (a, b) \otimes (c, d).$$

The matrix $(a, b) \otimes (c, d)$ has rank one and so determinant zero and so is singular. We denote the set of all 2×2 matrices over $GF(q)$ by $M_2(q)$ and note that it is isomorphic to $GF(q)^4$. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(q)$. Then $A \in M_2(q)$ is pure if and only if $\det(A) = 0$ if and only if $ad - bc = 0$. Hence we can define a quadratic form, Q, from $GF(q)^4$ to $GF(q)$ by

$$Q(a, b, c, d) = ad - bc.$$

Hence all pure vectors of $GF(q)^4$ are zeros of this form. (The associated bilinear form of Q is nondegenerate).

Define a map $\phi\colon K \to K/Z$ where we identify K/Z with $PG(3,q)$. Then $\phi(L_{\boldsymbol{a}}) = L$ where L a totally singular line and $\phi(R_{\boldsymbol{a}}) = R$ with R a totally singular line. The totally singular lines from $L_{\boldsymbol{a}}$ form a regulus of $PG(3,q)$ with opposite regulus from the totally singular lines of $R_{\boldsymbol{a}}$.

Now $O^+(4,q)$ space has as its singular vectors the pure tensors in $GF(q)^4 = GF(q)^2 \otimes GF(q)^2$. So K/Z and $O^+(4,q)$ are isomorphic as spaces for q even. Let A, $B \in GL(2,q)$. We have

$$A\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c & d \end{pmatrix} B = A \otimes B \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}.$$

Hence $A\otimes B$ acts on $GF(q)^4$ preserving the form Q. So $GL(2,q) \times GL(2,q) \le O^+(4,q)$.

In [**98**] Payne shows that by the Fundamental Theorem each collineation θ of GQ($\boldsymbol{C}$) of a q–clan $\boldsymbol{C}$ that fixes the two points $(\mathbf{0},0,\mathbf{0})$ and (∞) is induced by an automorphism of the elation group of K and such a collineation is represented by $\theta(\sigma, H, S)$ where $\sigma \in \operatorname{Aut} GF(q)$ and H and S are 4×4 matrices over $GF(q)$ with H being invertible. We will not go into the specifics of how θ acts on the 4-gonal family etc., instead we will say that in most circumstances we can define the map θ as $\theta(A\otimes B)$ where $H = A\otimes B$ with A, $B \in GL(2,q)$ and S is determined by A and B but in a slightly more complicated fashion. The matrix A acts on the totally singular lines L of $O^+(4,q)$ and the B matrices act on the totally singular lines R, and so on the regulus $\mathcal{R}$ and the opposite regulus of $\mathcal{R}$ respectively.

Below is a result extensively used by Penttila and Royle.

Theorem 187 (T. Penttila, private communication). *If $\mathcal{O}_1$ and $\mathcal{O}_2$ are equivalent ovals on $\{(0,1,0),(1,0,0),(1,1,1)\}$ with nucleus $(0,0,1)$ and $\mathcal{O}_1$ is in a herd then $\mathcal{O}_2$ is in a herd.*

The above Theorem was used extensively by Penttila and Royle in [**109**]. The classification of flocks for small q via the trace equation $\mathcal{T}_a(f,g)$ (page 100) requires the choice of two o-polynomials f and g. The choice is narrowed down by the Theorem since we can pick our favourite o-polynomial for each inequivalent hyperoval. This allows a complete search for flocks for q small where all hyperovals have been classified.

15.1. Cyclic q–clans

After Payne invented the tensor q–clan approach Payne, Penttila and Royle noted that the map $\theta(M \otimes M^{-5})$ was a collineation of the Subiaco GQ of order $q+1$. With this and other results it was decided that the collineations of GQ($\boldsymbol{C}$) of the form $\theta(M \otimes M^{-p})$ where $M \in GL(2,q)$ and p is some rational number should be investigated.

The assumption is: There is a normalised q–clan $\boldsymbol{C} = \{A_t \mid t \in GF(q)\}$ with $A_\eta = \begin{pmatrix} x_\eta & \eta^{1/2} \\ 0 & z_\eta \end{pmatrix}$ given and an integer p modulo $q+1$ for which $\theta(M \otimes M^{-p})$ is an automorphism of K leaving $\mathscr{F}$ invariant.

Basic goal is: Starting with $A_0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, A_η and θ as above we would like to construct the entire q–clan $\boldsymbol{C}$.

This can be done [**101**] by running a computer search where by

(i) fix η,
(ii) loop over values of p,
(iii) loop over values of x_η,
(iv) loop over values of z_η.

By using the map θ the rest of the q–clan can be constructed given the right values of η, p etc. Royle found there is a large number of (x_η, z_η) pairs. Payne constructed an involution that chooses a 'canonical' representative pair.

The results are summarised below:

(i) For $q = 64$ we have $p = 5$ which always give the Subiaco q–clan. Also we have $p = 21$ giving a q–clan related to the hyperoval $\mathcal{H}_{12}$ of Penttila and Royle (see page 67).
(ii) For $q = 256$ we have $p = 5$ the Subiaco q–clan, and we have $p = 85$ giving a new q–clan related to the sporadic hyperoval in $PG(2,256)$ (see Section 9.1, Chapter II).
(iii) For $q = 1024$ we have the Subiaco q–clan and a new q–clan for $p = 341$.

The new q–clans seem to be related as the p values are equal to $p = -2/3$ modulo $q+1$ for $q = 64$, 256, 1024 and new q–clans for $q = 4096$ and $q = 16384$.

16. Subquadrangles in GQs of order (s, s^2)

Recall the definitions of subquadrangle in Section 6, p. 91, and the construction of subGQs from EGQs in Section 11, p. 104. An example of a subquadrangle is given on page 93. As another example consider the GQ $T_3(\Omega)$ where Ω is an ovoid of $PG(3,q)$. Let π be a plane of $PG(3,q)$ such that $\pi \cap \Omega = \mathcal{O}$ an oval of $PG(2,q)$. Let Σ be a hyperplane of $PG(4,q)$ that intersects $PG(3,q)$ in π. Then we can construct $T_2(\mathcal{O})$ in Σ as a subGQ of $T_3(\Omega)$.

The work below will use the results of rosettes of ovoids of a subGQ, induced by a GQ.

THEOREM 188 ([**130**] 7.1). *Let $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ be a GQ of order (q, q^2), q even, having a subquadrangle $\mathcal{S}'$ isomorphic to $Q(4, q)$. If in $\mathcal{S}'$ each ovoid $\mathcal{O}_x$ consisting of all points collinear with a given point x of $\mathcal{S} \setminus \mathcal{S}'$ is an elliptic quadric, then $\mathcal{S}$ is isomorphic to $Q(5, q)$.*

Note we are using the fact that $Q(4, q) \cong W(q)$ for q even and each ovoid of $W(q)$ is an ovoid of $PG(3, q)$ (Theorems 151, 152 and 153).

By the work of O'Keefe and Penttila [**79**] (see Section 11.3, p. 71, Chapter II) we have:

COROLLARY 189. *If a GQ $\mathcal{S}$ of order $(16, 256)$ has a subquadrangle isomorphic to $Q(4, 16)$, then $\mathcal{S} \cong Q(5, 16)$.*

In [**18**] M. Brown extended this work.

THEOREM 190 ([**18**], 5.5). *If a GQ $\mathcal{S}$ of order (q, q^2), q even, has a subquadrangle isomorphic to $W(q)$ and each subtended ovoid is either an elliptic quadric or a Tits ovoid then $\mathcal{S}$ is isomorphic to the classical GQ $Q(5, q)$.*

COROLLARY 191 ([**18**], 5.6). *Suppose q is even and that the only ovoids of $W(q)$ are Tits ovoids and the elliptic quadric ovoids. Then if $\mathcal{S}$ is a GQ of order (q, q^2) containing a subquadrangle isomorphic to $W(q)$, then $\mathcal{S}$ is isomorphic to the classical GQ $Q(5, q)$.*

The below theorem shows (another!) possible way of trying to classify ovoids of $PG(3, q)$.

COROLLARY 192 ([**18**], 5.7). *If there exists a GQ $\mathcal{S}$ of order (q, q^2) such that $\mathcal{S}$ is not isomorphic to $Q(5, q)$ and $\mathcal{S}$ contains a subquadrangle isomorphic to $W(q)$, then there is a new ovoid of $PG(3, q)$.*

Using the results from Section 11.3, p. 71, Chapter II, we have:

COROLLARY 193 ([**18**], 5.8). *For $q \leq 32$, q even, if $\mathcal{S}$ is a GQ of order (q, q^2) containing a subquadrangle isomorphic to $W(q)$ then $\mathcal{S}$ is isomorphic to the classical GQ $Q(5, q)$.*

After a small result we shall look at the next possible cases for subGQs.

16.1. Flocks and subquadrangles

See Chapter IV for the definition of flocks. (Apology: This theorem seems more appropriate here than in the next chapter.)

THEOREM 194. *There is no flock which gives rise to a generalised quadrangle with a subquadrangle on (∞) isomorphic to a $T_2(\mathcal{O})$ with $\mathcal{O}$ a pointed conic for $q > 8$.*

Proof. Without loss of generality we let $f(x) = x^2$ and

$$\mathcal{O} = \{(1, t, f(t)) \mid t \in GF(q)\} \cup \{(0,1,0)\}.$$

For $T_2(\mathcal{O})$ to be a subquadrangle of a GQ($\boldsymbol{C}$) constructed from a q–clan, $\boldsymbol{C}$, we require $\mathcal{O}$ to be in a herd. That is,

$$\operatorname{trace}\left(\frac{(f(t)+f(u))(g(t)+g(u))}{(t+u)}\right) = \operatorname{trace}\left((t+u)(g(t)+g(u))\right) = 1 \text{ for all } t \neq u,$$

for some g. Now by Lemma 118, p. 72 and in its notation, this implies that we have $a = t$, $b = u$, $d = g$, and $\alpha = 1/2$.

By the proof of Theorem 119, p. 72, it is shown that there is no such g unless $\alpha = 2$ or $\alpha^2 = 2$, that is, unless $q = 2$, 4, or 8. □

For $q = 2$, 4, 8 such flocks exist.

17. Generalised quadrangles of order $(8, 64)$ with a subquadrangle of order 8

We show that only certain GQs of order (q, q^2) contain a given subquadrangle of order q via the ideas of rosettes introduced in Section 6, p. 91. Let $\mathscr{S}$ be the GQ(q, q^2) and $\mathscr{S}'$ be the GQ(q) that is a subGQ of $\mathscr{S}$. By Theorem 156, p. 92, we know that every point in the $\mathscr{S} \setminus \mathscr{S}'$ **subtends** an ovoid in $\mathscr{S}'$, and that every external line (they are all tangent lines for a GQ(q) in a GQ(q, q^2)) **subtends** a rosette of $\mathscr{S}'$. Hence every ovoid in $\mathscr{S}'$ gives rise to at least one point in $\mathscr{S} \setminus \mathscr{S}'$ (but at most two by Theorem 134, p. 83) and every rosette in $\mathscr{S}'$ gives rise to a line in $\mathscr{S}$. These results allow a construction of a GQ(q, q^2) from a GQ(q).

What we now plan to do is do the above backwards. Given a $\mathscr{S}$ = GQ(q) determine the ovoids in the GQ, and any ovoid will correspond to a point in $\mathscr{S} \setminus \mathscr{S}'$ and each rosette of the GQ(q) will correspond to a (tangent) line of $\mathscr{S}$. If fruitful this will give new GQs of order (q, q^2) with a subGQ of order q; if not it will give us back $\mathscr{S}$.

To use the above results to construct a GQ(q, q^2) one must know all the ovoids of the GQ(q). For large q this is computationally and theoretically difficult. For small q (for instance, $q = 8$) it is possible. Later on, all the ovoids of $T_2(\mathcal{O})$ will be constructed for $q = 8$. Another approach that can be used is to assume that only certain ovoids exist in the GQ(q) and construct rosettes from only these ovoids.

We continue the above line of thought: Which generalised quadrangles of order (q, q^2) contain a particular subGQ of order q? And can we characterise GQ(q, q^2) by their subGQs?

The first GQ of order q that is not classical is $T_2(\mathcal{O})$ where $\mathcal{O}$ is a pointed conic (see chapter 12 in Payne and Thas), this GQ is self-dual, for $q = 8$.

From now on we denote the pointed conic of $PG(2,8)$ by $\mathcal{O}$.

For $q = 8$ there are two known quadrangles of order $(8,64)$ containing $T_2(\mathcal{O})$ as a subquadrangle. They are

(i) the dual of GQ$(\boldsymbol{C}_2)$, denoted FTWKB$^\wedge$, where $\boldsymbol{C}_2$ is the the Fisher-Thas-Walker-Kantor-Betten q–clan defined on page 147 and

(ii) the GQ $T_3(\Omega)$ where Ω is a Tits ovoid.

We first start with the latter approach. The former approach is explained at the end of this section, using the computations by G. F. Royle. Together these results will appear in [**19**]. We would like to warn the reader that some of the results in this section are still preliminary.

17.1. Preliminaries

We define G, $\mathscr{F}$ and $\mathscr{S} = \mathscr{S}(G,\mathscr{F}) = \mathrm{GQ}(\boldsymbol{C})$ as in Section 10, p. 102.

We first look at the case when the ovoids of $T_2(\mathcal{O})$ are subtended from the GQ$(8,64)$ of the dual Fisher-Thas-Walker-Kantor-Betten GQ (page 147) GQ. We take advantage of the fact that $T_2(\mathcal{O})$ is self-dual by working in the FTWKB GQ of order $(64,8)$. Then every external line induces a spread of $T_2(\mathcal{O})$, this spread dualises to an ovoid of $T_2(\mathcal{O})$.

We will need to do some extensive calculations in a GQ constructed from a q–clan. Recall the calculations in Section 8.1, p. 98. Note the calculations in this section are for any subGQ $\mathscr{S}(\boldsymbol{a})$ in a GQ(q^2,q) $\mathscr{S}$.

It is easy to see that:

$$A(s)(\boldsymbol{c},c,\boldsymbol{d}) = A(s)(\boldsymbol{0},c+g_s(\boldsymbol{c}),s^{1/2}\boldsymbol{c}+\boldsymbol{d}), \text{ and}$$
$$A(\infty)(\boldsymbol{c},c,\boldsymbol{d}) = A(\infty)(\boldsymbol{c},c+\boldsymbol{d}\circ\boldsymbol{c},\boldsymbol{0}).$$

The line $A(s)(\boldsymbol{c},c,\boldsymbol{d})$ is secant to $\mathscr{S}(\boldsymbol{a})$ if and only if $\boldsymbol{d}+s^{1/2}\boldsymbol{c} \in \langle \boldsymbol{a}\rangle$. But which s?

If $\boldsymbol{c}$ and $\boldsymbol{a}$ are $GF(q)$-independent then there exists a unique solution for s in the equation

$$\boldsymbol{d}+s^{1/2}\boldsymbol{c} \in \langle \boldsymbol{a}\rangle.$$

So there is a unique line $A(s)(\boldsymbol{c},c,\boldsymbol{d})$ through $(\boldsymbol{c},c,\boldsymbol{d})$ secant to $\mathscr{S}(\boldsymbol{a})$ which intersects $\mathscr{S}(\boldsymbol{a})$ in the line

$$A_{\boldsymbol{a}}(s)(\boldsymbol{0},c+g_s(\boldsymbol{c}),s^{1/2}\boldsymbol{c}+\boldsymbol{d}).$$

If $\boldsymbol{c} = a\boldsymbol{a}$ for some $a \in GF(q)$ we have that the line $A(\infty)(\boldsymbol{c},c,\boldsymbol{d})$ being secant to $\mathscr{S}(\boldsymbol{a})$ and intersects $\mathscr{S}(\boldsymbol{a})$ in the line

$$A_{\boldsymbol{a}}(\infty)(\boldsymbol{c},c+\boldsymbol{d}\circ\boldsymbol{c},\boldsymbol{0}).$$

Every external line to $\mathscr{S}(\boldsymbol{a})$ gives rise to a spread in $\mathscr{S}(\boldsymbol{a})$. The only lines external to $\mathscr{S}(\boldsymbol{a})$ are of type $A(t)g$ and $A(\infty)g$. Every point on these lines has a unique secant line to $\mathscr{S}(\boldsymbol{a})$.

17.1.1. *Lines of the form $A(t)g$*

Let $g = (\boldsymbol{g}_1, g_2, \boldsymbol{g}_3)$ with $\boldsymbol{g}_1,\ \boldsymbol{g}_3 \in GF(q)^2$ and $g_2 \in GF(q)$. Then

$$\begin{aligned} A(t)g &= \{(\boldsymbol{b}, g_t(\boldsymbol{b}), t^{1/2}\boldsymbol{b})(\boldsymbol{g}_1, g_2, \boldsymbol{g}_3) \mid \boldsymbol{b} \in GF(q)^2\} \\ &= \{(\boldsymbol{b}+\boldsymbol{g}_1, g_t(\boldsymbol{b}) + g_2 + (t^{1/2}\boldsymbol{b}) \circ \boldsymbol{g}_1, t^{1/2}\boldsymbol{b}+\boldsymbol{g}_3) \mid \boldsymbol{b} \in GF(q)^2\}. \end{aligned}$$

The line $A(t)g$ is external to $\mathscr{S}(\boldsymbol{a})$ if and only if for all $\boldsymbol{b} \in GF(q)^2$ we have $\boldsymbol{b}+\boldsymbol{g}_1 \notin \langle \boldsymbol{a} \rangle$ or $t^{1/2}\boldsymbol{b}+\boldsymbol{g}_3 \notin \langle \boldsymbol{a} \rangle$. (This implies that $\boldsymbol{g}_1$ and $\boldsymbol{g}_3$ are $GF(q)$-independent of $\boldsymbol{a}$.)

Let $g' = (\boldsymbol{b}+\boldsymbol{g}_1, g_t(\boldsymbol{b}) + g_2 + (t^{1/2}\boldsymbol{b}) \circ \boldsymbol{g}_1, t^{1/2}\boldsymbol{b}+\boldsymbol{g}_3)$ for some $\boldsymbol{b} \in GF(q)^2$.

From above we have that if $\{\boldsymbol{b}+\boldsymbol{g}_1, \boldsymbol{a}\}$ are $GF(q)$-independent then the unique line secant to $\mathscr{S}(\boldsymbol{a})$ on g' is

$$A_{\boldsymbol{a}}(s)(\boldsymbol{0}, g_t(\boldsymbol{b}) + g_2 + (t^{1/2}\boldsymbol{b}) \circ \boldsymbol{g}_1 + g_s(\boldsymbol{b}+\boldsymbol{g}_1), t^{1/2}\boldsymbol{b}+\boldsymbol{g}_3 + s^{1/2}(\boldsymbol{b}+\boldsymbol{g}_1)), \tag{6}$$

with s being the unique solution to

$$t^{1/2}\boldsymbol{b}+\boldsymbol{g}_3+s^{1/2}(\boldsymbol{b}+\boldsymbol{g}_1) \in \langle \boldsymbol{a} \rangle.$$

If $\boldsymbol{b}+\boldsymbol{g}_1 = a\boldsymbol{a}$ for some $a \in GF(q)$ then the unique line secant to $\mathscr{S}(\boldsymbol{a})$ on g' in $\mathscr{S}(\boldsymbol{a})$ is

$$A_{\boldsymbol{a}}(\infty)(a\boldsymbol{a}, g_t(\boldsymbol{b}) + g_2 + (t^{1/2}\boldsymbol{b}) \circ \boldsymbol{g}_1 + (t^{1/2}\boldsymbol{b}+\boldsymbol{g}_3) \circ (a\boldsymbol{a}), \boldsymbol{0}). \tag{7}$$

The unique line of $\mathscr{S}(\boldsymbol{a})$ on the point $A^*(t)g$ on the line $A(t)g$ is

$$[A_{\boldsymbol{a}}(t)]. \tag{8}$$

Given an external line $A(t)g$ where $g = (\boldsymbol{g}_1, g_2, \boldsymbol{g}_3)$ we have a spread in $\mathscr{S}(\boldsymbol{a})$ being constructed from the q^2-q lines of Equation (6), q lines from (7) and the line (8).

17.1.2. *Lines of the form $A(\infty)g$*

Let $g = (\boldsymbol{g}_1, g_2, \boldsymbol{g}_3)$ with $\boldsymbol{g}_1,\ \boldsymbol{g}_3 \in GF(q)^2$ and $g_2 \in GF(q)$. Then

$$\begin{aligned} A(\infty)g &= \{(\boldsymbol{0}, 0, \boldsymbol{b})(\boldsymbol{g}_1, g_2, \boldsymbol{g}_3) \mid \boldsymbol{b} \in GF(q)^2\} \\ &= \{(\boldsymbol{g}_1, g_2 + \boldsymbol{b} \circ \boldsymbol{g}_1, \boldsymbol{b}+\boldsymbol{g}_3) \mid \boldsymbol{b} \in GF(q)^2\}. \end{aligned}$$

This line is external to $\mathscr{S}(\boldsymbol{a})$ if and only if for all $\boldsymbol{b} \in GF(q)^2$ we have $\boldsymbol{g}_1 \notin \langle \boldsymbol{a} \rangle$ or $\boldsymbol{b}+\boldsymbol{g}_3 \notin \langle \boldsymbol{a} \rangle$.

Let $g' = (\boldsymbol{g}_1, g_2 + \boldsymbol{b} \circ \boldsymbol{g}_1, \boldsymbol{b}+\boldsymbol{g}_3)$ with $\boldsymbol{b} \in GF(q)^2$.

From above we have that the unique secant line to $\mathscr{S}(\boldsymbol{a})$ on g' being

$$A_{\boldsymbol{a}}(s)(\boldsymbol{0}, g_s(\boldsymbol{g}_1) + g_2 + \boldsymbol{b} \circ \boldsymbol{g}_1, s^{1/2}\boldsymbol{g}_1 + \boldsymbol{b} + \boldsymbol{g}_3),$$

with s being the unique solution to

$$s^{1/2}\boldsymbol{g}_1 + \boldsymbol{b} + \boldsymbol{g}_3 \in \langle \boldsymbol{a} \rangle.$$

The above q^2 lines and the line $[A_{\boldsymbol{a}}(\infty)]$ constructs the spread in $\mathscr{S}(\boldsymbol{a})$ from the external line $A(\infty)g$.

17.2. Fisher-Thas-Walker-Kantor-Betten q–clan

Let $q = 8$.

Let the A_t be the q–clan associated with the Fisher-Thas-Walker-Kantor-Betten (FTWKB) q–clan $\boldsymbol{C}_2$ (see page 147), that is, for $q = 8$ we have

$$A_t = \begin{pmatrix} t^2 & t^4 \\ 0 & t^6 \end{pmatrix}.$$

Now A_t is a normalised q–clan since $t^4 = t^{1/2}$ when $q = 8$ and $A_0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

We now investigate spreads in the subGQ, $\mathscr{S}(\boldsymbol{a})$, of the GQ $\mathscr{S}$ constructed from the FTWKB q–clan. Again any external line of $\mathscr{S}(\boldsymbol{a})$ in $\mathscr{S}$ creates a spread in $\mathscr{S}(\boldsymbol{a})$. We need only look at the lines of type $A(t)g$ and $A(\infty)g$ with appropriate g as constructed in Section 17.1.

Since there is only one orbit on herds of A_t we are transitive on the set of $G(\boldsymbol{a})$, $\boldsymbol{0} \neq \boldsymbol{a} \in GF(q)^2$, so we choose

$$\boldsymbol{a} = (1, 0).$$

Now $A_{\boldsymbol{a}}(t) = \{(a\boldsymbol{a}, g_t(a\boldsymbol{a}), t^4 a\boldsymbol{a}) \mid a \in GF(q)\}$, with

$$g_t(a\boldsymbol{a}) = \left(\begin{pmatrix} a & 0 \end{pmatrix} \begin{pmatrix} t^2 & t^4 \\ 0 & t^6 \end{pmatrix} \begin{pmatrix} a \\ 0 \end{pmatrix} \right)^4 = at \quad \text{for } q = 8.$$

As in Section 11, p. 104, in the basis $(\boldsymbol{a}, 0, 0)$, $(0, 1, 0)$ and $(0, 0, \boldsymbol{a})$ we have $A_{\boldsymbol{a}}(t)$ describing the oval

$$\mathscr{O}_{\boldsymbol{a}} = \{(1, t, t^4) \mid t \in GF(q)\} \cup \{(0, 0, 1)\},$$

equivalent to the Tit's oval for $q = 8$. Hence the spreads of $\mathscr{S}(\boldsymbol{a})$ are in fact spreads of $T_2(\mathscr{O}_{\boldsymbol{a}})$.

17.2.1. *Lines of type $A(t)g$*

Let $g = (\boldsymbol{g}_1, g_2, \boldsymbol{g}_3)$ where $\boldsymbol{g}_1 = (g_{1x}, g_{1y})$, $\boldsymbol{g}_3 = (g_{3x}, g_{3y}) \in GF(q)^2$ and $g_2 \in GF(q)$. Let $\boldsymbol{b} = (b_x, b_y)$. The $q^2 - q$ $\boldsymbol{b}$'s with $b_y \neq g_{1y}$ give $q^2 - q$ lines of the spread in $\mathscr{S}(\boldsymbol{a})$

being

$$A_{\boldsymbol{a}}(s)(\mathbf{0}, tb_x + t^2b_y^4b_x^4 + b_yt^3 + g_2 + t^2b_x^4g_{1y}^4 + t^2b_y^4g_{1x}^4 + s(b_x + g_{1x}) + s^2(b_x^4 + g_{1x}^4)(b_y^4 + g_{1y}^4) + (b_y + g_{1y})s^3, (t^4b_x + g_{3x} + s^4(b_x + g_{1x}))\boldsymbol{a}),$$

with

$$s = \frac{tb_y^2 + g_{3y}^2}{b_y^2 + g_{1y}^2}.$$

When $b_y = g_{1y}$ then $\boldsymbol{b}+\boldsymbol{g}_1 = a\boldsymbol{a}$ for some $a \in GF(q)$ we have q lines of the spread of $\mathscr{S}(\boldsymbol{a})$ being

$$A_{\boldsymbol{a}}(\infty)((b_x + g_{1x})\boldsymbol{a}, tb_x + t^2b_y^4b_x^4 + b_yt^3 + g_2 + b_y^4g_{3x}^4 + g_{3x}^4g_{1y}^4 + g_{3y}^4b_x^4 + g_{3y}^4g_{1x}^4, \mathbf{0}).$$

The final line of the spread in $\mathscr{S}(\boldsymbol{a})$ containing (∞) is

$$[A_{\boldsymbol{a}}(t)].$$

Example 1. Look at the external line $A(0)(\mathbf{0}, 0, (0,1))$, note $\boldsymbol{a}$ is still $(1,0)$. For any $\boldsymbol{b} = (b_x, b_y) \in GF(q)^2$ such that $b_y \neq 0$ we have $q^2 - q$ lines of the spread being

$$A_{\boldsymbol{a}}(b_y^5)(\mathbf{0}, b_y^5b_x + b_x^4 + b_y^2, b_y^6b_x\boldsymbol{a}),$$

where $s = b_y^{-2} = b_y^5$. The q lines of the spread in $\mathscr{S}(\boldsymbol{a})$ being, for $b_x \in GF(q)$, when $b_y = 0$,

$$A_{\boldsymbol{a}}(\infty)(b_x\boldsymbol{a}, b_x^4, \mathbf{0}).$$

And the line of $\mathscr{S}(\boldsymbol{a})$ containing (∞) is

$$[A_{\boldsymbol{a}}(0)].$$

17.2.2. *Lines of type $A(\infty)g$*

Let $g = (\boldsymbol{g}_1, g_2, \boldsymbol{g}_3)$, $\boldsymbol{g}_1 = (g_{1x}, g_{1y})$, $\boldsymbol{g}_3 = (g_{3x}, g_{3y}) \in GF(q)^2$, and $g_2 \in GF(q)$. Let $\boldsymbol{b} = (b_x, b_y)$. Then for all $\boldsymbol{b}$ we have an element of the spread in $\mathscr{S}(\boldsymbol{a})$ being

$$A_{\boldsymbol{a}}(s)(\mathbf{0}, sg_{1x} + s^2g_{1y}^4g_{1x}^4 + g_{1y}s^3 + g_2 + b_x^4g_{1y}^4 + b_y^4g_{1x}^4, (s^4g_{1x} + b_x + g_{3x})\boldsymbol{a}),$$

with

$$s = \frac{b_y^2 + g_{3y}^2}{g_{1y}^2}.$$

The line of the spread containing (∞) in $\mathscr{S}(\boldsymbol{a})$ is

$$[A_{\boldsymbol{a}}(\infty)].$$

Example 2. Look at the external line $A(\infty)((0,1), 0, \mathbf{0})$. For any $\boldsymbol{b} = (b_x, b_y) \in GF(q)^2$ we have q^2 lines of the spread of $\mathscr{S}(\boldsymbol{a})$ being

$$A_{\boldsymbol{a}}(b_y^2)(\mathbf{0}, b_y^6 + b_x^4, b_x\boldsymbol{a}),$$

where $s = b_y^2$ and the line of the spread containing (∞) is

$$[A_{\boldsymbol{a}}(\infty)].$$

17.3. Constructing ovoids from spreads

The reference for this section is Chapter 12 of Payne and Thas and we recall that $\boldsymbol{a} = (1, 0)$.

Let $\mathcal{O}_{\boldsymbol{a}}$ be the oval described by $A_{\boldsymbol{a}}(s)$ (in Section 17.2, p. 127) be in $PG(2, 8)$. Embed $PG(2, 8)$ as the plane $x_0 = 0$ in $PG(3, 8)$ and consider this as the GQ $T_2(\mathcal{O}_{\boldsymbol{a}})$. Then we have a geometric structure to the above spread constructions.

The line $[A_{\boldsymbol{a}}(\infty)]$ of the GQ, $\mathscr{S}(\boldsymbol{a})$, is associated with the point $(0, 0, 0, 1)$ of $PG(3, 8)$. The lines $[A_{\boldsymbol{a}}(s)]$, $s \in GF(q)$, are associated with the points $(0, 1, s, s^4)$. The lines $A_{\boldsymbol{a}}(\infty)(b\boldsymbol{a}, c, \mathbf{0})$ of $\mathscr{S}(\boldsymbol{a})$ are associated with the lines of $PG(3, 8)$ tangent to the point $(0, 0, 0, 1)$ on the oval $\mathcal{O}_{\boldsymbol{a}}$ and containing the affine point $(1, b, c, 0)$. The lines of type $A_{\boldsymbol{a}}(s)(\mathbf{0}, c, b\boldsymbol{a})$ of $\mathscr{S}(\boldsymbol{a})$ are associated with the lines of $PG(3, 8)$ tangent to the point $(0, 1, s, s^4)$ on the oval $\mathcal{O}_{\boldsymbol{a}}$ and containing the affine point $(1, 0, c, b)$.

In the notation of Chapter 12 of Payne and Thas we have:

$$\begin{aligned} [A_{\boldsymbol{a}}(\infty)] &\leftrightarrow [\infty], \\ [A_{\boldsymbol{a}}(s)] &\leftrightarrow [s], \\ A_{\boldsymbol{a}}(\infty)(b\boldsymbol{a}, c, \mathbf{0}) &\leftrightarrow [b, c], \qquad \text{and} \\ A_{\boldsymbol{a}}(s)(\mathbf{0}, c, b\boldsymbol{a}) &\leftrightarrow [s, b, c]. \end{aligned}$$

Also in Payne and Thas, p. 276, there is a duality defined on the lines of $\mathscr{S}(\boldsymbol{a})$ as

$$\begin{aligned} [\infty] &\mapsto (\infty), \\ [s] &\mapsto (s^4), \\ [b, c] &\mapsto (b, c^4), \qquad \text{and} \\ [s, b, c] &\mapsto (s^4, b, c^4). \end{aligned}$$

This takes a spread of $\mathscr{S}(\boldsymbol{a}) = T_2(\mathcal{O}_{\boldsymbol{a}})$ to an ovoid of $\mathscr{S}(\boldsymbol{a})^\wedge = T_2(\mathcal{O}_{\boldsymbol{a}})^\wedge = T_2(\mathcal{O})$, where $\mathcal{O}$ is the pointed conic $\mathcal{O} = \{(1, t, t^{1/2}) \mid t \in GF(q)\} \cup \{(0, 0, 1)\}$.

The points (s^4) of the GQ, $\mathscr{S}(\boldsymbol{a})^\wedge$, are associated with the planes of $PG(3, 8)$ tangent to the point $(0, 0, 0, 1)$ on $\mathcal{O}_{\boldsymbol{a}}$ and containing the affine point $(1, s^4, 0, 0)$. The points (b, c^4) are associated with the planes of $PG(3, 8)$ tangent to the point $(0, 1, b, b^4)$ on $\mathcal{O}_{\boldsymbol{a}}$ and containing the affine point $(1, 0, 0, c^4)$. The points (s^4, b, c^4) in $\mathscr{S}(\boldsymbol{a})^\wedge$ are associated with the affine points $(1, s^4, b, c^4)$ of $PG(3, 8)$.

17.3.1. *Ovoids from lines of type $A(t)g$*

In the same notation as in Section 17.2.1 we have an external line $A(t)g$ to $\mathscr{S}(\boldsymbol{a})$ with $g = (\boldsymbol{g}_1, g_2, \boldsymbol{g}_3)$, where $\boldsymbol{g}_1 = (g_{1x}, g_{1y})$, $\boldsymbol{g}_3 = (g_{3x}, g_{3y})$ and $g_2 \in GF(q)$ if and only if for all $\boldsymbol{b} = (b_x, b_y) \in GF(q)$ we have $\boldsymbol{b} + \boldsymbol{g}_1 \notin \langle \boldsymbol{a} \rangle$ or $t^{1/2}\boldsymbol{b} + \boldsymbol{g}_3 \notin \langle \boldsymbol{a} \rangle$.

The points of the ovoid in $T_2(\mathcal{O})$ are:

(i) When $b_y \neq g_{1y}$ we have $q^2 - q$ affine points of $PG(3,8)$:

$$\begin{aligned}(1,\ &\frac{t^4 b_y + g_{3y}}{b_y + g_{1y}},\ t^4 b_x + g_{3x} + s^4(b_x + g_{1x}),\ t^4 b_x^4 + t b_y^2 b_x^2 + b_y^4 t^5 + g_2^4 + t b_x^2 g_{1y}^2 \\ &+ t b_y^2 g_{1x}^2 + s^4(b_x^4 + g_{1x}^4) + s(b_y^2 + g_{1y}^2)(b_x^2 + g_{1x}^2) + (b_y^4 + g_{1y}^4)s^5),\end{aligned}$$

where $s = (t b_y^2 + g_{3y}^2)/(b_y^2 + g_{1y}^2)$.

(ii) When $\boldsymbol{b} + \boldsymbol{g}_1 \in \langle \boldsymbol{a} \rangle$ we have q planes in $PG(3,8)$ tangent to $\mathcal{O}$ at the point

$$(0, 1, b_x + g_{1x}, b_x^4 + g_{1x}^4)$$

and containing the affine point

$$(1, 0, 0, t^4 b_x^4 + t b_y^2 b_x^2 + b_y^4 t^5 + g_2^4 + b_y^2 g_{3x}^2 + g_{3x}^2 g_{1y}^2 + g_{3y}^2 b_x^2 + g_{3y}^2 g_{1x}^2).$$

In plane co-ordinates of $PG(3,8)$ they are the planes

$$[t^4 b_x^4 + t b_y^2 b_x^2 + b_y^4 t^5 + g_2^4 + b_y^2 g_{3x}^2 + g_{3x}^2 g_{1y}^2 + g_{3y}^2 b_x^2 + g_{3y}^2 g_{1x}^2, b_x^4 + g_{1x}^4, 0, 1].$$

(iii) The plane in $PG(3,8)$ tangent to $\mathcal{O}$ at the point

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

and containing the affine point

$$(1, t^4, 0, 0):$$

In plane co-ordinates of $PG(3,8)$ it is the plane

$$[t^4, 1, 0, 0].$$

Example (Continuation of Example 1, p. 128). The external line $A(0)(\mathbf{0}, 0, (0,1))$ describes an ovoid in $T_2(\mathcal{O})$ as:

(1) The $q^2 - q$ affine points, with $b_y \neq 0$,

$$(1, b_y^6, b_y^6 b_x, b_y^6 b_x^4 + b_y + b_x^2).$$

(2) The q planes for $b_x \in GF(q)$ tangent to $\mathcal{O}$ at the point $(0, 1, b_x, b_x^4)$ and containing the affine point $(1, 0, 0, b_x^2)$.

(3) The plane tangent to $\mathcal{O}$ at the point $(0, 0, 0, 1)$ and containing the affine point $(1, 0, 0, 0)$.

17.3.2. *Ovoids from lines of type $A(\infty)g$*

In the same notation as in Section 17.2.2 we have an external line $A(\infty)g$ to $\mathscr{S}(\boldsymbol{a})$ with $g = (\boldsymbol{g}_1, g_2, \boldsymbol{g}_3)$, where $\boldsymbol{g}_1 = (g_{1x}, g_{1y})$, $\boldsymbol{g}_3 = (g_{3x}, g_{3y})$ and $g_2 \in GF(q)$ if and only if for all $\boldsymbol{b} = (b_x, b_y) \in GF(q)$ we have $\boldsymbol{g}_1 \notin \langle \boldsymbol{a} \rangle$ or $\boldsymbol{b} + \boldsymbol{g}_3 \notin \langle \boldsymbol{a} \rangle$.

The points of the ovoid in $T_2(\mathcal{O})$ are:

(i) The q^2 affine points, $\boldsymbol{b} \in GF(q)^2$,

$$(1, \frac{b_y + g_{3y}}{g_{1y}}, s^4 g_{1x} + b_x + g_{3x}, s^4 g_{1x}^4 + s g_{1y}^2 g_{1x}^2 + g_{1y}^4 s^5 + g_2^4 + b_x^2 g_{1y}^2 + b_y^2 g_{1x}^2),$$

where $s = (b_y^2 + g_{3y}^2)/g_{1y}^2$.

(ii) The point (∞).

Example (Continuation of Example 2, p. 128). The external line $A(\infty)((0,1), 0, \mathbf{0})$ describes an ovoid in $T_2(\mathcal{O})$ as:

(1) The q^2 affine points, $(b_x, b_y) \in GF(q)^2$

$$(1, b_y, b_x, b_y^3 + b_x^2).$$

(2) The point (∞).

17.4. Ovoids from the polarity

A polarity acts on the lines as such

$$\begin{aligned}
[\infty] &\mapsto (\infty), \\
[s] &\mapsto (s^2), \\
[b, c] &\mapsto (b^4, c^2), \\
[s, b, c] &\mapsto (s^2, b^4, c^2).
\end{aligned}$$

of $\mathscr{S}(\boldsymbol{a})^\wedge$ (see p. 276 of Payne and Thas):

An ovoid of $\mathscr{S}(\boldsymbol{a})^\wedge$ can be constructed from the absolute points of this polarity.

We have one absolute point via inspection: (∞).

Points (s^2) are never incident with lines $[s]$. Points (b^4, c^2) are never incident with lines $[b, c]$.

Points $P = (s^2, b^4, c^2)$ are incident with lines $[s, b, c]$ if and only if P is one of the affine points of $PG(3, 8)$,

$$(1, s^2, s^3 + c, c^2), \quad \text{for } s,\, c \in GF(q).$$

Together with the point (∞) these are the $q^2 + 1$ points of the ovoid.

Hence the affine points defined by the polarity are:

$$(1, u, v, u^3 + v^2) \quad u, v \in GF(q). \tag{9}$$

We can show that none of the ovoids in Section 17.3 come from polarities of $T_2(\mathcal{O})$.

17.5. Constructing GQ(q, q^2) from $T_2(\mathcal{O})$: FTWKB case

We now look at the special case of when $T_2(\mathcal{O})$ can be a subGQ for a GQ(q, q^2) when $q = 8$, $\mathcal{O}$ is a pointed conic, and all the ovoids of $T_2(\mathcal{O})$ are subtended from the dual FTWKB GQ. These ovoids where constructed in Section 17.1, p. 125. The GQ(q, q^2) is constructed from the ovoids by the correspondence that every ovoid of $T_2(\mathcal{O})$ is a point of GQ(q, q^2) and every rosette of $T_2(\mathcal{O})$ is a line of GQ(q, q^2). Now every point of $T_2(\mathcal{O})$ is on at least $q^2 - q$ rosettes, since these are the number of external lines of the dual FTWKB GQ to $T_2(\mathcal{O})$. Any point of $T_2(\mathcal{O})$ with more than $q^2 - q$ rosettes is a candidate for constructing lines of a GQ(q, q^2) not isomorphic to the dual FTWKB GQ. Determining new line sets is straightforward. Let x be a point of $T_2(\mathcal{O})$. Let $\mathscr{S}$ be the GQ(q, q^2) we are trying to construct. Put

$$\begin{aligned} Y &= \{\text{points of } \mathscr{S} \setminus T_2(\mathcal{O}) \text{ collinear with } x\} \\ &= \{\text{ovoids on } x\} \end{aligned}$$

(where ovoids on x really means ovoids from FTWKB construction on x). Now each partition of Y into lines corresponds to a set of $q^2 - q$ rosettes on x. If there is only one partitioning of Y into lines then we have only the original GQ(q, q^2) that gave the subtended ovoids.

To determine the partitioning we let Γ be a graph with vertices,

$$V(\Gamma) = \{\text{rosettes based at } x\}$$

and adjacency defined by

$$\mathscr{R}_1 \sim \mathscr{R}_2 \iff \mathscr{R}_1 \text{ and } \mathscr{R}_2 \text{ are rosettes not containing a common ovoid.}$$

(Note the rosettes are only constructed from FTWKB ovoids.)

The number of cliques of size $q^2 - q$ (56 in our case), determine the number of partitions into lines of Y. An easy calculation shows that we only find one clique for points of $T_2(\mathcal{O})$ when the ovoids are subtended from FTWKB GQ. Hence there are no new GQ(q, q^2) containing $T_2(\mathcal{O})$ as a subGQ, when all the ovoids are subtended from the dual FTWKB GQ. Though we should stress that we are assuming that one ovoid only yields one point in $\mathscr{S} \setminus T_2(\mathcal{O})$.

17.6. Subtended ovoids from $T_3(\Omega)$

Recall the definition of $T_3(\Omega)$ in Section 2.5, p. 86. We make a distinction between ovoids subtended by a POINT of type (i) of $T_3(\Omega)$ and POINTS of type (ii). We call the former **projected** ovoids and the latter **planar** ovoids. We call points of $PG(4, q) - PG(3, q)$ **affine points** and hyperplanes of $PG(4, q)$ meeting Ω in one point **affine hyperplanes**.

Also recall (page 122) how for a given secant plane π of $\Omega \subseteq PG(3,q)$ we can construct a $T_2(\mathcal{O})$ with $\mathcal{O} = \Omega \cap \pi$. We are interested when $\mathcal{O}$ is a pointed conic for $q = 8$, that is, a Tits oval. Hence Ω must be a Tits ovoid (see Section 11.3, p. 71, Chapter II). We label the projective three space that $T_2(\mathcal{O})$ lives in as $\Sigma = PG'(3,q)$, noting $\mathcal{O} \subseteq \pi$.

We now describe the two types of ovoids constructed in $T_2(\mathcal{O})$ by external points of $T_3(\Omega)$.

Result 195 (Planar Ovoids). Let x be a affine hyperplane. Then x intersects Ω at a point z and at a tangent plane π'. Let l be the line of intersection of π and π'. Let π'' be the plane of intersection of $PG'(3,q)$ and x (meeting at the line l). Then

$$\text{Planar ovoid} = \{\text{affine points of } \pi''\} \cup \{(\infty)\}.$$

Result 196 (Projected ovoid). Let x be an affine point. The projection, x_t, of the $q^2 - q$ points of $\Omega \setminus \mathcal{O}$ into $PG'(3,q)$ gives a set of $q^2 - q$ points of $T_2(\mathcal{O})$ that are not collinear in the subGQ. Let z be a point of $\mathcal{O}$ and let l be the unique tangent line on z in π. There is a unique tangent plane π' on z, these generate the 3-space $\langle \pi', x\rangle$. We label the plane of intersection of $\langle \pi', x\rangle$ and $PG'(3,q)$ as π_z (as there is a unique plane for every point of the pointed conic z).

$$\text{Projected ovoid} = \{x_t \mid t \in \Omega \setminus \mathcal{O}\} \cup \{\pi_z \mid z \in \mathcal{O}\}.$$

The number of external points to $T_2(\mathcal{O})$ in $T_3(\Omega)$ is:

$$\begin{aligned}(1+q)(1+q^3) - (1+q)(1+q^2) &= 4032 \text{ external points}\\ &= 4032 \text{ planar and projected ovoids.}\end{aligned}$$

These ovoids are divided into 3584 projected ovoids and 448 planar ovoids.

Let $\Omega = \{(s, 1, t, s^6 + st + t^4) \mid t \in GF(q)\} \cup \{(0,0,0,1)\}$ be the Tits ovoid in $PG(3,8)$. Then the Tits ovoid defines a symplectic polarity with (alternating) form on $PG(3,q)$

$$f(\boldsymbol{x}, \boldsymbol{y}) = x_2y_4 + x_4y_2 + x_3y_5 + x_5y_3$$

where points of $PG(4,q)$ are of the form $(x_1, x_2, x_3, x_4, x_5)$. (This is derived from the fact that given the Tits oval as $(s^{\sigma+2} + st + t^\sigma, 1, s, t)$ the polarity has the more usual form $x_1y_2 + x_2y_1 + x_3y_4 + x_4y_3$ in $PG(3,q)$. We then permute the coordinates.)

Now the tangent plane to the point x of $PG(3,q)$ is the perp of x under the polarity with form f. Let $x = (0, s, 1, t, s^6 + st + t^4)$, so

$$\begin{aligned}\text{tangent plane at } x &= \{y \mid f(x,y) = 0\} \cap [1,0,0,0,0]\\ &= \{y \mid sy_4 + ty_2 + y_5 + (s^6 + st + t^4)y_3 = 0\} \cap [1,0,0,0,0]\end{aligned}$$

Hence the hyperplanes on x are $[a, t, s^6 + st + t^4, s, 1]$ with $a \in GF(8)$. Though for the following computations we only need a to be in $GF(8)^*$ so that the hyperplanes are affine.

Let $x = (0, 0, 0, 0, 1)$. Then we have $f(x, y) = y_3 = 0$. Hence the planes on x are $[a, 0, 1, 0, 0]$ with a as above.

17.6.1. *Planar ovoids*

We have

$$\Omega \setminus \mathcal{O} = \{(0, s, 1, t, s^6 + st + t^4) \mid t, s \in GF(8), s \neq 0\}.$$

An affine point is of the form $(1, a, b, c, d)$ with a, b, c, $d \in GF(8)$ $a \neq 0$. An affine hyperplane is of the form $[a, t, s^6 + st + t^4, s, 1]$ with $s \neq 0$ s, t, $a \in GF(8)$ where the q affine hyperplanes meet at the point $(0, s, 1, t, s^6 + st + t^4)$.

It should be noted that planar ovoids have a curious feature; they are subtended by two external points of $T_3(\Omega)$. Recall that every ovoid of $Q(4, q)$ is subtended by exactly two external points of $Q(5, q)$. The proof is straightforward. We require:

LEMMA 197 ([**56**], Chapter 16). *For q even, every external line to an ovoid in $PG(3, q)$ is on two tangent planes of the ovoid.*

Using the notation of Result 195, p. 133, we have two affine hyperplanes on the line l intersecting $PG'(3, q)$ at π''. So each x gives exactly two planar ovoids in $T_2(\mathcal{O})$.

It is easy to see that only one external point of $T_3(\Omega)$ subtends a projected ovoid.

17.7. Constructing GQ(q, q^2) from $T_2(\mathcal{O})$: FTWKB and $T_2(\Omega)$ cases

This work is still in progress. There is the complication of ovoids being subtended by two points.

17.8. Ovoids of $T_2(\mathcal{O})$, $\mathcal{O}$ pointed conic, $q = 8$

We summarise the results of G. F. Royle on his exhaustive search of ovoids of $T_2(\mathcal{O})$. (As before $\mathcal{O}$ is a pointed conic and $q = 8$.) By using Brendan McKay's **nauty** package [**77**] the automorphism group of $T_2(\mathcal{O})$ can be determined and it has order 1204224 (though this can be easily worked out from the stabiliser of the pointed conic in $PG(2, q)$ and the duality).

The orbits of the collineation group have sizes 1, 8, 64 and 512 on points (and the same on lines).

An ovoid of this GQ has size 65. An exhaustive search for ovoids yields the results that there are 5 ovoids, named Type I to Type V.

No.	Name	$\|G\|$	Orbits	(n_0, n_1, n_2)	Plane intersections
I	FTWKB	168	$\{1, 8, 56\}$	$(0, 56, 9)$	$\{0^{10}, 5^{168}, 7^{288}, 8^{63}, 13^{56}\}$
II	Projected	168	$\{1, 8, 56\}$	$(0, 56, 9)$	$\{0^{10}, 1^{56}, 7^{288}, 8^{63}, 9^{168}\}$
III	Polarity	168	$\{1, 8, 56\}$	$(1, 64, 0)$	$\{0^{1}, 4^{112}, 8^{360}, 12^{112}\}$
IV	Planar	2688	$\{1, 64\}$	$(1, 64, 0)$	$\{0^{8}, 8^{576}, 64^{1}\}$
V	FTWKB	1344	$\{1, 64\}$	$(1, 64, 0)$	$\{0^{1}, 4^{112}, 8^{360}, 12^{112}\}$

The column *Name* gives the type of ovoid it is in the case of polarity, or if it is a planar or projected ovoid subtended from $T_3(\Omega)$ or subtended from the dual FTWKP GQs. The next column gives the size of the stabilisers of each ovoid and the column after that gives the orbits of the stabiliser on each type of ovoid. Let n_0 be 1 if an ovoid contains (∞) or 0 if not. Let n_1 be the number of affine points of $PG(3, q)$ (POINTS of type (i)) the ovoid has and n_2 be the number of affine planes (POINTS of type (ii)) the ovoid has. The last column shows how the 585 planes of $PG(3, q)$ intersect the affine points of each ovoid type, where X^Y is read as there are Y planes intersecting the ovoid in X points. From the last column it is obvious that ovoid of type II is a projected ovoid and that the ovoids of type IV are planar. Ovoids of type I, III and V have been conjectured to be FTWKB type, from a polarity and FTWKB type, respectively, though we, as yet, can not prove this.

We can now determine whether the ovoids lie in rosettes or otherwise:

No.	Point(orbit)	Candidates	Rosettes
I	569(1)	28 I, 28 II	15
	516(8)	14 I	2
	13(56)	6 I, 1 III, 1 V	1
II	569(1)	28 I, 28 II	15
	516(8)	7 II	1
	11(56)	6 II, 3 III, 1 IV	1
III	0(1)	35 III	30
	2(56)	3 II	0
	29(8)	7 I	0
IV	0(1)	7 IV	1
	2(64)	14 II	2
V	0(1)	35 V	30
	2(64)	7 I	1

Observe that there are 3584 ovoids of type I, II and III, 224 of type IV and 448 of type V. Furthermore note that to form a GQ$(8, 64)$ we need $4032 = 3584 + 448$ ovoids.

We can conjecture, after looking at the above table:

CONJECTURE 198. For $q = 8$ the only generalised quadrangles of order (q, q^2) with $T_2(\mathcal{O})$, $\mathcal{O}$ a pointed conic, as a subquadrangle of order q are $T_3(\Omega)$, Ω a Tits ovoid, and the dual of $\mathrm{GQ}(\boldsymbol{C}_2)$ where $\boldsymbol{C}_2$ is the FTWKB q–clan.

18. End Note

NOTES ON SECTION 1, P. 81. The results in this Section are well known.

NOTES ON SECTION 2, P. 83. The results in this Section are well known.

NOTES ON SECTION 3, P. 87. A subspace W of $PG(d, q)$ is **absolute** with respect to Δ if $W \subseteq \Delta(W)$. A polar space is the system of absolute subspaces where incidence is containment. Over a finite field, $d > 2$, this system is non-empty (in an infinite field we have counterexamples).

Properties of polar spaces: They satisfy **GQ1** and **ptGQ** axioms and the axiom

PS: Given an anti-flag (x, L) we have either **GQ2** or that x is collinear with all points of L

Proof that axiom PS is satisfied in a GQ if the polar space has rank two: Suppose x and y are absolute points. Then $\langle x, y\rangle$ is an absolute line if and only if $x \subseteq \Delta(y)$ if and only if $y \subseteq \pi(x)$, since $\langle x, y\rangle \subseteq \pi(\langle x, y, \rangle) = \pi(x) \cap \pi(y)$. Now let x be an absolute point and L an absolute line with x not incident with L. We have $\Delta(x)$ being a hyperplane with $x \subseteq \pi(x)$. Either $\pi(x)$ meets L in a point or contains L. As $y \subseteq \pi(x)$ if and only if $y \sim x$ we have one point collinear with x or all points on L collinear with x. Notice axiom **ptGQ** requires the use of finite fields.

Suppose we have the anti-flag (x, L) with x being collinear with all the points of L. Then $\langle x, L\rangle$ is an absolute plane. We have $L \subseteq \Delta(x)$, $x \subseteq \pi(L)$, $x \subseteq \pi(x)$ and $L \subseteq \pi(L)$, so

$$\langle x, L\rangle \subseteq \Delta(x) \cap \pi(L) = \pi(\langle x, L\rangle).$$

If there are no absolute planes then the polar space is a generalised quadrangle (given that there are absolute lines). Hence the polar space has rank two.

Below is the theorem of Buekenhout and Lefévre:

THEOREM 199 ([**25**]). *A GQ $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ whose incidence structure is a full substructure of a projective space $PG(d, q)$ must be obtained in one of the following ways:*

(i) *There is a unitary or symplectic polarity π of $PG(d, q)$, $d = 3$ or 4, such that $\mathcal{P}$ is a set of absolute points of π and $\mathcal{B}$ is the set of totally isotropic lines of π.*

(ii) *There is a nonsingular quadric Q of projective index 1 in $PG(d,q)$, $d = 4$, 5, such that $\mathscr{P}$ is the set of points of Q and $\mathscr{B}$ is the set of lines of Q.*

Hence the classical GQs are $W(q)$, $Q(4,q)$, $Q(5,q)$, $H(3,q^2)$ and $H(4,q^2)$.

The results in this Section are well known.

NOTES ON SECTION 4, P. 89. The results in this Section are well known. The proof of Theorem 151, p. 90, is different from the given reference and is due to Penttila.

NOTES ON SECTION 5, P. 91. The results in this Section are well known.

NOTES ON SECTION 6, P. 91. The results in this Section are well known. The model of $Q(5,q)$ is somewhat new and is by Penttila.

NOTES ON SECTION 7, P. 94. Let $\mathscr{S} = (\mathscr{P}, \mathscr{B}, \mathrm{I})$ be an EGQ(s,t) with two base points $x_1 \neq x_2$ and two elation groups G_1 and G_2. Then G_1 has orbits $\{x_1\}$, $x_1^{\perp} \setminus \{x_1\}$, and $\mathscr{P} \setminus x_1^{\perp}$, and G_2 has orbits $\{x_2\}$, $x_2^{\perp} \setminus \{x_2\}$, and $\mathscr{P} \setminus x_2^{\perp}$ on $\mathscr{P}$. So $\mathrm{Aut}\,\mathscr{S}$ has orbits being unions of both of the above orbits of G_1 and G_2. Therefore $\mathrm{Aut}\,\mathscr{S}$ is transitive. Hence $\mathrm{Aut}\,\mathscr{S}$ has rank 3 on $\mathscr{P}$. We have $\mathrm{Aut}\,\mathscr{S}$ being primitive since it has subdegrees 1, $s(t+1)$ and s^2t, and none of $1+s(t+1)$, $1+s^2t$, $s(t+1)+s^2t$ divides $|\mathscr{P}|$. Primitive rank 3 groups have been classified by Liebeck [**73**]. It is well known that this forces $\mathrm{Aut}\,\mathscr{S}$ to be classical. (Though the reference is hard to find. Folklore possibly?)

In $PG(2n+m-1,q)$ consider a set $O(n,m,q)$ of q^m+1 $(n-1)$–dimensional subspaces $[n-1]_0, \dots, [n-1]_{q^m}$, every three of which generate a $(3n-1)$-dimension (projective) space, and such that each element of $[n-1]_i$ of $O(n,m,q)$ is contained in a $[n+m-1]_i$ having no point in common with any other $[n-1]_j$ for $i \neq j$. The $[n+m-1]_i$ is uniquely determined and is called the **tangent space** of $O(n,m,q)$ at $[n-1]_i$.

Now we embed $PG(2n+m-1,q)$ in a $PG(2n+m,q)$ and construct a point-line geometry $T(n,m,q)$ as follows.

Points are of three types:

(i) The points of $PG(2n+m,q) - PG(2n+m-1,q)$.

(ii) The $(n+m)$–dimensional subspaces of $PG(2n+m,q)$ which intersect $PG(2n+m-1,q)$ in one of the $[n+m-1]_i$.

(iii) The symbol (∞).

Lines are of two types:

(a) The n–dimensional subspaces of $PG(2n+m,q)$ which intersect $PG(2n+m-1,q)$ in a $[n-1]_i$.

(b) The elements of $O(n,m,q)$.

Incidence: A type (i) point is incident only with type (a) lines (incidence of $PG(2n+$

$m, q)$). A type (ii) point is incident with all type (a) lines contained in it and with the unique element of $O(n, m, q)$ contained in it. The point (∞) is incident with no type (a) lines and all type (b) lines. There are no further incidences.

We have $O(1,1,q) = \mathcal{O}$ is an oval of $PG(2, q)$ and $T(1,1,q)$ is the GQ $T_2(\mathcal{O})$. We have $O(1,2,q) = \Omega$ is an ovoid of $PG(3, q)$ and $T(1,2,q)$ is the GQ $T_3(\Omega)$.

The only known TGQs for q even are the $T_2(\mathcal{O})$ and $T_3(\Omega)$ generalised quadrangles.

Let q be odd and Ω be an ovoid of $PG(3, q)$. That is, a set of $q^2 + 1$ 1-spaces in $GF(q)^4$. Let $q = q_0^m$. Then these $q^2 + 1$ 1-spaces are $q_0^{2m} + 1$ m-spaces (over $GF(q_0)$) in $GF(q_0)^{4m}$ with two distinct m-spaces generating a $2m$ space that is disjoint from the $q_0^{2m} + 1$ set. Any point of Ω is on a unique $3m$-space Σ with $\Sigma \cap \Omega = \{x\}$. Hence this collection of $q_0^{2m} + 1$ m-spaces is a $O(m, 2m, q_0)$, sometimes referred to as a **bad egg**, and so constructs a TGQ(q, q^2). Now the tangent spaces Σ form a bad egg, Ω^*, in $PG(4m - 1, q_0)$. The bad egg Ω^* constructs a TGQ that is not necessarily isomorphic to the original TGQ. For $q = 3^e$, e odd, there is a bad egg, Ω, that can be constructed from the semifield planes of Ganley [**41**]. The TGQ constructed from Ω is *not* isomorphic to the TGQ constructed by Ω^*. These TGQs from Ω^* are the **Roman** generalised quadrangles constructed by Payne [**94**][**95**].

The results in this Section are well known.

Notes on Section 8, p. 97. Theorem 168, p. 97 is proved for the construction of an EGQ $\mathcal{S}(G, \mathcal{F})$ of order (q^m, q^n) for positive integers m and n. Since we are already quite comprehensive for EGQs of order (q^2, q) to generalise even further will be of little benefit to the reader.

The results in this Section are well known.

Notes on Section 9, p. 99. The Theorem 169, p. 100, first appeared in [**30**]; a collaborative effort between the author, Penttila, Royle and Cherowitzo.

Notes on Section 10, p. 102. The results in this Section are well known.

Notes on Section 11, p. 104. The results in this Section are well known.

Notes on Section 12, p. 105. The Subiaco q–clan first appeared in [**30**]; a collaborative effort between the author, Penttila, Royle and Cherowitzo.

Notes on Section 13, p. 105. This Section is from the work of Payne [**102, 6, 96**].

Notes on Section 14, p. 108. The work first appeared in the papers of Payne. Lemma 184, p. 115, Lemma 185 and Theorem 186, p. 118, first appeared in [**100**]. The results were a collaborative effort between the author and Penttila, with contributions by Payne. They were influenced by the ideas in [**87**].

NOTES ON SECTION 15, P. 119. The question (I think) was asked by T. Penttila. It was asked in the view that it will hopefully make certain GQ calculations easier, in particular those requiring the Fundamental Theorem. The answer to that question was yes!

This Section is from [**98**] and [**101**].

NOTES ON SECTION 16, P. 122. The results in this Section are well known though recently published.

NOTES ON SECTION 17, P. 124. The introductory work in this Section is well known.

Work on the FTWKB q–clan: Sections 17.1–17.7 is by the author. Section 17.8, p. 134 is by Royle.

CHAPTER IV

Flocks

1. Introduction

Take an oval (or hyperoval, if q is even) $\mathcal{O}$ in $PG(2,q)$. Take a point v in $PG(3,q)$ not in $PG(2,q)$. The union of the points on the lines joining the vertex v to the oval (or hyperoval) $\mathcal{O}$ is called a **cone**. The oval (hyperoval) $\mathcal{O}$ is sometimes referred to as the **base** of the cone and the lines from the vertex to the base are occasionally referred to as the **generators** of the cone. A **quadratic cone** is a cone in which the base is a conic. A **translation oval cone** is a cone whose base is a translation oval (see Section 6, p. 46, Chapter II). A **flock** F of a cone K with vertex v is a set of q disjoint ovals (hyperovals) partitioning $K - \{v\}$. A flock F is called **linear** if all the planes containing the elements of the flock meet in a (external) line.

Let Ω be an ovoid of $PG(3,q)$. A **flock of** Ω is a partition of Ω into $q-1$ ovals with the remaining two points of the ovoid x and y, the **carriers** of the flock. If the planes containing the ovals of the flock meet in a (external) line then we say the flock is **linear**.

Let H be the hyperbolic quadric of $PG(3,q)$, (that is H is $O^+(4,q)$). A partition of H into $q+1$ irreducible conics is called a **flock** of H. If the planes containing the elements of the flock meet in a (external) line then we say the flock is **linear**.

In all of the above cases the ovals of the flocks uniquely define the planes containing them, hence we just as easily define flocks as a set of planes intersecting a cone (minus the vertex), ovoid (minus the carriers) or hyperbolic quadric.

2. Translation Planes from Flocks of Quadrics

We now look at flocks of quadrics, that is, flocks arising from a quadratic cone, hyperbolic quadric, or a elliptic quadric.

We denote $O^+(6,q)$, the Klein quadric in $PG(5,q)$, by $\mathcal{K}$.

We embed the flock of a quadratic cone, hyperbolic quadric, and elliptic quadric in $\mathcal{K}$. There is a unique embedding of a quadratic cone (up to similarity), hyperbolic quadric, and of an elliptic quadric in $\mathcal{K}$ since all 3-spaces intersecting $\mathcal{K}$ in a quadric are isomorphic (see Theorem 22.6.6 in [**57**]).

So each flock, F, is a set of planes in $PG(5,q)$ with each plane intersecting $\mathcal{K}$ in a conic. The polarity, $\perp$, defined by $\mathcal{K}$ of $PG(5,q)$ takes planes of this type to planes of this type. (That is because we have an orthogonal sum $O^+(6,q) = O(3,q) \perp O(3,q)$, since a plane of this type is an $O(3,q)$.)

Let Ω be the set of totally singular points x with x in $\pi^\perp$, for some π in F, a flock of a quadratic cone. That is,

$$\Omega = \bigcup_{\pi_i \in F} (\pi_i^\perp \cap \mathcal{K}).$$

We claim Ω is an ovoid.

Proof. Firstly we show $|\Omega| = q^2+1$: There are q planes in a flock of a quadratic cone. The cone lives in a solid, Σ, whose perp is a tangent line L (since Σ meets $\mathcal{K}$ in a cone). The point v of tangency of L is the vertex of the cone. Thus all $\pi^\perp$ are on L and so on v. Moreover, since the π's in F are distinct the $\pi^\perp$'s are distinct, so they pairwise intersect exactly in L. Other than v, each $\pi^\perp$ has q points of $\mathcal{K}$ on it; q^2 points in all. Adding v we have the result.

Secondly, no two points of Ω are perpendicular (that is, no two lie on a line of $\mathcal{K}$): If π, π' in F, then π intersects π' in an external line M to $\mathcal{K}$ (this is the first time we have used this fact). Thus $M^\perp$ is an elliptic quadric solid, as

$$O^+(6,q) = O^-(2,q) \perp O^-(4,q).$$

But $M^\perp$ is the span of $\pi^\perp$ and $\pi'^\perp$. In an elliptic quadric solid, no two points are perp. Therefore, if $x, y \in \Omega$ and $x \in \pi^\perp$, $y \in \pi'^\perp$ with π, π' distinct, x is not perp to y. If $\pi = \pi'$, then x and y both lie in a conic, so again they are not perp. □

For a hyperbolic quadric a flock has $q+1$ planes, and the perp of the solid is a secant line, so we have $(q+1)(q-1)+2 = q^2+1$. The rest of the proof is identical. For an elliptic quadric, a flock has $q-1$ planes, and two points not in the partition; so Ω must be taken to be the union of the $\pi^\perp$'s plus these two points; then we get $(q-1)(q+1)+2$ as for this case the perp of the solid is an external line.

Now each $\pi^\perp$ is a conic, and so under the Klein correspondence, which takes points of $\mathcal{K}$ to lines of $PG(3,q)$, (see Section 15.4 in [**56**]) there corresponds a regulus of $PG(3,q)$. Together, the q^2+1 points of Ω Klein correspond to a set of q^2+1 skew lines of $PG(3,q)$, that is, a spread, $\mathcal{S}$, of $PG(3,q)$ (see Chapter I, 10). We use the Bruck-Bose construction, Theorem 22, p. 10, to construct a translation plane of order q^2 with kernel containing $GF(q)$. (Note: For each of the $\pi^\perp$'s being a conic this says that the resulting translation planes have q, $q+1$ or q visible derivation sets [**36**, pp.

224–5] accordingly as the quadric is a cone, hyperbolic or elliptic. Of course, some of these may lead to the same derived plane up to isomorphism.)

Now the above translation plane is Desarguesian if and only if $\mathcal{S}$ is regular if and only if Ω is an elliptic quadric if and only if the π's have a common line if and only if F is linear.

3. Classification of Flocks of Ovoids

THEOREM 200. *Any flock of an ovoid in $PG(3,q)$ is linear.*

PROOF. For the q is odd case see [**88**], or [**40**] Theorem 3.2(b) for another proof. For the q even case see [**40**] Theorem 3.1. See also Sections 17.1 and 17.2 in [**56**]. □

Hence all translation planes from a flock of an elliptic quadric are Desarguesian.

4. Classification of Flocks of a Hyperbolic Quadric

Let H be the hyperbolic quadric $O^+(4,q)$ in $PG(3,q)$. The hyperbolic quadric can be thought of as a grid of type $(q+1,q+1)$. This is a regulus and its opposite regulus.

THEOREM 201. *Any flock of H in $PG(3,q)$, where q is even, is linear.*

PROOF. See [**40**] Theorem 3.1. □

In [**126**] we have a description of a non-linear flock for H in $PG(3,q)$ when q is odd: We let $\mathcal{C}$ be the set of irreducible conics of H, and define an equivalence relation on $\mathcal{C}$ by: $C_1 \sim C_2$ if and only if there exists a $C \in \mathcal{C}$ that is tangent to C_1 and C_2. This equivalence relation defines two equivalence classes which we denote by I and II. Let L be an exterior line to H. The polarity induced by H takes exterior lines to exterior lines, we let L' be the polar line of L with respect to H. Now we define some sets:

$$\begin{aligned}
V &= \{\text{planes on } L \text{ intersecting } H \text{ in a conic of class I}\},\\
V' &= \{\text{planes on } L \text{ intersecting } H \text{ in a conic of class II}\},\\
W &= \{\text{planes on } L' \text{ intersecting } H \text{ in a conic of class II},\\
&\qquad \text{if } q = 1 \mod 4, \text{ or class I, if } q = -1 \pmod 4\},\\
W' &= \{\text{planes on } L' \text{ intersecting } H \text{ in a conic of class I},\\
&\qquad \text{if } q = 1 \mod 4, \text{ or class II, if } q = -1 \pmod 4\}.
\end{aligned}$$

Then $V \cup W$ and $V' \cup W'$ describe a non-linear flock of H, called a **Thas flock**.

There are also the three **exceptional flocks** of H in $PG(3,q)$ for $q = 11$, 23, 59 [**4**]. Independently found by Baker-Ebert [**10**] for $q = 11$ and 23, and by Johnson [**63**] for $q = 59$.

THEOREM 202. *Any flock of the hyperbolic quadric $H = O^+(4,q)$ in $PG(3,q)$, q is even or odd, is:*

(i) *a linear flock, or*
(ii) *a Thas flock, or*
(iii) *one of the three exceptional flocks for $q = 11$, 23, 59.*

PROOF. See [**5**]. This paper uses the result of Thas [**128**] where the same result is proven under the extra hypothesis that $q \equiv 1 \pmod 4$. □

The non-linear flocks give rise to translation planes over **nearfields**. The Thas flock has the translation plane over a **regular nearfield** and the three exceptional flocks have their translation planes over some of the **exceptional nearfields** (hence their name) [**36**].

5. Flocks of Cones

In this section we will look at some results on flocks of cones over small fields.

THEOREM 203. *Any flock of a cone in $PG(3,2)$ is linear.*

PROOF. A flock consists of two planes of $PG(3,2)$. Any two planes meet in a line. □

THEOREM 204. *Let F and F' be two flocks of the same cone in $PG(3,q)$. If $|F \cap F'| > (q-1)/2$ then the flocks are equal.*

PROOF. See [**127**] First Theorem of Section 1.5.1. □

COROLLARY 205. *Any flock of a cone in $PG(3,3)$ is linear.*

The base of a cone can either be a hyperoval or an oval for q even. Now for q even we would like to know what happens to a flock, F, of a cone, K, in $PG(3,q)$ when its base changes from an oval to a hyperoval; call this hyperoval cone K^* and the flock F^*. The Theorem after Remark 1.5.2 in [**127**] shows that the flock F defines the flock F^*, so if $C \in F$ then $C \subset C^*$ with $C^* \in F^*$. The converse is straightforward; remove the generator of K^* that contains the point to be removed from the hyperoval to make it into an oval. This removes a point from each hyperoval of the flock F^* to make a flock F. In short, when q is even, we can obtain flocks of K from K^* and flocks of K^* from K.

We can also understand flocks via the dual setting when q is even. Take a flock, F^*, of a cone, K^* with a hyperoval as its base in $PG(2,q)$. Denote the planes that contain the elements of the flock π_i for $i = 1,\dots,q$, and the generators of K^* denoted by L_i for $i = 1,\dots,q+2$. The generators L_i of K^* have no three lying on a plane, this dualises to the lines $\hat{L}_i$ no three concurrent. The $\hat{L}_i$'s lie in $PG(2,q)$ since the L_i's intersect at the vertex of K^*. Now the points of $PG(2,q)$ not incident with the lines $\hat{L}_i$ form a maximal $(0,q/2)$-arc, $\mathcal{M}$, of size $q(q-1)/2$ (see [**49**] for discussions about maximal arcs). The planes π_i dualise to the points $\hat{\pi}_i$ in $PG(3,q) - PG(2,q)$. Each line containing $\hat{\pi}_i$ and $\hat{\pi}_j$ with $i \neq j$ intersects $PG(2,q)$ in a point of the maximal arc $\mathcal{M}$. So the flock F^* is linear if and only if the q points $\hat{\pi}_i$ are collinear.

THEOREM 206. *Any flock of a cone in $PG(3,4)$ is linear.*

PROOF. Use the results in the dual setting and use the remarks on flocks of hyperovals being flocks of ovals. $\square$

6. Flocks of QuadraticCones

In this section we look at flocks of quadratic and translation oval cones settings in a more algebraic setting. We will also comment on the links between q-clans (see Section 9, p. 99, Chapter III) and flocks of quadratic cones and later of translation oval cones. We take the quadratic cone, K, in $PG(3,q)$ to be the one defined by

$$xy = z^2.$$

Now the q planes, π_i with $i = 1,\dots,q$, of a flock F which do not contain the vertex $(0,0,0,1)$ of K can be described by the set of equations

$$a_i x + b_i y + c_i z + w = 0, \qquad \text{for } i = 1,\dots,q.$$

THEOREM 207. *Let $\mathcal{T}$ be a set of q ordered triples (a_i,b_i,c_i) with a_i, b_i, $c_i \in GF(q)$.*

If q is odd then,

$$(c_i - c_j)^2 - 4(a_i - a_j)(b_i - b_j) = \not\square, \qquad \textit{for } i \neq j$$

if and only if $\mathcal{T}$ describes a flock of a quadratic cone.

If q is even, with $c_i \neq c_j$ whenever $i \neq j$, then

$$\operatorname{trace}\left(\frac{(a_i+a_j)(b_i+b_j)}{(c_i+c_j)^2}\right) = 1 \qquad \textit{for all } i \neq j$$

if and only if $\mathcal{T}$ describes a flock of a quadratic cone.

PROOF. See [**127**]. $\square$

Hence, $\boldsymbol{C} = \left\{ \begin{pmatrix} a_i & b_i \\ 0 & c_i \end{pmatrix} \;\middle|\; i \in GF(q) \right\}$ is a q–clan (Section 9, p. 99), if and only if $\{a_i x + c_i y + b_i z + w = 0 \mid i \in GF(q)\}$ is a flock of a quadratic cone, denoted $\mathcal{F}(\boldsymbol{C})$. We denote the translation plane from the flock $\mathcal{F}(\boldsymbol{C})$ by $\pi(\boldsymbol{C})$.

Two flocks $\mathcal{F} = \{\pi_t \mid t \in GF(q)\}$ and $\mathcal{F} = \{\pi'_t \mid t \in GF(q)\}$ of a quadratic cone K are **equivalent**, or **projectively equivalent**, if there is an element of $P\Gamma L(4,q)$ fixing K (so an element of $P\Gamma O(4,q)$) and mapping the set of planes $\{\pi_t \mid t \in GF(q)\}$ onto the set of planes $\{\pi'_t \mid t \in GF(q)\}$. More formally:

THEOREM 208 ([**55**]). *The flocks $\mathcal{F}$ and $\mathcal{F}'$ of a quadratic cone $y^2 = xz$ are equivalent if and only if there exists the following*

(i) $\sigma \in \operatorname{Aut} GF(q)$,
(ii) $0 \neq u \in GF(q)$,
(iii) $B = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in GL(2,q)$, *and*
(iv) *a permutation of* $GF(q)$ $\pi \colon t \mapsto \bar{t}$,

such that for some x_0, y_0, $z_0 \in GF(q)$ *we have*

$$\begin{pmatrix} x'_{\bar{t}} \\ y'_{\bar{t}} \\ z'_{\bar{t}} \\ 1 \end{pmatrix} = \begin{pmatrix} ua^2 & uab & ub^2 & x_0 \\ 0 & u(ad+bc) & 0 & y_0 \\ uc^2 & ucd & ud^2 & z_0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_t^\sigma \\ y_t^\sigma \\ z_t^\sigma \\ 1 \end{pmatrix} \quad \textit{for all } t.$$

It is of interest to the reader to compare the Fundamental Theorem of q–clan Geometry (page 106) to the above theorem.

7. Derivation of flocks of quadratic cones in $PG(3,q)$, q odd

A **BLT-set** is a set of $q+1$ (skew) lines in $W(q)$ such that all lines of $W(q)$ meets at most two of the lines of the set [**7**].

It has been shown (see for example [**96**]) that new flocks can be obtained from old, the fundamental object of study is a BLT-set in $W(q)$.

We understand the construction of new flocks from old via the Knarr construction [**24**] where BLT-sets correspond to a generalised quadrangle, $\mathscr{S}$ (q^2, q).

For q odd we have $W(q)^\wedge \cong Q(4,q)$. A BLT-set in $Q(4,q)$ is a set, X, of $q+1$ (pairwise non-perpendicular) points of $Q(4,q)$ such that all points of $Q(4,q)$ are perpendicular to at most two of the points of the set. Let $x \in X$. Then $x^\perp$ is a quadratic cone K; and $y^\perp \cap x^\perp$ (for $y \in X - \{x\}$) is a flock $\mathcal{F}_x$ of K. Let y, $z \in X - \{x\}$, $y \nsim x \nsim z$, so $y^\perp \cap K$ is a conic of K, $z^\perp \cap K$ is a conic of K. We must show that $y^\perp \cap z^\perp \cap K$ is an external line. For simplicity we assume that it is a line; if $w \in y^\perp \cap z^\perp \cap K$ is singular, then $\{x, y, z\} \subseteq w^\perp \cap X$ a contradiction.

The flock $\mathcal{F}_x$ gives a q-clan $\boldsymbol{C}_x$ so hence a generalised quadrangle $GQ(\boldsymbol{C}_x) \cong \mathscr{S}$. For any two points, x, y, of a BLT-set we have $GQ(\boldsymbol{C}_x) \cong GQ(\boldsymbol{C}_y)$. We say $\mathcal{F}_x$ is **derived** from $\mathcal{F}_y$.

If $\mathcal{F}$ is a flock of a quadratic cone K (with vertex x); embed K in the quadric $\mathcal{P}$ in $PG(4,q)$. Each plane π in $\mathcal{F}$ is mapped under the polarity of $\mathcal{P}$ (in $PG(4,q)$) to a secant line l on x. Let y_π be the other singular point on l and let

$$X = \{x\} \cup \{y_\pi \mid \pi \in \mathcal{F}\}$$

Then X is a BLT-set.

From the results above and in Chapter III given a q–clan we can obtain from GQ($\boldsymbol{C}$) a flock $\mathcal{F}(\boldsymbol{C})$, but if $GQ(\boldsymbol{C}_1) \cong$ GQ($\boldsymbol{C}_2$) this does not imply that $\mathcal{F}(\boldsymbol{C}_1) \cong \mathcal{F}(\boldsymbol{C}_2)$. This is the source of much subtlety.

8. Known q–clans for q Even

Since we have defined the links between herds, flocks and q-clans we now list the known q-clans and hence flocks of quadratic cones for q even.

The q–clan associated with the linear flocks [**127**] for even q:

$\boldsymbol{C}_1$:
$$A_t = \begin{pmatrix} t & t \\ 0 & at \end{pmatrix},$$

where $a \in GF(q)$ and trace$(a) = 1$. The herd $H(\boldsymbol{C}_1)$ consists of $q+1$ (nondegenerate) conics. The elation generalised quadrangle associated with this q–clan is isomorphic to $H(3,q^2)$ [**103**].

The q–clan of Fisher-Thas-Walker-Kantor-Betten [**40**] [**135**] [**65**] [**14**] for $q = 2^e$, e odd:

$\boldsymbol{C}_2$:
$$A_t = \begin{pmatrix} t & t^2 \\ 0 & t^3 \end{pmatrix}.$$

Theorem 209. *We have $\boldsymbol{C}_2$ is a q-clan for $q = 2^e$, e odd.*

Proof. We need to show that for all $x \neq y$ we have

$$\operatorname{trace}\left(\frac{(x+y)(x^3+y^3)}{(x^2+y^2)^2}\right) = 1.$$

Now

$$\begin{aligned}\frac{(x+y)(x^3+y^3)}{(x^2+y^2)^2} &= \frac{x^4+xy^3+x^3y+y^4}{x^4+y^4} = 1 + \frac{xy^3+x^3y}{(x^2+y^2)^2} \\ &= 1 + \frac{xy(x^2+y^2)}{(x^2+y^2)^2} = 1 + \frac{xy}{x^2+y^2} \\ &= 1 + \frac{x}{x+y} + \frac{x^2}{x^2+y^2}.\end{aligned}$$

Since $\operatorname{trace}(\frac{x}{x+y} + \frac{x^2}{x^2+y^2}) = 0$ we have that

$$\operatorname{trace}\left(\frac{(x+y)(x^3+y^3)}{(x^2+y^2)^2}\right) = \operatorname{trace}(1).$$

But $\operatorname{trace}(1) = 1$ if and only if $q = 2^e$ with e odd. $\square$

The flock associated with this q–clan is linear when $q = 2$. The herd $H(\boldsymbol{C}_2)$ consists of $q+1$ non-conical translation ovals if $q > 2$. The translation plane is due to Walker [**135**] for a similar q–clan for q odd ($q \equiv -1 \pmod 3$) and Betten [**14**] for q even. The flock is due to Thas and Fisher [**40**] and the generalised quadrangle due to Kantor [**65**].

The q–clan of Payne [**93**] for $q = 2^e$, e odd:

$\boldsymbol{C}_3$:
$$A_t = \begin{pmatrix} t & t^3 \\ 0 & t^5 \end{pmatrix}.$$

See Section 103, p. 49, for a proof that $\boldsymbol{C}_3$ is a q–clan. The flock associated with this q–clan is linear when $q = 2$. The herd $H(\boldsymbol{C}_3)$ consists of 2 Segre-Bartocci ovals and $q-1$ Payne ovals, for $q > 8$. When $q = 8$, $\boldsymbol{C}_3$ is equivalent to $\boldsymbol{C}_2$. The translation planes were found by Cohen and Ganley [**31**] deriving from a spread constructed by O. Barriga [**11**]. Kantor constructed a similar q–clan for q odd [**67**].

The q–clan, $\boldsymbol{C}_4$, associated with the flock of De Clerck and Herssens [**35**] for $q = 16$. The herd $H(\boldsymbol{C}_4)$ consists of 17 Lunelli-Sce ovals (see Section 10.1, p. 158).

Payne [**96**] has shown that given an elation generalised quadrangle, $GQ(\boldsymbol{C})$, associated with a q-clan $\boldsymbol{C}$, it is possible to construct new flocks from $GQ(\boldsymbol{C})$. This is, in some sense, the characteristic two analogue of derivation in the sense of BLT sets (see End Notes). Each of the above q-clans give rise to a unique flock except for the q-clan $\boldsymbol{C}_3$. This non-linear flock, denoted $\mathcal{F}(\boldsymbol{C}_5)$, of Payne [**96**] for $q = 2^e$, $e > 3$ odd, is constructed by recoordinatising one of the lines on the point (∞) of $GQ(\boldsymbol{C}_3)$ to obtain $\boldsymbol{C}_5$. (Of course, $GQ(\boldsymbol{C}_5)$ is isomorphic to $GQ(\boldsymbol{C}_3)$).

There are some q-clans for $q = 64$, 256, 1024, 4096 and 16384 that appear in [**109**][**101**].

In earlier versions of [**129**] Thas gave as an open problem the construction of q–clans associated with non-linear flocks for q even, q square. The first example, $\mathcal{F}(\boldsymbol{C}_4)$, of such a flock was found for $q = 16$ by De Clerck and Herssens [**35**]. We shall construct an infinite family of q-clans for all q even, which includes $\boldsymbol{C}_4$ for $q = 16$.

9. The Subiaco q–clans

Let us recall the definition of $\mathcal{T}_a(f,g)$. For two permutation functions, f, g, defined on $GF(q)$ with $f(0)=g(0)=0$ and $f(1)=g(1)=1$ with trace$(a)=1$ then

$$A_t = \begin{pmatrix} f(t) & t^{1/2} \\ 0 & g(t) \end{pmatrix}$$

is a q–clan if and only if

$$\mathcal{T}_a(f,g): \qquad \operatorname{trace}\left(\frac{a(f(s)+f(t))(g(s)+g(t))}{s+t}\right) = 1 \text{ for all } s \neq t.$$

9.1. The case $q = 2^e$ where e is odd.

THEOREM 210. *Let $q = 2^e$, e odd. Let*

$$f(x) = \frac{x^2+x}{(x^2+x+1)^2} + x^{1/2} \quad \textit{and} \quad g(x) = \frac{x^4+x^3}{(x^2+x+1)^2} + x^{1/2}.$$

Then

$$\boldsymbol{S}'' = \left\{ A_x = \begin{pmatrix} f(x) & x^{1/2} \\ 0 & g(x) \end{pmatrix} \;\middle|\; x \in GF(q) \right\}$$

is a q–clan.

PROOF. We show that the matrices $\begin{pmatrix} f(x) & x^{1/2} \\ 0 & g(x) \end{pmatrix}$, $x \in GF(q)$, form a q–clan by showing that $(f(x)+f(y))(g(x)+g(y))/(x+y)$ has trace one for all $x \neq y$; noting that trace$(1)=1$ whenever $q=2^e$ for e odd. From now on we assume $x \neq y$:

$$\begin{aligned}
&\frac{(f(x)+f(y))(g(x)+g(y))}{x+y} \\
&= \frac{1}{x+y}\left(\frac{x^2+x}{(x^2+x+1)^2} + x^{1/2} + \frac{y^2+y}{(y^2+y+1)^2} + y^{1/2}\right) \\
&\qquad \times \left(\frac{x^4+x^3}{(x^2+x+1)^2} + x^{1/2} + \frac{y^4+y^3}{(y^2+y+1)^2} + y^{1/2}\right) \\
&= \frac{1}{x+y}\left(\frac{(x^2+x)(x^4+x^3)}{(x^2+x+1)^4} + \frac{(x^2+x)(y^4+y^3)}{(x^2+x+1)^2(y^2+y+1)^2} + (x+y)^{1/2}\frac{x^2+x}{(x^2+x+1)^2}\right. \\
&\qquad + \frac{(y^2+y)(y^4+y^3)}{(y^2+y+1)^4} + \frac{(x^4+x^3)(y^2+y)}{(x^2+x+1)^2(y^2+y+1)^2} + (x+y)^{1/2}\frac{y^2+y}{(y^2+y+1)^2} \\
&\qquad \left. + (x+y)^{1/2}\frac{x^4+x^3}{(x^2+x+1)^2} + (x+y)^{1/2}\frac{y^4+y^3}{(y^2+y+1)^2} + (x+y)\right).
\end{aligned}$$

We can express this last line as

$$A + B + 1$$

where

$$A = \frac{1}{x+y}\left(\frac{(x^2+x)(x^4+x^3)}{(x^2+x+1)^4} + \frac{(x^2+x)(y^4+y^3)}{(x^2+x+1)^2(y^2+y+1)^2}\right.$$
$$\left. + \frac{(y^2+y)(y^4+y^3)}{(y^2+y+1)^4} + \frac{(x^4+x^3)(y^2+y)}{(x^2+x+1)^2(y^2+y+1)^2}\right), \text{ and}$$
$$B = \frac{1}{(x+y)^{1/2}}\left(\frac{x^2+x}{(x^2+x+1)^2} + \frac{y^2+y}{(y^2+y+1)^2} + \frac{x^4+x^3}{(x^2+x+1)^2} + \frac{y^4+y^3}{(y^2+y+1)^2}\right).$$

Hence we have "reduced" the problem to showing that $A+B$ has trace zero, as trace$(1) = 1$ for e odd. Since all elements of trace zero are of the form $X+X^2$, this is equivalent to showing that $A+B = X+X^2$ for some expression X. Since trace is additive, we have trace$(A+B) = $ trace$(A+B) + $ trace$(B+B^2) = $ trace$(A+B^2)$. (By showing $A+B^2$ has trace zero, instead of $A+B$, we can eliminate the $x^{1/2}$ terms from the latter.)

Now

$$A+B^2 = \frac{1}{x+y}\left(\frac{(x^2+x)(x^4+x^3)}{(x^2+x+1)^4} + \frac{(x^2+x)(y^4+y^3)}{(x^2+x+1)^2(y^2+y+1)^2}\right.$$
$$+ \frac{(y^2+y)(y^4+y^3)}{(y^2+y+1)^4} + \frac{(x^4+x^3)(y^2+y)}{(x^2+x+1)^2(y^2+y+1)^2}$$
$$\left. + \frac{x^4+x^2}{(x^2+x+1)^4} + \frac{y^4+y^2}{(y^2+y+1)^4} + \frac{x^8+x^6}{(x^2+x+1)^4} + \frac{y^8+y^6}{(y^2+y+1)^4}\right)$$
$$= \frac{1}{x+y}\left(\frac{x^8+x^2}{(x^2+x+1)^4} + \frac{y^8+y^2}{(y^2+y+1)^4}\right.$$
$$\left. + \frac{(x^2+x)(y^4+y^3)+(x^4+x^3)(y^2+y)}{(x^2+x+1)^2(y^2+y+1)^2}\right).$$

Since $x^8+x^2 = (x^4+x^2)(x^2+x+1)^2$ all the terms can be placed over a common denominator, giving:

$$\frac{1}{x+y}\left(\frac{(x^4+x^2)(y^2+y+1)^2+(y^4+y^2)(x^2+x+1)^2}{(x^2+x+1)^2(y^2+y+1)^2}\right.$$
$$\left. + \frac{(x^2+x)(y^4+y^3)+(x^4+x^3)(y^2+y)}{(x^2+x+1)^2(y^2+y+1)^2}\right).$$

We expand, group, noting that $x^3+y^3 = (x+y)(x^2+xy+y^2)$, and divide by $x+y$ to obtain:

$$\frac{(x+y)^3+x+y+x^2y^2(x+y)+x^2y^2+xy(x^2+xy+y^2)+xy(x+y)}{(x^2+x+1)^2(y^2+y+1)^2}.$$

With some cancellation we continue with:

$$\begin{aligned}
&\frac{x^3+y^3+x+y+x^3y^2+x^2y^3+x^3y+xy^3}{(x^2+x+1)^2(y^2+y+1)^2}\\
&=\frac{(x+y)(x^2+x+1)(y^2+y+1)+(x+y)^2}{(x^2+x+1)^2(y^2+y+1)^2}\\
&=\frac{x+y}{(x^2+x+1)(y^2+y+1)}+\frac{(x+y)^2}{(x^2+x+1)^2(y^2+y+1)^2}.
\end{aligned}$$

Which is of the form $X+X^2$ where

$$X=\frac{x+y}{(x^2+x+1)(y^2+y+1)}. \quad \square$$

9.2. The case $q=4^e$, where e is odd

THEOREM 211. *Let $q=4^e$, e odd, with $\omega\in GF(q)$ satisfying $\omega^2+\omega+1=0$. Let*

$$f(x)=\frac{x^2(x^2+\omega x+\omega)}{(x^2+\omega x+1)^2}+\omega^2x^{1/2}, \text{ and } g(x)=\frac{\omega x(x^2+x+\omega^2)}{(x^2+\omega x+1)^2}+\omega^2x^{1/2}.$$

Then

$$\boldsymbol{S}'=\left\{A_x=\begin{pmatrix} f(x) & x^{1/2}\\ 0 & \omega g(x)\end{pmatrix}\ \Big|\ x\in GF(q)\right\}$$

is a q–clan.

PROOF. The proof is similar to that of Theorem 210, p. 149.

For brevity we denote f and g by

$$f(x)=\frac{N_f(x)}{D(x)^2}+\omega^2x^{1/2} \quad\text{and}\quad g(x)=\frac{N_g(x)}{D(x)^2}+\omega^2x^{1/2},$$

where

$$D(x)=x^2+\omega x+1,\ N_f(x)=x^2(x^2+\omega x+\omega),\ \text{and } N_g(x)=\omega x(x^2+x+\omega^2).$$

We show that $\operatorname{trace}(\omega(f(x)+f(y))(g(x)+g(y))/(x+y))=1$ for all $x\neq y$. From now on we assume $x\neq y$, so:

$$\begin{aligned}
&\frac{\omega}{x+y}(f(x)+f(y))(g(x)+g(y))\\
&=\frac{\omega}{x+y}\left(\frac{N_f(x)}{D(x)^2}+\omega^2x^{1/2}+\frac{N_f(y)}{D(y)^2}+\omega^2y^{1/2}\right)\left(\frac{N_g(x)}{D(x)^2}+\omega^2x^{1/2}+\frac{N_g(y)}{D(y)^2}+\omega^2y^{1/2}\right)\\
&=\frac{\omega}{x+y}\left(\frac{N_f(x)N_g(x)}{D(x)^4}+\frac{N_f(x)N_g(y)+N_f(y)N_g(x)}{D(x)^2D(y)^2}+\frac{N_f(y)N_g(y)}{D(y)^4}\right)\\
&\qquad+\frac{1}{(x+y)^{1/2}}\left(\frac{N_f(x)}{D(x)^2}+\frac{N_f(y)}{D(y)^2}+\frac{N_g(x)}{D(x)^2}+\frac{N_g(y)}{D(y)^2}\right)+\omega^2.
\end{aligned}$$

We can express the last line as

$$A+B+\omega^2$$

where

$$A = \frac{\omega}{x+y}\left(\frac{N_f(x)N_g(x)}{D(x)^4} + \frac{N_f(x)N_g(y) + N_f(y)N_g(x)}{D(x)^2D(y)^2} + \frac{N_f(y)N_g(y)}{D(y)^4}\right), \text{ and}$$

$$B = \frac{1}{(x+y)^{1/2}}\left(\frac{N_f(x)}{D(x)^2} + \frac{N_f(y)}{D(y)^2} + \frac{N_g(x)}{D(x)^2} + \frac{N_g(y)}{D(y)^2}\right).$$

As ω^2 has trace one in $GF(q)$, $q = 4^e$, for any e odd, we have reduced the problem to showing that $A+B$ has trace zero. As $\mathrm{trace}(A+B) = \mathrm{trace}(A+B^2)$ this is equivalent to showing that $A+B^2$ has trace zero:

$$A + B^2 = \frac{1}{x+y}\left(\frac{\omega N_f(x)N_g(x) + N_f(x)^2 + N_g(x)^2}{D(x)^4}\right.$$
$$\left. + \frac{\omega N_f(y)N_g(y) + N_f(y)^2 + N_g(y)^2}{D(y)^4} + \frac{\omega N_f(x)N_g(y) + \omega N_f(y)N_g(x)}{D(x)^2D(y)^2}\right).$$

Now $\omega N_f(x)N_g(x) + N_f(x)^2 + N_g(x)^2$ simplifies to $x^2(x^2+\omega^2x+1)(x^2+\omega x+1)^2 = x^2(x^2+\omega^2x+1)D(x)^2$. Then the expression, placed over a common denominator $D(x)^2D(y)^2$, becomes:

$$\frac{1}{x+y}\left(\frac{x^2(x^2+\omega^2x+1)(y^2+\omega y+1)^2 + y^2(y^2+\omega^2y+1)(x^2+\omega x+1)^2}{D(x)^2D(y)^2}\right.$$
$$\left. + \frac{\omega^2x^2y(x^2+\omega x+\omega)(y^2+y+\omega^2) + \omega^2y^2x(y^2+\omega y+\omega)(x^2+x+\omega^2)}{D(x)^2D(y)^2}\right).$$

By expanding the terms we get

$$\frac{1}{x+y}\left(\frac{\omega^2x^4y^3 + \omega^2x^4y^2 + \omega x^4y + \omega^2x^3y + \omega^2x^2y}{D(x)^2D(y)^2}\right.$$
$$\left. + \frac{\omega^2x^3y^4 + \omega^2x^2y^4 + \omega xy^4 + \omega^2xy^3 + \omega^2xy^2}{D(x)^2D(y)^2}\right),$$

and then grouping to obtain

$$\frac{1}{x+y}\left(\frac{\omega^2x^3y^3(x+y) + \omega^2x^2y^2(x^2+y^2) + \omega xy(x^3+y^3)}{D(x)^2D(y)^2}\right.$$
$$\left. + \frac{\omega^2xy(x^2+y^2) + \omega^2xy(x+y)}{D(x)^2D(y)^2}\right).$$

Divide by $x+y$ and simplify to get:

$$\frac{x^3y^2 + x^2y^3 + \omega x^3y + \omega x^2y + \omega xy^3 + \omega xy^2 + x^3 + \omega^2x^2 + x + y^3 + \omega^2y^2 + y}{(x^2+\omega x+1)^2(y^2+\omega y+1)^2}$$
$$= \frac{(x+y)(x^2+\omega x+1)(y^2+\omega y+1) + x^2 + y^2}{(x^2+\omega x+1)^2(y^2+\omega y+1)^2}$$
$$= \frac{x+y}{(x^2+\omega x+1)(y^2+\omega y+1)} + \frac{(x+y)^2}{(x^2+\omega x+1)^2(y^2+\omega y+1)^2}.$$

Which is of the form $X + X^2$. $\square$

9.3. The case $q = 16^e$ where e is odd

THEOREM 212. *Let $q = 16^e$, e odd, with $\eta \in GF(q)$ satisfying $\eta^4 = \eta + 1$. Let*

$$f(x) = \frac{\eta^{13}x^4 + x^3 + \eta^2 + \eta^6 x}{(x^2 + \eta^3 x + 1)^2} + \eta^{12}x^{1/2}$$
$$g(x) = \frac{\eta^3 x^4 + \eta^7 x^3 + \eta^4 x^2 + \eta^{12}x}{(x^2 + \eta^3 x + 1)^2}.$$

Then

$$\boldsymbol{S}''' = \left\{ A_x = \begin{pmatrix} f(x) & x^{1/2} \\ 0 & \eta^{14}g(x) \end{pmatrix} \mid x \in GF(q) \right\}$$

is a q–clan.

PROOF. The proof is similar to that of Theorem 210, p. 149 and Theorem 211, p. 151. For brevity we denote f and g by

$$f(x) = \frac{N_f(x)}{D(x)^2} + \eta^{12}x^{1/2} \text{ and } g(x) = \frac{N_g(x)}{D(x)^2} + \eta^{13}x^{1/2},$$

where

$$\begin{aligned} D(x) &= x^2 + \eta^3 x + 1, \\ N_f(x) &= \eta^{13}x^4 + x^3 + \eta^2 x^2 + \eta^6 x, \text{ and} \\ N_g(x) &= \eta^3 x^4 + \eta^7 x^3 + \eta^4 x^2 + \eta^{12}x. \end{aligned}$$

We show that $\operatorname{trace}(\eta^{14}(f(x)+f(y))(g(x)+g(y))/(x+y)) = 1$ for all $x \neq y$. From now on we assume $x \neq y$, so:

$$\begin{aligned} &\frac{\eta^{14}}{x+y}(f(x)+f(y))(g(x)+g(y)) \\ &= \frac{\eta^{14}}{x+y}\left(\frac{N_f(x)}{D(x)^2} + \eta^{12}x^{1/2} + \frac{N_f(y)}{D(y)^2} + \eta^{12}y^{1/2}\right)\left(\frac{N_g(x)}{D(x)^2} + \eta^{13}x^{1/2} + \frac{N_g(y)}{D(y)^2} + \eta^{13}y^{1/2}\right) \\ &= \frac{\eta^{14}}{x+y}\left(\frac{N_f(x)N_g(x)}{D(x)^4} + \frac{N_f(x)N_g(y) + N_f(y)N_g(x)}{D(x)^2 D(y)^2} + \frac{N_f(y)N_g(y)}{D(y)^4}\right) \\ &\quad + \frac{\eta^{12}}{(x+y)^{1/2}}\left(\frac{N_f(x)}{D(x)^2} + \frac{N_f(y)}{D(y)^2}\right) + \frac{\eta^{11}}{(x+y)^{1/2}}\left(\frac{N_g(x)}{D(x)^2} + \frac{N_g(y)}{D(y)^2}\right) + \eta^9. \end{aligned}$$

We can express the last line as

$$A + B + \eta^9$$

where

$$\begin{aligned} A &= \frac{\eta^{14}}{x+y}\left(\frac{N_f(x)N_g(x)}{D(x)^4} + \frac{N_f(x)N_g(y) + N_f(y)N_g(x)}{D(x)^2 D(y)^2} + \frac{N_f(y)N_g(y)}{D(y)^4}\right), \text{ and} \\ B &= \frac{\eta^{12}}{(x+y)^{1/2}}\left(\frac{N_f(x)}{D(x)^2} + \frac{N_f(y)}{D(y)^2}\right) + \frac{\eta^{11}}{(x+y)^{1/2}}\left(\frac{N_g(x)}{D(x)^2} + \frac{N_g(y)}{D(y)^2}\right). \end{aligned}$$

As η^9 has trace one in $GF(q)$, $q = 16^e$, for any e odd, we have reduced the problem to showing that $A+B$ has trace zero. As $\mathrm{trace}(A+B) = \mathrm{trace}(A+B^2)$ this is equivalent to showing that $A+B^2$ has trace zero:

$$A + B^2 = \frac{1}{x+y}\left(\frac{\eta^{14}N_f(x)N_g(x) + \eta^9 N_f(x)^2 + \eta^7 N_g(x)^2}{D(x)^4}\right.$$
$$\left. + \frac{\eta^{14}N_f(y)N_g(y) + \eta^9 N_f(y)^2 + \eta^7 N_g(y)^2}{D(y)^4} + \frac{\eta^{14}N_f(x)N_g(y) + \eta^{14}N_f(y)N_g(x)}{D(x)^2 D(y)^2}\right).$$

Now $\eta^{14}N_f(x)N_g(x)+\eta^9 N_f(x)^2+\eta^9 N_g(x)^2$ simplifies to $(\eta^9 x^4+\eta^{10}x^3+\eta^9 x^2)D(x)^2$. Then the above expression, placed over a common denominator $D(x)^2D(y)^2$, becomes:

$$\frac{1}{x+y}\left(\frac{\eta^9 x^4 y^2 + \eta^{12}x^4 y + \eta^{12}x^3 y + \eta^9 x^2 y^4 + \eta^{12}x^2 y^3 + \eta^{10}x^2 y + \eta^{12}xy^4 + xy^3}{D(x)^2 D(y)^2}\right.$$
$$\left. + \frac{\eta^{10}xy^2 + \eta^9 x^4 + \eta x^3 + \eta^9 x^2 + \eta^9 y^4 + \eta^{10}y^3 + \eta^9 y^2}{D(x)^2 D(y)^2}\right).$$

We group terms together in such a way that we can divide by $(x+y)$ to get:

$$\frac{\eta^9 x^3 y^2 + \eta^9 x^2 y^3 + \eta^{12}x^3 y + \eta^{12}xy^3 + \eta^7 x^2 y + \eta^7 xy^2}{D(x)^2 D(y)^2}$$
$$+ \frac{\eta^9 x^3 + \eta^9 y^3 + \eta^{10}x^2 + \eta^{10}y^2 + \eta^9 x + \eta^9 y}{D(x)^2 D(y)^2}$$
$$= \frac{\eta^9 x + \eta^9 y}{D(x)D(y)} + \frac{\eta^3 x^2 + \eta^3 y^2}{D(x)^2 D(y)^2}.$$

Which is of the form $X + X^2$ so has trace zero. □

9.4. Existence of Subiaco q–clans, in general

THEOREM 213. *Let $d \in GF(q)$, q even, such that $d^2+d+1 \neq 0$ and $\mathrm{trace}(1/d) = 1$. Let*

$$a = \frac{d^2 + d^5 + d^{1/2}}{d(1+d+d^2)},$$
$$f(x) = \frac{d^2(x^4+x) + d^2(1+d+d^2)(x^3+x^2)}{(x^2+dx+1)^2} + x^{1/2}, \text{ and}$$
$$g(x) = \frac{d^4x^4 + d^3(1+d^2+d^4)x^3 + d^3(1+d^2)x}{(d^2+d^5+d^{1/2})(x^2+dx+1)^2} + \frac{d^{1/2}}{d^2+d^5+d^{1/2}}x^{1/2}.$$

Then

$$\boldsymbol{S} = \boldsymbol{S}_d = \left\{ A_x = \begin{pmatrix} f(x) & x^{1/2} \\ 0 & ag(x) \end{pmatrix} \;\middle|\; x \in GF(q) \right\}$$

is a q–clan.

PROOF. This proof is similar to the proof of Theorem 210, p. 149, and the proof of Theorem 211, p. 151, and the proof of Theorem 212, p. 153.

We start by showing trace$(a) = 1$ for all q even:

$$\begin{aligned}\operatorname{trace}(a) &= \operatorname{trace}(a^2)\\ &= \operatorname{trace}\left(\frac{d^9+d^3+1}{d(d^2+d+1)^2}\right)\\ &= \operatorname{trace}\left(\frac{1}{d}\right) + \operatorname{trace}\left(d + \frac{d^4}{d^2+d+1}\right) + \operatorname{trace}\left(d^2 + \frac{d^8}{(d^2+d+1)^2}\right).\end{aligned}$$

So trace$(a) =$ trace$(1/d) = 1$.

In this form the equations will become quite unwieldy, so initially we will simplify f and g to

$$f(x) = \frac{N_f(x)}{D(x)^2} + x^{1/2} \quad\text{and}\quad g(x) = \frac{1}{d^2+d^5+d^{1/2}}\frac{N_g(x)}{D(x)^2} + \frac{d^{1/2}}{d^2+d^5+d^{1/2}}x^{1/2}.$$

We now show for $GF(q)$, $q = 2^e$, that the matrices $\begin{pmatrix} f(t) & t^{1/2} \\ 0 & ag(t)\end{pmatrix}$, $t \in GF(q)$, form a q–clan. We do this by showing that $\mathcal{T}_a(f,g)$ is true. That is we show $a(f(x) + f(y))(g(x) + g(y))/(x + y)$ has trace one for all $x \neq y$. From now on we assume that $x \neq y$, so:

$$\begin{aligned}&\frac{(f(x)+f(y))(ag(x)+ag(y))}{x+y}\\ &= \frac{1}{x+y}\left(\frac{N_f(x)}{D(x)^2} + x^{1/2} + \frac{N_f(y)}{D(y)^2} + y^{1/2}\right)\left(\frac{N_g(x)}{d(1+d+d^2)D(x)^2} + \frac{d^{1/2}}{d(1+d+d^2)}x^{1/2}\right.\\ &\qquad\left. + \frac{N_g(y)}{d(1+d+d^2)D(y)^2} + \frac{d^{1/2}}{d(1+d+d^2)}y^{1/2}\right)\\ &= \frac{1}{x+y}\left(\frac{N_f(x)N_g(x)}{d(1+d+d^2)D(x)^4} + \frac{N_f(x)N_g(y)}{d(1+d+d^2)D(x)^2D(y)^2} + \frac{(x+y)^{1/2}}{d^{1/2}(1+d+d^2)}\frac{N_f(x)}{D(x)^2}\right.\\ &\qquad + \frac{N_f(y)N_g(y)}{d(1+d+d^2)D(y)^4} + \frac{N_f(y)N_g(x)}{d(1+d+d^2)D(x)^2D(y)^2} + \frac{(x+y)^{1/2}}{d^{1/2}(1+d+d^2)}\frac{N_f(y)}{D(y)^2}\\ &\qquad\left. + \frac{(x+y)^{1/2}}{d(1+d+d^2)}\frac{N_g(x)}{D(x)^2} + \frac{(x+y)^{1/2}}{d(1+d+d^2)}\frac{N_g(y)}{D(y)^2} + \frac{x+y}{d^{1/2}(1+d+d^2)}\right).\end{aligned}$$

If we let $E_1, \dots, E_8$ correspond to the first eight terms inside the brackets of the above expression, we can express the last line as

$$\begin{aligned}\frac{1}{x+y}\Big(&E_1 + E_2 + E_3\\ &+ E_4 + E_5 + E_6\\ &+ E_7 + E_8 + \frac{x+y}{d^{1/2}(1+d+d^2)}\Big).\end{aligned}$$

We will do a further substitution on the above line to obtain

$$A + B + \frac{1}{d^{1/2}(1+d+d^2)}$$

where

$$A = \frac{1}{x+y}\left(E_1 + E_2 + E_4 + E_5\right), \text{ and}$$
$$B = \frac{1}{x+y}\left(E_3 + E_6 + E_7 + E_8\right).$$

Now

$$\begin{aligned}
\operatorname{trace}\left(\frac{1}{d^{1/2}(1+d+d^2)}\right) &= \operatorname{trace}\left(\frac{1}{d(1+d^2+d^4)}\right) \\
&= \operatorname{trace}\left(\frac{1}{d}\right) + \operatorname{trace}\left(\frac{d+d^3}{1+d^2+d^4}\right) \\
&= \operatorname{trace}\left(\frac{1}{d}\right) + \operatorname{trace}\left(\frac{d}{1+d+d^2}\right) + \operatorname{trace}\left(\frac{d^2}{1+d^2+d^4}\right) \\
&= \operatorname{trace}\left(\frac{1}{d}\right) = 1.
\end{aligned}$$

So it is now left to show that $A+B$ has trace zero. Since $\operatorname{trace}(A+B) = \operatorname{trace}(A+B^2)$, this is equivalent to showing that $A+B^2$ has trace zero.

$$\begin{aligned}
A + B^2 = \frac{1}{x+y}\Bigg(&E_1 + E_2 + E_4 + E_5 + \frac{N_f(x)^2}{d(1+d^2+d^4)D(x)^4} \\
&+ \frac{N_f(y)^2}{d(1+d^2+d^4)D(y)^4} + \frac{N_g(x)^2}{d^2(1+d^2+d^4)D(x)^4} + \frac{N_g(y)^2}{d^2(1+d^2+d^4)D(y)^4}\Bigg) \\
= \frac{1}{x+y}\Bigg(&E_2 + E_5 + \frac{d(1+d+d^2)N_f(x)N_g(x) + dN_f(x)^2 + N_g(x)^2}{d^2(1+d^2+d^4)D(x)^4} \\
&+ \frac{d(1+d+d^2)N_f(y)N_g(y) + dN_f(y)^2 + N_g(y)^2}{d^2(1+d^2+d^4)D(y)^4}\Bigg).
\end{aligned}$$

After much simplification we obtain:

$$\begin{aligned}
\frac{1}{x+y}\Bigg(&E_2 + E_5 + \frac{d^5(1+d+d^2)x^8 + d^6(1+d^6)x^7 + d^5(1+d^6)x^6 + d^8(1+d^6)x^5}{d^2(1+d^2+d^4)D(x)^4} \\
&+ \frac{d^5(1+d^6)x^4 + d^6(1+d^6)x^3 + d^5(1+d+d^2)^2x^2}{d^2(1+d^2+d^4)D(x)^4} \\
&+ \frac{d^5(1+d+d^2)y^8 + d^6(1+d^6)y^7 + d^5(1+d^6)y^6 + d^8(1+d^6)y^5}{d^2(1+d^2+d^4)D(y)^4} \\
&+ \frac{d^5(1+d^6)y^4 + d^6(1+d^6)y^3 + d^5(1+d+d^2)^2y^2}{d^2(1+d^2+d^4)D(y)^4}\Bigg).
\end{aligned}$$

Using $1 + d^6 = (1 + d^2 + d^4)(1 + d^2)$ with more simplification, dividing by $D(x)^2$ (or $D(y)^2$), and then placing over a common denominator, we obtain:

$$\begin{aligned}
&\frac{1}{x+y}\Bigg(E_2 + E_5 + \frac{d^3x^8 + d^4(1+d^2)x^7 + d^3(1+d^2)x^6 + d^6(1+d^2)x^5}{D(x)^4} \\
&\qquad + \frac{d^3(1+d^2)x^4 + d^4(1+d^2)x^3 + d^3x^2}{D(x)^4} \\
&\qquad + \frac{d^3y^8 + d^4(1+d^2)y^7 + d^3(1+d^2)y^6 + d^6(1+d^2)y^5}{D(y)^4} \\
&\qquad + \frac{d^3(1+d^2)y^4 + d^4(1+d^2)y^3 + d^3y^2}{D(y)^4}\Bigg) \\
&= \frac{1}{x+y}\Bigg(E_2 + E_5 + \frac{d^3(x^4 + d(1+d^2)x^3 + x^2)D(x)^2}{D(x)^4} \\
&\qquad + \frac{d^3(y^4 + d(1+d^2)y^3 + y^2)D(y)^2}{D(y)^4}\Bigg) \\
&= \frac{1}{x+y}\Bigg(\frac{N_f(x)N_g(y)}{d(1+d+d^2)D(x)^2D(y)^2} + \frac{N_f(y)N_g(x)}{d(1+d+d^2)D(x)^2D(y)^2} \\
&\qquad + \frac{d^3(x^4 + d(1+d^2)x^3 + x^2)}{D(x)^2} + \frac{d^3(y^4 + d(1+d^2)y^3 + y^2)}{D(y)^2}\Bigg) \\
&= \frac{1}{x+y}\Bigg(\frac{d^5(1+d^3)(1+d)x^4y^3 + d^6(1+d+d^2)x^4y^2 + d^5(1+d+d^2)x^4y}{d(1+d+d^2)D(x)^2D(y)^2} \\
&\qquad + \frac{d^5(1+d^3)(1+d)x^3y^4 + d^6(1+d+d^2)x^2y^4 + d^5(1+d+d^2)xy^4}{d(1+d+d^2)D(x)^2D(y)^2} \\
&\qquad + \frac{d^5(1+d+d^2)^3x^3y^2 + d^6(1+d+d^2)x^3y + d^5(1+d)(1+d^3)xy^2}{d(1+d+d^2)D(x)^2D(y)^2} \\
&\qquad + \frac{d^5(1+d+d^2)^3x^2y^3 + d^6(1+d+d^2)xy^3 + d^5(1+d^3)(1+d)x^2y}{d(1+d+d^2)D(x)^2D(y)^2} \\
&\qquad + \frac{d^3(x^4 + d(1+d^2)x^3 + x^2)D(y)^2}{D(x)^2D(y)^2} + \frac{d^3(y^4 + d(1+d^2)y^3 + y^2)D(x)^2}{D(x)^2D(y)^2}\Bigg).
\end{aligned}$$

After some substantial simplification, dividing by $d(1+d+d^2)$ where appropriate and grouping, we obtain:

$$\begin{aligned}
&\frac{1}{x+y}\Bigg(\frac{d^3x^2y^2(x^2+y^2) + d^4x^2y^2(x+y) + d^4xy(x^3+y^3) + d^5xy(x^2+y^2)}{D(x)^2D(y)^2} \\
&\qquad + \frac{d^4(1+d^2)xy(x+y) + d^3(x^4+y^4) + d^3(x^2+y^2) + d^4(1+d^2)(x^3+y^3)}{D(x)^2D(y)^2}\Bigg).
\end{aligned}$$

We divide by $x + y$ and collect terms to obtain:

$$\begin{aligned}
&\frac{d^4x^3y + d^4xy^3 + (d^5+d^3)x^2y + (d^5+d^3)xy^2 + d^3x^3y^2 + d^3x^2y^3}{D(x)^2D(y)^2} \\
&\qquad + \frac{d^3x^3 + d^3y^3 + d^4(1+d^2)x^2 + d^4(1+d^2)y^2 + d^3x + d^3y}{D(x)^2D(y)^2}
\end{aligned}$$

$$= \frac{(d^3x + d^3y)(x^2 + dx + 1)(y^2 + dy + 1) + d^6x^2 + d^6y^2}{(x^2 + dx + 1)^2(y^2 + dy + 1)^2}$$
$$= \frac{d^3x + d^3y}{(x^2 + dx + 1)(y^2 + dx + 1)} + \frac{d^6x^2 + d^6y^2}{(x^2 + dx + 1)^2(y^2 + dy + 1)^2}.$$

Which is of the form $X + X^2$. □

We call $\boldsymbol{S}$ the **Subiaco** q–clan. We call the ovals of $H(\boldsymbol{S})$ the **Subiaco** ovals and the resulting hyperovals the **Subiaco** hyperovals. We also call the flocks $\mathcal{F}(\boldsymbol{S})$ the **Subiaco** flocks, $GQ(\boldsymbol{S})$ the **Subiaco** elation generalised quadrangles, and $\pi(\boldsymbol{S})$ the **Subiaco** translation planes.

The q–clan $\boldsymbol{S}'$ is a Subiaco q–clan for $q = 4^e$, e odd. Hence the herd of ovals $H(\boldsymbol{S}')$, the flocks of the quadratic cone $\mathcal{F}(\boldsymbol{S}')$, the elation generalised quadrangles $GQ(\boldsymbol{S}')$, and the translation planes $\pi(\boldsymbol{S}')$ from the q–clan $\boldsymbol{S}'$ are all Subiaco, for $q = 4^e$, e odd. Similarly for $\boldsymbol{S}'''$. For $q = 2^e$, where e is odd, we can let $d = 1$, hence we find $\boldsymbol{S}'' = \boldsymbol{S}_1$. This gives a family of o-polynomials of the herd $H(\boldsymbol{S}_1)$ over $GF(2)$ for $q = 2^e$, e odd.

The construction of $\boldsymbol{S}''$ for $q = 2^e$, e odd was the first Subiaco q–clan to be found. This was followed by the constructions of $\boldsymbol{S}'$ for $q = 4^e$, e odd, and $\boldsymbol{S}'''$ for $q = 16^e$, e odd. From these three constructions it was possible to generalise to construct $\boldsymbol{S}$.

10. Concluding Remarks

10.1. The Subiaco q–clans

In Chapter III it is shown that if d and d' are elements of $GF(q)$ with $\operatorname{trace}(1/d) = \operatorname{trace}(1/d') = 1$, for $q = 2^e$, then $\boldsymbol{S}_d$ is equivalent to $\boldsymbol{S}_{d'}$. In Chapter III it is shown that $\boldsymbol{S}$ is equivalent to $\boldsymbol{S}'$, for $q = 2^e$, $e \equiv 2 \pmod 4$, $e \neq 2$ and the automorphism group of $GQ(\boldsymbol{S})$ is calculated. For $q = 2$, 4, $GQ(\boldsymbol{S}) \cong H(3, q^2)$. For $q = 8$, $GQ(\boldsymbol{S}) \cong GQ(\boldsymbol{C}_2)$. For $q = 16$, $GQ(\boldsymbol{S}) \cong GQ(\boldsymbol{C}_4)$ by results of [**35**]. For $q \geq 32$, $GQ(\boldsymbol{S})$ is new, (although for $q = 32$, 64, 128, 256, they appear as computer results of Penttila and Royle [**111**]). This can be seen from the automorphism groups. Alternatively, no previously known q–clans $\boldsymbol{C}$ gave rise to a generalised quadrangle $GQ(\boldsymbol{C})$ with subquadrangle on (∞) and $(\boldsymbol{0}, 0, \boldsymbol{0})$ isomorphic to $T_2(\mathcal{O})$, for $\mathcal{O}$ a Subiaco oval. This follows from the results on the Subiaco hyperovals that follow in Section 8.4 for $q \geq 64$. For $q = 32$, note that while the Subiaco hyperovals are Payne hyperovals, the *ovals* of the Subiaco herd, $H(\boldsymbol{S})$, are not equivalent to the ovals of the Payne herd, $H(\boldsymbol{C}_3)$.

As $H(\boldsymbol{S})$ contains no ovals that give rise to regular hyperovals, by [**47, 80**] we have all the ovals being from Lunelli-Sce hyperovals for $q = 16$. Since the Subiaco 16–clan is equivalent to $\boldsymbol{C}_4$, it follows that $H(\boldsymbol{C}_4)$ consists of 17 Lunelli-Sce ovals.

10.2. The Subiaco flocks

In Chapter III it is shown that each Subiaco q–clan, $\boldsymbol{S}$, gives rise to exactly one Subiaco flock of a quadratic cone in $PG(3,q)$, up to isomorphism, by showing that the automorphism group of $GQ(\boldsymbol{S})$ is transitive on the lines on (∞). This also determines the stabiliser in $P\Gamma L(4,q)$ of the Subiaco flock in $PG(3,q)$.

10.3. The Subiaco planes

In Section 7 of [**6**] the automorphism groups of the Subiaco planes $\pi(\boldsymbol{S})$ are studied. The planes appear to be new for $q \geq 16$.

10.4. The Subiaco hyperovals

In Chapter III it is shown that all Subiaco hyperovals in $PG(2,q)$ are equivalent for $q=2^e$, $e \not\equiv 2 \pmod 4$. Also it is shown that there are two orbits in $PG(2,q)$, for $q=2^e$, $e \equiv 2 \pmod 4$.

For $q = 2$, 4, 8, the Subiaco hyperovals are regular. For $q = 16$, they are Lunelli-Sce hyperovals [**75**]. For $q = 32$, they are Payne hyperovals. For $q = 64$, they are the hyperovals discovered by Penttila and Pinneri [**107**], with groups of orders 15 and 60. For $q = 128$, 256, they are the hyperovals discovered by Penttila and Royle [**111**].

In [**87**], it is shown that the stabiliser in $P\Gamma L(3,q)$ of a Subiaco hyperoval in $PG(2,q)$ is cyclic of order $2e$, for $q=2^e$, $e \not\equiv 2 \pmod 4$. In Chapter III the stabilisers in $P\Gamma L(3,q)$ of the Subiaco hyperovals in $PG(2,q)$ for $q=2^e$, $e \equiv 2 \pmod 4$ are computed.

It is important to see how elements of the Subiaco herd intersect particular subplanes:

(i) For $q=4^e$, e odd, if $f \in H(\boldsymbol{S}')$ then $\mathcal{D}(f) \cap PG(2,4)$ is a regular hyperoval.
(ii) For $q=2^e$, e odd, if $f \in H(\boldsymbol{S}'')$ then $\mathcal{D}(f) \cap PG(2,2)$ is the fundamental quadrangle.
(iii) For $q=16^e$, e odd, if $f \in H(\boldsymbol{S}''')$ then $\mathcal{D}(f) \cap PG(2,16)$ is a Lunelli-Sce hyperoval.

11. History of the Subiaco Constructions

We end this work with a story!

In 1992 I wanted to transfer from a Masters to a PhD. In doing so I needed to expand my mathematical horizons. My supervisor, T. Penttila, thought that the connection between hyperovals and GQs should be investigated first; since it seemed to be a natural extension of my work on hyperovals. (Always in the back of our minds were the possibilities of generalising the irregular hyperovals $\mathcal{H}_{60}$ and $\mathcal{H}_{15}$ of $PG(2,64)$.) We decided that the first paper to understand was the paper [**93**] by S. Payne. It seemed to be a ground breaking paper and was virtually a text for my initial work in this new area. Of course, at the time we didn't know how influential the paper would be. I should also mention that in 1992 J. A. Thas gave the newly formed Combinatorial Computing Research Group (CCRG) a series of lectures on flocks of quadratic cones. The trace equation entered our minds and stayed there, in the background, until it was needed in a few months time. We decided the ideas of [**93**] needed to be simplified. This simplification introducted of the concept of herds — hyperovals from EGQs of order (q^2,q) — and the initial connection between flocks of quadratic cones. The concept of herd was refined to the point that we now had a more efficient way of searching for flocks of quadratic cones in $PG(3,q)$ for small q. By January 1993 these ideas allowed Penttila and Royle to verify that the only non-linear flock in $PG(3,16)$ was the one constructed by De Clerck and Herssens. Also early in 1993 Penttila and Royle constructed a new flock in $PG(3,32)$ (later to be shown to be part of the Subiaco family) and two new flocks in $PG(3,64)$; one related to the hyperovals $\mathcal{H}_{60}$ and $\mathcal{H}_{15}$ of $PG(2,64)$ and one related to the Penttila-Royle hyperoval $\mathcal{H}_{12}$ of $PG(2,64)$. The numerology of the flock related to $\mathcal{H}_{60}$ and $\mathcal{H}_{15}$ forced us to look in $PG(2,4^e)$, e odd for any possible generalisations of the hyperovals. (For the later part of 1991 and most of 1992, Penttila and myself were certain that any generalisations of $\mathcal{H}_{60}$ and $\mathcal{H}_{15}$ must be in $PG(2,q^3)$; we (vainly) looked at the case for $q = 512 = 8^3$ instead of $q = 1024 = 4^5$.) Penttila and Royle then showed that any new flocks of $PG(3,64)$ must arise from new hyperovals in $PG(2,64)$.

In Feburary of 1994 we studied the o-polynomials of $\mathcal{H}_{60}$ over $GF(4)$ and this was when we first noticed the pseudo-periodicity of the coefficients of the o-polynomial. With this information about the coefficients of the o-polynomial Penttila and myself constructed a new hyperoval in $PG(2,1024)$ with group of order 100. Penttila and Royle also classified all flocks of $PG(3,32)$ (using the classification of all hyperovals in $PG(2,32)$).

In March 1993 Penttila and Royle constructed a new hyperoval in $PG(2,128)$ stabilised by an element of order 14 (this hyperoval was later to be part of the Subiaco family). This hyperoval also had pseudo-periodicity. This lead to a new construction of a flock in $PG(2,128)$ with the related o-polynomial (the "g") also exhibiting pseudo-periodicity.

Around the beginning of the year W. Cherowitzo arrived in Perth from Denver, Colorado. Cherowitzo introduced the link between the pseudo-periodic o-polynomials and rational functions. By the end of March W. Cherowitzo proved the existence of a infinite family of flocks, hyperovals, etc. for q even but not a square (later to be part of the Subiaco family). Earlier it was noted that some of the o-polynomials of

Payne's hyperovals were pseudo-periodic, and together with the new hyperovals of $PG(2,128)$ the conjecture for the right form of the q non-square o-polynomials was found by Cherowitzo.

In April, Penttila and Royle constructed two new hyperovals in $PG(3,256)$. Penttila conjectured that a new family of hyperovals, flocks, translation planes, etc. existed for all q even and parameterised by an element of trace one, and that $x^4 + d^2x^2 + 1$ would be the denominator for the rational o-polynomials with $\mathrm{trace}(1/d) = 1$. Cherowitzo continued his tradition of naming configurations from local names. The term Subiaco (from Subiaco Oval, the football stadium in the suburb Subiaco near the University of Western Australia and having as a sister city Subiaco, Italy) came to name the infinite family of hyperovals etc, firstly for the q non square case and then for the (then conjectured) q even infinite family. This conjectured infinite family of hyperovals would include all the hyperovals found to date except $\mathcal{H}_{12}$. Penttila and Royle constructed a new flock in $PG(3,512)$ believing it to be in the Subiaco family and two new flocks in $PG(3,256)$.

In May Penttila and I found the "correct" rational function forms for the o-polynomials of $\mathcal{H}_{60}$ and $\mathcal{H}_{15}$. This then lent to the proof of an infinite family of hyperovals, flocks, translation planes, etc for $q = 4^e$, e odd, so generalising the hyperovals that we found in 1991! Penttila then generalised the De Clerck-Herssens flock, so generalising the Lunelli-Sce hyperoval of discovered in 1958, for $q = 16^e$, e odd.

Meanwhile, Cherowitzo, using his work on hyperovals of $PG(2,16)$ found the general form of the Subiaco o-polynomials and in doing so allowed for the proof of an infinite family of hyperovals, flocks etc for all q even, to be produced. (The proof was pieced together a few months later in Perth.)

It must be noted that this work was a truly collaborative effort. A special mention should go to G. Royle for his computational work that allowed the conjectures to be tested, corrected or discarded as soon as we thought of them.

12. End Notes

NOTES ON SECTION 1, P. 141. The term flock was popularised by Dembowski [**36**] in relation to inversive planes.

The results in this Section are well known.

NOTES ON SECTION 2, P. 141. The results in this Section are well known.

NOTES ON SECTION 3, P. 143. The results in this Section are well known.

NOTES ON SECTION 4, P. 143. There are two isometry classes of conics in $PG(2,q)$, q odd, (but only one class up to similarity). When extended to $GF(q)^4$

there are still two isometry classes of conics in $O^+(4,q)$ giving the two classes in Thas' construction of the Thas flocks.

The results in this Section are well known.

NOTES ON SECTION 5, P. 144. The results in this Section are well known.

NOTES ON SECTION 7, P. 146. Let $\boldsymbol{C} = \{A_t \mid t \in GF(q)\}$ be a q–clan. Fix s and let $B_t = A_t - A_s$. Let $d_t = \det(B_t + B_t^T)$ for $t \neq 0$ and let $d_0 = 1$. Let $C_t = B_t/d_t$ and $\boldsymbol{C}' = \{C_t \mid t \in GF(q)\}$. Then $\boldsymbol{C}'$ is a q–clan and corresponds to a derivation of a flock of the original flock $\mathcal{F}(\boldsymbol{C})$ [**104**]. The q choices of s give the q derived flocks. The above derivation is true for q even or odd, though there is no BLT setting for q even. (These matrices C_t are formed by hitting $\boldsymbol{C}$ with the map φ on page 107, the flip map.)

Let X be a BLT-set. The orbits of $P\mathit{\Gamma}O(5,q)_X$ on X correspond to the isomorphism classes of flocks. Also, for $x \in X$, $P\mathit{\Gamma}O(5,q)_{X,x}$ is isomorphic to the group of the flock corresponding to x.

The results in this Section are well known.

NOTES ON SECTION 8, P. 147. The results in this Section are well known.

NOTES ON SECTION 9, P. 149. The theorems in this Section appear in [**30**]. Theorem 210, p. 149, is by Cherowitzo; Theorem 211, p. 151, is by the author and Penttila; Theorem 212, p. 153, is by Penttila; and Theorem 213, p. 154, is by the author with initial work by Cherowitzo.

NOTES ON SECTION 10, P. 158. The results in this Section appear in [**30, 100, 6**].

CHAPTER V

Open Problems

Standard open problems for configurations in projective geometries are:

- Classify all ovoids of $PG(3,q)$ for q even.
- Classify all ovals of $PG(2,q)$ for q even.
- Classify all flocks of a quadratic cone of $PG(3,q)$.

BLT sets give a geometric interpretation of a GQ($\boldsymbol{C}$) arising from a flock $\mathcal{F}(\boldsymbol{C})$ for q odd.

- Is there a geometric interpretation of the GQ($\boldsymbol{C}$) arising from a flock $\mathcal{F}(\boldsymbol{C})$ for q even?

- Is every TGQ of order q isomorphic to a $T_2(\mathcal{O})$ for some oval $\mathcal{O}$?
- Is every TGQ of order (q,q^2), q even, isomorphic to a $T_3(\Omega)$ for some ovoid Ω?

At the time of writing W. Cherowitzo proved that his hyperovals form an infinite family using flocks of a translation oval cone, hence extending the link between hyperovals and flocks of cones.

- Is there a link between flocks of translation oval cones and GQs?
- Is the O'Keefe-Penttila hyperoval related to flocks of a translation oval cone?

Which leads us to more questions on the O'Keefe-Penttila hyperoval:

- Does the O'Keefe-Penttila hyperoval live in an infinite family?
- Does it have an associated algebraic curve?
- Is normalising the q–clan in a different way a possible way of generalising this hyperoval?

It should be noted that it took over 35 years to generalise the Lunelli-Sce hyperoval.

Let Ω be an ovoid of $PG(3,q)$ and let $\mathcal{O} = \Omega \cap \pi$ where π is a secant plane to Ω. Then $T_2(\mathcal{O})$ is a subquadrangle of $T_3(\Omega)$.

- Given a $T_2(\mathcal{O})$ when is it a subGQ for a $T_3(\Omega)$, for some ovoid Ω?
- Could progress be made on classifying ovoids in $PG(3,q)$ by investigating sufficient conditions for a GQ of order (q^2,q) to be an EGQ, especially a GQ admitting a 3-regular point.

Determining all types of the above embedding is equivalent to determining all secant plane sections of ovoids.

- Can a herd be characterised by some of the ovals it contains?
- Similarly, can a GQ of order (q^2, q), q even, be characterised by the subquadrangles of the form $T_2(\mathcal{O})$ it contains?

- For each flock for q even there corresponds an analogous flock for q odd, except for the Subiaco flock. Is there one for Subiaco?
- What is the connection of the use of the trace equation in [**108**] and the trace condition for q–clans.

- Are the cyclic q–clans for $q = 4^e$, $e = 3$, 4, 5, 6, 7, part of an infinite family?
- Classify all cyclic q–clans for q even.

Bibliography

[1] B. A. Anderson, *Hyperovals and Howell designs*, Ars Combin. **9** (1980), 29–38.

[2] J. André, *Über nicht-Desarguessche Ebenen mit transitiver Translationgruppe*, Math. Z. **60** (1954), 156–186.

[3] E. Assmus and J. Key, *Designs and their codes*, Cambridge University Press, 1992.

[4] L. Bader, *Some new examples of flocks of* $Q^+(3,q)$, Geom. Ded. **27** (1989), 213–218.

[5] L. Bader and G. Lunardon, *On the flocks of* $Q^+(3,q)$, Geom. Ded. **29** (1989), 177–183.

[6] L. Bader, G. Lunardon, and S. E. Payne, *On q–clan geometry* $q = 2^e$, Bull. Belgian Math. Soc. **1** (1994), 301–328.

[7] L. Bader, G. Lunardon, and J. A. Thas, *Derivation of flocks of quadratic cones*, Forum Math. **2** (1990), 163–194.

[8] R. Baer, *Polarities in finite projective planes*, Bull. Amer. Math. Soc. **52** (1946), 77–93.

[9] ———, *Projectivities with fixed points on every line of the plane*, Bull. Amer. Math. Soc. **52** (1946), 273–286.

[10] R. D. Baker and G. L. Ebert, *A non-linear flock in the Minkowski plane of order 11*, Congr. Numer. **58** (1989), 75–81.

[11] O. Barriga, *On the planes of Narayana Rao and Satyanarayana*, J. Combin. Theory (A) **45** (1987), 148–151.

[12] L. M. Batten and A. Beutelspacher, *The theory of finite linear spaces: Combinatorics of points and lines*, Cambridge University Press, 1993.

[13] C. T. Benson, *Generalized Quadrangles and* (B,N)*-pairs*, Ph.D. thesis, Cornell University, 1965.

[14] D. Betten, *4-dimensionale Translationsebenen mit 8-dimensionaler Kollineations gruppe*, Geom. Ded. **2** (1973), 327–339.

[15] M. Biliotti and G. Korchmáros, *Hyperovals with a transitive collineation group*, Geom. Ded. **24** (1987), 269–281.

[16] R. C. Bose, *Mathematical theory of the symmetrical factorial design*, Sankhyā **8** (1947), 107–166.

[17] R. C. Bose and S. S. Shrikhande, *Geometric and pseudo-geometric graphs* $(q^2+1, q+1, 1)$, J. Geometry **(2/1)** (1972), 75–94.

[18] M. R. Brown, *Generalised quadrangles of order* (q,q^2)*, q even, containing* $W(q)$ *as a subquadrangle*, (to appear).

[19] M. R. Brown, I. Pinneri, and G. F. Royle, *Generalised quadrangles of order* $(8,64)$ *with a subquadrangle of order* 8, (in preparation).

[20] B. H. Bruck and R. C. Bose, *The construction of translation planes from projective spaces*, Journal of Algebra **1** (1964), 85–102.

[21] F. Buekenhout, *Etude intrinsèque des ovales*, Rend. Mat. (5) **25** (1966), 333–393.

[22] ———, *Plans projectifs à ovoides pascaliens*, Arch. Math. **17** (1966), 333–393.

[23] ———, *On the orbits of collineation groups*, Math. Z. **119** (1971), 273–275.

[24] F. Buekenhout (ed.), *Handbook of incidence geometry*, Elsevier Science B. V., 1995.

[25] F. Buekenhout and C. Lefèvre, *Generalized quadrangles in projective spaces*, Arch. Math. **25** (1974), 540–552.

[26] J. J. Cannon, *An introduction to the group theory language CAYLEY*, Computational Group Theory (M. Atkinson, ed.), London Mathematical Society, Academic Press, 1984, pp. 145–183.

[27] W. Cherowitzo, *Alpha flocks and hyperovals*, (preprint).

[28] ———, *Hyperovals in Desarguesian planes of even order: an update*, (preprint).

[29] ———, *Hyperovals in Desarguesian planes of even order*, Annals Disc. Math. **37** (1988), 87–94.

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

[31] S. D. Cohen and M. J. Ganley, *Commutative semifields, two-dimensional over their middle nuclei*, J. Algebra **75** (1982), 373–385.

[32] J. A. Conklin and S. E. Payne, *An unusual generalized quadrangle of order 16*, J. Combin. Theory (A) **24** (1978), 50–74.

[33] C. W. Curtis and I. Reiner, *Representation thoery of finite groups and associated algebras*, Interscience, New York, 1962.

[34] N. G. de Bruijn and P. Erdös, *On a combinatorial problem*, Indagationes Math. **10** (1948), 421–423.

[35] F. De Clerck and C. Herssens, *Flocks of the quadratic cone in $PG(3,q)$ for q small*, The CAGe Report 8, Computer Algebra Group, The University of Gent, Belgium, 1992.

[36] P. Dembowski, *Finite geometries*, Springer, 1968.

[37] L. E. Dickson, *Linear groups with an exposition of the Galois field theory*, Dover, New York, 1958.

[38] M. M. Eich and S. E. Payne, *Nonisomorphic symmetric block designs derived from generalized quadrangles*, Atti Accad. Naz. Lincei Rend. **52** (1972), 893–902.

[39] G. Faina, *The B-ovals of order $q \leq 8$*, J. Combin. Theory (A) **36** (1984), 307–314.

[40] J. C. Fisher and J. A. Thas, *Flocks in $PG(3,q)$*, Math. Z. **169** (1979), 1–11.

[41] M. J. Ganley, *Central weak nucleus semifields*, Europ. J. Combin. **2** (1981), 339–347.

[42] D. G. Glynn, *Two sequences of ovals in finite Desarguesian planes of even order*, Combinatorial mathematics X: Lecture notes in mathematics (L. R. A. Casse, ed.), vol. 1036, Springer, 1983, pp. 217–229.

[43] ———, *The Hering classification for inversive planes of even order*, Simon Stevin **58** (1984), 319–353.

[44] ———, *A condition for the existence of ovals in $PG(2,q)$*, Geom. Ded. **32** (1989), 247–252.

[45] M. Hall, Jr., Mathematical reviews **14** (1953), 1008, AMS.

[46] ———, *The theory of groups*, Macmillan Company, 1959.

[47] ———, *Ovals in Desarguesian plane of order 16*, Ann. Mat. Pura Appl. **102** (1975), 159–176.

[48] ———, *Combinatorial theory*, 2 ed., Wiley, 1986.

[49] N. Hamilton, *Maximal arcs in finite projective planes and associated structures in projective spaces*, Ph.D. thesis, University of Western Australia, 1995.

[50] C. Hering, *Transitive linear groups and linear groups which contain irreducible subgroups of prime order*, Geom. Ded. **2** (1974), 425–460.

[51] ———, *Transitive linear groups and linear groups which contain irreducible groups of prime order II*, J. Algebra **93** (1985), 151–164.

[52] D. G. Higman, *Partial geometries, generalized quadrangles and strongly regular graphs*, Atti convegno di geometria e sue applicazioni (A. Barlotti, ed.), Perugia, 1971, pp. 263–293.

[53] ———, *Invariant relations, coherent configurations and generalized polygons*, Combinatorics, part 3 (M. Hall, Jr. and J. H. van Lint, eds.), vol. 57, Math. Centre Tracts, 1974, pp. 27–43.

[54] J. W. P. Hirschfeld, *Ovals in Desarguesian planes of even order*, Ann. Mat. Pura Appl. **102** (1975), 79–89.
[55] ———, *Projective geometries over finite fields*, Oxford University Press, 1979.
[56] ———, *Finite projective spaces of three dimensions*, Oxford University Press, 1985.
[57] J. W. P. Hirschfeld and J. A. Thas, *General Galois geometries*, Oxford University Press, 1991.
[58] D. R. Hughes, *Generalized incidence matrices over group algebras*, Illinois Journal of Mathematics **1** (1957), 545–551.
[59] D. R. Hughes and F. C. Piper, *Projective planes*, Graduate texts in mathematics, vol. 6, Springer-Verlag, New York, 1973.
[60] S. H. Y. Hung and N. S. Mendelsohn, *On Howell designs*, J. Combin. Theory (A) **16** (1974), 174–198.
[61] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, 1967.
[62] G. Järnefelt and P. Kustaanheims, *An observation of finite geometries*, Den Ilte Skandinaviske Matematikerkongress, Trondheim, 1949 (Johan Grundt, ed.), Tanums Forlag, Oslo, 1952, pp. 166–182.
[63] N. L. Johnson, *Flocks of hyperbolic quadrics and translation planes admitting affine homologies*, J. Geometry **34** (50–73), 50–73.
[64] W. M. Kantor, *Classical groups from a non-classical viewpoint*, Oxford Lectures 1978, Mathematical Institute, Oxford, 1979.
[65] ———, *Generalized quadrangles associated with $G_2(q)$*, J. Combin. Theory (A) **29** (1980), 212–219.
[66] ———, *Ovoids and translation planes*, Canad. J. Math. **34** (1982), 1195–1207.
[67] ———, *Some generalized quadrangles with parameters (q^2, q)*, Math. Z. **192** (1986), 45–50.
[68] G. Korchmáros, *Grappi di collineazioni transitivi sui punti di un ovale [$(q+1)$-arco] di $S_{2,q}$, q pari*, Atti. Sem. Mat. Fis. Univ. Modena **27** (1978), 89–105.
[69] C. W. H. Lam, L. Thiel, and S. Swiercz, *The non-existence of finite projective planes of order 10*, Canad. J. Math. **41** (1989), 1117–1123.
[70] C. W. H. Lam, L. Thiel, S. Swiercz, and J. McKay, *The non-existence of ovals in a projective plane of order 10*, Discrete Math. **45** (1983), 319–321.
[71] E. S. Lander, *Symmetric designs: an algebraic approach*, Cambridge Univeristy Press, 1983.
[72] S. Lang, *Algebra*, Addison-Wesley Publishing Company, 1965.
[73] M. W. Liebeck, *The finite primitive permutation groups of rank three*, Bull. London Math. Soc. **18** (1986), 165–172.
[74] H. Lüneburg, *Über projektive Ebenen, in denen jede Fahne von einer nichttrivialen Elation invariant gelassen wird*, Abh. Hamburg **29** (1965), 37–76.
[75] L. Lunelli and M. Sce, *k-archi completi nei piani proiettivi Desarguesiani di rango 8 e 16*, Tech. report, Centro di Calcoli Numerici, Politecnico di Milano, 1958.
[76] R. Mathon, *The partial geometries $pg(5, 7, 3)$*, Congr. Numer. **31** (1981), 129–139.
[77] B. D. McKay, *nauty user's guide (version 1.5)*, Department of Computer Science, Australian national University, 1990.
[78] C. M. O'Keefe, *Ovals in Desarguesian planes*, Australas. J. Combin. **1** (1990), 149–159.
[79] C. M. O'Keefe and T. Penttila, *Ovoids of $PG(3, 16)$ are elliptic quadrics*, J. Geometry **38** (1990), 95–106.
[80] ———, *Hyperovals in $PG(2, 16)$*, Europ. J. Combin. **12** (1991), 51–59.
[81] ———, *Polynomials for hyperovals of Desarguesian planes*, J. Aust. Math. Soc. (A) **51** (1991), 436–447.
[82] ———, *A new hyperoval in $PG(2, 32)$*, J. Geometry **44** (1992), 117–139.
[83] ———, *Ovoids of $PG(3, 16)$ are elliptic quadrics, II*, J. Geometry **44** (1992), 140–159.

[84] ———, *Symmetries of arcs*, J. Combin. Theory (A) **66** (1994), 53–67.

[85] C. M. O'Keefe, T. Penttila, and C. E. Praeger, *Stabilisers of hyperovals in $PG(2,32)$*, Advances in finite geometries and designs (J. W. P. Hirschfeld, D. R. Hughes, and J. A. Thas, eds.), Oxford University Press, 1991, pp. 337–351.

[86] C. M. O'Keefe, T. Penttila, and G. F. Royle, *Classification of ovoids in $PG(2,32)$*, J. Geometry **50** (1994), 143–150.

[87] C. M. O'Keefe and J. A. Thas, *Collineations of Subiaco and Cherowitzo hyperovals*, (to appear).

[88] W. F. Orr, *The Miquelian inversive plane $IP(q)$ and the associated projective planes*, Ph.D. thesis, Madison Wisc., 1973.

[89] T. G. Ostrom, *Semi-translation planes*, Trans. Amer. Math. Soc. **111** (1964), 1–48.

[90] S. E. Payne, *The Subiaco notebook.*

[91] ———, *Quadrangles of order $(s-1,s+1)$*, J. Algebra **22** (1972), 97–119.

[92] ———, *Generalized quadrangles as group coset geometries*, Congr. Numer. **29** (1980), 717–734.

[93] ———, *A new infinite family of generalized quadrangles*, Congr. Numer. **49** (1985), 115–128.

[94] ———, *q-clans e quadrangoli generalizzati*, Sem. Geom. Combin. **79** (1988), 1–16.

[95] ———, *An essay on skew translation generalized quadrangles*, Geom. Ded. **32** (1989), 93–118.

[96] ———, *Collineations of the generalized quadrangles associated with q–clans*, Annals of Disc. Math. **52** (1992), 449–461.

[97] ———, *Collineations of the Subiaco generalized quadrangles*, Bull. Belgian Math. Soc. **1** (1994), 427–438.

[98] ———, *A tensor product action on q–clan geometries with $q = 2^e$*, Linear algebra and its applications **226-228** (1995), 115–137.

[99] S. E. Payne and C. C. Maneri, *A family of skew-translation generalized quadrangles of even order*, Congr. Numer. **36** (1982), 127–135.

[100] S. E. Payne, T. Penttila, and I. Pinneri, *Isomorphisms between Subiaco q–clan geometries*, Bull. Belgian Math. Soc. **2** (1994), 197–222.

[101] S. E. Payne, T. Penttila, and G. F. Royle, *Cyclic q–clans*, (in preparation).

[102] S. E. Payne and L. A. Rogers, *Local group actions on generalized quadrangles*, Simon Stevin **64** (1990), 249–284.

[103] S. E. Payne and J. A. Thas, *Finite generalized quadrangles*, Research notes in mathematics, no. 110, Pitman Publishing, 1984.

[104] ———, *Conical flocks, partial flocks, derivation and generalized quadrangles*, Geom. Ded. **38** (1991), 229–243.

[105] T. Penttila, *The Plane Equivalence Theorem*, (in preparation).

[106] T. Penttila and I. Pinneri, *Hyperovals*, (in preparation).

[107] ———, *Irregular hyperovals in $PG(2,64)$*, J. Geometry **51** (1994), 89–100.

[108] T. Penttila and C. E. Praeger, *Ovoids and translation ovals*, (in preparation).

[109] T. Penttila and G. F. Royle, *Flocks of quadratic cones in $PG(3,q)$, q small*, (in preparation).

[110] ———, *Classification of hyperovals in $PG(2,32)$*, J. Geometry **50** (1994), 151–158.

[111] ———, *On hyperovals in small projective planes*, J. Geometry (1994), (to appear).

[112] T. Penttila, G. F. Royle, and M. K. Simpson, *Hyperovals in the known projective planes of order 16*, (preprint).

[113] F. C. Piper, *Collineation groups containing elations*, Math. Z. **92** (1966), 281–287.

[114] B. Qvist, *Some remarks concerning curves of the second degree*, Ann. Acad. Sci. Fenn. (A) **134** (1952), 4–27.

[115] R. Roth, *Collineation groups of finite projective planes*, Math. Z. **83** (1964), 409–421.

[116] B. Segre, *Ovals in a finite projective plane*, Canad. J. Math. **7** (1955), 414–416.

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

[118] ———, *Le geometrie di Galois*, Ann. Mat. Pura Appl. **48** (1959), 1–97.

[119] ———, *On complete caps and ovaloids in three dimensional Galois spaces of characteristic two*, Acta Arithm. **5** (1959), 315–332.

[120] ———, *Ovali e curve σ nei piani di Galois di caratteristica due*, Atti Accad. Naz. Lincei Rend. (8) **32** (1962), 785–790.

[121] B. Segre and U. Bartocci, *Ovali ed altre curve nei piani di Galois di caratteristica due*, Acta Arith. **8** (1971), 423–449.

[122] J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. **43** (1938), 377–385.

[123] J. J. Sylvester, *Collected mathematical papers*, Cambridge University Press, 1904.

[124] D. E. Taylor, *The geometry of the classical groups*, Sigma series in pure mathematics, no. 9, Heldermann Verlag, Berlin, 1992.

[125] J. A. Thas, *Ovoidal translation planes*, Arch. Math. **23** (1972), 110–112.

[126] ———, *Flocks of nonsingular ruled quadrics in $PG(3,q)$*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **59** (1975), 83–85.

[127] ———, *Generalized quadrangles and flocks of cones*, Europ. J. Combin. **8** (1987), 441–452.

[128] ———, *Flocks, maximal exterior sets and inversive planes*, Finite geometries and combinatorial designs (E. S. Kramer and S. S. Magliveras, eds.), AMS, 1990, pp. 187–218.

[129] ———, *Projective geometry over a finite field*, In Buekenhout [**24**], pp. 295–347.

[130] J. A. Thas and S. E. Payne, *Spreads and ovoids in finite generalized quadrangles*, Geom. Ded. **52** (1994), 227–253.

[131] J. A. Thas, S. E. Payne, and H. Gevaert, *A family of ovals with few collineations*, European J. Combin. **9** (1988), 353–362.

[132] J. Tits, *Sur la trialité ét certains groupes qui s'en déduisent*, Inst. Hautes Etudes Sci. Publ. Maths. **2** (1959), 14–60.

[133] ———, *Ovoïdes et groupes de Suzuki*, Arch. Math. **13** (1962), 187–198.

[134] O. Veblen and J. W. Young, *Projective geometry*, Ginn and Co (Blaisdell, 1965), 1916, (two volumes).

[135] M. Walker, *A class of translation planes*, Geom. Ded. **5** (1976), 133–146.

[136] H. Wielandt, *Finite permutation groups*, Academic Press, 1964.

[137] H. Zassenhaus, *Über endliche Fastkörper*, Abh. Math. Sem. Univ. Hamburg **11** (1936), 187–220.

[138] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. für Math. u. Phys. **3** (1892), 265–284.

Index