DISSERTATION

# HYPEROVALS, LAGUERRE PLANES AND HEMISYSTEMS – AN APPROACH VIA SYMMETRY

Submitted by

Luke Bayens

Department of Mathematics

In partial fulfillment of the requirements

For the Degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Spring 2013

Doctoral Committee:

Advisor: Tim Penttila

Jeff Achter
Willem Bohm
Chris Peterson

ABSTRACT

HYPEROVALS, LAGUERRE PLANES AND HEMISYSTEMS – AN APPROACH VIA SYMMETRY

In 1872, Felix Klein proposed the idea that geometry was best thought of as the study of invariants of a group of transformations. This had a profound effect on the study of geometry, eventually elevating symmetry to a central role. This thesis embodies the spirit of Klein's Erlangen program in the modern context of finite geometries – we employ knowledge about finite classical groups to solve long-standing problems in the area.

We first look at hyperovals in finite Desarguesian projective planes. In the last 25 years a number of infinite families have been constructed. The area has seen a lot of activity, motivated by links with flocks, generalized quadrangles, and Laguerre planes, amongst others. An important element in the study of hyperovals and their related objects has been the determination of their groups – indeed often the only way of distinguishing them has been via such a calculation. We compute the automorphism group of the family of ovals constructed by Cherowitzo in 1998, and also obtain general results about groups acting on hyperovals, including a classification of hyperovals with large automorphism groups.

We then turn our attention to finite Laguerre planes. We characterize the Miquelian Laguerre planes as those admitting a group containing a non-trivial elation and acting transitively on flags, with an additional hypothesis – a quasiprimitive action on circles for planes of odd order, and insolubility of the group for planes of even order. We also prove a correspondence between translation ovoids of translation generalized quadrangles arising from a pseudo-oval $\mathcal{O}$ and translation flocks of the elation Laguerre plane arising from the dual pseudo-oval $\mathcal{O}^*$.

The last topic we consider is the existence of hemisystems in finite hermitian spaces. Hemisystems were introduced by Segre in 1965 – he constructed a hemisystem of $\mathrm{H}(3,3^2)$ and rasied the question of their existence in other spaces. Much of the interest in hemisystems is due to their connection to other combinatorial structures, such as strongly regular graphs, partial quadrangles, and association schemes. In 2005, Cossidente and Penttila constructed a family of hemisystems in $\mathrm{H}(3, q^2)$, $q$ odd, and in 2009, the same authors constructed a family of hemisystem in $\mathrm{H}(5, q^2)$, $q$ odd. We develop a new approach that generalizes the previous constructions of hemisystems to $\mathrm{H}(2r-1, q^2)$, $r > 2$, $q$ odd.

TABLE OF CONTENTS

# Chapter 1

# Incidence geometry

## 1.1 Introduction

Klein's **Erlangen Program** 1872 [95] had a spectacular effect on the study of geometry, eventually elevating transformation geometry to a similar status to that of analytic geometry – for which Descartes' **La Géométrie** 1637 [2] had played a similar role – and that of synthetic geometry, for which the most influential work was Euclid of Alexandria's **Elements** ca. 300 BCE [61]. The result was the elevation of symmetry to a central role, as the third pillar of geometry, together with the older approaches of Euclid via axiomatic deduction and of Descartes via coordinates.

Symmetry plays a central role in this thesis – in the context of finite geometries. All four major aspects of the use of groups are exemplified: construction, characterisation, classification and calculation.

The first topic is hyperovals of finite Desarguesian planes, where hyperovals with a large automorphism group are classified, and where the hyperovals of Cherowitzo 1998 [43] have their automorphism groups calculated. In a process reminiscent of the use of homology groups (and of fundamental groups) in algebraic topology, this result is used to show that these hyperovals are not equivalent to any previously known. These results complete the calculation of the automorphism groups of the known hyperovals of these planes. Previous attempts to calculate the automorphism groups of the Cherowitzo hyperovals include that of O'Keefe–Thas 1996 [112] (predating the proof of their conjectured existence!) and that of Penttila–Pinneri 1999 [126], who built on the O'Keefe–Thas results to obtain an involved proof on the inequivalence result mentioned above.

The next topic is finite Laguerre planes, where the Miquelian planes are characterised via their automorphism group, in terms of a flag-transitive action and existence of a non-trivial elation, together with a slightly differing weak further hypothesis depending on the parity of the order of the plane – quasiprimitivity on circles for odd order, and insolubility of the group for even order. This result uses the full force of the classification of finite simple groups. The Miquelian planes are the classical planes, and this type of result has a long history – the corresponding result of Buekenhout–Delandtsheer–Doyen–Kleidman–Liebeck–Saxl 1990 [35] for flag-transitive linear spaces (also relying on the classification of finite simple groups) was (aptly) described by Bill Kantor in 1993 [93] in the following terms "the object is known or the group is dull". Along the way, a connection is established between flocks of Laguerre plane and ovoids of generalised quadrangles, in greater generality than in previous work of Thas 1997 [155] and Lunardon 1997 [100], largely owing to taking greater care with duality; having two constructions, one in a projective space and the other in the dual space was the key to achieving greater clarity here, rather than needing a self-dual hypothesis, as in the earlier work.

The third and final topic is that of hemisystems of finite hermitian varieties, where their construction for all ranks (in odd projective dimension and odd characteristic) is achieved by the use of an orthogonal subgroup of the corresponding unitary group, completely solving for the first time the problem posed by the great Italian geometer Beniamino Segre in 1965 [138]. (Results had earlier been obtained for projective dimensions three and five by Cossidente–Penttila 2005 [49] and 2009 [50].) Here a hemisystem is a kind of halving of the variety and finding a symmetry group admitting an appropriate halving is the key to success.

The topics are connected not only by the approach via symmetry, but also through connections with other combinatorial structures: generalised quadrangles, partial geometies, partial quadrangles, designs and strongly regular graphs to name a few. Other geometric concepts are used along the way: pseudo-ovals for the material on Laguerre planes, line spreads, Bruen's 1972 [31] representation of spreads and polarities in the material on hemisystems, for instance. But the recurring role of most importance is played by the finite classical groups, with the level of knowledge of group theory required varying greatly in the three different topics; hyperovals require only Hartley's 1928 [75] determination of the subgroups of the three-dimensional finite projective semilinear groups in characteristic two, hemisystems require a good knowledge of the subfield Aschbacher class (Aschbacher 1984 [4]) of maximal subgroups of finite projective semilinear unitary groups in even dimension and odd characteristic, while the results on Laguerre planes depend on earlier results by Bamberg–Penttila 2006 [12] on pseudo-ovals, which in turn depend on the classification of finite simple groups.

The results on the automorphism group of the Cherowitzo hyperovals go from the structures to the groups, while those on hemisystems go from groups to the structures. The characterisation and classification results on Laguerre planes and hyperovals travel in both directions.

Thus the spirit of Klein Erlangen Program is embodied in this thesis in the modern context of finite geometries, with group-theoretic knowledge leading the way to solution of long-standing problems.

## 1.2 Some examples

We will now give examples of some beautiful theorems that demonstrate connections between the different pillars of geometry. Our treatment will remain informal throughout this section; a formal discussion of many concepts appearing here will follow in subsequent sections.

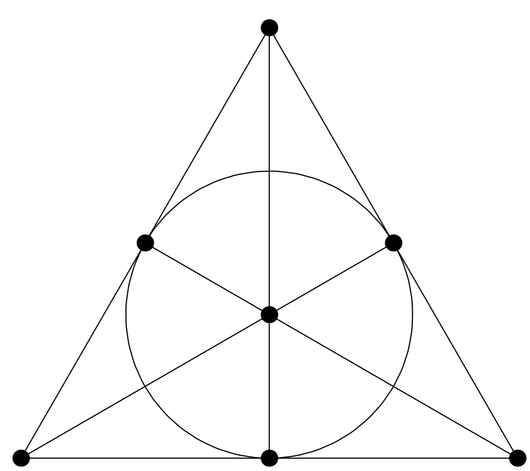

Figure 1.1: The projective plane PG(2, 2) (the Fano plane).

**Example 1.2.1** (Synthetic $\longleftrightarrow$ Analytic) A (synthetic) **projective space** is a collection of points and lines such that:

- there is a unique line through two distinct points
- every line contains at least three points
- there is at least one line
- if a line meets two sides of a triangle, not at a vertex, then the line meets the third side of the triangle.

If a synthetic projective space contains only one line it is called a (synthetic) **projective line**. A (synthetic) **projective plane** is a collection of points and lines such that:

- there is a unique line through two distincts points
- every pair of distinct lines intersect in a unique point
- there exists 4 points, no three of which are collinear.

The smallest projective plane, the so called **Fano plane**, is shown in Figure 1.1. The **classical projective space** $\mathrm{PG}(d, D)$ is the collection of subspaces of $D^{d+1}$, for a division ring $D$, and is the canonical (analytic) example of a projective space. When $D = \mathrm{GF}(q)$, the finite field of order $q$, this is denoted $\mathrm{PG}(d, q)$. The classical projective plane $\mathrm{PG}(2, D)$ is the canonical example of projective plane. The subspaces of (algebraic) dimension 1, 2, 3, and $d$, are called (projective) points, lines, planes and hyperplanes, respectively. It is common to abuse notation and denote the point $\langle(x_1, \ldots, x_{d+1})\rangle$ of $\mathrm{PG}(d, D)$ by its **homogeneous coordinates** $(x_1, \ldots, x_{d+1})$, which are defined up to multiplication by an element of $D^*$. We often think of the hyperplane $x_{d+1} = 0$ as being "at infinity", so that $\mathrm{PG}(d, D)$ consists of the **affine points** $(x_1, \ldots, x_d, 1)$, which can be identified with points of the **affine space** $\mathrm{AG}(d, D)$, together with a **hyperplane at infinity**. The affine plane $\mathrm{AG}(2, 3)$ over the finite field $\mathrm{GF}(3)$ is shown in Figure 1.2. The completion of $\mathrm{AG}(2, 3)$ to the projective plane $\mathrm{PG}(2, 3)$ by adding a points and a line at infinity is shown in Figure 1.3.

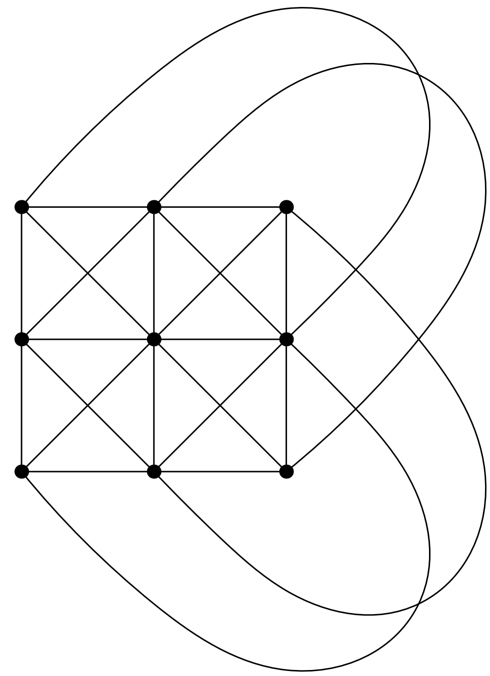

Figure 1.2: The affine plane $\mathrm{AG}(2,3)$.

So there exist simple analytic examples of synthetic projective spaces. The obvious question is whether there are others. The extent to which the synthetic axioms characterize the analytic object is addressed in the following theorem.

**Theorem 1.2.2** (Veblen–Young 1908 [171] (see also [172], [173])) *A finite-dimensional projective space is either a projective line, a projective plane, or isomorphic to* $\mathrm{PG}(d, D)$ *for some division ring* $D$.

This theorem is interesting because we get a very strong analytic conclusion out of quite weak synthetic hypotheses. We will see in the next example that we also get a great deal of symmetry from a projective space, and this is one of the attractions of incidence geometry – getting large amount of symmetry out of very few axioms.

A projective line is a trivial incidence structure, and so the question turns to the existence of non-classical projective planes. In fact, there do exist non-classical projective planes, and the question of the existence of a non-classical projective plane of non prime-power order is a famous open problem in combinatorics.

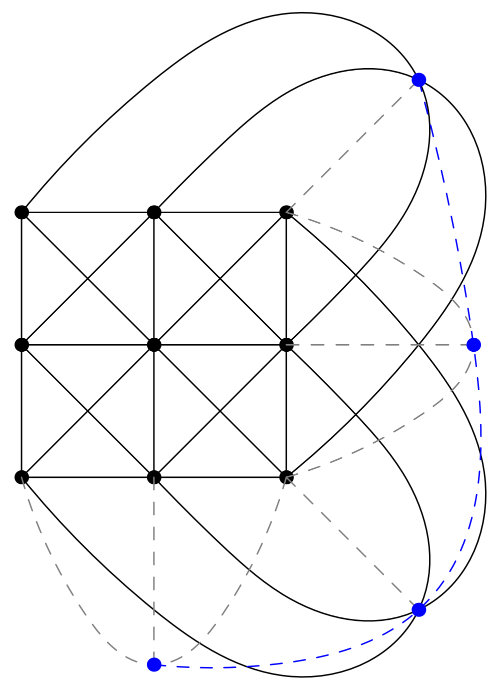

Figure 1.3: The completion of the affine plane AG$(2,3)$ to the projective plane PG$(2,3)$ by adding points at infinity and a line at infinity.

**Example 1.2.3** (Synthetic $\longleftrightarrow$ Analytic) A **triangle** in a projective plane is a set of 3 non-collinear points, and a **quadrangle** is a set of 4 points, no three collinear. Two triangles $P_1Q_1R_1$ and $P_2Q_2R_2$ are said to be **in perspective from a point** $P$ if the lines $P_1P_2$, $Q_1Q_2$, $R_1R_2$ all pass through $P$. They are **in perspective from a line** $\ell$ if the points $P_1Q_1 \cap P_2Q_2$, $Q_1R_1 \cap Q_2R_2$, $P_1R_1 \cap P_2R_2$ all lie on $\ell$.

**Theorem 1.2.4** (Desargues' Theorem 1693 [1]) *Two triangles in* PG$(2, D)$*, for a division ring* $D$*, are in perspective from a point if and only if they are in perspective from a line. This theorem is illustrated in Figure 1.4.*

**Theorem 1.2.5** (Pappas' Theorem 340 [107]) *In* PG$(2, F)$*, for a field* $F$*, if the vertices of a hexagon lie alternatingly on two lines, then the intersection of opposite sides are collinear. In other words, if* $P_1$*,* $Q_1$*,* $R_1$ *lie on a line* $\ell$ *and* $P_2$*,* $Q_2$*,* $R_2$ *lie on a line* $m \neq \ell$*, such that* $P_1Q_1P_2Q_2$ *is a quadrangle, then the points* $P_1Q_2 \cap P_2Q_1$*,* $P_1R_2 \cap P_2R_1$*,* $Q_1R_2 \cap Q_2R_1$ *are collinear. This theorem is illustrated in Figure 1.5.*

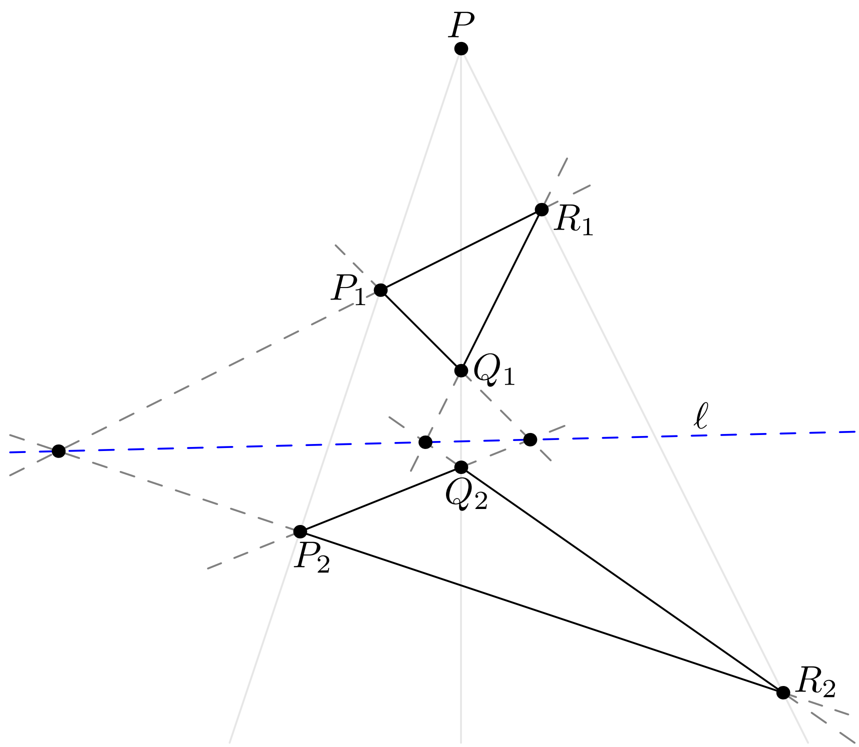


Figure 1.4: Desargues' Theorem: In $\mathrm{PG}(2, D)$, for a division ring $D$, the triangles $P_1Q_1R_1$ and $P_2Q_2R_2$ are in perspective from a point $P$ if and only if they are in perspective from a line $\ell$.

These are analytic results about certain configurations in projective planes. We can ask to what extent these configurations characterize the analytic planes. In other words, what can we say about a plane if we make the (synthetic) assumption that the Desargues or Pappas configuration holds? This question was answered by Hilbert.

**Theorem 1.2.6** (Hilbert 1899 [80]) *Desargues' configuration holds in a projective plane* $\Pi$ *if and only if* $\Pi$ *is isomorphic to* $\mathrm{PG}(d, D)$*, for some division ring* $D$*. Pappas' configuration holds in a projective plane* $\Pi$ *if and only if* $\Pi$ *is isomorphic to* $\mathrm{PG}(d, F)$*, for some field* $F$*.*

By Wedderburn 1905 [179], every finite division ring is a field, and so the finite classical projective spaces $\mathrm{PG}(d, q)$ are called **Desarguesian**.

**Example 1.2.7** (Analytic $\longleftrightarrow$ Transformation) We have seen some synthetic characterizations of the analytic Desarguesian projective spaces $\mathrm{PG}(d, q)$. If we want to study these spaces from a transformation geometry perspective, then we first need to calculate the amount of

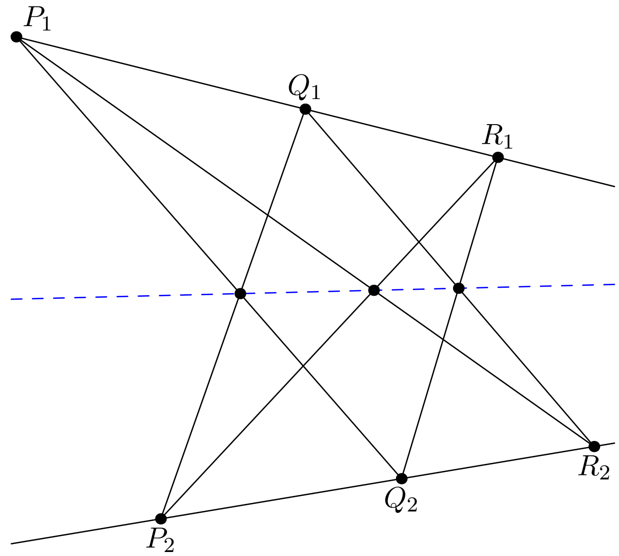


Figure 1.5: Pappas' Theorem: In $\mathrm{PG}(2, F)$, for a field $F$, if the vertices of a hexagon lie alternatingly on two lines, then the intersection of opposite sides are collinear.

symmetry these spaces contain. An **automorphism** (or **collineation**) of $\mathrm{PG}(d, q)$ is an incidence preserving bijection of the point set. We would therefore like to describe the automorphisms of $\mathrm{PG}(d, q)$. Multiplication by an invertible matrix $A$ is a linear map of the underlying vector space $\mathrm{GF}(q)^{d+1}$ that preserves inclusion of subspaces, and we can also think of this matrix as acting on the projective space by multiplication on the homogeneous coordinates of points in $\mathrm{PG}(d, q)$. However, this means that our matrix is only defined up to multiplication by an element of $\mathrm{GF}(q)^*$. Thus, we know the group $\mathrm{PGL}(d+1, q) = \mathrm{GL}(d+1, q)/Z$, where $Z = \{\lambda I : \lambda \in \mathrm{GF}(q)^*\}$, is a subgroup of $\mathrm{Aut}\,\mathrm{PG}(d, q)$. The elements of $\mathrm{PGL}(d, q)$ are called **homographies**. However, these are not the only symmetries of $\mathrm{PG}(d, q)$. A map of the form $x \mapsto x^\alpha$, for $\alpha \in \mathrm{Aut}\,\mathrm{GF}(q)$, is also an automorphism of $\mathrm{PG}(d, q)$; these are the **automorphic collineations**. The composition of an automorphic collineation with a homography is clearly an automorphism, and this leads to the group $\mathrm{P\Gamma L}(d+1, q) = \{x \mapsto Ax^\alpha : A \in \mathrm{PGL}(d+1, q),\ \alpha \in \mathrm{Aut}\,\mathrm{GF}(q)\}$. It turns out that any symmetry of $\mathrm{PG}(d, q)$ has this form.

**Theorem 1.2.8** (The Fundamental Theorem of Projective Geometry) *For $d \geq 2$,* $\mathrm{Aut}\,\mathrm{PG}(d, q) = \mathrm{P\Gamma L}(d+1, q)$.

**Example 1.2.9** (Synthetic $\longleftrightarrow$ Transformation) The last bridge we will consider between the three pillars concerns the relationship between the existence of particularly nice symmetries of finite projective planes and the existence of particularly nice synthetic configurations. First, we need to decide which properties collineations make them desirable to study from this point of view. One possibility is that the collineations fix a lot of points and lines. A **central collineation** (or **perspectivity**) of a projective plane is an automorphism that fixes a point (the **center**) linewise and a line (the **axis**) pointwise. The perspectivities are the non-trivial homographies fixing the maximum number of points, and are thus a natural class of symmetries to study. Given a point $P$ and a line $\ell$ in a projective plane $\Pi$, we say that $\Pi$ is $(P, \ell)$**-transitive** if for any line $m \neq \ell$, the group of perspectivites with center $P$ and axis $\ell$ acts transitively on the points of $m$ not on $\ell$, and not equal to $P$. If $\Pi$ is $(P, \ell)$-transitive for all $V$ on $\ell$, then $\ell$ is a **translation line**, and $\Pi$ is a **translation plane**. A $(P, \ell)$-transitive plane is considered to be highly symmetric.

It turns out that $(P, \ell)$-transitivity is related to a variation of the Desargues configuration described above. Given a point $P$ and line $\ell$ in a projective plane $\Pi$, we say that $\Pi$ is $(P, \ell)$**-Desarguesian** if whenever the triangles $P_1Q_1R_1$ and $P_2Q_2R_2$ are in perspective from $P$, and both $P_1Q_1 \cap P_2Q_2$ and $Q_1R_1 \cap Q_2R_2$ lie on $\ell$, then so does $P_1R_1 \cap P_2R_2$, that is, the triangles $P_1Q_1R_1$ and $P_2Q_2R_2$ are in perspective from a line.

**Theorem 1.2.10** (Baer 1946 [7]) *A projective plane is $(P, \ell)$-transitive if and only if it is $(P, \ell)$-Desarguesian.*

Again, this theorem is of considerable interest because we get large amounts of symmetry out of a fairly weak synthetic assumption. It is also of some historical importance because it elevated the transformation geometry perspective to be on equal footing with the synthetic and analytic pillars for the first time.

In this thesis we approach geometry from each of these perspectives. Hyperovals in $\mathrm{PG}(2, q)$ are defined synthetically as subsets of an analytic projective space, and we obtain results about their automorphism groups. The classical Laguerre planes are analytically defined, and we give a group-theoretic characterization. Finally, we use the automorphism group of an analytic hermitian space to construct synthetically defined hemisystems. We therefore demonstrate the interplay between the various pillars of geometry. In the remaining sections we will define these terms properly, survey the existing literature, and provide some motivation and context to the aforementioned results.

## 1.3 Projective spaces and forms

An **incidence structure** is a triple $(X, t, I)$, where $X$ is a set, $t$ is a function with domain $X$, and $I$ is a symmetric relation on $X$, such that $x\,I\,y$ and $t(x) = t(y)$ implies $x = y$. We think of $X$ as the **objects** of our incidence structure, $t(x)$ as the **type** of $x$, and $I$ as the **incidence relation** on $X$.

**Example 1.3.1** Let us describe formally the projective spaces mentioned earlier. Let $V$ be a finite-dimensional vector space of dimension $d + 1$ over the finite field $\mathrm{GF}(q)$. Let $X$ be the set of proper, non-trivial subspaces of $V$, $t(U) = \dim U$, with incidence defined by symmetrized inclusion. The resulting incidence structure is the **projective geometry** $\mathcal{P}V = \mathrm{PG}(d, q)$. The one-dimensional subspaces are called (projective) **points**, and the two-dimensional subspaces are the (projective) **lines**. When $d = 2$ we have the **projective plane** $\mathrm{PG}(2, q)$.

A **correlation** of $(X, t, I)$ is a bijection $\sigma : X \to X$ such that $x\,I\,y$ if and only if $x^\sigma\,I\,y^\sigma$ and $t(x) = t(y)$ if and only if $t(x^\sigma) = t(y^\sigma)$. In other words, a correlation is a bijection that restricts appropriately with respect to type and preserves incidence. Correlations of $\mathcal{P}V$ fall into two classes – those that preserve inclusion are **collineations** and those that reverse inclusion are **dualities**. A duality of the Fano plane is shown in Figure 1.6.

**Example 1.3.2** In $\mathcal{P}V$, the map

$$\Delta : (a_1, \dots, a_d) \longmapsto \{(x_1, \dots, x_d) : a_1x_1 + \cdots + a_dx_d = 0\}$$

is a duality (the **standard duality**).

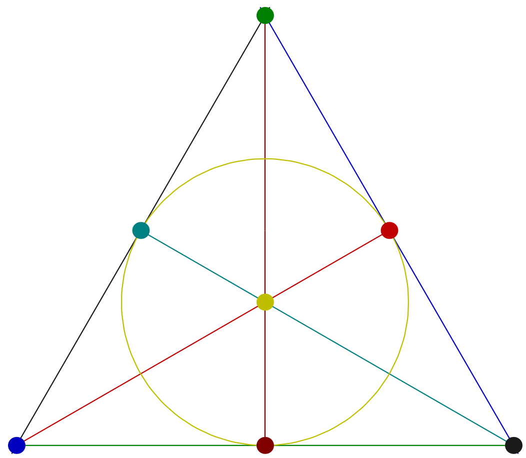

Figure 1.6: A duality of the Fano plane. The image of a point (line) under the duality is the line (point) of the same color.

**Example 1.3.3** Let $F = \mathrm{GF}(q)$, $V = F^{d+1}$, $A \in \mathrm{GL}(d+1,q)$ , $\alpha \in \mathrm{Aut}\, F$. Let $\beta$ be the function defined by $\beta : V \times V \to F$, $\beta(x,y) = x^t A y^\alpha$. Then $\beta$ is a **sesquilinear form**, that is, $\beta$ is linear in the first variable and semilinear in the second variable. The matrix $A$ is the **Gram matrix** of $\beta$. The form is **non-degenerate** in the sense that its **radical**, $\mathrm{rad}(\beta) = \{v \in V : \beta(u,v) = 0 \text{ for all } u \in V\}$ is trivial. For $U \leq V$, define $U^\perp = \{v \in V : \beta(u,v) = 0 \text{ for all } u \in U\}$. Then the map $U \mapsto U^\perp$ is a duality of $\mathcal{P}\,V$.

Hence, non-degenerate sesquilinear forms on $V$ induce dualitites on $V$. Birkhoff and Von-Neumann proved that the converse also holds.

**Theorem 1.3.4** (Birkhoff–Von-Neumann 1936 [20]) *Every duality of $\mathcal{P}\,V$ is induced by a non-degenerate sesquilinear form on $V$.*

Sesquilinear forms and dualities provide a rich source of examples of interesting incidence structures. We will therefore devote some time to exploring this connection. The most important dualities of $\mathcal{P}\,V$ are the dualities of order 2, these are the **polarities** of $\mathcal{P}\,V$. A subspace of $\mathcal{P}\,V$ contained in its image under a polarity is an **absolute** subspace with respect to that polarity. A polarity with the property that all points are absolute is a **null** polarity. A polarity with the property that no points are absolute is a **conull** polarity. It is natural to ask which non-degenerate sesquilinear forms induce polarities. It turns out that such a form $\beta$ is **reflexive**, that is, $\beta$ satisfies the condition $\beta(x, y) = 0$ if and only if $\beta(y, x) = 0$. It turns out that the reflexive, non-degenerate sesquilinear forms fall into three classes.

**Theorem 1.3.5** (Dickson 1901 [58]) *Up to scalar multiple, a non-degenerate, reflexive, sesquilinear form $\beta$ on a vector space $V$ over the finite field $\mathrm{GF}(q)$ is either:*

- **symmetric bilinear** – $\beta(u, v) = \beta(v, u)$ *for all* $u, v \in V$
- **alternating** – $\beta(u, u) = 0$ *for all* $u \in V$*, or*
- **hermitian** – $\beta(u, v) = \beta(v, u)^\alpha$ *for all* $u, v \in V$*, where* $\alpha \in \mathrm{Aut}\,\mathrm{GF}(q)$ *has order* 2*, and* $q$ *is square.*

A vector space with an alternating form is a **symplectic space**, and the polarity arising from this space is called a **symplectic polarity** (this is an example of a null polarity). However, in characteristic 2, an alternating bilinear form is also symmetric, whereas a symmetric bilinear form need not be alternating. In order to distinguish these cases, over a field of characteristic 2, we call a polarity **symplectic** (or **null**) if it arises from an alternating symmetric bilinear form as above, and **pseudo-symplectic** if it arises from a non-alternating symmetric bilinear form. Over fields of odd characteristic, a vector space with a symmetric bilinear form is an **orthogonal space**, and it gives rise to an **orthogonal polarity**. A vector space (over any field) with a hermitian form is called a **unitary space**, and it gives rise to a **unitary polarity**. These names correspond to the classical groups described in Section 1.7.

A map $Q : V \to F$ satisfying $Q(\lambda v) = \lambda^2 v$, for all $v \in V$, for all $\lambda \in F$, and such that $\beta_Q(u, v) = Q(u + v) - Q(u) - Q(v)$ is bilinear, is called a **quadratic form**, and $\beta_Q$ is the **polarization** of $Q$. A quadratic form is **non-degenerate** if its **singular radical**, $\mathrm{singrad}(Q) = \{v \in \mathrm{rad}(\beta_Q) : Q(v) = 0\}$ is trivial. If the characteristic of $F$ is odd, then each of $Q$ and $\beta_Q$ determines the other, and the study of quadratic forms is equivalent to the study of symmetric bilinear forms. However, in even characteristic, a vector space with a quadratic form has an alternating polarization, and is therefore symplectic, but not pseudo-symplectic.

Moreover, the quadratic form $Q$ cannot be recovered from the polarization $\beta_Q$, indeed, many quadratic forms correspond to the same polarization. For this reason we do not consider vector spaces with symmetric bilinear forms, except when they arise as polarizations of some quadratic form. Hence, in characteristic 2, an **orthogonal space** is a vector space with a quadratic form (with a necessarily alternating polarization). Thus, in even characteristic, we exclude the possibility of a pseudo-symplectic form. There is no loss of generality as far as geometery is concerned, since it turns out that the geometry arising from a pseudo-symplectic form is isomorphic to the geometry arising from an alternating form over a vector space of smaller dimension.

It is also possible to classify quadratic forms, but we need to introduce the appropriate concepts of equivalence of vector spaces equipped with such forms. Let $V$ and $V'$ be vector spaces over a field $F$, with respective quadratic forms $Q$ and $Q'$. A linear bijection $g : V \to V'$ is an **isometry** if $Q'(gv) = Q(v)$, for all $v \in V$, and a **similarity** if $Q'(gv) = \lambda Q(v)$, for all $v \in V$, for some fixed $\lambda \in F^*$. If an isometry, respectively similarity, exists between $(V, Q)$ and $(V', Q')$, we call the forms **isometric**, respectively **similar**. We will return to these concepts in Section 1.7.

**Theorem 1.3.6** (Dickson 1901 [58]) *Let $V$ be a finite-dimensional vector space over the finite field $\mathrm{GF}(q)$, and let $x = (x_1, \ldots, x_d) \in V$. A non-degenerate quadratic form $Q$ on $V$ is isometric to exactly one of the following forms:*

- **plus type** – $Q(x) = x_1x_2 + \cdots + x_{2n-1}x_{2n}$
- **blank type I** – $Q(x) = x_1x_2 + \cdots + x_{2n-1}x_{2n} + x_{2n+1}^2$, *for $q$ even*
- **blank type II**– $Q(x) = x_1x_2 + \cdots + x_{2n-1}x_{2n} + \eta x_{2n+1}^2$, *where $\eta$ is a non-square in $F$, and $q$ is odd, or*
- **minus type** – $Q(x) = x_1x_2 + \cdots + x_{2n-1}x_{2n} + x_{2n+1}^2 + ax_{2n+1}x_{2n+2} + bx_{2n+2}^2$, *where $x^2 + ax + b$ is irreducible over $\mathrm{GF}(q)$.*

*Note that blank type I and blank type II are similar forms, but not isometric forms.*

## 1.4 Polar spaces

We can use reflexive sesquilinear and quadratic forms to build an important class of incidence structures. Let $V$ be a vector space of dimension $d+1$ together with either an alternating, hermitian, or quadratic form. In each case we have both a reflexive sesquilinear form $\beta$ in two variables and a quadratic form $Q$ in one variable – either $Q$ is defined by $Q(v) = \beta(v, v)$, or $\beta$ is obtained by polarizing $Q$ – and we can make use of both forms. A subspace of $V$ on which $\beta$ vanishes identically is called **totally isotropic**, while a subspace of $V$ on which $Q$ vanishes identically is called **totally singular**. Alternatively, a subspace $U$ is totally isotropic if $U \subseteq U^{\perp}$, that is, if $U$ is absolute with respect to the polarity induced by $\beta$. A totally singular subspace is totally isotropic, but not conversely. In the case of alternating forms, every subspace is totally singular. The set of totally singular points of a quadratic form is called a **quadric**. We say a quadric is non-degenerate if the quadratic form defining it is non-degenerate.

**Example 1.4.1** Let $\beta$ be an alternating or hermitian form on $\mathrm{GF}(q)^{d+1}$, and let $\rho$ be the polarity induced by $\beta$ on $\mathrm{PG}(d, q)$. Let $\Pi(\rho) = (X, t, I)$ be the incidence structure where $X$ is the set of all totally isotropic subspaces of $\beta$ (equivalently, the absolute subspaces of $\rho$), $t(U) = \dim U$, with incidence defined by symmetrized inclusion Then $\Pi(\rho)$ is a polar space. Similarly, let $Q$ be a quadratic form on $\mathrm{GF}(q)^{d+1}$, $d \geq 3$, and let $\mathscr{Q}$ be the associated quadric. Let $\Pi(\mathscr{Q}) = (X, t, I)$ be the incidence structure where $X$ is the set of all totally singular subspaces of $Q$, $t(U) = \dim U$, with incidence defined by symmetrized inclusion. Then $\Pi(\mathscr{Q})$ is a polar space. Polar spaces of this form are the **classical polar spaces**.

A polar space arising from an alternating form (symplectic polarity) is a **symplectic space**, denoted $\mathrm{W}(d, q)$, a polar space arising from a hermitian form (unitary polarity) is called a **unitary space**, denoted[1] $\mathrm{H}(d, q^2)$, and a polar spaces arising from a quadratic

[1] Since hermitian forms can only occur over fields of square order, we adopt the convention that $\mathrm{H}(d, q^2)$ refers to the geometry arising from a vector space of dimension $d+1$ over the finite field $\mathrm{GF}(q^2)$. Some

form is an **orthogonal space**, either **hyperbolic**, **parabolic**, or **elliptic**, accordingly as the quadratic form is of plus, blank, or minus type, denoted $Q^+(d,q)$, $Q(d,q)$, $Q^-(d,q)$, respectively. This information is summarized in Table 1.1. The symplectic space $W(3,2)$ is shown in Figure 1.7.

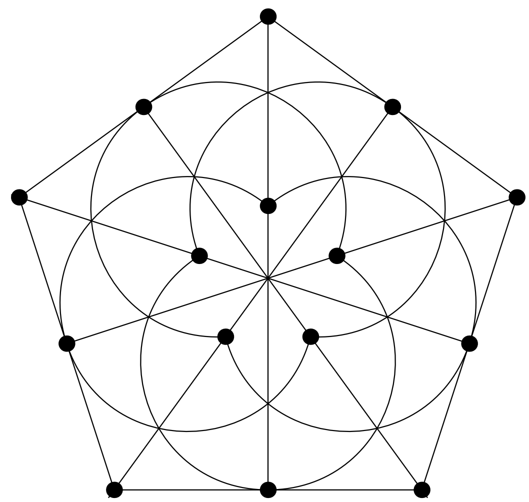

Figure 1.7: The symplectic polar space $W(3,2)$, a generalized quadrangle of order 2.

The **rank** of a classical polar space is the largest dimension of any totally isotropic or totally singular subspace. A **maximal** is a totally isotropic or totally singular subspace contained in no other. We use the terms point, line, and so on, in the same way as for projective spaces. Polar spaces describe the geometry of a vector space carrying a reflexive sesquilinear form or quadratic form in the same way that projective spaces describe the geometry of vector spaces.

It is also possible to give a synthetic treatment of polar spaces. The first set of synthetic axioms are due to Tits 1974 [166] building on work of Veldkamp 1959 [174] (see also Veldkamp 1962 [175]) . They defined an abstract polar space of rank $r$ as a set of points together with a distinguished set of subsets called **subspaces** such that

---

authors use the convention that $H(d,q)$ refers to the geometry arising from a vector space over the finite field $GF(q^2)$.

Table 1.1: The classical polar spaces arising from a vector space and a either a reflexive sesquilinear form or a quadratic form.

| Form | Geometry | Notation |
|---|---|---|
| alternating | symplectic | $\mathrm{W}(d, q)$ |
| hermitian | unitary | $\mathrm{H}(d, q^2)$ |
| quadratic (plus) | hyperbolic | $\mathrm{Q}^+(d, q)$ |
| quadratic (blank) | parabolic | $\mathrm{Q}(d, q)$ |
| quadratic (minus) | elliptic | $\mathrm{Q}^-(d, q)$ |

- any subspace together with the subspaces it contains is a projective space of dimension at most $r - 1$
- the intersection of two subspaces is a subspace
- given a subspace $U$ of dimension $r - 1$ and a point $P$ not in $U$, there exists a unique subspace $M$ containing $P$ such that $U \cap M$ has dimension $r - 2$ and $M$ contains all points of $U$ collinear with $P$
- there exist two disjoint subspaces of dimension $r - 1$.

These axioms were simplified by Buekenhout and Shult 1974 [36] who provided a set of axioms for a polar space in terms of only the points and lines, from which all other subspaces could be reconstructed. They define a **synthetic polar space** as an incidence structure with two types (points and lines), with incidence satisfying the following axioms:

- every pair of distinct points are incident with at most one line
- every line is incident with at least 3 points, and every point is incident with least 3 lines
- no point is collinear with all points
- given a line $\ell$ and a point $P$ not on $\ell$, $P$ is collinear with one or all points incident with $\ell$.

We can also give synthetic definitions of previously analytic concepts in terms of only the points and lines of the Buekenhout–Schult axioms. A **subspace** of a (synthetic) polar space is a set of points $U$ such that for every pair of distinct collinear points $P, Q \in U$, the line incident with $P$ and $Q$ is contained in $U$. A subspace $U$ is **singular** if every pair of distinct points in $U$ are collinear. The **rank** of a (synthetic) polar space is the length of a maximal chain of singular subspaces. A **maximal** is a singular subspace contained in no other singular subspace. Of course, the canonical examples of synthetic polar spaces are the classical polar spaces. The interesting question is whether there are synthetic polar spaces that are non-classical. The following theorem addresses part of this question.

**Theorem 1.4.2** (Buekenhout–Shult 1974 [36]) *A finite polar space of rank $r \geq 3$ is classical.*

This leaves open the question of non-classical rank 2 polar spaces. A rank 2 polar space is a **generalized quadrangle**. Generalized quadrangles will be studied in Section 1.5.

## 1.5 Generalized quadrangles

In previous sections we have seen an analogy between projective spaces and polar spaces. In particular, Theorem 1.2.2 and Theorem 1.4.2 characterize these spaces in a canonical way with one exception – the dimension 2 projective spaces and the rank 2 polar spaces behave differently to the others. Each of these exceptions is a point/line incidence structure, and we can connect the two by viewing these incidence structures in a wider setting. We will see that generalized quadrangles (along with the various generalizations in terms of partial geometries) are connected to all of the structures appearing in this thesis – often in multiple ways – and it is therefore worth devoting some time to an exposition of some of their most important properties, and a discussion of the vast number of connections to other combinatorial objects.

### 1.5.1 Generalized polygons

Let $\mathscr{I} = (\mathcal{P}, \mathcal{L}, I)$ be a point/line incidence structure, with the set of points $\mathcal{P}$, and lines $\mathcal{L}$, with $\mathcal{P} \cap \mathcal{L} = \phi$, and $I \subseteq \mathcal{P} \times \mathcal{L}$ defining incidence. Note that the incidence graph of

$\mathscr{I}$ is bipartite; this motivates the definition of a nice class of incidence structures known as **generalized polygons**. A **generalized $n$-gon**, $n \geq 3$, is a bipartite graph of diameter $n$ and girth $2n$. We call a generalized $n$-gon **thick** if the degree of each vertex is at least 3. Generalized polygons were introduced by Tits 1959 [164] while studying finite simple groups of Lie type in prime characteristic.

**Example 1.5.1** (Tits 1959 [164]) Consider an incidence structure $\mathscr{I} = (\mathcal{P}, \mathcal{L}, I)$. An element $(\mathcal{P}, \mathcal{L})$ of $I$ is a **flag**. If a subgroup $G$ of automorphisms of $\mathscr{I}$ acts transitively on the set of flags, then $G$ is **flag-transitive**. Now suppose that $H$ and $K$ are subgroups of some group $G$. Take $\mathcal{P} = (G : H)$ to be the set of cosets of $H$ in $G$, and $\mathcal{L} = (G : K)$ to be the set of cosets of $K$ in $G$, and $I = \{(gH, \ell K) \subseteq \mathcal{P} \times \mathcal{L} : gH \cap \ell K \neq \phi\}$ to be non-empty intersection of cosets. Then $\mathscr{I} = (\mathcal{P}, \mathcal{L}, I)$ is an incidence structure on which the subgroup $G$ of automorphisms acts flag-transitively. Tits 1956 [163] proved the remarkable fact is that every flag-transitive incidence structure is of this form for some group $G$.

Flag-transitivity will be studied in the context of Laguerre planes in Chapter 3. We can use the construction of Example 1.5.1 to obtain flag-transitive generalized polygons from groups of Lie type of Lie rank 2.

**Example 1.5.2** (Tits 1959 [164]) Let $G$ be a finite simple group of Lie type in characteristic $p$, for prime $p$. Let $U$ be a Sylow $p$-subgroup of $G$, and let $B = N_G(U)$ be the normalizer of $U$ in $G$. Let $M_1, \ldots, M_r$ be the maximal subgroups of $G$ containing $B$. Then $r$ is the Lie rank of $G$ and if $r = 2$, the incidence structure with points $(G : M_1)$, and lines $(G : M_2)$, with incidence as nonempty intersection, is a flag-transitive generalized polygon. The generalized polygons arising are essentially the classical examples in each class. For example, the generalized triangles arising from $\mathrm{PSL}(3, q)$ are the Desarguesian projective planes $\mathrm{PG}(2, q)$, and the generalized quadrangles appearing are the classical rank 2 polar spaces. When $r > 2$, we obtain the finite Desarguesian projective spaces of dimension $r$ and the finite classical polar spaces of dimension $r$.

It is not hard to see that generalized triangles are precisely projective planes, or that generalized quadrangles are precisely the rank 2 polar spaces. We have already seen examples of both of these generalized polygons. It is natural to ask which values of $n$ give generalized $n$-gons. The answer to this problem lies in the following result.

**Theorem 1.5.3** (Feit–Higman 1964 [62]) *A finite, thick, generalized $n$-gon exists if and only if $n = 3, 4, 6,$ or $8$.*

For a comprehensive guide to generalized polygons, see Van Maldeghem 1998 [170]. We will now focus our attention on generalized quadrangles.

### 1.5.2 Rank 2 polar spaces

We have seen that we can view generalized quadrangles as either the rank 2 polar spaces, or as generalized $n$-gons with $n = 2$. We can also describe generalized quadrangles synthetically as follows. A (finite) **synthetic generalized quadrangle** $X = (\mathcal{P}, \mathcal{L}, I)$ is a point/line incidence structure such that there exist positive integers $s$ and $t$ such that

- each point is incident with $t + 1$ lines
- each line is incidenct with $s + 1$ points
- two distinct points are incident with at most one line
- two distinct lines are incident with at most one point
- given a line $\ell$ and a point $P$ not on $\ell$, there is a unique point on $\ell$ collinear with $P$.

We say that $X$ has **order** $(s, t)$, and if $s = t$, we say that $X$ has order $s$. The point/line dual of a generalized quadrangle of order $(s, t)$ is a generalized quadrangle of order $(t, s)$. For $P, Q \in \mathcal{P}$ we often write $P \sim Q$ when $P$ and $Q$ are collinear. We also define $P^\perp = \{R \in \mathcal{P} : R \sim P\}$, $\{P, Q\}^\perp = P^\perp \cap Q^\perp$, and $\{P, Q\}^{\perp\perp} = \bigcap_{R \in \{P,Q\}^\perp} R^\perp$. If $P \nsim Q$, we call $\{P, Q\}^{\perp\perp}$ a **hyperbolic line** of $X$. A point $P \in \mathcal{P}$ is **regular** if $\left|\{P, Q\}^{\perp\perp}\right| = t + 1$ for all $Q \nsim P$.

We are interested in various spectral questions about generalized quadrangles. The first result of this kind is due to Higman.

**Theorem 1.5.4** (Higman 1974 [79]) *In a generalized quadrangle of order* $(s,t)$ *with* $s,t > 1$*, we have* $s \leq t^2$*, and dually* $t \leq s^2$*.*

**Example 1.5.5** The following classical polar spaces are generalized quadrangles. These are the **classical generalized quadrangles**.

(1) $\mathrm{W}(3,q) = \Pi(\rho)$, where $\rho$ is a symplectic polarity of $\mathrm{PG}(3,q)$, is a generalized quadrangle of order $q$

(2) $\mathrm{Q}^+(3,q) = \Pi(\mathscr{Q})$, where $\mathscr{Q}$ is a hyperbolic quadric of $\mathrm{PG}(3,q)$, is a generalized quadrangle of order $(q,1)$

(3) $\mathrm{Q}(4,q) = \Pi(\mathscr{Q})$, where $\mathscr{Q}$ is a parabolic quadric of $\mathrm{PG}(4,q)$, is a generalized quadrangle of order $q$

(4) $\mathrm{Q}^-(5,q) = \Pi(\mathscr{Q})$, where $\mathscr{Q}$ is a elliptic quadric of $\mathrm{PG}(5,q)$, is a generalized quadrangle of order $(q,q^2)$

(5) $\mathrm{H}(3,q^2) = \Pi(\rho)$, where $\rho$ is a unitary polarity of $\mathrm{PG}(3,q^2)$, is a generalized quadrangle of order $(q^2,q)$

(6) $\mathrm{H}(4,q^2) = \Pi(\rho)$, where $\rho$ is a unitary polarity of $\mathrm{PG}(4,q^2)$, is a generalized quadrangle of order $(q^2,q^3)$

Note that $\mathrm{Q}^+(3,q)$ is a thin generalized quadrangle, and is therefore considered trivial as a point/line incidence structure (having the structure of a grid). However, as a quadric, $\mathrm{Q}^+(3,q)$ is still associated with many interesting combinatorial objects (see, for example Section 3.2.2). The following results answer some questions about isomorphisms between the classical generalized quadrangles.

**Theorem 1.5.6** (Benson 1970 [16]) *A generalized quadrangle* $X$ *is isomorphic to* $\mathrm{W}(3,q)$ *if and only if all points of* $X$ *are regular.*

**Theorem 1.5.7** (Payne–Thas 1984 [121]) *The dual of* $\mathrm{Q}(4,q)$ *is isomorphic to* $\mathrm{W}(3,q)$*. The dual of* $\mathrm{Q}^-(5,q)$ *is isomorphic to* $\mathrm{H}(3,q^2)$*.*

**Theorem 1.5.8** (Payne–Thas 1984 [121]) $Q(4,q)$ *is isomorphic to* $W(3,q)$ *if and only if* $q$ *is even.*

Some of the first examples of non-classical generalized quadrangles were given by Tits, and first appeared in Dembowski 1968 [55]. They arise by generalizing certain properties of the classical generalized quadrangles. In order to make sense of this, we first need to introduce some fundamental structures in low dimensional projective spaces.

An **oval** of $PG(2,q)$ is a set of $q+1$ points such that no 3 points are collinear. Ovals will be studied intensively in Chapter 2. The canonical example of an oval in $PG(2,q)$ is the set of zeroes of a non-degenerate homogeneous quadratic polynomial in three variables over $GF(q)$. Such a set is called a **conic**, however there are many examples of ovals that are not conics, and these will be discussed at some length in Section 2.2.

**Example 1.5.9** Let $P$ be a point of $Q(4,q)$. Project $P$ onto a hyperplane $PG(3,q)$ not on $P$. Then $P^{\perp} \cap PG(3,q)$ is a plane $\pi$. The lines through $P$ project a conic $\mathcal{C}$ of $\pi$. Each line through $P$ not in $P^{\perp}$ is secant to the parabolic quadric $\mathscr{Q}$ defining $Q(4,q)$, so the points not collinear with $P$ project the whole of $PG(3,q) \setminus \pi$. The lines not on $P$ project to lines $\ell$ of $PG(3,q)$ with $\ell \cap \pi$ a point of $\mathcal{C}$. The points collinear with $P$ are in one-to-one correspondence with their tangent spaces, which project to planes $\pi'$ meeting $\pi$ in a tangent line to $\mathcal{C}$.

Since an oval is a conic, the above discussion motivates the following construction of a generalized quadrangle from an oval of $PG(2,q)$.

**Example 1.5.10** (Dembowski 1968 [55]) Let $\mathcal{O}$ be an oval of $PG(2,q)$. Embed $PG(2,q)$ as a hyperplane in $PG(3,q)$, and define the incidence structure $T_2(\mathcal{O})$ as follows. Points of $T_2(\mathcal{O})$ are of three types: (i) points of $PG(3,q) \setminus PG(2,q)$; (ii) planes of $PG(3,q)$ meeting $PG(2,q)$ in a tangent line to $\mathcal{O}$; (iii) the symbol $(\infty)$. Lines of $T_2(\mathcal{O})$ are of two types: (a) lines of $PG(3,q)$ not contained in $PG(2,q)$ that intersect $PG(2,q)$ in a point of $\mathcal{O}$; (b) points of $\mathcal{O}$. Incidence is defined as follows: lines of type (b) are incident with points of type (ii) which contain them, and with $(\infty)$; lines of type (a) are incident with points of type

(i) contained in them, and with points of type (ii) which contain them. Then $T_2(\mathcal{O})$ is a generalized quadrangle of order $q$. $T_2(\mathcal{O})$ is isomorphic to $\mathrm{Q}(4,q)$ if and only if $\mathcal{O}$ is a conic.

An **ovoid** of $\mathrm{PG}(3,q)$ is a set of $q^2+1$ points such that no 3 are collinear. The canonical example of an ovoid of $\mathrm{PG}(3,q)$ is an elliptic quadric. When $q$ is odd, these are the only examples.

**Theorem 1.5.11** (Barlotti 1955 [13], Panella 1955 [114]) *Every ovoid of* $\mathrm{PG}(3,q)$, *$q$ odd, is an elliptic quadric.*

When $q$ is even, there is a non-classical ovoid of $\mathrm{PG}(3,q)$.

**Example 1.5.12** (Tits 1962 [165]) Let

$$\Omega = \{(1,s,t,s^\sigma + st + t^{\sigma+2}) : s,t \in \mathrm{GF}(q)\} \cup \{(0,0,0,1)\},$$

where $q = 2^{2e+1}$, $e \geq 1$, and $x^\sigma = x^{2^{e+1}}$ for all $x \in \mathrm{GF}(q)$. Then $\Omega$ is an ovoid of $\mathrm{PG}(3,q)$ that is not equivalent to an elliptic quadric. This is the **Tits ovoid**.

At this time, these are the only known ovoids of $\mathrm{PG}(3,q)$. We can mimic the construction of Example 1.5.10 using $\mathrm{Q}^-(5,q)$ instead of $\mathrm{Q}(4,q)$. A tangent hyperplane to an elliptic quadric in $\mathrm{PG}(5,q)$ meets the quadric in a cone projecting to an elliptic quadric of $\mathrm{PG}(3,q)$. Since elliptic quadrics are ovoids, we can constuct a generalized quadrangle from an ovoid as follows.

**Example 1.5.13** (Dembowski 1968 [55]) Let $\Omega$ be an ovoid in $\mathrm{PG}(3,q)$. Embed $\mathrm{PG}(3,q)$ as a hyperplane of $\mathrm{PG}(4,q)$. Define the incidence structure $T_3(\Omega)$ as follows. Points of $T_3(\Omega)$ are of three types: (i) points of $\mathrm{PG}(4,q) \setminus \mathrm{PG}(3,q)$; (ii) hyperplanes of $\mathrm{PG}(4,q)$ meeting $\mathrm{PG}(3,q)$ in a tangent plane to $\Omega$; (iii) the symbol $(\infty)$. Lines of $T_3(\Omega)$ are of two types: (a) lines of $\mathrm{PG}(4,q)$ not contained in $\mathrm{PG}(3,q)$ that intersect $\mathrm{PG}(3,q)$ in a point of $\Omega$; (b) points of $\Omega$. Incidence is defined as follows: lines of type (b) are incident with points of type (ii) which contain them, and with $(\infty)$; lines of type (a) are incident with points of type (i) contained in them, and with points of type (ii) which contain them. Then $T_3(\mathcal{O})$ is a generalized quadrangle of order $(q^2, q)$. $T_3(\Omega)$ is isomorphic to $\mathrm{Q}^-(5,q)$ if and only if $\Omega$ is an elliptic quadric.

Since there exist ovals that are not conics (see Section 2.2) and ovoids that are not elliptic quadrics (see Example 1.5.12), the constructions in Example 1.5.10 and Example 1.5.13 show that there exist non-classical generalized quadrangles of order $q$ and $(q^2, q)$. The constructions of Example 1.5.10 and Example 1.5.13 will be generalized in Section 3.5 (see Example 3.5.2).

We can also construct generalized quadrangles from hyperovals.

**Example 1.5.14** (Hall 1971 [72]) Let $\mathcal{H}$ be a hyperoval of $\mathrm{PG}(2,q)$, and embed $\mathrm{PG}(2,q)$ as a hyperplane at infinity in $\mathrm{PG}(3,q)$. Define an incidence structure $T_2^*(\mathcal{H})$ as follows. The points of $T_2^*(\mathcal{H})$ are the points of $\mathrm{PG}(3,q) \setminus \mathrm{PG}(2,q)$. The lines of $T_2^*(\mathcal{H})$ are the lines of $\mathrm{PG}(3,q)$ not contained in $\mathrm{PG}(2,q)$ that meet $\mathcal{H}$ in a unique point. Incidence in $T_2^*(\mathcal{H})$ is inherited from $\mathrm{PG}(3,q)$. Then $T_2^*(\mathcal{H})$ is a generalized quadrangle of order $(q-1, q+1)$.

The following construction shows how to obtain a new generalized quadrangle from a generalized quadrangle of order $s$ with a regular point.

**Example 1.5.15** (Payne 1971 [116]) Let $x$ be a regular point of the generalized quadrangle $\mathcal{S} = (\mathcal{P}, \mathcal{L}, I)$ of order $s$. Define the incidence structure $\mathcal{S}' = (\mathcal{P}', \mathcal{L}', I')$ as follows. Points of $\mathcal{S}'$ are the points of $\mathcal{S}$ not collinear with $x$. Lines of $\mathcal{S}'$ are of two types: the lines of type (a) are the lines of $\mathcal{L}$ which are not incident with $x$, lines of type (b) are the hyperbolic lines $\{x,y\}^{\perp\perp}$, for $y \not\sim x$. Incidence in $\mathcal{S}'$ is defined as follows: if $y \in \mathcal{P}'$ and $L \in \mathcal{L}'$ is type (a), then $y \, I' \, L$ if and only if $y \, I \, L$; if $y \in \mathcal{P}'$ and $L \in \mathcal{L}'$ is of type (b), then $y \, I' \, L$ if and only if $y \in L'$. Then $\mathcal{S}'$ is a generalized quadrangle of order $(s-1, s+1)$.

### 1.5.3 Partial geometries

A (finite) **partial geometry** with parameters $s, t, \alpha$ is a point/line incidence structure $(\mathcal{P}, \mathcal{L}, I)$ such that there exist integers $s, t, \alpha \geq 1$ such that

- each point is incident with $t+1$ lines

- each line is incident with $s+1$ points
- two distinct points are incident with at most one line
- two distinct lines are incidence with at most one point
- given a line $\ell$ and a point $P$ not on $\ell$, there are $\alpha$ points on $\ell$ collinear with $P$

The dual of a partial geometery with parameters $s, t, \alpha$ is a partial geometry with parameters $s' = t$, $t' = s$, $\alpha' = \alpha$. A partial geometry is a **generalized quadrangle** if and only if $\alpha = 1$. A partial geometry with $\alpha = s+1$ (dually, $\alpha = t+1$) is a $2-(v, s+1, 1)$ design, a so-called **block design**. A partial geometry with $\alpha = s$ (dually, $\alpha = t$) is a **net** or **transversal design** (see Bruck 1963 [29]). A partial geometry with $1 < \alpha < \min(s,t)$ is a **proper partial geometry**. This are the most important class of partial geometries, since the others have a literature of their own.

A **maximal arc** of degree $n$ in $\mathrm{PG}(2,q)$ is a set of points $\mathcal{K}$ such that every line of $\mathrm{PG}(2,q)$ contains either 0 or $n$ points of $\mathcal{K}$. Maximal arcs are discussed in Section 1.6.1. The next two results show that we can obtain partial geometries from maximal arcs.

**Example 1.5.16** (Thas 1974 [148], Wallis 1973 [178]) Let $\mathcal{K}$ be a maximal arc of degree $n$ in a projective plane $\pi$ of order $q$. Define an incidence structure $\mathcal{S}(\mathcal{K})$ as follows. The points of $\mathcal{S}(\mathcal{K})$ are the points of $\pi \setminus \mathcal{K}$. The lines of $\mathcal{S}(\mathcal{K})$ are the lines of $\pi$ secant to $\mathcal{K}$. Incidence is inherited from $\pi$. Then $\mathcal{S}(\mathcal{K})$ is a partial geometry with parameters $s = q-n$, $t = q - q/n$, $\alpha = q - q/n - n + 1$.

**Example 1.5.17** (Thas 1974 [148]) Let $\mathcal{K}$ be a maximal arc of degree $n$ in $\mathrm{PG}(2,q)$. Embed $\mathrm{PG}(2,q)$ as a hyperplane $\pi$ of $\mathrm{PG}(3,q)$. Define an incidence structure $T_2^*(\mathcal{K})$ as follows. The points of $T_2^*(\mathcal{K})$ are the points of $\mathrm{PG}(3,q) \setminus \pi$. The lines of $T_2^*(\mathcal{K})$ are the lines of $\mathrm{PG}(3,q)$ that meet $\pi$ in a unique point of $\mathcal{K}$. Incidence is induced from the incidence of $\mathrm{PG}(3,q)$. Then $T_2^*(\mathcal{K})$ is a partial geometry with parameters $s = q-1$, $t = (q+1)(n-1)$, $\alpha = n-1$.

The partial geometry $T_2^*(\mathcal{K})$ constructed in Example 1.5.17 of degree $2^k$, $0 < k < h$, in $\mathrm{PG}(2, 2^h)$ has parameters $s = 2^h - 1$, $t = (2^h+1)(2^k-1)$, $\alpha = 2^k - 1$. Hence, $T_2^*(\mathcal{K})$ is a generalized quadrangle if and only if $k = 1$, that is, if $\mathcal{K}$ is a hyperoval. Therefore, we can see $T_2^*(\mathcal{K})$ as a generalization of the construction $T_2^*(\mathcal{H})$ of Example 1.5.14.

A (finite) **partial quadrangle** with parameters $s, t, \mu$ is a point/line incidence structure $(\mathcal{P}, \mathcal{L}, I)$ such that there exist integers $s, t, \alpha \geq 1$ such that

- each point is incident with $t + 1$ lines
- each line is incident with $s + 1$ points
- two distinct points are incident with at most one line
- two distinct lines are incident with at most one point
- given a line $\ell$ and a point $P$ not on $\ell$, there is at most one point on $\ell$ collinear with $P$
- given two non-collinear points $P$ and $Q$, there are $\mu$ points collinear with both $P$ and $Q$.

Partial quadrangles were introduced by Cameron 1975 [38]. A generalized quadrangle is a partial quadrangle with $\mu = t + 1$. A strongly regular graph with $\lambda = 0$ is a partial quadrangle with $s = 1$ and $t = k - 1$. Stongly regular graphs are discussed in Section 1.6.2. Examples of strongly regular graphs with $\lambda = 0$ include the pentagon and the Petersen graph (see Figure 1.8) We can construct partial quadrangles from certain generalized quadrangles as follows.

**Example 1.5.18** (Cameron–Goethals–Seidel 1979 [40]) Let $\mathcal{S}$ be a generalized quadrangle of order $(s, s^2)$. Let $p$ be any point of $\mathcal{S}$ and define the incidence structure $\mathcal{S}(p)$ as follows. The points of $\mathcal{S}(p)$ are the points of $\mathcal{S}$ not collinear with $p$. The lines of $\mathcal{S}(p)$ are the lines of $\mathcal{S}$ not containing $p$. Incidence is induced from $\mathcal{S}$. Then $\mathcal{S}(p)$ is a partial quadrangle of order $(s - 1, s^2, s(s - 1))$.

Let us now generalize the construction of Example 1.5.17. Let $\mathcal{K}$ be a set of points in $\mathrm{PG}(n, q)$. Embed $\mathrm{PG}(n, q)$ as a hyperplane $H$ in $\mathrm{PG}(n + 1, q)$. Define an incidence structure $T_n^*(\mathcal{K})$ as follows. The points of $T_n^*(\mathcal{K})$ are the points of $\mathrm{PG}(n + 1, q) \setminus H$. The lines of $T_n^*(\mathcal{K})$

are the lines of $\mathrm{PG}(n+1,q)$ that meet $H$ in a unique point of $\mathcal{K}$. Incidence is induced from the incidence of $\mathrm{PG}(n+1,q)$.

If $T_n^*(\mathcal{K})$ gives a partial quadrangle, then $\mathcal{K}$ has to be a set of points in $\mathrm{PG}(n,q)$ such that any line in $\mathrm{PG}(n,q)$ is external, tangent or secant to $\mathcal{K}$, and each point of $\mathrm{PG}(n,q) \setminus \mathcal{K}$ is on $\mu/2$ secants. Thus, $\mathcal{K}$ is a $(t+1)-$**cap** in $\mathrm{PG}(n,q)$ such that each point in $\mathcal{K}$ lies on $t+1-\mu$ tangents. A few such $\mathcal{K}$ are known.

**Example 1.5.19** The following $T_n^*(\mathcal{K})$ are partial quadrangles.

(1) $T_3^*(\mathcal{O})$, with $\mathcal{O}$ an ovoid of $\mathrm{PG}(3,q)$ is a partial quadrangle with parameters $s=q-1$, $t=q^2$, $\mu=q(q-1)$. These quadrangles were first constructed by Cameron 1975 [38].

(2) Suppose $q=3$ and $\mathcal{K}$ is not an ovoid. Then $\mathcal{K}$ is either an 11-cap in $\mathrm{PG}(4,3)$ (see Coxeter 1958 [51] or Pellegrino 1974 [123]) and the partial quadrangle has parameters $s=2$, $t=10$, $\mu=2$, or $\mathcal{K}$ is the unique 56-cap in $\mathrm{PG}(5,3)$ first constructed by Segre 1965 [138], and the partial quadrangle $T_5^*(\mathcal{K})$ has parameters $s=2$, $t=55$, $\mu=20$.

(3) Suppose $q=4$. Then either $\mathcal{K}$ is an ovoid of $\mathrm{PG}(3,4)$, or a 78-cap in $\mathrm{PG}(5,4)$ discovered by Hill 1976 [81] and the resulting partial quadrangle $T_5^*(\mathcal{K})$ has parameters $s=3$, $t=77$, $\mu=14$, or an (as yet undiscovered) 430-cap in $\mathrm{PG}(6,4)$.

(4) Suppose $q \geq 5$. Then a partial quadrangle of the form $T_n^*(\mathcal{K})$ must be $T_3^*(\mathcal{O})$, for some ovoid $\mathcal{O}$ in $\mathrm{PG}(3,q)$ (see Tzanakis–Wolfskill 1987 [167]).

A (finite) **semipartial geometry** with parameters $s,t,\alpha,\mu$ is a point/line incidence structure $(\mathcal{P},\mathcal{L},I)$ such that there exist integers $s,t,\alpha,\mu \geq 1$ such that

- each point is incident with $t+1$ lines
- each line is incident with $s+1$ points
- two distinct points are incident with at most one line
- two distinct lines are incident with at most one point

- given a line $\ell$ and a point $P$ not on $\ell$, there are either 0 or $\alpha$ points on $\ell$ collinear with $P$
- given two non-collinear points $P$ and $Q$, there are $\mu$ points collinear with both $P$ and $Q$.

Semipartial geometries were introduced by Debroey–Thas 1978 [53]. They generalize both partial geometries and partial quadrangles. A semipartial geometry with $\alpha = 1$ is a partial quadrangle. A semipartial geometry is a partial geometry if and only if $\mu = (t+1)\alpha$, and a generalized quadrangle if and only if $\alpha = 1$ and $\mu = t+1$. The dual of a semipartial geometry is a semipartial geometry if and only if either $s = t$ or the semipartial geometry is in fact a partial geometry. Semipartial geometries that are not partial geometries are called **proper**.

**Example 1.5.20** (De Clerck–Van Maldeghem 1995 [52]) We can construct semipartial geometries from the $T_n^*(\mathcal{K})$ construction given above. These constructions involve **unitals** and **Baer subspaces**, which are defined in Section 1.6.1. Let $\mathcal{U}$ be a unital in $\mathrm{PG}(2,q)$. Then $T_2^*(\mathcal{U})$ is a semipartial geometry with $s = q^2-1$, $t = q^3$, $\alpha = q$, $\mu = q^2(q^2-1)$. If $\mathcal{B}$ is a Baer subspace of the projective space $\mathrm{PG}(n,q)$, then $T_n^*(\mathcal{B})$ is a semipartial geometry with $s = q^2-1$, $t = \frac{q^{n+1}-1}{q-1}$, $\alpha = q$, $\mu = q(q+1)$.

# 1.6 Related combinatorics

In this section we give some examples of combinatorial objects that are related to some of the structures of primary interest in this thesis. We do not intend to give a comprehensive survey, instead the focus is on the connections to hyperovals, circle planes and hemisystems.

## 1.6.1 Two intersection sets

A **$k$-set of type** $(m,n)$ with respect to hyperplanes in $\mathrm{PG}(d,q)$, $m < n$, is a set of points $\mathcal{K}$, with $|\mathcal{K}| = k$, such that every hyperplane contains either $m$ or $n$ points of $\mathcal{K}$ (and $m < n$). Such a set is often referred to as a **$k$-$(m,n)$ set**. The values $m$ and $n$ are the **intersection numbers** of $\mathcal{K}$, and such as set is often called a **two intersection set**).

Sets of type $(0,2)$ in $\mathrm{PG}(2,q)$ occur only in planes of even order and are **hyperovals**. Hyperovals of $\mathrm{PG}(2,q)$ are studied in detail in Chapter 2. An **ovoid** of $\mathrm{PG}(3,q)$ is a $(q^2+1)-(1,q+1)$ set of $\mathrm{PG}(3,q)$.

More generally, sets of type $(0,n)$ in $\mathrm{PG}(2,q)$ are called **maximal arcs**. The parameter $n$ is the **degree** of $\mathcal{K}$. Several families of maximal arcs in exist projective planes (for example, see Denniston 1969 [56], Thas 1974 [148], Thas 1980 [150], Hamilton 1995 [73], Hamilton–Mathon 2003 [74].) These families contain examples of maximal arcs for all values of $n$ dividing $q$. There are no known examples of maximal arcs in planes of odd order.

Sets of type $(1,n)$ in $\mathrm{PG}(2,q)$ fall into two classes based on their size.

**Theorem 1.6.1** (Tallini Scafati 1966 [145]) *Let $\mathcal{K}$ be a $k-(1,n)$ set in a projective plane of order $q$, $q$ a prime power, with $n \neq q+1$. Then $q$ is a square, $n=\sqrt{q}+1$, and either $k=q^{3/2}+1$ or $k=q+\sqrt{q}+1$.*

The $(q^2+q+1)-(1,q+1)$ sets in $\mathrm{PG}(2,q^2)$ are the **Baer subplanes**. These are the subgeometries that arise from the fixed points of the **Baer involution** $x \mapsto x^q$ in $\mathrm{PG}(2,q^2)$. Baer subgeometries play a role in Chapter 4.

A **unital** $\mathcal{U}$ in $\mathrm{PG}(2,q^2)$ is a $(q^3+1)-(1,q+1)$ set. A line is **tangent** or **secant** to $\mathcal{U}$ if it intersects $\mathcal{U}$ in 1 or $q+1$ points. The set of tangent lines to a unital form a unital in the dual plane called a **dual unital**. The study of unitals begin in 1946 by Baer. He showed that polarities were linked to ovals and unitals

**Theorem 1.6.2** (Baer 1946 [8]) *A polarity $\rho$ of a projective plane of order $n$ has at least $n+1$ absolute points. If $\rho$ has $n+1$ absolute points, then the set of absolute points of $\rho$ is an oval if $n$ is odd, and a line if $n$ is even. If $\rho$ has more than $n+1$ absolute points, then $n$ is square, and if every non-absolute line has $\sqrt{n}+1$ absolute points, then the set of absolute points is a unital.*

This result was sharpened by Seib 1970 [141], who showed that a polarity of a finite projective plane of order $n$ has at most $n^{3/2}+1$ absolute points, and if equality occurs, then the set of points is a unital. Unitals in $\mathrm{PG}(2,q^2)$ arising in this way are the **classical unitals**.

**Example 1.6.3** (Buekenhout 1976 [34], Metz 1979 [104], see also Grüning 1987 [71]) Let $H$ be a hyperplane in $\mathrm{PG}(4,q)$ and $v$ a point of $H$. Let $\mathcal{O}$ be an ovoid of $\mathrm{PG}(4,q)/v$ for which the plane $H/v$ is a tangent plane. Then $\mathcal{O}$ is the set of generators of an ovoidal cone $\mathcal{C}$ in $\mathrm{PG}(4,q)$ with vertex $v$, and $H$ contains a unique generator $\ell$. Let $\mathcal{S}$ be a spread of $H$ containing $\ell$. Then in the Bruck–Bose translation plane $\pi$ corresponding to the spread $\mathcal{S}$, $\mathcal{U} = \mathcal{C} \setminus \ell \cup \{\ell\}$ is a unital. These are the **Buekenhout–Metz unitals**.

Other than hyperovals, maximal arcs, unitals and Baer subgeometries, $k-(m,n)$ sets do not have special names. Until recently, all known examples $k-(m,n)$ sets with $m > 0$ existed in planes of square order $q$, and satisfied $n = m + \sqrt{q}$. However, so called "non-standard" two intersection sets exist (for example, see Batten–Dover 1999 [14]). Penttila–Royle 1995 [128] classified the two intersection sets in projective planes of order 9.

### 1.6.2 Strongly regular graphs

A graph $\Gamma$ with $v$ vertices is **strongly regular** if there exist non-negative integers $k, \lambda, \mu$ such that

- each vertex is adjacent to $k$ other vertices (i.e. $\Gamma$ is **regular** with degree $k$)
- for any pair of distinct adjacent vertices, there are $\lambda$ vertices adjacent to both
- for any pair of distinct non-adjacent vertices, there are $\mu$ vertices adjacent to both.

Strongly regular graphs were first defined by Bose 1963 [24] and are fundamental objects of study in combinatorics. They are important in their own right, as well as being of interest due to the vast number of connections betwen strongly regular graphs and other combinatorial structures. The most famous strongly regular graph is the **Petersen graph**, shown in Figure 1.8. See Hubaut 1975 [84] for an introduction to strongly regular graphs[2]. The following example shows that strongly regular graphs are connected to polar spaces.

[2]Note however that the survey given in this paper is somewhat out of date by now.

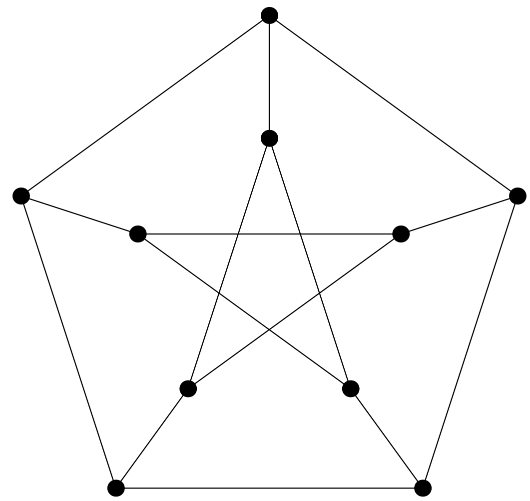

Figure 1.8: The Petersen graph, a strongly regular graph with $v = 10$, $k = 3$, $\lambda = 0$, $\mu = 1$.

**Example 1.6.4** (see Cohen–Neumaier 1989 [26]) Let $\Pi$ be a finite polar space with $n$ points, $s + 1$ points on every line, and $t + 1$ lines through every point. The **collinearity graph** $\Gamma(\Pi)$ of $\Pi$ is the graph with vertices the points of $\Pi$, with vertices adjacent if and only if their corresponding points are collinear in $\Pi$. Then $\Gamma(\Pi)$ is strongly regular with parameters $v = n$, $k = s(t + 1)$, $\lambda = s(t + 1) - \frac{n-s(t+1)-1}{s} - 1$, and $\mu = t + 1$.

Most of the structures described in the preceding sections are associated with strongly regular graphs in some way. The next two examples show that strongly regular graphs can be constructed from semipartial geometries.

**Example 1.6.5** (Bose 1963 [24]) Let $P$ be a partial geometry with parameters $s, t, \alpha$. Define the graph $\Gamma(P)$ as follows. The vertices of $\Gamma(P)$ are the points of $P$, with vertices adjacent if and only if their corresponding points are collinear in $P$. Then $\Gamma(P)$ is a strongly regular graph with parameters $v = (s+1)(st+\alpha)/t$, $k = s(t+1)$, $\lambda = (\alpha-1)t+s-1$, $\mu = \alpha(t+1)$.

**Example 1.6.6** (Cameron 1975 [38]) Let $P$ be a partial quadrangle with parameters $s, t, \mu'$. Define the graph $\Gamma(P)$ as follows. The vertices of $\Gamma(P)$ are the points of $P$, with vertices adjacent if and only if their corresponding points are collinear in $P$. Then $\Gamma(P)$ is a strongly regular graph with parameters $v = 1 + s(t + 1)(\mu' + st)/\mu'$, $k = s(t + 1)$, $\lambda = s - 1$, $\mu = \mu'$.

We can also construct strongly regular graphs from two intersection sets. Note the similarity to the construction in Example 1.5.17.

**Example 1.6.7** (Calderbank–Kantor 1986 [37]) Let $\mathcal{K}$ be a $k-(m,n)$ set in $\mathrm{PG}(2,q)$. Embed $\mathrm{PG}(2,q)$ as a hyperplane $\pi$ of $\mathrm{PG}(3,q)$. Define a graph $\Gamma$ as follows. The vertices of $\Gamma$ are the points of $\mathrm{PG}(3,q) \setminus \pi$, with vertices adjacent if and only if the line joining them in $\mathrm{PG}(3,q)$ meets $\pi$ in a point of $\mathcal{K}$. Then $\Gamma$ is a strongly regular.

We can construct strongly regular graphs from $2-(v,k,1)$ designs. We give some examples of such designs in Section 1.6.3. Since many $2-(v,k,1)$ designs are known, this construction yields many strongly regular graphs.

**Example 1.6.8** (Goethals–Seidel 1970 [70]) Let $\mathcal{D}$ be a $2-(v',k',1)$ design. Define the graph $\Gamma(\mathcal{D})$ as follows. The vertices of $\Gamma(\mathcal{D})$ are the blocks of $\mathcal{D}$, with vertices adjacent if and only if their corresponding blocks meet in a unique point of $\mathcal{D}$. Then $\Gamma(\mathcal{D})$ is a strongly regular graph with parameters $v = \frac{v'(v'-1)}{k'(k'-1)}$, $k = \frac{k'(v'-k')}{k'-1}$, $\lambda = \frac{v'-1}{k'-1} + (k'-1)^2 - 1$, $\mu = k'^2$.

### 1.6.3 Designs

A $t-(v,k,\lambda)$ **design** is an incidence structure $(\mathcal{P},\mathcal{B},I)$ with two types, usually called points $\mathcal{P}$ and blocks $\mathcal{B}$, with incidence defined by $I = \{(P,B) \in \mathcal{P} \times \mathcal{B} : P \in B\}$, such that

- $|\mathcal{P}| = v$
- $|B| = k$ for all $B \in \mathcal{B}$
- every $t$-subset of $\mathcal{P}$ is incident with exactly $\lambda$ blocks.

A design is **symmetric** if the number of points is the same as the number of blocks.

We give some examples of designs that are related to the structures appearing in this thesis. Firstly, designs can be constructed from projective and affine spaces in a natural way.

**Example 1.6.9** Let $\pi$ be a projective plane of order $n$. Define a design $\mathcal{D}(\pi) = (\mathcal{P},\mathcal{B},I)$ as follows. The points $\mathcal{P}$ of the design are the points of $\pi$, and the blocks $\mathcal{B}$ of the design are the lines of $\pi$, with natural incidence. Then $\mathcal{D}(\pi)$ is a $2-(n^2+n+1, n+1, 1)$ design. Conversely, if $\mathcal{D}$ is a $2-(n^2+n+1, n+1, 1)$ design, we can define a plane $\pi(\mathcal{D})$ whose points are the points of $\mathcal{D}$, and whose lines are the blocks of $\mathcal{D}$, with natural incidence. Then $\pi(\mathcal{D})$ is a projective plane of order $n$. Similarly, we can construct a $2-(n^2+n, n, 1)$ design from an affine plane of order $n$, and conversely. We can generalize this construction to obtain designs from subspaces from projective and affine spaces. Consider the design $\mathcal{PD}(m, n, q)$ whose points are the points of $\mathrm{PG}(n, q)$ and whose blocks are the $m$-spaces in $\mathrm{PG}(n, q)$. Then $\mathcal{PD}(m, n, q)$ is a $2-(v, k, \lambda)$ design with $v = \begin{bmatrix} n+1 \\ 1 \end{bmatrix}_q$, $k = \begin{bmatrix} m+1 \\ 1 \end{bmatrix}_q$, $\lambda = \begin{bmatrix} n-1 \\ m-1 \end{bmatrix}_q$, where $\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})}$ are the **Gaussian coefficients** over $\mathrm{GF}(q)$. Similarly, the design $\mathcal{AD}(n, m, q)$ whose points are the points of $\mathrm{AG}(n, q)$ and whose blocks are the $m$-spaces of $\mathrm{AG}(n, q)$ is a $2-(q^n, q^m, \lambda)$ design with $\lambda = \begin{bmatrix} n-1 \\ m-1 \end{bmatrix}_q$.

The next two examples show how to construct designs from various two intersection sets.

**Example 1.6.10** Let $\mathcal{U}$ be a unital in $\mathrm{PG}(2, q^2)$. Define $\mathcal{D}(\mathcal{U})$ to be design whose points are the points of $\mathcal{U}$, and whose blocks are the $(q^3+1)$-secants of $\mathrm{PG}(2, q^2)$, together with natural incidence. Then $\mathcal{D}(\mathcal{U})$ is a $2-(q^3+1, q+1, 1)$ design.

**Example 1.6.11** (Wallis 1973 [178]) Let $\mathcal{K}$ be a maximal arc of degree $n$ in a projective plane $\pi$ of order $q$. Define $\mathcal{D}(\mathcal{K})$ as follows. Let the points of $\mathcal{D}(\mathcal{K})$ be the points of $\mathcal{K}$. Let the blocks of $\mathcal{D}(\mathcal{K})$ be the secant lines of $\pi$. Incidence is induced from $\pi$. Then $\mathcal{D}(\mathcal{K})$ is a $2-(q(n-1)+n, n, 1)$ design. In particular, hyperovals $\mathcal{H}$ in $\mathrm{PG}(2, q)$ correspond to $2-(q+2, 2, 1)$ designs.

Generalized quadrangles of order $q$ and $(q-1, q+1)$ are related to strongly regular graphs, and certain 2-designs with a polarity.

**Example 1.6.12** (Payne–Thas 1984 [121]) Let $\mathcal{S}$ be a generalized quadrangle of order $q$. Then we can define a design $\mathcal{D}(\mathcal{S})$ as follows. The points of $\mathcal{D}(\mathcal{S})$ are the points of $\mathcal{S}$, and the blocks of $\mathcal{D}(\mathcal{S})$ are the sets of the form $x^\perp$ for $x \in \mathcal{S}$, together with natural incidence. Then $\mathcal{D}$ is a symmetric $2-(q^3+q^2+q+1, q^2+q+1, q+1)$ design. The map $x \mapsto x^\perp$ is a a null polarity of $\mathcal{D}$. The incidence graph of this design is strongly regular with $\mu = \lambda + 1$. Conversely, any strongly regular graph with $\mu = \lambda + 1$ is associated with a symmetric design with a null polarity. Similarly, let $\mathcal{T}$ be a generalized quadrangle of order $(q-1, q+1)$. Define the design $\mathcal{D}(\mathcal{T})$ as follows. The points of $\mathcal{D}(\mathcal{T})$ are the points of $\mathcal{T}$, and the blocks of $\mathcal{D}(\mathcal{T})$ are sets of the form $x^\perp \setminus \{x\}$, together with natural incidence. Then $\mathcal{D}(\mathcal{T})$ is a symmetric $2-(q^3+2q^2, q^2+q, q)$ design. The map $x \mapsto x^\perp \setminus \{x\}$ is a conull polarity of $\mathcal{D}(\mathcal{T})$. The incidence graph of this design is strongly regular with $\mu = \lambda$. Conversely, any strongly regular graph with $\mu = \lambda$ is associated with a symmetric design with a conull polarity. Note that via the construction of Example 1.5.14, hyperovals in $\mathrm{PG}(2, q)$ give generalized quadrangles of order $(q-1, q+1)$, and hence are associated with $2-(q^3+2q^2, q^2+q, q)$ designs and strongly regular graphs with $\mu = \lambda$.

## 1.7 Classical groups

One of the most successful approaches to the study of polar spaces is via symmetry. Let $V$ denote a vector space of dimension $d+1$ over the finite field $F = \mathrm{GF}(q)$. The **general linear group** $\mathrm{GL}(d+1, q)$ consists of the invertible linear maps from $V$ to $V$. The **special linear group** $\mathrm{SL}(d+1, q)$ consists of those maps in $\mathrm{GL}(d+1, q)$ of determinant 1. The center of $\mathrm{GL}(d+1, q)$ consists of the non-zero scalar matrices, which is isomorphic to $F^*$, and with a slight abuse of notation we write $F^* \leq \mathrm{GL}(d+1, q)$. The **projective general linear group** $\mathrm{PGL}(d+1, q)$ is $\mathrm{GL}(d+1, q)/F^*$, and if $X$ is any subgroup of $\mathrm{GL}(d+1, q)$, we write $\mathrm{P\,X}$ for the corresponding projective group $X/\left(X \cap F^*\right)$. Thus, for example, the **projective special linear group** is defined to be $\mathrm{PSL}(d+1, q) = \mathrm{SL}(d+1, q)/\left(F^* \cap \mathrm{SL}(d+1, q)\right)$. The **general semilinear group** $\Gamma\mathrm{L}(d+1, q)$ consists of the invertible semilinear transformations from $V$ to $V$, and clearly $\Gamma\mathrm{L}(d+1, q)/\mathrm{GL}(d+1, q)$ is isomorphic to $\mathrm{Aut}\,F$. As above, we can consider the **projective semilinear group** $\mathrm{P}\Gamma\mathrm{L}(d+1, q) = \Gamma\mathrm{L}(d+1, q)/F^*$, and more generally, define $\mathrm{P\,X}$ for any subgroup $X$ of $\Gamma\mathrm{L}(d+1, q)$.

Now let us add some more structure to $V$. Motivated by our earlier discussion, let $\kappa$

denote either a reflexive sesquilinear form[3], or a quadratic form on $V$. Thus $\kappa : V^m \to F$, where $m = 1$ or 2. We sometimes call $(V, \kappa)$ a **space with form**. Let $v = (v_1, \ldots, v_m) \in V^m$ denote a tuple in the domain of $\kappa$, and for $g \in \Gamma\mathrm{L}(d+1, q)$, define $gv = (gv_1, \ldots, gv_m)$.

Let $g \in \mathrm{GL}(d+1, q)$. Then $g$ is an **isometry** of $(V, \kappa)$ if $\kappa(gv) = \kappa(v)$ for all $v \in V^m$. The set of isometries of $(V, \kappa)$ is denoted $I(d+1, q, \kappa)$. An element $g \in I(d+1, q, \kappa)$ is a **special isometry** if $g$ is also in $\mathrm{SL}(d+1, q)$. The special isometries form a group denoted $S(d+1, q, \kappa)$. An element $g \in \mathrm{GL}(d+1, q)$ is a **similarity** if there exists some $\lambda \in F^*$ such that $\kappa(gv) = \lambda\kappa(v)$ for all $v \in V^m$. The constant $\lambda$ is the **constant of similitude** of $g$. The group of similarities is denoted $\Delta(d+1, q, \kappa)$. An element $g \in \mathrm{GL}(d+1, q)$ is a **semisimilarity** if there exists some $\lambda \in F^*$, and some $\alpha \in \mathrm{Aut}\, F$, such that $\kappa(gv) = \lambda\kappa(v)^\alpha$ for all $v \in V^m$. The group of semisimilarities is denoted $\Gamma(d+1, q, \kappa)$. It turns out that in the case that $\kappa$ is orthogonal, the group $S(d+1, q, \kappa)$ contains a certain subgroup of index 2. We define $\Omega(d+1, q, \kappa)$ to be this certain subgroup when $\kappa$ is orthogonal, and $\Omega(d+1, q, \kappa) = S(d+1, q, \kappa)$ otherwise.

As a matter of convenience, we shall write $X = X(d+1, q, \kappa)$, where $X$ ranges over the symbols $\Omega$, $S$, $I$, $\Delta$, and $\Gamma$. We therefore obtain a chain of subgroups

$$\Omega \leq S \leq I \leq \Delta \leq \Gamma.$$

Information about terminology and notation for the various cases of $\kappa$ is given in Table 1.2. For the sake of efficiency, when $\kappa$ is orthogonal, we use $\epsilon \in \{+, -, \cdot\}$ to denote the three classes of orthogonal forms. For example, the group $I(d+1, q, \kappa)$ is denoted $\mathrm{O}^+(d+1, q)$ when $\kappa$ is the quadratic form of plus type, $\mathrm{O}^-(d+1, q)$, when $\kappa$ is the quadratic form of minus type, and $\mathrm{O}(d+1, q)$ when $\kappa$ is the quadratic form of blank type. To denote the projective versions of these groups, we precede the symbol appearing in the fourth column of Table 1.2 with the symbol P. For example, the group $\mathrm{PGU}(d+1, q)$ denotes the group $\mathrm{GU}(d+1, q)$ modulo scalars.

---

[3]If $\kappa$ is hermitian, then $V$ is over the field $F = \mathrm{GF}(q^2)$, but we will continue to use $q$ while considering

Table 1.2: A summary of information relevant to certain classical groups.

| Name | $\kappa$ | X | Notation | Geometry |
|---|---|---|---|---|
| linear | zero | $\Omega = S$ | $\mathrm{SL}(d+1,q)$ | $\mathrm{PG}(d,q)$ |
| | | $I = \Delta$ | $\mathrm{GL}(d+1,q)$ | |
| | | $\Gamma$ | $\Gamma\mathrm{L}(d+1,q)$ | |
| unitary | hermitian | $\Omega = S$ | $\mathrm{SU}(d+1,q^2)$ | $\mathrm{H}(d,q^2)$ |
| | | $I$ | $\mathrm{U}(d+1,q^2)$ | |
| | | $\Delta$ | $\mathrm{GU}(d+1,q^2)$ | |
| | | $\Gamma$ | $\Gamma\mathrm{U}(d+1,q^2)$ | |
| symplectic | alternating | $\Omega = S = I$ | $\mathrm{Sp}(d+1,q)$ | $\mathrm{W}(d,q)$ |
| | | $\Delta$ | $\mathrm{GSp}(d+1,q)$ | |
| | | $\Gamma$ | $\Gamma\mathrm{Sp}(d+1,q)$ | |
| orthogonal | quadratic | $\Omega$ | $\Omega^{\epsilon}(d+1,q)$ | $\mathrm{Q}^{\epsilon}(d,q)$ |
| | | $S$ | $\mathrm{SO}^{\epsilon}(d+1,q)$ | |
| | | $I$ | $\mathrm{O}^{\epsilon}(d+1,q)$ | |
| | | $\Delta$ | $\mathrm{GO}^{\epsilon}(d+1,q)$ | |
| | | $\Gamma$ | $\Gamma\mathrm{O}^{\epsilon}(d+1,q)$ | |

We end with a powerful result from the theory of categories, first proved by Witt in 1936 for symmetric and hermitian forms over fields of characteristic not 2.

**Theorem 1.7.1** (Witt 1936 [181]) *Suppose $V_1$ and $V_2$ are spaces with forms, and $U_1$ and $U_2$ are subspaces of $V_1$ and $V_2$, respectively. Then any isometry from $U_1$ to $U_2$ extends to an isometry from $V_1$ to $V_2$.*

We remark that we can replace isometries by special isometries in the statement of Witt's theorem, provided that the dimension of $V_1$ and $V_2$ is at least 2.

This seemingly innocuous theorem has many important consequences. Indeed, it is a fundamental tool in the study of the classical polar spaces. For example, we can use Witt's Theorem to show that any two maximal totally isotropic subspaces of a space with form have the same dimension.

Let $M$, $N$ be maximal totally isotropic subspaces of $V$. Without loss of generality,

general $\kappa$, so as not to furthur complicate the notation (see Footnote 1).

$\dim M \leq \dim N$. There is clearly an isomorphism $g$ from $M$ into $N$, and this is an isometry since $M$ and $N$ are totally isotropic. By Witt's Theorem, this isometry extends to an isometry $h$ from $V$ onto $V$, and $M \subseteq h^{-1}(N)$. Since $M$ is maximal and $h^{-1}(N)$ is totally isotropic, $M = h^{-1}(N)$, and hence $\dim M = \dim N$. The dimension of a maximal totally isotropic subspace is called the **Witt index** of $V$, and when the form is non-degenerate, is at most half the dimension of the underlying vector space. A similar argument holds for totally singular subspaces in the case of an orthogonal space. In this case, the Witt index will be equal to one more than the dimension of a maximal totally singular subspace contained in the quadric.

# Chapter 2

# Hyperovals in Desarguesian planes

## 2.1 Introduction

Studying symmetries of configurations in finite Desarguesian projective planes need not involve the use of deep group theory, since the subgroup structure of the collineation groups of these planes has been known since the work of Mitchell 1911 [105] for odd characteristic, and of his student Hartley 1925 [75] for characteristic two. Despite this advantage we still know very little about even the symmetries of well-studied objects like hyperovals. For example, we do not even know whether or not the regular hyperovals are characterized (for planes of order greater than 2) by the property of admitting an insoluble group. Indeed, the results of Section 2.4 can be viewed as a failed attempt at such a characterization. The rich man/poor man result in Theorem 2.4.8 can be considered a post facto explanation of the fact that all hyperovals of finite Desarguesian projective planes discovered since 1957 have such small groups. The final section in the chapter, Section 2.5, deals with the original motivating purpose for this work – the calculation of the groups of the last family of known hyperovals for which the problem is still open – those of Cherowitzo 1998 [43].

The groups of the Adelaide hyperovals of Cherowitzo–O'Keefe–Penttila 2003 [45] were calculated by Payne–Thas 2005 [122], the groups of the Subiaco hyperovals of Cherowitzo–Penttila–Pinneri–Royle 1996 [44] were calculated by combined results of O'Keefe–Thas 1996 [112] and Payne–Penttila–Pinneri (1995) [120], and the groups of the hyperovals of Payne 1985 [118] were calculated by Thas–Payne–Gevaert 1988 [159], with all three using the beautiful method of associating a curve of fixed degree with the hyperoval and using Bezout's theorem. (For earlier hyperovals, see, for example O'Keefe–Penttila 1994 [110]). But the attempt of O'Keefe–Thas 1996 [112] to apply this method to the Cherowitzo hyperovals only gave partial results, leading to the technical difficulties and subtlety of the proof of Penttila–Pinneri 1999

[126] that the Cherowitzo hyperovals are new for fields of order greater than 8. Subtlety is only necessary when faced with paucity of knowledge, and their results are an immediate corollary of our determination of the groups of the Cherowitzo hyperovals in Section 2.5. But our methods are far from beautiful. We apply the magic action of O'Keefe–Penttila 2002 [111], to perform fiendishly difficult computations in order to show that the homography groups of the Cherowitzo hyperovals are trivial. We resort to the use of the computer algebra packages Mathematica and Magma at crucial stages in the computations. The preceding sections form yet another failed attempt to perform this computation purely theoretically.

It seems that we still understand these hyperovals poorly. It is of note that it took 14 years to prove the generalization of the first examples found to an infinite family, and that the proof is lengthy and involved. Perhaps a beautiful proof exists and merely eludes us, owing to our poor understanding of these mysterious objects.

To be more exact about the general results about stabilizers of hyperovals that we obtain, combining Theorem 2.4.6 and the Remark that follows it shows that if a hyperoval $\mathcal{H}$ of $\mathrm{PG}(2,q)$, $q > 4$ admits an insoluble group $G$, then there is a subplane $\pi_0$ of order $q_0 > 2$ meeting $\mathcal{H}$ in a regular hyperoval such that $G \cap \mathrm{PGL}(3,q)$ induces $\mathrm{PGL}(2,q_0)$ on $\pi_0$, and if $\mathcal{H}$ is irregular, then $q > q_0^2$. We also (sharply) bound above the order of the homography stabilizer of a non-translation hyperoval of $\mathrm{PG}(2,q)$ by $3(q-1)$ in Theorem Theorem 2.4.8.

## 2.2 A Survey of hyperovals in $\mathrm{PG}(2,q)$

### 2.2.1 Elementary results

An **arc** in a projective plane is a set of points such that no three are collinear. Bose 1947 [23] proved that an arc in a projective plane of order $n$ has size at most $n+1$ if $n$ is odd, and size at most $n+2$ if $n$ is even. An **oval** of a projective plane of order $n$ is an arc of size $n+1$ and a **hyperoval** of a projective plane of order $n$

**Example 2.2.1** (Baer 1946 [8], Bose 1947 [23]) A **conic** in $\mathrm{PG}(2,q)$ is the set of zeroes of a non-degenerate homogeneous quadratic polynomial in three variables over $\mathrm{GF}(q)$. A conic in $\mathrm{PG}(2,q)$ is an oval of $\mathrm{PG}(2,q)$. Since all conics are equivalent under the automorphism group $\mathrm{P\Gamma L}(2,q)$ of $\mathrm{PG}(2,q)$, we may assume that a conic $\mathcal{C}$ is the set of zeroes of $y^2 - xz$, and hence up to equivalence a conic $\mathcal{C}$ in $\mathrm{PG}(2,q)$ can be written as

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

This example shows that conics give ovals, and it is natural to ask about the converse. At a conference in Trodheim, Järnefelt and Kustaanheimo 1949 [86] conjectured that every oval of $\mathrm{PG}(2,p)$, $p$ prime, is a conic. In his review of [86], Marshall Hall Jr. said that he found this conjecture implausible.

**Theorem 2.2.2** (Segre 1955 [134]) *An oval of* $\mathrm{PG}(2,q)$, *$q$ odd, is a conic.*

In his review of [134], Marshall Hall Jr. said "The fact that this conjecture seemed implausible to the reviewer seems to have been at least a partial incentive to the author to undertake this work. It would be very gratifying if further expressions of doubt were as fruitful."

A line in a projective plane is **external**, **tangent** or **secant** to an arc, accordingly as it meets the arc in 0, 1 or 2 points.

**Theorem 2.2.3** (Qvist 1952 [130]) *The tangent lines to an oval of a projective plane are concurrent if the order of the plane is even, and form an oval of the dual plane if the order of the plane is odd.*

The intersection of the tangent lines to an oval in a projective plane of even order is called the **nucleus** of the oval. The union of an oval and its nucleus is a hyperoval.

**Example 2.2.4** (Bose 1947 [23]) The union of a conic of $\mathrm{PG}(2,q)$, $q$ even, and its nucleus is a hyperoval of $\mathrm{PG}(2,q)$. A hyperoval of this form is called a **regular hyperoval**. Up to equivalence, a regular hyperoval $\mathcal{H}$ of $\mathrm{PG}(2,q)$ can be wriiten as

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

Two ovals arising from the same hyperoval $\mathcal{H}$ are equivalent if and only if their nuclei are in the same orbit of the stabilizer of $\mathcal{H}$ in the collineation group of the plane. This gives one motiviation for interest in stabilizers of hyperovals.

**Theorem 2.2.5** (Segre 1957 [135], Segre 1962 [136]) *The stabilizer of a regular hyperoval* $\mathcal{H}$ *of* $\mathrm{PG}(2,q)$*,* $q$ *even, in* $\mathrm{P\Gamma L}(3,q)$ *acts transitively if* $q=2$*, in which case it is permutation equivalent in its action on* $\mathcal{H}$ *to* $S_4$ *on* $\{1,2,3,4\}$ *or if* $q=4$*, in which case it is permutation equivalent in its action on* $\mathcal{H}$ *to* $S_6$ *on* $\{1,2,3,4,5,6\}$ *but fixes a point (the nucleus of the unique conic* $\mathcal{C}$ *it contains) if* $q>4$*, in which case it is permutation equivalent in its action on* $\mathcal{C}$ *to* $\mathrm{P\Gamma L}(2,q)$*)on* $\mathrm{PG}(1,q)$.

For $q$ even, $q>4$, if $\mathcal{C}$ is a conic with nucleus $N$ and $P\in\mathcal{C}$, then $(\mathcal{C}\cup\{N\})\setminus\{P\}$ is an oval inequivalent to a conic, called a **pointed conic**. The next result classifies ovals and hyperovals in Desarguesian projective planes of order up to 8.

**Theorem 2.2.6** (Segre 1957 [135], Sce 1960 [131]) *All hyperovals of* $\mathrm{PG}(2,q)$ *are regular for* $q=2,4,8$*. Hence all ovals of* $\mathrm{PG}(2,q)$ *are conics for* $q=2,4$ *and all ovals of* $\mathrm{PG}(2,8)$ *are conics or pointed conics.*

The next natural question is whether **irregular hyperovals** of $\mathrm{PG}(2,q)$ exist for $q>8$. The following construction answers this question in the affirmative.

**Example 2.2.7** (Segre 1957 [135]) The set

$$\mathcal{H}=\{(1,t,t^{\alpha}):t\in\mathrm{GF}(q)\}\cup\{(0,1,0),(0,0,1)\}$$

is a hyperoval of $\mathrm{PG}(2,q)$, $q$ even, if $\alpha$ is a generator of $\mathrm{Aut}\,\mathrm{GF}(q)$. It is irregular if neither $\alpha$ nor $\alpha^{-1}$ is the Frobenius map $x\mapsto x^2$. In this case, the stabilizer of $\mathcal{H}$ in $\mathrm{P\Gamma L}(3,q)$ fixes $(0,1,0)$ and $(0,0,1)$ and is permutation equivalent in its action on $\mathcal{H}\setminus\{(0,1,0),(0,0,1)\}$ to $\mathrm{A\Gamma L}(1,q)$ on $\mathrm{GF}(q)$.

The hyperovals arising from this construction have a particularly nice property. A **translation oval** $\mathcal{O}$ is an oval for which there is a tangent line $\ell$ such that the group of all elations with axis $\ell$ and stabilising $\mathcal{O}$ acts regularly on $\mathcal{O} \setminus \ell$. In this case, $\ell$ is called an **axis** of $\mathcal{O}$. A **translation hyperoval** is a hyperoval containing a translation oval. It is not hard to see that the hyperovals of Example 2.2.7 are translation hyperovals of $\mathrm{PG}(2, q)$, $q$ even. In particular, conics are translation ovals, and every tangent line to a conic is an axis, and so regular hyperovals are translation hyperovals. It turns out that all translation hyperovals arise this way.

**Theorem 2.2.8** (Payne 1971 [115]) *Every translation hyperoval of* $\mathrm{PG}(2, q)$ *is equivalent to*

$$\{(1, t, t^\alpha) : t \in \mathrm{GF}(q)\} \cup \{(0, 1, 0), (0, 0, 1)\},$$

*for some generator* $\alpha$ *of* $\mathrm{Aut}\,\mathrm{GF}(q)$.

The translation hyperovals give examples of irregular hyperovals in $\mathrm{PG}(2, 32)$ and in $\mathrm{PG}(2, 2^h)$ for $h > 6$, while Example 2.2.6 shows that there are no irregular hyperovals in $\mathrm{PG}(2, 2^h)$ for $h < 4$. This raises the question of the existence of irregular hyperovals in $\mathrm{PG}(2, 16)$ and $\mathrm{PG}(2, 64)$, first raised by Segre in 1955 [134]. We will answer this question in Section 2.2.3.

Given the form of the hyperovals in Example 2.2.4, Example 2.2.7 and Theorem 2.2.19, it is not surprising that hyperovals can be put in a canonical form.

**Theorem 2.2.9** (Segre 1962 [136]) *Any hyperoval* $\mathcal{H}$ *of* $\mathrm{PG}(2, q)$*, $q$ even, through* $(0, 1, 0)$ *and* $(0, 0, 1)$ *can be written as*

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

*for some permutation* $f : \mathrm{GF}(q) \to \mathrm{GF}(q)$*. Moreover, if* $f : \mathrm{GF}(q) \to \mathrm{GF}(q)$ *is a permutation,*

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

*is a hyperoval if and only if for all* $x \in \mathrm{GF}(q)$*, the slopes* $\frac{f(x)+f(y)}{x+y}$ *are distinct for all* $y \in GF(q)$*, with* $y \neq x$.

Such a permutation $f$ is called an **o-polynomial** for $\mathcal{H}$, provided $f(0) = 0$ and $f(1) = 1$. If we drop the condition that $f(1) = 1$ (or equivalently, we drop the condition that the oval passes through $(1, 1, 1)$) but retain the other conditions, then $f$ is called an **o-permutation** for $\mathcal{H}$. We can say more about the terms appearing in an o-polynomial.

**Theorem 2.2.10** (Segre 1962 [136], Segre–Bartocci 1971 [140]) *Every o-polynomial can be written in the form*

$$a_2x^2 + a_4x^4 + \cdots + a_{q-2}x^{q-2},$$

*for* $q > 2$.

In light of Theorem 2.2.9 and Theorem 2.2.10, it makes sense to try to categorize hyperovals in terms of their o-polynomials. The simplest case is when a hyperoval has a monomial o-polynomial.

### 2.2.2 Monomial hyperovals

A **monomial hyperoval** of $\mathrm{PG}(2, q)$ is a hyperoval equivalent to $\mathcal{D}(x^n)$ for some integer $n$. We sometimes write $\mathcal{D}(n)$ for $\mathcal{D}(x^n)$ when a hyperoval is monomial. We have already described some monomial hyperovals, namely the regular hyperoval $\mathcal{D}(x^2)$ of Example 2.2.4, and the hyperovals $\mathcal{D}(x^\alpha)$ of Example 2.2.7, where $\alpha$ is a generator of $\mathrm{Aut}\,\mathrm{GF}(q)$. Using Theorem 2.2.9 it is possible to derive necessary and sufficient conditions for the polynomial $x^n$ to be an o-polynomial.

**Theorem 2.2.11** (Segre 1962 [136], Segre–Bartocci 1971 [140]) $\mathcal{D}(x^n)$ *is a hyperoval of* $\mathrm{PG}(2, q)$, $q$ *even, if and only if* $(n, q-1) = (n-1, q-1) = 1$ *and* $x \mapsto ((x+1)^n + 1)/x$ *is a permutation of* $\mathrm{GF}(q)^*$. *In this case* $n$ *and* $n-1$ *are units modulo* $q-1$, *and* $\mathcal{D}(x^n)$ *is equivalent to* $\mathcal{D}(x^m)$ *if and only if* $m = n, 1-n, n/(n-1), 1/n, (n-1)/n$ *or* $1/(1-n)$*modulo* $q-1$.

We can apply this result to get the following hyperovals.

**Theorem 2.2.12** (Segre 1962 [136], Segre–Bartocci 1971 [140]) *$\mathcal{D}(x^6)$ is a hyperoval of* $\mathrm{PG}(2, 2^h)$ *for $h$ odd. It is not a translation hyperoval for $h \geq 5$.*

The hyperoval $\mathcal{D}(x^6)$ of $\mathrm{PG}(2, 2^h)$, $h$ odd, is known as the **Segre–Bartocci hyperoval**.

**Theorem 2.2.13** (Eich–Payne 1972 [60], Hirschfeld 1975 [82]) *$\mathcal{D}(x^{20})$ is a hyperoval of* $\mathrm{PG}(2, 128)$. *It is not a translation hyperoval, nor is it equivalent to $\mathcal{D}(x^6)$.*

In Glynn 1989 [69], a partial order $G$ was introduced on the integers modulo $q-1$ by $a\,G\,b$ if the binary expansion of $b$ dominates the binary expansion of $a$.

**Theorem 2.2.14** (Glynn 1989 [69]) *A polynomial $f$ over $\mathrm{GF}(q)$ with $f(0) = 0$ and $f(1) = 1$ is an o-polynomial over $\mathrm{GF}(q)$ 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 $1 \leq b \leq c \leq q-1$ with $b \neq q-1$ and $b\,G\,c$.*

Applying Theorem 2.2.14 to a monomial function $x^n$, for $n = 1, 2, \ldots, q-2$, we see that $\mathcal{D}(x^n)$ is an o-polynomial if and only if for all $d = 1, 2, \ldots, q-2$, it is not that case that $d\,G\,nd$. This result appears in Glynn 1983 [67] (and so predates [69]) and allowed for efficient programs to search for monomial hyperovals over small fields. By doing this Glynn discovered two new infinite families of hyperovals.

**Theorem 2.2.15** (Glynn 1983 [67]) *Let $q = 2^h$, $h$ odd, $\sigma \in \mathrm{Aut}\,\mathrm{GF}(q)$ such that $\sigma^2 \equiv 2 \pmod{q-1}$, and let $\lambda \in \mathrm{Aut}\,\mathrm{GF}(q)$ such that $\lambda^2 \equiv \sigma \pmod{q-1}$. Then $D(x^{\sigma+\lambda})$ is a hyperoval of* $\mathrm{PG}(2, 2^h)$. *Also, $\mathcal{D}(x^{3\sigma+4})$ is a hyperoval of* $\mathrm{PG}(2, 2^h)$.

$\mathcal{D}(x^{\sigma+\lambda})$ is regular for $h = 1, 3$, irregular translation for $h = 5$, Eich–Payne/Hirschfield for $h = 7$, and new for $h > 7$. $\mathcal{D}(x^{3\sigma+4})$ is regular for $h = 1, 3$, irregular translation for $h = 5$, Segre–Bartocci for $h = 7$, equivalent to $\mathcal{D}(x^{\sigma+\lambda})$ for $h = 9$, and new for $h > 9$.

At the time of their construction the **Glynn hyperovals** were the first new infinite family of hyperovals for over twenty years; their discovery marked the beginning of an era in which a constant stream of new hyperovals emerged. It is also significant that this was the first instance of a computer being used in the construction of an infinite family of hyperovals.

Although the proofs in Glynn 1983 [67] are computer free, the use of computer technology was essential in the discovery of these hyperovals, and this is true of the discovery of most subsequent hyperovals. We look more closely at computer searches for hyperovals in Section 2.2.3.

In his paper Glynn also conjectured that there were no more monomial hyperovals, and this question is still open. Using Theorem 2.2.14, he implemented a fast algorithm and searched for all monomial o-polynomials in $\mathrm{PG}(2, 2^h)$ for $h \leq 19$. He subsequently extended the search and found no new hyperovals.

**Theorem 2.2.16** (Glynn 1989 [69], computer assisted) *For $h \leq 28$ the only monomial hyperovals of $\mathrm{PG}(2, 2^h)$ are the translation hyperovals, the Segre-Bartocci hyperovals and the two families of Glynn hyperovals.*

It seems likely that with the increase of computer power since 1989 that this result could be extended to larger field orders, however the fact that no new hyperovals were found for $h \leq 28$ suggests that a classification of the monomial hyperovals is required and that further computer searches will not be of any use. The first significant result on the classification of monomial hyperovals is the following two bit theorem.

**Theorem 2.2.17** (Cherowitzo–Storme 1998 [46]) *$\mathcal{D}(k)$ with $k = 2^i + 2^j$, $i \neq j$, is a hyperoval in $\mathrm{PG}(2, 2^h)$ if and only if $h = 2e - 1$ is odd, and one of the following holds: (1) $k = 6$ (Segre–Bartocci hyperoval); (2) $k = \sigma + 2$ and $\sigma = 2^e$ (translation hyperoval); (3) $\sigma + \lambda$ with $\sigma = 2^e, \lambda^2 = \sigma$ (Glynn hyperoval); (4) $k = 3/4$ (translation hyperoval).*

This theorem has been extended to a classification of all monomial hyperovals with exponent having three bits.

**Theorem 2.2.18** (Cherowitzo–Vis 2012 [176]) *If $\mathcal{D}(k)$ with $k = 2^{i_1} + 2^{i_2} + 2^{i_3}$ is a hyperoval in $\mathrm{PG}(2, q)$, then it is either a translation hyperoval, a Segre hyperoval, or a Glynn hyperoval.*

### 2.2.3 Hyperovals from computer searches

In 1958, Lunelli and Sce conducted a computer search for hyperovals in small order planes at the suggestion of Segre. They found an irregular hyperoval in $\mathrm{PG}(2,128)$, thus answering the question posed by Segre only a year earlier.

**Theorem 2.2.19** (Lunelli–Sce 1958 [102]) *The set*

$$\begin{aligned}\mathcal{L} =&\{(1,t,\eta^{12}t^2+\eta^{10}t^4+\eta^3t^8+\eta^{12}t^{10}+\eta^9t^{12}+\eta^4t^{14}) : t \in \mathrm{GF}(q)\}\\ &\cup\{(0,1,0),(0,0,1)\}\end{aligned}$$

*is an irregular hyperoval of* $\mathrm{PG}(2,16)$*, where* $\eta \in \mathrm{GF}(16)$ *satisfies* $\eta^4 = \eta + 1$*.*

The **Lunelli–Sce Hyperoval** was the first hyperoval discovered that was not equivalent to one described by a monomial o-polynomial. For many years it was unclear whether $\mathcal{L}$ was contained in an infinite family of hyperovals or was in some sense sporadic. It was only recently that the question was resolved, as $\mathcal{L}$ was placed into two infinite families of hyperovals. The construction of these infinite families is complex, and reveals a deep connection between seemingly unrelated structures. We shall review these constructions in Section 2.2.4.

In O'Keefe–Penttila 1991 [109], the authors search for hyperovals in $\mathrm{PG}(2,32)$ under certain hypotheses on the order of the automorphism group of the putative hyperoval.

**Theorem 2.2.20** (O'Keefe–Penttila 1992 [109], computer assisted) $\mathcal{D}(f)$ *is a new hyperoval of* $\mathrm{PG}(2,32)$*, where*

$$\begin{aligned}f(t) = t^4 &+ \eta^{11}t^6+\eta^{20}t^8+\eta^{11}t^{10}+\eta^6t^{12}+\eta^{11}t^{14}+t^{16}\\ &+\eta^{11}t^{18}+\eta^{20}t^{20}+\eta^{11}t^{22}+\eta^6t^{24}+\eta^{11}t^{26}+t^{28},\end{aligned}$$

*and* $\eta \in \mathrm{GF}(32)$ *satisfies* $\eta^5 = \eta^2+1$*. The full stabiliser of this hyperoval in* $\mathrm{P\Gamma L}(3,32)$ *has order* 3*.*

One of the intriguing properties of the **O'Keefe-Penttila hyperoval** is its reluctance to be a member of an infinite family. It is known not to be a member of any of the existing infinite families of hyperovals, and moreover, it is also known not to arise by general construction methods that yield all other known hyperovals.

By extending the methods of [109] to PG(2, 64), Penttila and Pinneri were able to search for hyperovals whose automorphism group admitted a collineation of order 5. They found two such hyperovals and showed that no other hyperovals with this property existed, thus solving the part of Segre's question left open by Lunelli and Sce 36 years earlier.

**Theorem 2.2.21** (Penttila–Pinneri 1994 [125], computer assisted) *There is an irregular hyperoval* $\mathcal{D}(f)$ *in* PG(2, 64) *with full stabiliser in* $\mathrm{P\Gamma L}(3, 64)$ *of order* 60*, and another* $\mathcal{D}(g)$ *with full stabiliser in* $\mathrm{P\Gamma L}(3, 64)$ *of order* 15*, where*

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

*and*

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

*and* $\beta$ *is a primitive element of* GF(64) *satisfying* $\beta^6 = \beta + 1$.

By refining the previous search algorithm, Penttila and Royle were able to extend the search to hyperovals admitting an automorphism of order 3, and found further hyperovals.

**Theorem 2.2.22** (Penttila–Royle 1995 [127], computer assisted) *There is an irregular hyperoval* $\mathcal{D}(f)$ *in* $\mathrm{PG}(2,64)$ *with full stabiliser in* $\mathrm{P\Gamma L}(3,64)$ *of order* 12*, where*

$$\begin{aligned} f(x) = x^4 + x^8 + x^{14} + x^{34} + x^{42} + x^{48} + x^{62} \\ + \ \beta^{21}(x^6 + x^{16} + x^{26} + x^{28} + x^{30} + x^{32} + x^{40} + x^{58}) \\ + \ x^{18} + x^{24} + x^{36} + x^{44} + x^{50} + x^{52} + x^{60} \end{aligned}$$

*where* $\beta$ *is a primitive element of* $\mathrm{GF}(64)$ *satisfying* $\beta^6 = \beta + 1$.

**Theorem 2.2.23** (Penttila–Royle 1995 [127], computer assisted) *There is a non-monomial hyperoval of* $\mathrm{PG}(2,128)$ *with full stabilizer in* $\mathrm{P\Gamma L}(3,128)$ *of order* 14 *which is inequivalent to the Payne and Cherowitzo hyperovals. There are at least two inequivalent non-translation hyperovals of* $\mathrm{PG}(2,256)$ *with full stabiliser in* $\mathrm{P\Gamma L}(3,256)$ *of order* 16*.*

It is clear from the complexity of the o-polynomials associated with these hyperovals that they were not found by traditional analytic techniques. Indeed, the existence of such complicated o-polynomials seems to suggest that classification of hyperovals is a very difficult problem. Before further progress could be achieved, it was clear that new techniques were required. We investigate some of these techniques in Section 2.2.4.

### 2.2.4 Hyperovals from $q$-clans

Let $\mathcal{C}$ be a conic in $\mathrm{PG}(2,q)$, and let $\mathrm{PG}(2,q)$ be embedded as a hyperplane in $\mathrm{PG}(3,q)$. For a point $v \in \mathrm{PG}(3,q) \setminus \mathrm{PG}(2,q)$, the union of the points on the lines incident with $v$ and a point of $\mathcal{C}$ is the **quadratic cone** with **vertex** $v$ and **base** $\mathcal{O}$. A **flock** of a quadratic cone $\mathcal{K}$ with vertex $v$ is a set of $q$ planes which partitions $K \setminus \{v\}$ into disjoint conics. Flocks will be explored in detail in Chapter 3.

Choose $\mathcal{K} = \{(x,y,z,w) : y^2 = xz\}$ as the quadratic cone. The planes determining the flock would thus satisfy equations of the form $a_t x + b_t y + c_t y + w = 0$ for $t \in \mathrm{GF}(q)$. The set of matrices

$$\left\{ \begin{pmatrix} a_t & b_t \\ 0 & c_t \end{pmatrix} : t \in \mathrm{GF}(q) \right\}$$

has the property that the difference of any two distinct matrices is **anisotropic**, that is, the equation $x(A_s - A_t)x^t = 0$ has only the trivial solution for $s \neq t$. A set of $q$ matrices $\{A_t : t \in \mathrm{GF}(q)\}$ indexed by $\mathrm{GF}(q)$ such that the difference of distinct matrices is anisotropic is called a $q$-**clan**. Without loss of generality we an assume that $A_t = \begin{pmatrix} f(t) & t^{1/2} \\ 0 & ag(t) \end{pmatrix}$, where $\mathrm{trace}\,(a) = 1$, $f, g : \mathrm{GF}(q) \to \mathrm{GF}(q)$, $f(0) = g(0) = 0$, $f(1) = g(1) = 1$, and

$$\mathrm{trace}\left(\frac{a(f(s) + f(t))(g(s) + g(t))}{s + t}\right) = 1$$

for all $s, t \in \mathrm{GF}(q)$, $s \neq t$. Such a $q$-clan is called **normalized** if it is in this standard form. The relationship between $q$-clans and ovals is described in the following theorem.

**Theorem 2.2.24** (Payne 1985 [118], Cherowitzo–Penttila–Pinneri–Royle 1996 [44]) *Let $q$ be even. Let $f, g : \mathrm{GF}(q) \to \mathrm{GF}(q)$ with $f(0) = g(0) = 0$, $f(1) = g(1) = 1$. Then*

$$\mathrm{trace}\left(\frac{\kappa(f(s) + f(t))(g(s) + g(t))}{s + t}\right) = 1$$

*if and only if $g$ is an o-polynomial, $f_s$ is an o-polynomial for all $s \in \mathrm{GF}(q)$, where*

$$f_s(x) = \frac{f(x) = \kappa s g(x) + s^{1/2}x^{1/2}}{1 + \kappa s + s^{1/2}},$$

*and* $\mathrm{trace}\,(\kappa) = 1$.

A **herd** of ovals in $\mathrm{PG}(2, q)$, $q$ even, is a family of $q + 1$ ovals $\{\mathcal{O}_s : s \in \mathrm{GF}(q) \cup \{\infty\}\}$, each containing $(1, 0, 0)$, $(0, 1, 0)$, and $(1, 1, 1)$, and with nucleus $(0, 0, 1)$, with

$$\mathcal{O}_s = \{(1, t, f_s(t)) : t \in \mathrm{GF}(q)\} \cup \{(0, 1, 0)\},\ s \in \mathrm{GF}(q),$$
$$\mathcal{O}_\infty = \{(1, t, g(t)) : t \in \mathrm{GF}(q)\} \cup \{(0, 1, 0)\},$$

where

$$f_s(t) = \frac{f(x) = \kappa s g(x) + s^{1/2}x^{1/2}}{1 + \kappa s + s^{1/2}},$$

for some $\kappa$ with $\mathrm{trace}\,(\kappa) = 1$. We define a herd of hyperovals in the natural way.

Thus, Theorem 2.2.24 says that for $q$ even, a $q$-clan gives rise to a herd of ovals of $\mathrm{PG}(2, q)$, and conversely. $q$-clans are also linked to other structures, for example, there is a connection between $q$-clans and generalized quadrangles, a connection between $q$-clans and flocks of the quadratic cone, and a connection between flocks of the quadratic cone and translation planes. These connections will be explored in Chapter 3. Given a $q$-clan $\mathcal{C}$, we denote by $\mathrm{H}(C)$ the corresponding herd, $\mathrm{GQ}(C)$ the corresponding generalized quadrangle, $\mathcal{F}(C)$ the corresponding flock, and $\pi(C)$ the corresponding translation plane.

**Example 2.2.25** (Thas 1987 [151]) For $q = 2^h$,

$$C_1 = \left\{ \begin{pmatrix} t^{1/2} & t^{1/2} \\ 0 & \kappa t \end{pmatrix} : t \in \mathrm{GF}(q) \right\},$$

for $a \in \mathrm{GF}(q)$, $\mathrm{trace}\,(a) = 1$, is the **classical $q$-clan**. The associated flocks $\mathcal{F}(C_1)$ are the **linear flocks**. The herd $\mathrm{H}(C_1)$ consists of $q+1$ nondegenerate conics. The generalized quadrangle $\mathrm{GQ}(C_1)$ is isomorphic to $\mathrm{H}(3, q^2)$, and the translation plane $\pi(C_1)$ is Desarguesian.

**Example 2.2.26** (Fisher–Thas 1979 [64], Walker 1976 [177], Kantor 1980 [90], Betten 1973 [17]) For $q = 2^h$, $h$ odd,

$$C_2 = \left\{ \begin{pmatrix} t^{1/4} & t^{1/2} \\ 0 & t^{3/4} \end{pmatrix} : t \in \mathrm{GF}(q) \right\}$$

is the **FTWKB $q$-clan**. The flock $\mathcal{F}(C_2)$ is due to Fisher–Thas 1979 [64], and is linear when $q = 2$. The translation plane $\pi(C_2)$ is due to Walker 1976 [177], and independently, Betten 1973 [17]. The generalized quadrangle $\mathrm{GQ}(C_2)$ is due to Kantor 1980 [90]. The herd $\mathrm{H}(C_2)$ consists of $q+1$ irregular translation ovals if $q > 2$.

The examples of $q$-clans given so far have not yielded any new hyperovals. At the time of publication, the following example of Payne 1985 [118] constructs the first infinite family of non-monomial hyperovals, and the only known examples of such a hyperoval apart from the example of Lunelli Sce 1958 [102].

**Example 2.2.27** (Payne 1985 [118]) For $q = 2^h$, $h$ odd,

$$C_3 = \left\{ \begin{pmatrix} t^{1/6} & t^{1/2} \\ 0 & t^{5/6} \end{pmatrix} : t \in \mathrm{GF}(q) \right\}$$

is the **Payne $q$-clan**. It is classical if and only if $q = 2$, and FTWKB if and only $q = 8$. The herd $\mathrm{H}(C_3)$ consists of two Segre–Bartocci hyperovals and $q-1$ previously unknown hyperovals, the **Payne hyperovals**, which are equivalent to $D(x^{1/6} + x^{1/2} + x^{5/6})$.

**Example 2.2.28** (Cherowitzo–Penttila–Pinneri–Royle 1996 [44]) For $q = 2^h$,

$$C_4 = \left\{ \begin{pmatrix} f(t) & t^{1/2} \\ 0 & \kappa g(t) \end{pmatrix} : t \in \mathrm{GF}(q) \right\}$$

is a $q$-clan, where

$$\begin{aligned} \kappa &= \frac{d^2 + d^5 + d^{1/2}}{d(1 + d + d^2)} \\ f(x) &= \frac{d^2(x^4 + x) + d^2(1 + d + d^2)(x^3 + x^2)}{(x^2 + dx + 1)^2} + x^{1/2} \\ g(x) &= \frac{d^4x^4 + d^3(1 + d^2 + d^4)x^3 + d^3(1 + d^2)x}{(d^2 + d^5 + d^{1/2})(x^2 + dx + 1)^2} + \frac{d^{1/2}}{(d^2 + d^5 + d^{1/2})}x^{1/2} \end{aligned}$$

and $d \in \mathrm{GF}(q)$ with $d^2 + d + 1 \neq 0$ and $\mathrm{trace}\,(1/d) = 1$. This is the **Subiaco $q$-clan**. It is classical if and only if $q = 2$ or 4, and FTWKB (or Payne) if and only if $q = 8$. The herd $\mathrm{H}(C_4)$ consists of new hyperovals, the so-called **Subiaco hyperovals** $\mathcal{D}(f)$, $\mathcal{D}(g)$, and $\mathcal{D}(f(x) + sg(x) + s^{1/2}x^{1/2})$, for each $s \in \mathrm{GF}(q)$. When $h \equiv 2 \pmod 4$, up to isomorphism there are two Subiaco hyperovals, and when $h \not\equiv 2 \pmod 4$, up to isomorphism there is only one. The Subiaco hyperovals are not equivalent to any other known family for $q > 32$. When $q = 16$, the associated flock $\mathcal{F}(C_4)$ is due to DeClerk–Herssens 1993 [157]. The Subiaco hyperovals include the Penttila–Royle 1995 [127] hyperovals for $q = 128$ and $q = 256$ (in the former case just one of them), the Penttila–Pinneri 1994 [125] hyperovals for $q = 64$ (both of them), the Payne 1985 [118] hyperoval for $q = 32$ and the Lunelli–Sce 1958 [102] hyperoval for $q = 16$ as special cases.

**Example 2.2.29** (Cherowitzo–O'Keefe–Penttila 2003 [45]) Let $\beta \in \mathrm{GF}(q^2)$, $\beta \neq 1$ such that $\beta^{q+1} = 1$. Define $T(x) = x + x^q$ for all $x \in \mathrm{GF}(q^2)$, $q = 2^h$, $m = (q - 1)/3$. Then

$$\mathcal{C}_5 = \left\{ \begin{pmatrix} f(t) & t^{1/2} \\ 0 & \kappa g(t) \end{pmatrix} : t \in \mathrm{GF}(q) \right\}$$

is a $q$-clan, for $q = 4^h$, where

$$\begin{aligned} \kappa &= \frac{T(\beta^m)}{T(\beta)} + \frac{1}{T(\beta^m)} + 1 \\ f(t) &= \frac{T(\beta^m)(t + 1)}{T(\beta)} + \frac{T((\beta t + \beta^q)^m)}{t(\beta)(t + T(\beta)t^{\frac{1}{2}} + 1)^{m-1}} + t^{\frac{1}{2}} \\ \kappa g(t) &= \frac{T(\beta^m)}{T(\beta)}t + \frac{T((\beta^2 + 1)^m)}{t(\beta)T(\beta^m)(t + T(\beta)t^{1/2} + 1)^{m-1}} + \frac{1}{T(\beta^m)}t^{1/2}. \end{aligned}$$

This is the **Adelaide $q$-clan**, and the hyperovals $\mathcal{D}(f)$ are the **Adelaide hyperovals**. The Adelaide hyperovals include the second Penttila–Royle 1995 [127] hyperoval for $q = 256$, the Penttila–Royle 1994 [125] hyperoval for $q = 64$ and the Lunelli–Sce 1958 [102] hyperoval for $q = 16$, as special cases. They are not translation hyperovals for $q > 4$ and not Subiaco hyperovals for $q > 16$, and are hence not equivalent to a known family.

### 2.2.5 Hyperovals from $\alpha$-flocks

Cherowitzo 1998 [43] generalizes the work in Section 2.2.4 by applying the concept of a flock to the more general cones over translation ovals, and develops the analogous theory which depends on automorphisms of the underlying field. He defines an **$\alpha$-cone** in $\mathrm{PG}(3, q)$ to be the set of points $\Sigma_\alpha = \{(x, y, z, w) : y^\alpha = xz^{\alpha-1}\}$ together with vertex $(0, 0, 0, 1)$, where $\alpha$ is an automorphism of $\mathrm{GF}(q)$ generating $\mathrm{Aut}\,\mathrm{GF}(q)$. An $\alpha$-flock is a set of $q$ planes of $\mathrm{PG}(3, q)$ not passing through the vertex which do not intersect each other in a point of $\Sigma_\alpha$. An **$\alpha$-clan** is a set of $q$ upper triangular matrices

$$\left\{ \begin{pmatrix} a_t & b_t \\ 0 & c_t \end{pmatrix} : t \in \mathrm{GF}(q) \right\}$$

such that there exists a $\kappa \in \mathrm{GF}(q)$ with $\mathrm{trace}\,(\kappa) = 1$ such that

$$\mathrm{trace}\left( \kappa \frac{(a_t + a_s)^{1/(\alpha-1)}(c_t + c_s)}{(b_t + b_s)^{\alpha/(\alpha-1)}} \right) = 1$$

for all $s \neq t$. A new definition of a herd is also given. With these definitions, there are connections between $\alpha$-clans, $\alpha$-flocks, and hyperovals, the most important for us is given in the following theorem.

**Theorem 2.2.30** (Cherowitzo 1998 [43]) *If*

$$\left\{ \begin{pmatrix} f(t) & t^{1/\alpha} \\ 0 & g(t) \end{pmatrix} : t \in \mathrm{GF}(q) \right\}$$

*is an $\alpha$-clan then $f(t)$ is an o-polynomial.*

By using this theorem, the last known family of hyperovals is constructed.

**Theorem 2.2.31** (Cherowitzo 1998 [43]) *Let $q = 2^h$, $h$ odd, $\sigma^2 \equiv 2 \pmod{q-1}$. Then*

$$\left\{ \begin{pmatrix} f(t) & t^{1/\alpha} \\ 0 & g(t) \end{pmatrix} : t \in \mathrm{GF}(q) \right\}$$

*is an $\alpha$-clan, for $\alpha = \sigma$, where*

$$f(t) = t^{\sigma} + t^{\sigma+2} + t^{3\sigma+4},$$

$$g(t) = t^{\sigma} + t^{3\sigma+2} + t^{3\sigma+6} + t^{5\sigma+4} + t^{5\sigma+8} + x^{7\sigma+10} + x^{9\sigma+12}.$$

*Hence, $\mathcal{D}(x^{\sigma} + x^{\sigma+2} + x^{3\sigma+4})$ are hyperovals of $\mathrm{PG}(2, 2^h)$, $h$ odd, known as the* ***Cherowitzo hyperovals****. These hyperovals are not equivalent to any known family of hyperovals for $q > 8$.*

Note that the definition of an $\alpha$-clan includes $q$-clans in the special case $\alpha = 2$. Cherowitzo 1998 [43] shows that both of the Glynn hyperovals have o-polynomials arising from an $\alpha$-clan for $\alpha = \sigma$. This means that all known hyperovals with the exception of the O'Keefe-Penttila 1991 hyperoval in $\mathrm{PG}(2, 32)$ contain ovals equivalent to one contained in an oval herd of an $\alpha$-clan. Cherowitzo 1998 [43] conjectures that there is a missing $\alpha$-clan having an oval herd containing ovals from this hyperoval, however this has been disproved by Brown–O'Keefe–Penttila–Royle 2007 [28].

### 2.2.6 Summary

There are 10 known infinite families of hyperovals in $\mathrm{PG}(2, q)$: the regular hyperovals, the translation hyperovals of Segre 1957 [135], the hyperovals of Segre–Bartocci 1971 [140], the two families of hyperovals of Glynn 1983 [67], the hyperovals of Payne 1985 [118], the two families of Subiaco hyperovals of Cherowitzo–Penttila–Pinneri–Royle 1996 [44], the hyperovals of Cherowitzo 1998, and the Adelaide hyperovals of Cherowitzo–O'Keefe–Penttila 2003 [45]. Moreover, there is only one known hyperoval that does not fit into one of these families, namely the O'Keefe Penttila 1991 [109] hyperoval of $\mathrm{PG}(2, 32)$. For convenience, we list the known hyperovals and their automorphism groups in Table 2.1. Notice that in general, the hyperovals with the large automorphism groups were discovered before hyperovals with smaller automorphism groups. We will discuss this phenomenon more in Section 2.5.

Table 2.1: The known hyperovals $\mathcal{H} = \mathcal{D}(f)$ of $\mathrm{PG}(2,q)$ and their automorphism groups, where $q = 2^h$, and $\lambda^4 \equiv \sigma^2 \equiv 2 \pmod{q-1}$.

| Name | $f(x)$ | Field Restriction | Aut $\mathcal{H}$ |
|---|---|---|---|
| Regular | $x^2$ | $q = 2$<br>$q = 4$<br>$q > 4$ | $S_4$<br>$S_6$<br>$\mathrm{P\Gamma L}(2,q)$ |
| Translation | $x^{2^i}$, $(i,h) = 1$ | none | $\mathrm{A\Gamma L}(1,q)$ |
| Segre–Bartocci | $x^6$ | $q = 32$<br>$q > 32$, $h$ odd | $(C_{q-1} \rtimes C_3) \rtimes C_h$<br>$C_{q-1} \rtimes C_h$ |
| Glynn I | $x^{3\sigma+4}$ | $q = 128$<br>$q > 128$, $h$ odd | $(C_{q-1} \rtimes C_3) \rtimes C_h$<br>$C_{q-1} \rtimes C_h$ |
| Glynn II | $x^{\sigma+\lambda}$ | $q > 512$, $h$ odd | $C_{q-1} \rtimes C_h$ |
| Payne | $x^{1/6} + x^{1/2} + x^{5/6}$ | $q \geq 32$, $h$ odd | $C_{2h}$ |
| Adelaide | see Example 2.2.29 | $q \geq 64$, $h$ even | $C_{2h}$ |
| Subiaco I | see Example 2.2.28 | $q \geq 32$ | $C_{2h}$ |
| Subiaco II | see Example 2.2.28 | $q \geq 64$, $h \equiv 2$ (mod 4) | $C_5 \rtimes C_{2h}$ |
| Cherowitzo | $x^{\sigma} + x^{\sigma+2} + x^{3\sigma+4}$ | $q \geq 32$, $h$ odd | $C_h$ |
| O'Keefe–Penttila | see Theorem 2.2.20 | $q = 32$ | $C_3$ |

## 2.3 Background results

In Section 2.4, we derive some general results about groups acting on hyperovals in Desarguesian planes. We will need some preliminary results, which we collect in this section. The mainstay of our approach to groups of hyperovals of Desarguesian planes are the following two fundamental results of Hartley on groups of homographies of Desarguesian planes.

A **Singer cycle** is a cyclic subgroup of $\mathrm{PGL}(3, q)$ of order $q^2 + q + 1$.

**Theorem 2.3.1** (Hartley 1925 [75]) *A proper subgroup of* $\mathrm{PSL}(3, q)$*, $q$ even, fixes a point, a line, a triangle, a subplane, or a classical unital, or is contained in the normalizer of a Singer cycle, or $q = 4$ and the subgroup fixes a hyperoval.*

**Theorem 2.3.2** (Hartley 1925 [75]) *A proper subgroup of* $\mathrm{PSU}(3, q)$*, $q$ even and a square, fixes a point, a line, a triangle or a subplane, or is contained in the normalizer of a Singer cycle, or* $q = 4$ *and the order of the subgroup is 36.*

A group of collineations of a projective plane is **irreducible** if it fixes no point, line or triangle. It is **strongly irreducible** if it is irreducible and fixes no proper subplane.

**Corollary 2.3.3** *A strongly irreducible proper subgroup $G$ of* $\mathrm{PSL}(3, q)$*, $q$ even, $q > 4$, is contained in the normalizer of a Singer cycle, or $q$ is a square and $G =$* $\mathrm{PSU}(3, q)$*.*

We also need information about the subgroups of $\mathrm{PGL}(2, q)$, $q$ even, for which a convenient reference is Dickson 1901 [58], although the result is due, independently, to Wiman 1899 [180] and Moore 1903 [106].

**Theorem 2.3.4** (Dickson 1901 [58]) *The only non-abelian composition factors of subgroups of* $\mathrm{PGL}(2, q)$*, $q$ even, are* $\mathrm{PSL}(2, q_0)$*, with $q$ a power of $q_0$. The subgroups of* $\mathrm{PGL}(2, q)$*, $q$ even, $q > 8$, of order greater than* $3(q - 1)$ *contain a Sylow 2-subgroup of* $\mathrm{PGL}(2, q)$*.*

**Corollary 2.3.5** *The only non-abelian composition factors of subgroups of* $\mathrm{P\Gamma L}(3, q)$*, $q$ even, are* $\mathrm{PSL}(3, q_0)$*,* $\mathrm{PSL}(2, q_0)$*,* $\mathrm{PSU}(3, q_0)$ *and $A_6$, where $q$ is a power of $q_0$.*

**Proof** Let $H$ be an insoluble subgroup of $\mathrm{P\Gamma L}(3,q)$, $q$ even. Then $H \cap \mathrm{PSL}(3,q)$ is insoluble. By Theorem 2.3.1, Theorem 2.3.2 and Theorem 2.3.4, either $H \cap \mathrm{PSL}(3,q)$ contains $\mathrm{PSL}(3,q_0)$ or $\mathrm{PSU}(3,q_0)$ or $A_6$, since the stabilizer of a triangle is soluble, and the groups of collineations with centre a point or axis a line are soluble, and the group induced by the stabilizer of a point in $H \cap \mathrm{PSL}(3,q)$ on the lines through that point is a subgroup of $\mathrm{PGL}(2,q)$. □

We now survey elementary results on groups of hyperovals that also apply in the non-Desarguesian case. Deeper results, using theorems about simple groups, can be found in the papers of Korchmáros.

Recall, a collineation of a projective plane is **central** if it fixes a point (the center) linewise, and a line (the axis) pointwise. If the center is incident with the axis, the collineation is an **elation**, and if the center is not incident with the axis, it is a **homology**.

Involutions play an important role. Their action on projective planes is determined by the following result of Baer.

**Theorem 2.3.6** (Baer 1946 [8]) *An involutory collineation of a projective plane of order $q$, $q$ even, is either an elation or a Baer involution, in which case $q$ is a square.*

More can be said when the involution is an elation and fixes a hyperoval.

**Theorem 2.3.7** (Biliotti–Korchmáros 1987 [19]) *A non-trivial central collineation of a projective plane of order $q$, $q$ even, fixing a hyperoval is necessarily an involutory elation with centre not on the hyperoval.*

**Proof** Since the orbits of a point, not the centre, not on the axis, are collinear and have length the order of the collineation, any point on the hyperoval, not on the axis, not the centre, has an orbit of length 2. The collineation is therefore involutory. By Theorem 2.3.6, it is an elation. Since there is a point on the hyperoval not on the axis, the orbit of that point, together with the centre, forms a collinear triple; so the centre is not on the hyperoval. □

The following result of Hughes controls involutions for planes of order 2 modulo 4.

**Theorem 2.3.8** (Hughes 1957 [85]) *A projective plane of order $q > 2$, $q \equiv 2 \pmod 4$, has no involutory collineations.*

Further control of elations fixing hyperovals follows from the next result of Penttila–Royle.

**Theorem 2.3.9** (Penttila–Royle 1995 [127]) *A non-trivial central collineation of a finite projective plane of even order $q > 2$ fixing a hyperoval $\mathcal{H}$, is necessarily an elation with axis secant to $\mathcal{H}$ and centre not on $\mathcal{H}$.*

**Proof** By Theorem 2.3.7, we need only show that the axis is a secant line for $q > 2$. By Theorem 2.3.8, $q \equiv 0 \pmod 4$. So the number of points on the hyperoval is congruent to 2 modulo 4. Thus the number of secant lines on any point $P$ on the axis, not the centre, and not on the hyperoval, is odd. Hence a secant line is fixed. But the only fixed line on $P$ is the axis, so it follows that the axis is a secant line. □

The following elementary observation of Biliotti–Korchmáros about two elations fixing a hyperoval is fundamental.

**Theorem 2.3.10** (Biliotti–Korchmáros 1987 [19]) *Two non-trivial central collineations of a finite projective plane of even order $q > 4$ fixing a hyperoval have different centres.*

More detailed information is given in the next result of Biliotti–Korchmáros, an alternative proof of which was found by Penttila–Pinneri.

**Theorem 2.3.11** (Biliotti–Korchmáros 1987 [19], Penttila–Pinneri 1999 [126]) *Let $\mathcal{H}$ be a hyperoval in a projective plane $\pi$ of order $q$, and suppose that two distinct non-trivial elations of $\pi$ stabilize $\mathcal{H}$. Then one of the following holds:*

*(1) the elations have different centres but the same axis, which is secant to $\mathcal{H}$, and the product of the elations is an involutory elation with the same axis but a different centre;*

*(2) the axes are distinct and meet at a point of $\mathcal{H}$, 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* $q+1$*;*

*(3) the axes are distinct secant lines which meet at a point not on* $\mathcal{H}$*, the centres are distinct and the line joining the centres is external to* $\mathcal{H}$*, the product of the elations has order 3, and* $q \equiv 1 \pmod 3$*;*

*(4)* $q = 2$ *or* $4$*.*

**Corollary 2.3.12** *No hyperoval of a projective plane of order* $q$*, with* $q \not\equiv 1 \pmod 3$*, is stabilized by 3 non-trivial elations with axes forming a triangle.*

A bound on the order of the homography stabilizer of a hyperoval of a Desarguesian plane is given in the following theorem.

**Theorem 2.3.13** (O'Keefe–Penttila 1991 [108]) *The stabilizer in* $\mathrm{P\Gamma L}(3,q)$ *of a hyperoval in* $\mathrm{PG}(2,q)$*,* $q > 2$*, has order dividing* $(q+2,3)(q+1)q(q-1)$*.*

The next result allows greater control of one of Hartley's cases, when a hyperoval is fixed.

**Corollary 2.3.14** *A subgroup of the normalizer in* $\mathrm{PGL}(3,q)$*,* $q$ *even, of a Singer cycle stabilizing a hyperoval is a 3-group, and fixes a point or a triangle.*

**Proof** The greatest common divisor of $(q+2,3)(q+1)q(q-1)$ and $3(q^2+q+1)$ divides 9. □

## 2.4 Groups of hyperovals in $\mathrm{PG}(2,q)$

**Lemma 2.4.1** [15] *A strongly irreducible proper subgroup of* $\mathrm{PSL}(3,4)$ *that does not fix a classical unital is the stabilizer* $A_6$ *in* $\mathrm{PSL}(3,4)$ *of a hyperoval of* $\mathrm{PG}(2,4)$*.*

**Proof** By Theorem 2.3.1, the only case to eliminate is that of a subgroup of the normalizer of a Singer cycle. But when $q = 4$, the intersection of the normalizer in $\mathrm{PGL}(3,q)$ of a Singer cycle with $\mathrm{PSL}(3,q)$ fixes a subplane. □

The following Lemma is reminiscent of results in Bonisoli–Korchmáros 2002 [22]. The reader may find it helpful to compare and contrast the approaches.

**Lemma 2.4.2** [15] *If the stabilizer $G$ in* $\mathrm{PGL}(3,q)$ *of a hyperoval in* $\mathrm{PG}(2,q)$, $q > 4$, *is irreducible, then* $G \cap \mathrm{PSL}(3,q)$ *is irreducible.*

**Proof** Suppose $G \cap \mathrm{PSL}(3,q)$ is not irreducible. If $G \neq G \cap \mathrm{PSL}(3,q)$, then $|G : G \cap \mathrm{PSL}(3,q)| = 3$. Suppose $G \cap \mathrm{PSL}(3,q)$ fixes a point $P$. Then $G_P \geq G \cap \mathrm{PSL}(3,q)$, and so the orbit of $P$ under $G$ has length 1 or 3, a contradiction. Hence $G \cap \mathrm{PSL}(3,q)$ does not fix a point, and dually, $G \cap \mathrm{PSL}(3,q)$ does not fix a line. So $G \cap \mathrm{PSL}(3,q)$ fixes a triangle $\Delta$, and $G_\Delta = G \cap \mathrm{PSL}(3,q)$. We show that $G_{(\Delta)}$ is a 3-group. Suppose not. Let $p$ be a prime dividing $\left|G_{(\Delta)}\right| \,\Big|\, \left|\mathrm{PGL}(3,q)_{(\Delta)}\right| = (q-1)^2$. Then $p \neq 2$, since elations do not pointwise fix a triangle. So $p > 3$. Let $1 \neq P \in \mathrm{Syl}_p\left(G_{(\Delta)}\right)$. Since $P$ is not generated by a homology, $|P| \mid q-1$. Hence $\mathrm{fix}(P) = \Delta$. However, $\mathrm{PGL}(3,q)_{(\Delta)} = C_{q-1} \times C_{q-1}$ is abelian, so $P$ is its unique Sylow $p$-subgroup. Therefore $P$ char $G_{(\Delta)} \lhd G \cap \mathrm{PSL}(3,q)$ implies $P$ char $G \cap \mathrm{PSL}(3,q) \lhd G$. Hence $P \lhd G$, and so $G$ fixes $\Delta$, a contradiction.

Without loss of generality, $\Delta = \{(1,0,0),(0,1,0),(0,0,1)\}$. For all $a \in \mathrm{GF}(q)^*$ such that there exists $b \in \mathrm{GF}(q)^*$ with $\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & 1 \end{pmatrix} \in G_{(\Delta)}$, $b$ is unique (otherwise $G_{(\Delta)}$ would contain a homology). So

$$G_{(\Delta)} = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & f(a) & 0 \\ 0 & 0 & 1 \end{pmatrix} : a \in S \right\}$$

where $S \leq \mathrm{GF}(q)^*$ and $f : S \to \mathrm{GF}(q)^*$ is a homomorphism. Since $S$ is the unique cyclic group of $\mathrm{GF}(q)^*$ of order $|S|$, and $f(S) \leq S$, it follows that $f(x) = x^n$ for some $n$. Hence

$$G_{(\Delta)} = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & a^n & 0 \\ 0 & 0 & 1 \end{pmatrix} : a \in S \right\}.$$

But $\begin{pmatrix} a^n & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & a \end{pmatrix} = \begin{pmatrix} a^{n-1} & 0 & 0 \\ 0 & a^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix} \in G_{(\Delta)}$, and so $a^{n(n-1)} = a^{-1}$, forcing $n^2 - n + 1 \equiv 0 \pmod{|S|}$. Since there are no solutions to this congruence modulo 9, it follows that $|S| = 3$. But now $|G| = 9$ or 18, and up to conjugacy $G \leq \mathrm{PGU}(3,4)$, and $G$ fixes a triangle, a contradiction. $\square$

**Theorem 2.4.3** [15] *The stabilizer $G$ in* $\mathrm{PGL}(3,q)$ *of a hyperoval in* $\mathrm{PG}(2,q)$ *fixes a point, line, triangle, or a subplane* $\pi_0$ *of order 4. If $G$ is irreducible, then either* $q = 4$ *and* $G \cong A_6$*, or* $q > 4$ *and the group induced by $G$ on* $\pi_0$ *is a subgroup of* $\mathrm{PGU}(3,4)$.

**Proof** Suppose $q > 4$ and $G$ is irreducible. Then $G \cap \mathrm{PSL}(3,q)$ is irreducible by Theorem 2.4.2. Since $\mathrm{PSU}(3,q_0)$ contains a group of order $q_0$ of elations with the same centre, $G \cap \mathrm{PSL}(3,q)$ cannot induce $\mathrm{PSU}(3,q_0)$ on any subplane of order $q_0 > 2$ by Theorem 2.3.10, and is not contained in the normalizer of a Singer cycle by Theorem 2.3.14. Hence, $G \cap \mathrm{PSL}(3,q)$ is a proper subgroup of $\mathrm{PSL}(3,q)$, and fixes a subplane by Theorem 2.3.3.

Let $\pi_0$ be a minimal non-trivial subplane of order $q_0$ fixed by $G \cap \mathrm{PSL}(3,q)$ and let $L$ be the group induced by $G \cap \mathrm{PSL}(3,q)$ on $\pi_0$. Then $L$ is strongly irreducible, and by Theorem 2.3.3 applied to $L \cap \mathrm{PSL}(3,q_0)$, it follows that $\pi_0$ has order 4. (Note that a group inducing a subgroup of the normalizer of a Singer cycle of $\pi_0$ either fixes a triangle of $\mathrm{PG}(2,q)$, or is a subgroup of the normalizer of a Singer cycle of $\mathrm{PG}(2,q)$, which eliminates this case.) If $L \cap \mathrm{PSL}(3,q)$ is not a subgroup of $\mathrm{PSU}(3,4)$, then $L \cap \mathrm{PSU}(3,4)$ fixes a hyperoval of $\mathrm{PG}(2,4)$ by Theorem 2.4.1 and Theorem 2.3.1. Thus $L \cap \mathrm{PSL}(3,4) = A_6$ or $\mathrm{PSL}(2,5)$, however both of these contain distinct elations with the same centre, contradicting Theorem 2.3.10. Since $G$ normalizes $G \cap \mathrm{PSL}(3,q)$, it follows that in this case $G = G \cap \mathrm{PSL}(3,q)$ and has order 36 by Theorem 2.3.2. □

Which insoluble groups can act on hyperovals of Desarguesian planes? The following example is instructive.

**Example 2.4.4** $\mathrm{PGL}(2,q_0) \leq \mathrm{PGL}(3,q)_{\mathcal{H}}$, where

$$\mathcal{H} = \{(1,t,t^2) : t \in \mathrm{GF}(q)\} \cup \{(0,1,0),(0,0,1)\}$$

is a regular hyperoval and $q = q_0^h$. Moreover, it is the stabilizer of the subplane

$$\pi_0 = \{(x,y,z) : x,y,z \in \mathrm{GF}(q_0)\}$$

in $\mathrm{PGL}(3,q)_{\mathcal{H}}$, and $\pi_0 \cap \mathcal{H}$ is a regular hyperoval of $\pi_0$, consisting of a conic $\mathcal{C}_0$ and its nucleus $N$. The points of $\pi_0$ are of three kinds: $N$, the points of $\mathcal{C}_0$, and the centres of elations of

$\mathrm{PGL}(2, q_0)$. The lines of $\pi_0$ are of three kinds: the tangent lines to $\mathcal{C}_0$, the secant lines to $\mathcal{C}_0$ and the external lines to $\mathcal{C}_0$.

In the theorem that follows we need to deduce the existence of an invariant subplane from knowledge of a group fixing a hyperoval. The preceding example allows us to construct this subplane from the group *without needing its action on the plane.*

**Example 2.4.5** The incidence structure $\mathcal{I}(G)$ with points

(i) $\infty$

(ii) Sylow 2-subgroups $T$of $G$

(iii) involutions $t$ of $G$

and lines

(a) Sylow 2-subgroups $[T]$ of $G$

(b) dihedral subgroups $U$ of order $2(q_0 - 1)$ of $G$

(c) dihedral subgroups $V$ of order $2(q_0 + 1)$ of $G$

with incidence

$$\infty \mathrel{\mathrm{I}} [T],\ T \mathrel{\mathrm{I}} [T],\ t \mathrel{\mathrm{I}} [T] \iff t \in T$$

$$\infty \mathrel{\not\mathrm{I}} U,\ T \mathrel{\mathrm{I}} U \iff \langle T, U \rangle \cong \mathrm{AGL}(1, q_0),\ t \mathrel{\mathrm{I}} U \iff t \in U$$

$$\infty \mathrel{\not\mathrm{I}} V,\ T \mathrel{\not\mathrm{I}} V,\ t \mathrel{\mathrm{I}} V \iff t \in V$$

is isomorphic to $\mathrm{PG}(2, q_0)$, since the correspondence

$$\infty \longleftrightarrow N$$

$$T \longleftrightarrow \mathrm{fix}(T) \cap (\pi_0 \cap \mathcal{H})$$

$$t \longleftrightarrow \text{centre of } t$$

$$[T] \longleftrightarrow \text{tangent line to } \pi_0 \cap \mathcal{H} \text{ at } \mathrm{fix}(T) \cap (\pi_0 \cap \mathcal{H})$$

$$U \longleftrightarrow \text{unique fixed line of } U$$

$$V \longleftrightarrow \text{unique fixed line of } V$$

is an isomorphism with $\pi_0$.

**Theorem 2.4.6** [15] *If the stabilizer $G$ in $\mathrm{P\Gamma L}(3,q)$ of a hyperoval $\mathcal{H}$ is insoluble, then either $q=4$ and $G \cong S_6$, or $G$ fixes a subplane $\pi_0$ of order $q_0 > 2$. In the latter case, $\pi_0 \cap \mathcal{H}$ is a regular hyperoval of $\pi_0$ and $G$ has a normal subgroup isomorphic to* $\mathrm{PGL}(2,q_0)$.

**Proof** Suppose $q > 4$. By Theorem 2.4.3, $G$ is reducible, since both $\mathrm{P\Gamma U}(3,4)$ and the pointwise stabilizer of a subplane are soluble. Since the stabilizer of a triangle is also soluble, $G$ fixes a point or line. $G \cap \mathrm{PSL}(3,q)$ is insoluble, and so by [63][1] and Theorem 2.3.6, $G \cap \mathrm{PSL}(3,q)$ contains an elation. Suppose $G$ fixes no point. Then $G$ fixes a line $\ell$. If $\ell$ is not the axis of any non-trivial elation in $G$, then $G$ acts faithfully on $\ell$, and hence $G$ is isomorphic to a subgroup of $\mathrm{P\Gamma L}(2,q)$. Since $G$ is insoluble, $G$ has a normal subgroup $N$ isomorphic to $\mathrm{PGL}(2,q_0)$, for $q_0 > 2$, $q = q_0^h$, by Theorem 2.3.4. Since $N$ contains at least two non-trivial elations that commute, by Theorem 2.3.11 $\ell$ is the common axis, a contradiction. Thus $\ell$ is the axis of some non-identity elation in $G$, hence secant to $\mathcal{H}$ by Theorem 2.3.9. This implies that the stabilizer of $\ell \cap \mathcal{H}$ is soluble, contradicting the insolubility of $G$.

Therefore $G$ fixes a point $P$ which is on the axis of every elation of $G \cap \mathrm{PSL}(3,q)$. By Theorem 2.3.10, if $P$ is not on $\mathcal{H}$, then $P$ is not the centre of a non-trivial elation fixing $\mathcal{H}$. If $P$ is on $\mathcal{H}$, then $P$ is not the centre of any non-trivial elation by Theorem 2.3.7. Hence $G$ acts faithfully on the lines through $P$, and as above, $G$ is isomorphic to a subgroup of $\mathrm{P\Gamma L}(2,q)$, and has a normal subgroup $N$ isomorphic to $\mathrm{PGL}(2,q_0)$, for $q_0 > 2$, $q$ a power of $q_0$. If $P$ is not on $\mathcal{H}$, then $G$ acts on the $q/2$ external lines through $P$, contrary to the action of $\mathrm{PGL}(2,q_0)$ on $\mathrm{PG}(1,q_0)$. Hence $P$ is on $\mathcal{H}$.

Let $\mathcal{C}_0$ be the intersection of $\mathcal{H}$ with the orbit of length $q_0+1$ of $N$ on the subpencil of lines through $P$. Then $\mathcal{I}(N) \cong \mathrm{PG}(2,q_0)$, but also $\mathcal{I}(N)$ is isomorphic to the incidence

[1] We only need the fact that all subgroups of $\mathrm{PGL}(3,q)$ of odd order are soluble, which is much easier to prove.

structure with points

(i) $P$

(ii) the points of $\mathcal{C}_0$

(iii) centres of involutions of $N$

and lines

(a) $PQ$, where $Q \in \mathcal{C}_0$

(b) $QQ'$, where $Q, Q' \in \mathcal{C}_0$, $Q \neq Q'$

(c) the unique line fixed by $V$, where $V \leq N$, $V \cong D_{2(q_0+1)}$

with incidences inherited from $\mathrm{PG}(2,q)$, by applying Theorem 2.3.11. Hence $G$ fixes the subplane $\pi_0 = \mathcal{I}(N)$, and $\pi_0 \cap \mathcal{H}$ is a hyperoval $\mathcal{H}_0$ of $\pi_0$. By [110, Theorem 3.3], $\mathcal{H}_0$ is regular. □

**Remark 2.4.7** If $q = q_0^2$, then the hyperoval is regular, for an orbit of $\mathrm{PGL}(2,q_0)$ on points of the hyperoval not in $\mathrm{PG}(2,q_0)$ has length at most $q_0^2 - q_0$, but elements of order $q_0 - 1$ have all fixed points in $\mathrm{PG}(2,q_0)$. Such an orbit consists of points stabilized by a cyclic $q_0 + 1$, and there are 2 such points (for each cyclic $q_0 + 1$) and they must lie on a regular hyperoval. Hence, if the stabilizer is insoluble and the hyperoval is not regular, then the homography stabilizer has order less than $q - 1$.

The following result gives a rich man/poor man classification of hyperovals of $\mathrm{PG}(2,q)$.

**Theorem 2.4.8** *A hyperoval of* $\mathrm{PG}(2,q)$ *with homography stabilizer greater than* $3(q-1)$ *is a translation hyperoval.*

**Proof** Let $G$ be the homography stabilizer of the hyperoval $\mathcal{H}$, with $|G| > 3(q-1)$. If $G$ fixes a subplane of order 4, then $|G| = 36$ by Theorem 2.3.2, so $q = 4$, a contradiction. If not, $G$ fixes a point, line or triangle by Theorem 2.4.3. By the above remark and Theorem 2.4.6, we can assume $G$ is soluble. If $G$ fixes a point or line, $G$ induces a soluble subgroup of $\mathrm{PGL}(2,q)$

on the lines through the point (points on the line). By [110, Theorem 3.6], Theorem 2.3.13 and Theorem 2.3.4, it follows that $G$ has order divisible by $q$, in which case $\mathcal{H}$ is translation. Suppose $G$ fixes a triangle $\Delta$. By Theorem 2.3.7, $G_{(\Delta)}$ contains no homologies. Hence $G_{(\Delta)}$ acts faithfully on any side of $\Delta$, and so $|G|$ divides $6(q-1)$. If $|G| = 6(q-1)$, then since $G_{(\Delta)}$ acts semiregularly on points on no side of $\Delta$, it follows that $\Delta$ is a subset of $\mathcal{H}$. Since $G_{(\Delta)}$ acts transitively on $\mathcal{H} \setminus \Delta$, it follows from [110, Lemma 3.8], that $\mathcal{H}$ is monomial, contradicting [110, Theorem 4.4]. $\square$

**Example 2.4.9** The known hyperovals that achieve equality in the above bound are the hyperovals of Segre–Bartocci 1971 [140] in $\mathrm{PG}(2,32)$ and Eich–Payne–Hirschfeld–Glynn 1972 [60] in $\mathrm{PG}(2,128)$ (see [110]).

## 2.5 The stabilizer of the Cherowitzo hyperoval

In order to calculate the group of the title of this section, we first need to recall the representation of hyperovals by o-polynomials (and o-permutations). For reasons that will become apparent, our focus will shift to *ovals* for a period of time.

By the transitivity of $\mathrm{P\Gamma L}(3,q)$ on ordered quadrangles of $\mathrm{PG}(2,q)$, we can assume that a given oval has nucleus $(0,0,1)$ and contains the points $(1,0,0)$, $(0,1,0)$ and $(1,1,1)$. Such an oval can be written in the form

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

where $f$ is a permutation polynomial of degree less than $q-1$ satisfying $f(0) = 0$, $f(1) = 1$ and such that for each $s \in \mathrm{GF}(q)$, the function $f_s$ where $f_s(0) = 0$, $f_s(x) = (f(x+s)+f(s))/x$ is a permutation (see, for example Hirschfeld 1985 [83]). Conversely, any polynomial $f$ satisfying the above conditions gives rise to an oval $\mathcal{D}(f)$ with nucleus $(0,0,1)$. Such a polynomial is called an **o-polynomial**. Note that we have altered the notation in earlier section – now $\mathcal{D}(f)$ is an *oval*, with associated hyperoval $\mathcal{D}(f) \cup \{(0,0,1)\}$.

If we drop the condition that $f(1) = 1$ (or equivalently, we drop the condition that the oval contains $(1,1,1)$) but retain the other conditions, then $f$ is an o-permutation. Associated with an o-polynomial are $q-1$ o-permutations, namely the non-zero multiples of the o-polynomial. With an o-permutation $f$, is associated a unique o-polynomial $(1/f(1))f$. If $f$ is an o-polynomial then $\langle f \rangle$ comprises the zero polynomial together with the $q-1$ o-permutations associated with $f$. Clearly, the $q-1$ ovals $\mathcal{D}(f_i)$, where the $f_i$ are o-permutations associated with an o-polynomial $f$ are equivalent under $\mathrm{PGL}(3,q)$.

We now turn to a method for computing an *oval* stabilizer (and hence hyperoval stabilizer).

Let $\mathcal{F}$ denote the collection of all functions $f : \mathrm{GF}(q) \to \mathrm{GF}(q)$ such that $f(0) = 0$. Note that each element of $\mathcal{F}$ can be expressed as a polynomial in one variable of degree at most $q-1$ and that $\mathcal{F}$ is a vector space over $\mathrm{GF}(q)$. If $f(x) = \sum a_i x^i \in \mathcal{F}$ and $\gamma \in \mathrm{Aut}\,\mathrm{GF}(q)$ then we write $f^\gamma(x) = \sum a_i^\gamma x^i$ or equivalently, $f^\gamma(x) = (f(x^{1/\gamma}))^\gamma$. As usual, we write $x^\gamma$ for componentwise action by $\gamma \in \mathrm{Aut}\,\mathrm{GF}(q)$ on $x$ in $\mathrm{GF}(q^n)$.

**Lemma 2.5.1** (O'Keefe–Penttila 2002 [111]) *For each $f \in \mathcal{F}$ and $\psi \in \mathrm{P\Gamma L}(2,q)$, where $\psi : \mathrm{GF}(q)^2 \to \mathrm{GF}(q)^2$, $x \mapsto Ax^\gamma$ for $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,q)$ and $\gamma \in \mathrm{Aut}\,\mathrm{GF}(q)$ , let the image of $f$ under $\psi$ be the function $\psi f : \mathrm{GF}(q) \to \mathrm{GF}(q)$ such that*

$$\psi f(x) = |A|^{-1/2} \left[ (bx+d) f^\gamma \left( \frac{ax+c}{bx+d} \right) + bxf^\gamma \left( \frac{a}{b} \right) + df^\gamma \left( \frac{c}{d} \right) \right]$$

*Then this definition yields an action of $\mathrm{P\Gamma L}(2,q)$ on $\mathcal{F}$, which is called the magic action.*

We remark that in each term in the formula of the magic action, the denominator of the argument of $f^\gamma$ is always a factor. Thus, for example, $df^\gamma(c/d)$ is interpreted as 0 if $d = 0$ and so on.

The following result elucidates the relationship between o-permutations that are equivalent under the magic action of $\mathrm{P\Gamma L}(2,q)$ and ovals that are equivalent under the natural action of $\mathrm{P\Gamma L}(3,q)$ on $\mathrm{PG}(2,q)$. We remark that Theorem 2.5.2 holds for $\mathrm{PGL}(3,q)$ in place of $\mathrm{P\Gamma L}(3,q)$.

**Theorem 2.5.2** (O'Keefe–Penttila 2002 [111]) *Let $f$ and $g$ be o-permutations for $\mathrm{PG}(2,q)$ and suppose that $\mathcal{D}(f)$ and $\mathcal{D}(g)$ are equivalent under $\mathrm{P\Gamma L}(3,q)$. Then there exists $\psi \in$*

$\mathrm{P\Gamma L}(2,q)$ *such that* $\psi f \in \langle g\rangle$. *Moreover, there is a one-to-one correspondence between* $\{\varphi \in \mathrm{P\Gamma L}(3,q) : \varphi\mathcal{D}(f) = \mathcal{D}(g)\}$ *and* $\{\psi \in \mathrm{P\Gamma L}(2,q) : \psi f \in \langle g\rangle\}$.

We now outline our strategy. From now on let $f(t) = t^\sigma + t^{\sigma+2} + t^{3\sigma+4}$, $\sigma^2 \equiv 2 \pmod{q-1}$ so that $\mathcal{H} = \mathcal{D}(f) \cup \{(0,0,1)\}$ is the Cherowitzo hyperoval. We determine $\mathrm{PGL}(3,q)_\mathcal{H}$ by finding

$$\{g \in \mathrm{PGL}(3,q)_\mathcal{H} : g(0,0,1) = P\}$$

for each $P \in \mathcal{H}$; that is

$$\{g \in \mathrm{PGL}(3,q)_\mathcal{H} : g\mathcal{D}(f) = \mathcal{H} \setminus \{P\}\}.$$

Since $\mathcal{D}(f)$ and $\mathcal{H}\setminus\{P\}$ are *ovals*, we may apply the magic action by finding an o-permutation $h$ such that $\mathcal{D}(f)$ is equivalent to $\mathcal{D}(h)$ under $\mathrm{PGL}(3,q)$. This reduces our calculation to a calculation with 2 by 2 matrices. In fact, there is a slight subtlety that complicates our approach which will be apparent below (this revolves around the difficulty of computing an explicit formula for the inverse of a certain function).

Two admissions belong here. The calculations are fiendishly difficult, so require the use of computer algebra software. Also, fields of small order (namely 32, 128 and 512) need to be treated separately. Fortunately, a straighforward stabilizer calculation in Magma is feasible for these orders and resolves the issue. The other calculation was performed in Mathematica, in characteristic 2, with variables for the unknown quantities, thereby avoiding the need to compute in infinitely many finite fields. We give some of the details below.

Our tactics involved equating the coefficients of the polynomial equations that result from the magic action (after reducing modulo $x^q - x$). Indeed, for small field orders the exponents coalesce, which is why we resort to Magma in these cases.

The following result is also proved in O'Keefe–Thas [112] using very different methods.

**Lemma 2.5.3** *Let* $g \in \mathrm{PGL}(3,q)_\mathcal{H}$, $q > 32$, *such that* $g(0,0,1) = (0,0,1)$. *Then* $g$ *is the identity map on* $\mathrm{PG}(2,q)$.

**Proof** By Theorem 2.5.2, we must show that if $\psi \in \mathrm{PGL}(2,q)$ such that $\psi f = kf$ for some fixed $k \in \mathrm{GF}(q)^*$ then $\psi$ is the identity map. Let $\psi : x \mapsto Ax$ where $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,q)$. From the definition of the magic action, $\psi f$ is a rational function, and so we can write $\psi f = \nu/\delta$, and hence

$$\nu(x) = k\delta(x)f(x) \tag{2.1}$$

where this equation is interpreted modulo $x^q - x$. If $q > 32$, then the terms appearing in Equation (2.1) are distinct.

If $b = 0$ and $d \neq 0$, then consideration of the $x^4$ terms gives $ka^4c^{3\sigma} = 0$, and hence $c = 0$. Looking at the $x^\sigma$ and $x^{\sigma+2}$ terms we see that $ka^\sigma d^{2\sigma+4} = ka^{\sigma+2}d^{2\sigma+2}$, and hence $a = d$. Thus $\psi$ is the identity map on $\mathrm{PG}(2,q)$.

If $b \neq 0$ and $d = 0$, then equating constant terms gives $c^{3\sigma+4} = 0$, and hence $c = 0$, a contradiction. Thus the only case left to consider is $b \neq 0$, $d \neq 0$. Consideration of the $x^2$ terms gives

$$b^{3\sigma+5}c^{\sigma+2}d^{5\sigma+6} + a^2b^{3\sigma+3}c^\sigma d^{5\sigma+8} = 0,$$

and hence

$$b^2c^{\sigma+2} + a^2c^\sigma d^2 = 0.$$

If $c \neq 0$ we have $(ad + bc)^2 = 0$, a contradiction. Hence $c = 0$. Equating $x$ terms gives

$$a^{3\sigma+4}d^{6\sigma+9} + a^{\sigma+2}b^{2\sigma+2}d^{6\sigma+9} + a^\sigma b^{2\sigma+2}d^{6\sigma+9} = 0$$

and so

$$a^{3\sigma+4} + a^{\sigma+2}b^{2\sigma+2} = a^\sigma b^{2\sigma+4}. \tag{2.2}$$

Consideration of the $x^{\sigma+1}$ terms gives

$$a^{3\sigma+4}b^\sigma d^{5\sigma+9} + a^{\sigma+2}b^{3\sigma+2}d^{5\sigma+9} = 0$$

which implies

$$a^{3\sigma+4} + a^{\sigma+2}b^{2\sigma+2} = 0$$

and Equation (2.2) then forces

$$a^\sigma b^{2\sigma+4} = 0$$

Now $b \neq 0$ by assumption, which means that $|A| = 0$, a contradiction. $\square$

**Lemma 2.5.4** *Let $g \in \mathrm{PGL}(3,q)_{\mathcal{H}}$, $q > 128$. Then $g(0,0,1) \neq (0,1,0)$.*

**Proof** Suppose $g \in \mathrm{PGL}(3,q)_{\mathcal{H}}$ with $g(0,0,1) = (0,1,0)$. Let $\phi \in \mathrm{PGL}(3,q)$ be $\phi : x \mapsto Ax$, where $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \in \mathrm{GL}(3,q)$. Then $(\phi\, g)\mathcal{D}(f) = \mathcal{D}(f^{-1})$, and so by Theorem 2.5.2 there exists $\psi \in \mathrm{PGL}(2,q)$ such that $\psi f \in \langle f^{-1} \rangle$. Let $\psi : x \mapsto Bx$, where $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,q)$. From the definition of the magic action it follows that $\psi f h$ is a rational function, and so we can write $\psi f h = \nu/\delta$, for $\nu, \delta \in \mathcal{F}$. Now $f^{-1}(x) = \dfrac{x^{1/\sigma}(1 + x + x^{\sigma})}{1 + x^2 + x^{\sigma}}$ (see Penttila–Pinneri 1994 [126]), and so for some $k \in \mathrm{GF}(q)^*$ we have

$$\nu(x)(1 + x^2 + x^{\sigma}) = k\delta(x)x^{1/\sigma}(1 + x + x^{\sigma}) \tag{2.3}$$

where this equation is interpreted modulo $x^q - x$. The terms in this equation are distinct when $q > 128$. We consider the case where $b \neq 0$, $d \neq 0$ (the other cases are similar).

In this case, consideration of the $x^2$ coefficients of Equation (2.3) gives

$$b^{3\sigma+5}c^{\sigma+2}d^{5\sigma+6} + a^2b^{3\sigma+3}d^{5\sigma+8} = 0,$$

and hence

$$b^2c^{\sigma+2} = a^2c^{\sigma}d^2,$$

which forces $c = 0$. Consideration of the $x$ terms gives

$$a^{3\sigma+4}d^{6\sigma+9} + a^{\sigma+2}b^{2\sigma+2}d^{6\sigma+9} + a^{\sigma}b^{2\sigma+4}d^{6\sigma+9} = 0,$$

and thus

$$a^{3\sigma+4} + a^{\sigma+2}b^{2\sigma+2} = a^{\sigma}b^{2\sigma+4}. \tag{2.4}$$

Now, looking at the $x^{2\sigma+2}$ terms of Equation (2.3), gives

$$a^{\sigma+2}b^{3\sigma+3}d^{3\sigma+8} + a^{\sigma}b^{3\sigma+5}d^{5\sigma+8} = 0$$

and hence

$$a^{\sigma+2} = a^{\sigma}b^2.$$

Substituting in Equation (2.4) gives $a = 0$, a contradiction. $\square$

**Lemma 2.5.5** [15] *Let* $g \in \mathrm{PGL}(3,q)_{\mathcal{H}}$*,* $q > 512$*. Then* $g(0,0,1) \neq (1,t,f(t))$ *for any* $t \in \mathrm{GF}(q)$*.*

**Proof** Suppose $g(0,0,1) = (1,t,f(t))$ for $g \in \mathrm{PGL}(3,q)_{\mathcal{H}}$ and $t \in \mathrm{GF}(q)$. Define the permutation $h : \mathrm{GF}(q) \to \mathrm{GF}(q)$ by $h(0) = 0$, $h : x \mapsto x\big(f(x^{-1}+t)+f(t)\big)$ and let $\phi \in \mathrm{PGL}(3,q)$ be $\phi : x \mapsto Ax$, where $A = \begin{pmatrix} t & 1 & 0 \\ f(t) & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \in \mathrm{GL}(3,q)$. Then $(\phi\, g)\mathcal{D}(f) = \mathcal{D}(h^{-1})$, and so by Theorem 2.5.2 there exists $\psi \in \mathrm{PGL}(2,q)$ such that $\psi f \in \langle h^{-1}\rangle$. Let $\psi : x \mapsto Bx$, where $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,q)$. From the definition of the magic action it follows that $\psi f h$ is a rational function, and so we can write $\psi f h = \nu/\delta$, for $\nu, \delta \in \mathcal{F}$. Hence, for some $k \in \mathrm{GF}(q)^*$ we have

$$\nu(x) = kx\delta(x) \tag{2.5}$$

for all $x \in \mathrm{GF}(q)$. A technical calculation shows that the terms appearing in (Equation (2.5)) are distinct when $q > 512$, and we can therefore equate coefficients modulo $q-1$ to deduce conditions on $\psi$. Without loss of generality, $b \neq 0$ and $d \neq 0$. Consideration of the $x^{-14}$ coefficients of Equation (2.5) gives

$$k(c^{1/2}d^{3\sigma+3}t^{6\sigma} + a^{1/2}b^{6\sigma+9}d^{3\sigma+7/2}t^{6\sigma}) = 0$$

and so $t = 0$. From the $x^{-9}$ and $x^{-7}$ coefficients we deduce

$$\begin{aligned} &b^{3\sigma+4}c^{3\sigma+4} + b^{3\sigma+4}c^{\sigma+2}d^{2\sigma+2} + b^{3\sigma+4}c^{\sigma}d^{2\sigma+4} \\ &+a^{\sigma}b^{2\sigma+4}c^{2}d^{3\sigma+2} + a^{3\sigma+4}d^{3\sigma+4} + a^{\sigma}b^{2\sigma+4}d^{3\sigma+4} = 0 \end{aligned}$$

and

$$\begin{aligned} &b^{3\sigma+4}c^{3\sigma+4} + b^{3\sigma+4}c^{\sigma+2}d^{2\sigma+2} + b^{3\sigma+4}c^{\sigma}d^{2\sigma+4} \\ &+a^{3\sigma+4}d^{3\sigma+4} + a^{\sigma+2}b^{2\sigma+2}d^{3\sigma+4} + a^{\sigma}b^{2\sigma+4}d^{3\sigma+4} = 0 \end{aligned}$$

respectively. Adding these two equations forces $a = 0$. The constant terms now give $b^{3\sigma+10}c^{\sigma}d^{5\sigma+3} = 0$, and so $c = 0$. But this gives $|A| = 0$, a contradiction. □

**Theorem 2.5.6** [15] *Let $\mathcal{H}$ denote the Cherowitzo hyperovals in* $\mathrm{PG}(2,q)$, $q = 2^h$, *$h$ odd. The stabilizer of $\mathcal{H}$ in* $\mathrm{PGL}(3,q)$ *is trivial, and hence the full stabilizer of $\mathcal{H}$ in* $\mathrm{P\Gamma L}(3,q)$ *is*

$$\mathrm{P\Gamma L}(3,q)_{\mathcal{H}} = \{(x,y,z) \mapsto (x^\alpha, y^\alpha, z^\alpha) : \alpha \in \mathrm{Aut}\,\mathrm{GF}(q)\}.$$

**Proof** Apply Lemma 2.5.3, Lemma 2.5.4, Lemma 2.5.5. □

The somewhat delicate argument in Penttila–Pinneri 1999 [126] showing that the Cherowitzo hyperovals are new for $q > 8$, is now unnecessary.

**Corollary 2.5.7** *The Cherowitzo hyperovals are new for $q > 8$.*

**Proof** All other known hyperovals $\mathcal{H}$ have $\mathrm{PGL}(3,q)_{\mathcal{H}} \neq 1$. □

A final remark about the reasons for the difficulty in determining the stabilizers of the Cherowitzo hyperovals is in order. Since the group is so small, there are many candidates for the stabilizer above the group in the lattice of all subgorups of $\mathrm{P\Gamma L}(3,q)$. This may account for the present lack of a satisfying proof.

# Chapter 3

# Flag-transitive Laguerre planes

## 3.1 Introduction

Characterizing classical incidence structures by group-theoretic properties has a long history. Here we contribute a characterization of Miquelian Laguerre planes of odd order of this type. Our hypotheses are that the finite Laguerre plane admit a group containing a nontrivial elation acting quasiprimitively on the circles and transitively on the (point, circle) flags. To achieve this, we show that a Laguerre plane admitting a group containing a nontrivial elation and acting quasiprimitively on circles is an elation Laguerre plane. We then apply the theorems of Steinke 1991 [142] and Löwen 1994 [99] to reduce our situation to the study of pseudo-ovals admitting an irreducible transitive group. Applying a recent theorem of Bamberg-Penttila 2006 [12] completes the proof.

We then turn to a generalization of a theorem of Thas 1997 [155] and Lunardon 1997 [100] concerning semifield flocks of the quadratic cone in $\mathrm{PG}(3, q)$ and translation ovoids of $\mathrm{Q}(4, q)$, $q$ odd. We generalize this to even characteristic, and to a correspondence between translation flocks of elation Laguerre planes and translation ovoids of the corresponding translation generalized quadrangles.

Finally, we extend the characterization to all Miquelian Laguerre planes of finite order by dropping the hypothesis of quasiprimitivity on circles and adding the hypothesis of insolubility.

The functors constructing translation generalized quadrangles from pseudo-ovals, and elation Laguerre planes from (dual) pseudo-ovals (together with the theorems that establish the reverse) mean that *these subjects should be studied in conjunction.* We illustrate this perspective not only with our main result, but also by studying how this correspondence enlightens the study of translation ovoids of translation generalized quadrangles and translation flocks of elation Laguerre planes. This correspondence also elevates the importance of the study of pseudo-ovals.

## 3.2 Circle planes

A **circle plane** is an incidence structure $(\mathcal{P}, \mathcal{L}, \mathcal{C})$, of points, lines, and circles, with an equivalence relation on $\mathcal{L}$ (parallelism) such that

- (Joining) 3 pairwise non-collinear points lie on a unique circle
- (Touching) Given a point $P$ on a circle $C$, and $P'$ not on $C$, not collinear with $P$, there is a unique circle $C'$ on $P'$ with $C \cap C' = \{P\}$
- (Tangency) A circle and a line meet in a unique point
- (Parallelism) Every point lies one exactly 1 line from each parallel class, and non-parallel lines meet in a unique point
- (Non-degeneracy) $|\mathcal{C}| \geq 2$ and $|C| \geq 3$ for all $C \in \mathcal{C}$.

A circle plane with 0, 1, or 2 parallel classes is called an **inversive plane** (or **Möbius plane**), a **Laguerre plane** or a **Minkowski plane**, respectively.

**Example 3.2.1** Let $P$ be a point in a circle plane $\mathcal{S}$. The **internal structure** at $P$, denoted $\mathcal{S}_P$, is a point/line incidence structure. The points of $\mathcal{S}_P$ are the points of $\mathcal{S}$ not collinear with $P$, and the lines of $\mathcal{S}_P$ are the circles of $\mathcal{S}$ through $P$, together with the lines of $\mathcal{S}$ not through $P$, with incidence inherited from $\mathcal{S}$. This is an affine plane, called the **derived affine plane** at $P$. The joining axiom shows that $\mathcal{S}_P$ is a linear space, the touching axiom is the parallel postulate, and non-degeneracy of $\mathcal{S}$ implies non-degeneracy of $\mathcal{S}_P$. The completion of $\mathcal{S}_P$ is called the **derived projective plane** at $P$, denoted by $\pi_P$.

Suppose $C$ is a circle not through $P$. Then the set of points of $C$ not collinear with $P$ together with the points of $\ell_\infty$ corresponding to the parallel classes in $\mathcal{S}$ form an oval of $\pi_P$. From the set of all circles not on $P$, there arises in this way a set of ovals $\mathcal{H}_P$ of $\pi_P$, such that any triangle of $\pi_P \setminus \ell_\infty$ with no side on the (0, 1, or 2) special points of $\ell_\infty$ lies on a unique oval $\mathcal{O}$ of $\mathcal{H}_P$. Conversely, suppose we are given such a set of ovals of a projective plane $\pi$, there is a circle plane such that $\pi$ is the derived projective plane at a point $P$, and this set of ovals arises from the circles not on $P$.

The following quote from Steinke 1995 [143] summarizes the previous example concisely: "the investigation of circle planes is equivalent to the study of projective planes with sufficiently many ovals of a certain kind."

A **bundle** of a circle plane is the set of circles through two distinct non-collinear points. A **pencil** is a set of circles through a point that are pairwise tangent. A **flock** is a partition of the points into circles in the case of a Minkowski or Laguerre plane, and a partition of all but 2 points into circles in the case of an inversive plane. Every circle plane has bundles by definition. To construct pencils, take a point $P$, and a circle $C$ on $P$. Then the set of circles through $P$ that are tangent to $C$ at $P$ form a pencil (this pencil becomes the parallel class containing the line $C$ in the derived affine plane at $P$). It is not so clear that flocks exist, indeed, there are infinite circle planes having no flocks. In the next sections we will survey some of the main results about finite circle planes.

### 3.2.1 Inversive planes

An **inversive plane** (or **Möbius plane**) is an incidence structure $\mathcal{I} = (\mathcal{P}, \mathcal{C})$ of points and circles such that

- (Joining) 3 pairwise non-collinear points lie on a unique circle
- (Touching) Given a point $P$ on a circle $C$, and $P'$ not on $C$, not collinear with $P$, there is a unique circle $C'$ on $P'$ with $C \cap C' = \{P\}$
- (Non-degeneracy) $|\mathcal{C}| \geq 2$ and $|C| \geq 3$ for all $C \in \mathcal{C}$.

In a finite inversive plane, there exists a positive integer $n$, called the **order** of $I$ such that $|\mathcal{P}| = n^2 + 1$, $|\mathcal{C}| = n^3 + n$, and $|C| = n + 1$ for all $C \in \mathcal{C}$. Hence, a finite non-degenerate inversive plane of order $n$ is a $3-(n^2+1, n+1, 1)$ design, and conversely. All the inversive planes that follow will be finite and non-degenerate.

**Example 3.2.2** The **classical inversive plane** $\mathcal{I}(q)$ of order $q$ is constructed from an elliptic quadric $\mathrm{Q}^-(3,q)$ in $\mathrm{PG}(3,q)$. The points of $\mathcal{I}(q)$ are the points of $\mathrm{Q}^-(3,q)$, the circles of $\mathcal{I}(q)$ are the non-tangent planes to $\mathrm{Q}^-(3,q)$, and incidence is inherited from $\mathrm{PG}(3,q)$. Up to isomorphism, this does not depend on the choice of elliptic quadric.

We can generalize this construction by replacing $\mathrm{Q}^-(3,q)$ by an ovoid of $\mathrm{PG}(3,q)$.

**Example 3.2.3** Let $\Omega$ be an ovoid of $\mathrm{PG}(3,q)$. Define the structure $\mathcal{I}(\Omega)$ as follows. The points of $\mathcal{I}(\Omega)$ are the points of $\Omega$, the circles are the secant planes to $\Omega$, and incidence is inherited from $\mathrm{PG}(3,q)$. Then $\mathcal{I}(\Omega)$ is an inversive plane of order $q$, called an **egglike inversive plane**. $\mathcal{I}(\Omega)$ is classical if and only if $\Omega \cong \mathrm{Q}^-(3,q)$. Hence, there exist non-classical inversive planes of orders $2^{2e+1}$, $e \geq 1$, from the ovoids of Tits 1962 [165].

**Theorem 3.2.4** (Dembowski 1964 [54]) *Every inversive plane of even order is egglike. Hence its order is a power of 2.*

This is slightly frustrating, since Theorem 3.2.4 says that we know an inversive plane of even order comes from an ovoid, but we do not have a classification of ovoids of $\mathrm{PG}(2,q)$, $q$ even. On the other hand, we know that an ovoid in $\mathrm{PG}(2,q)$, $q$ odd, is an elliptic quadric due to Barlotti 1955 [13] and Panella 1955 [114] , but we do not know that an inversive plane of odd order comes from an ovoid of $\mathrm{PG}(3,q)$. At present, all known inversive planes are egglike.

We have the following result connecting an inversive plane to its derived affine plane.

**Theorem 3.2.5** (Thas 1990 [153], [152]) *Let $\mathcal{I}$ be an inversive plane of odd order. Then the derived affine plane of $\mathcal{I}$ at some point is Desarguesian if and only if $\mathcal{I}$ is classical.*

We now turn to the question of flocks of inversive planes.

**Example 3.2.6** Let $\Omega$ be an ovoid of $\mathrm{PG}(3,q)$, and let $\ell$ be a line external to $\Omega$. The set of all secant planes to $\Omega$ on $\ell$ is a flock of $\mathcal{I}(\Omega)$, called a **linear flock** of $\mathcal{I}(\Omega)$

The following theorem classifies flocks of egglike inversive planes.

**Theorem 3.2.7** (Orr 1973 [113], Thas 1973 [147]) *Any flock of an inversive egglike plane is linear.*

### 3.2.2 Minkowski planes

A **Minkowski plane** is an incidence structure $M = (\mathcal{P}, \mathcal{L}, \mathcal{C})$ of points, lines, and circles such that

- (Joining) 3 pairwise non-collinear points lie on a unique circle
- (Touching) Given a point $P$ on a circle $C$, and $P'$ not on $C$, not collinear with $P$, there is a unique circle $C'$ on $P'$ with $C \cap C' = \{P\}$
- (Tangency) A circle and a line meet in a unique point
- (Parallelism) $\mathcal{L}$ can be partitioned into two sets $\mathcal{L}_1$ and $\mathcal{L}_2$, such that each points lies on a unique line of $\mathcal{L}_1$ and a unique line of $\mathcal{L}_2$.
- (Non-degeneracy) $|\mathcal{C}| \geq 2$ and $|C| \geq 3$ for all $C \in \mathcal{C}$.

In a finite Minkowski plane, there exists a positive integer $n$ called the **order** of $M$ such that $|\mathcal{P}| = n^2 + n + 1$, $|\mathcal{L}| = 2n + 2$, $|\mathcal{C}| = n^3 - n$, $|\ell| = n + 1$ for all $\ell \in \mathcal{L}$, $|C| = n + 1$ for all $C \in \mathcal{C}$. All Minkowski planes that follow will be finite and non-degenerate.

**Example 3.2.8** The **classical Minkowski plane** $\mathcal{M}(q)$ of order $q$ is constructed from a hyperbolic quadric $\mathrm{Q}^+(3,q)$ in $\mathrm{PG}(3,q)$. The points of $\mathcal{M}(q)$ are the points of $\mathrm{Q}^+(3,q)$, the lines of $\mathcal{M}(q)$ are the generators of $\mathrm{Q}^+(3,q)$, the circles of $\mathcal{M}(q)$ are the non-tangent planes to $\mathrm{Q}^+(3,q)$, and incidence is inherited from $\mathrm{PG}(3,q)$. Up to isomorphism, this does not depend on the choice of hyperbolic quadric.

We can obtain non-classical Minkowski planes from sharply 3-transitive sets of permutations.

**Example 3.2.9** (Segre 1965 [139]) Let $\mathcal{S}$ be a sharply 3-transitive set of permuations of a set $X$. Define the incidence structure $\mathcal{M}(\mathcal{S})$ as follows. The points of $\mathcal{M}(\mathcal{S})$ are the elements of $X^2$, the lines of $\mathcal{M}(\mathcal{S})$ are sets of the form $\{(c,x) : x \in X\}$ and $\{(x,c) : x \in X\}$, the circles of $\mathcal{M}(\mathcal{S})$ are the graphs $\{(x, x^\sigma) : \sigma \in \mathcal{S}\}$, with natural incidence. Then $\mathcal{M}(\mathcal{S})$ is a Minkowski plane. $\mathcal{M}(\mathcal{S})$ is classical if and only the action of $\mathcal{S}$ on $X$ is isomorphic to the action of $\mathrm{PGL}(2,q)$ on $\mathrm{PG}(1,q)$.

We have a classification result for Minkowski planes of even order.

**Theorem 3.2.10** (Heise 1974 [76], Percsy 1974 [129]) *Every Minkowski plane of even order is classical. Hence its order is a power of 2.*

There is also an analogous result to Theorem 3.2.5 connecting a Minkowski plane of odd order to its derived affine plane.

**Theorem 3.2.11** (Chen–Kaerlein 1973 [42]) *Let $\mathcal{M}$ be a Minkowski plane of odd order. The derived affine plane of $\mathcal{M}$ at some point is Desarguesian if and only if $\mathcal{M}$ is classical.*

There are many known flocks of Minkowski planes.

**Example 3.2.12** Let $\ell$ be an external line to hyperbolic quadric $\mathrm{Q}^+(3,q)$ in $\mathrm{PG}(3,q)$. The set of all planes on $\ell$ is a flock of $\mathcal{M}(q)$, called the **linear flock** of $\mathcal{M}(q)$.

**Theorem 3.2.13** (Thas 1975 [149]) *Any flock of a Minkowski plane of even order is linear.*

There exist non-linear flocks of Minkowski planes of odd order.

**Example 3.2.14** (Thas 1975 [149]) Let $q$ be odd. Let $Q$ be a quadratic form of plus type on $V = \mathrm{GF}(q)^4$, so that the zeros of $Q$ form a hyperbolic quadric $\mathrm{Q}^+(3,q)$ in $\mathrm{PG}(3,q)$, and let $\beta$ be the polarization of $Q$. Let $\ell$ be external to $\mathrm{Q}^+(3,q)$, and let $m = \ell^\perp = \{v \in V :$

$\beta(u,v) = 0$ for all $u \in \ell\}$. Then

$$\mathcal{F} = \big\{P^\perp : P \in \ell \text{ and } Q(v) = (\mathrm{GF}(q)^*)^2 \pmod{(\mathrm{GF}(q)^*)^2}$$
$$\text{or } P \in m \text{ and } Q(v) = -(\mathrm{GF}(q)^*)^2 \pmod{(\mathrm{GF}(q)^*)^2}\big\}$$

is a flock of $\mathcal{M}(q)$, called the **Thas flock of $\mathcal{M}(q)$**.

**Example 3.2.15** (Baker–Ebert 1987 [9], Bader 1988 [5], Bonisoli 1988 [21], Johnson 1989 [88]) There are 3 exceptional flocks of $\mathcal{M}(q)$, one each for $q = 11, 23, 59$, associated with the irregular nearfields of Dickson 1905 [57] of orders $11^2, 23^2, 59^2$.

The following theorem completes the classification of flocks of classical Minkowksi planes.

**Theorem 3.2.16** (Bader–Lunardon 1989 [6]) *Any flock of a finite classical Minkowski plane of odd order is linear, Thas, or exceptional.*

### 3.2.3 Laguerre planes

A **Laguerre plane** is an incidence structure $L = (\mathcal{P}, \mathcal{L}, \mathcal{C})$ of points, lines, and circles such that

- (Joining) 3 pairwise non-collinear points lie on a unique circle
- (Touching) Given a point $P$ on a circle $C$, and $P'$ not on $C$, not collinear with $P$, there is a unique circle $C'$ on $P'$ with $C \cap C' = \{P\}$
- (Tangency) A circle and a line meet in a unique point
- (Parallelism) Every point is on a unique line
- (Non-degeneracy) $|\mathcal{C}| \geq 2$ and $|C| \geq 3$ for all $C \in \mathcal{C}$.

In a finite Laguerre plane, there exists a positive integer $n$ called the **order** of $M$ such that $|\mathcal{P}| = n^2 + n$, $|\mathcal{L}| = n + 1$, $|\mathcal{C}| = n^3$, $|\ell| = n$ for all $\ell \in \mathcal{L}$, $|C| = n + 1$ for all $C \in \mathcal{C}$. All Laguerre planes that follow will be finite and non-degenerate.

We begin by defining a quadratic cone of $\mathrm{PG}(3, q)$.

**Example 3.2.17** Let $\mathcal{C}$ be a conic in $\mathrm{PG}(2,q)$, and embed $\mathrm{PG}(2,q)$ as a hyperplane $\pi$ of $\mathrm{PG}(3,q)$. For a point $V$ not on $\pi$, take the lines through $V$ which meet $\mathcal{C}$ in a point. There are necesarily $q+1$ such lines, and the set of $q^2+q+1$ points on these lines form a **quadratic cone** $\mathcal{K}$. The point $V$ is the **vertex** of $\mathcal{K}$, the lines through $V$ meeting $\mathcal{C}$ in a point are the **generators** of $\mathcal{K}$, and $\mathcal{K}$ is said to **project** to the conic $\mathcal{C}$. Since all conics of $\mathrm{PG}(2,q)$ are equivalent under $\mathrm{P\Gamma L}(3,q)$, it follows that all quadratic cones are equivalent under $\mathrm{P\Gamma L}(4,q)$. Hence, if we label coordinates for $\mathrm{PG}(4,q)$ by $(x,y,z,w)$, we can take $\pi$ to be the plane $w=0$, and our vertex to be $V=(0,0,0,1)$. Then

$$\mathcal{K}=\{(x,y,z,w): y^2=xz\},$$

and $\mathcal{K}$ meets $\pi$ in the conic

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

Hence, $\mathcal{K}$ is the quadric of $\mathrm{PG}(3,q)$ defined by the degenerate form $Q$ given by $Q(x,y,z,w)=y^2-xz$.

We can obtain a Laguerre plane from a quadratic cone as follows.

**Example 3.2.18** The **classical Laguerre plane** $L(q)$ of order $q$ is obtained from a quadratic cone $\mathcal{K}$ of $\mathrm{PG}(3,q)$ with vertex $V$. Points of $L(q)$ are points of $\mathcal{K}$ other than $V$, the lines of $L(q)$ are generators of $\mathcal{K}$, and the circles of $L(q)$ are plane sections of $\mathcal{K}$ not on $V$, with incidence inherited from $\mathrm{PG}(3,q)$. Up to isomorphism, this does not depend on the choice of quadratic cone.

We can generalize this construction by replacing a conic of $\mathrm{PG}(2,q)$ with an oval of $\mathrm{PG}(2,q)$.

**Example 3.2.19** Let $\mathcal{O}$ be an oval of $\mathrm{PG}(2,q)$ and embed $\mathrm{PG}(2,q)$ as a hyperplane $\pi$ in $\mathrm{PG}(3,q)$. For a point $V$ not on $\pi$, take the lines through $V$ which meet $\mathcal{C}$ in a point. This is the **oval cone** $\mathcal{K}$ with vertex $V$ projecting to $\mathcal{O}$. Given an oval $\mathcal{O}$ of $\mathrm{PG}(2,q)$ with associated oval cone $\mathcal{K}$ with vertex $V$, we can construct the incidence structure $L(\mathcal{K})$ as follows. The points of $L(\mathcal{K})$ are the points of $\mathcal{K}$ other than $V$, the lines of $L(\mathcal{K})$ are the generators of $L(\mathcal{K})$, and the circles of $L(\mathcal{K})$ are the planes of $\mathrm{PG}(3, q)$ not on $V$. Then $L(\mathcal{K})$ is a Laguerre plane of order $q$, called an **egglike Laguerre plane** (or an **ovoidal Laguerre plane**). $L(\mathcal{K})$ is classical if and only if $\mathcal{O}$ is a conic. This construction gives non-classical Laguerre planes for $q = 2^h$, $h \geq 3$ (see Section 2.2 and Table 2.1). At present, all known Laguerre planes are egglike (see Steinke 1995 [143]). The question of whether or not there exist non-egglike Laguerre planes is very important, but difficult open problem.

We have an analogous result of Theorem 3.2.11 for Laguerre planes.

**Theorem 3.2.20** (Chen–Kaerlein 1973 [42]) *Let $L$ be a Laguerre plane of odd order. The derived affine plane of $L$ at some point is Desarguesian if and only if $L$ is classical.*

There are many known flocks of Laguerre planes. As in the inversive and Minkowski case, there is a concept of a linear flock of a Laguerre plane.

**Example 3.2.21** Let $\mathcal{K}$ be an oval cone in $\mathrm{PG}(3, q)$ projecting to the oval $\mathcal{O}$ in $\mathrm{PG}(2, q)$, and let $\ell$ be a line external to $\mathcal{K}$. Then the set of all planes on $\ell$, but not on the vertex of $\mathcal{K}$ is a flock of $L(\mathcal{K})$, called a **linear flock** of $L(\mathcal{K})$.

Recall from Section 2.2.4 that a $q$-clan is a set of $q$ $(2 \times 2)$ matrices such that the difference between any two distinct matrices is anisotropic. We have already seen a connection between $q$-clans and ovals via Theorem 2.2.24. The following theorem demonstrates the connection between $q$-clans and flocks of the classical Laguerre plane

**Theorem 3.2.22** (Thas 1987 [151]) *Let $\mathcal{K} = \{(x, y, z, w) : y^2 - xz = 0\}$ be a quadratic cone in $\mathrm{PG}(3, q)$ with vertex $V = (0, 0, 0, 1)$. Then*

$$C = \left\{ \begin{pmatrix} a_t & b_t \\ 0 & c_t \end{pmatrix} : t \in \mathrm{GF}(q) \right\}$$

*is a $q$-clan if and only if*

$$\mathcal{F}(C) = \{[a_t, b_t, c_t, 1] : t \in \mathrm{GF}(q)\}$$

*is a flock of $\mathcal{K}$.*

Thus we have flocks of the classical Laguerre plane $L(q)$, $q$ even, from the $q$-clans of Example 2.2.25 (the linear flocks), Example 2.2.26 (the **FTWKB flocks**), Example 2.2.27 (the **Payne flocks**), Example 2.2.28 (the **Subiaco flocks**), Example 2.2.29 (the **Adelaide flocks**). We can also use Theorem 3.2.22 to construct non-linear flocks of $L(q)$, $q$ odd. Examples of infinite families include the work of Fisher–Thas 1979 [64], Walker 1976 [177], Kantor 1980 [90], Betten 1973 [17], for $q \equiv -1 \pmod 3$, Kantor 1986 [92] for $q$ odd, Kantor 1986 [92] for $q \equiv \pm 2 \pmod 5$, Gevaert–Johnson 1988 [66], Kantor 1982 [91] for $q = 5^h$, Gevaert–Johnson 1988 [66], Ganley 1981 [65] for $q = 3^h$, and Law–Penttila 2001 [97] for $q = 3^h$. Flocks of $L(q)$ have been classified for $q \leq 29$ by Law–Penttila 2003 [98]. There are 28 flocks of $L(29)$.

If $\alpha = 2^i$, $1 \leq i < h$, with $(i, h) = 1$, then $\mathcal{D}(x^\alpha)$ is a translation oval of $\mathrm{PG}(2, q)$ (see Example 2.2.7). Let $L(\alpha) = L(\mathcal{K})$, where $\mathcal{K}$ is the cone over the oval $\mathcal{D}(x^\alpha)$. We call $L(\alpha)$ a **translation Laguerre plane**. Examples of non-linear flocks of translation Laguerre planes are given in Fisher–Thas 1979 [64], and Cherowitzo 1998 [43] (5 families). Each flock of $L(\alpha)$ is also a flock of $L(1/\alpha)$ if the first two coordinates are transposed. The theory of flocks of $L(\alpha)$ only differs from the theory of flocks of $L(q)$ if $q \neq 2, q/2$. Hence, it is first of interest in its own right when $q = 32$ and $x^\alpha = x^4$. Flocks of $L(\alpha)$ have been classified in this case by Brown–O'Keee–Payne–Penttila–Royle 2007 [28], and the only examples are the ones given above.

## 3.3 Characterizations of Laguerre planes

The classical Laguerre planes are characterized geometrically as those satisfying the **Miquelian** property (also known as **condition M1**) – whenever 8 distinct points $P_1$, $P_2$, $P_3$, $P_4$, $Q_1$, $Q_2$, $Q_3$, $Q_4$ are given such that each of the sets $\{P_1, P_2, P_3, P_4\}$, $\{P_1, P_2, Q_3, Q_4\}$, $\{P_3, P_4, Q_1, Q_2\}$, and $\{P_2, P_3, Q_2, Q_3\}$, $\{P_4, P_1, Q_4, Q_1\}$ are contained in a circle, then the set $\{Q_1, Q_2, Q_3, Q_4\}$ is also contained in a circle, or consists of two pairs of collinear points. This property characterizes the classical Laguerre planes.

**Theorem 3.3.1** (van der Waerden–Smid 1935 [169]) *A Laguerre plane satisfies the Miquelian property if and only if it is classical.*

The equivalent geometric characterization for egglike Laguerre planes is given by the **bundle axiom** – for any eight pairwise non-collinear points $P_1$, $P_2$, $P_3$, $P_4$, $Q_1$, $Q_2$, $Q_3$, $Q_4$, if 5 of the 6 quadruples $\mathcal{Q}_{ij} = \{P_i, Q_i, P_j, Q_j\}$, $i < j$, lie on at least 4 circles, then so does the last.

**Theorem 3.3.2** (Kahn 1980 [89]) *A Laguerre plane satisfies the bundle axiom if and only if it is egglike.*

This paper is concerned with characterizing Laguerre planes based on their symmetry, and so we define the following group theoretic properties of Laguerre planes. The **kernel** $T$ of a Laguerre plane $L$ is the kernel of the action of $\mathrm{Aut}\, L$ on the lines of $L$. The **elation group** $\Delta$ of $L$ consists of the identity and all elements of $T$ fixing no circle. We remark that $\Delta$ is a normal subgroup of $\mathrm{Aut}\, L$ (see Steinke 1991 [142]). An **elation Laguerre plane** is a Laguerre plane with $\Delta$ acting regularly on circles. Egglike Laguerre planes are elation Laguerre planes. It turns out that elation Laguerre planes are related to combinatorial objects known as (dual) pseudo-ovals.

An $n$-dimensional **pseudo-oval** of $\mathrm{PG}(3n-1, q)$ is a set $\mathcal{O}$ of $q^n+1$ subspaces of dimension $n-1$ such that any three span $\mathrm{PG}(3n-1, q)$. Notice that from any element $E$ of $\mathcal{O}$, the other elements of $\mathcal{O}$ project a partial $(n-1)$-spread of deficiency one of $\mathrm{PG}(2n-1, q)$, which can be uniquely completed to a spread (see Beutelspacher 1980 [18]). Hence $E$ is contained in a unique subspace $T_E$ of dimension $2n-1$ disjoint from the other elements of $\mathcal{O}$. These subspaces are the **tangents** to $\mathcal{O}$.

**Example 3.3.3** There is a bijective, $\mathrm{GF}(q)$-linear map from the underlying vector space $\mathrm{GF}(q^n)^3$ of $\mathrm{PG}(2, q^n)$ (thought of as a vector space over $\mathrm{GF}(q^n)$) to the underlying vector space $\mathrm{GF}(q)^{3n}$ (thought of as a vector space over $\mathrm{GF}(q)$) of $\mathrm{PG}(3n-1, q)$. Hence, we can identify points of $\mathrm{PG}(2, q^n)$ with $(n-1)$-spaces of $\mathrm{PG}(3n-1, q)$. This is an example of **field reduction**. Let $\mathcal{O}$ be an oval of $\mathrm{PG}(2, q^n)$. By field reduction, each point of the oval corresponds to a $(n-1)$-space of $\mathrm{PG}(3n-1,q)$. The condition that no 3 points of $\mathcal{O}$ are collinear means that any three of the corresponding $(n-1)$-spaces span $\mathrm{PG}(3n-1,q)$. Hence, field reduction applied to an oval of $\mathrm{PG}(2,q^n)$ gives an $n$-dimensional pseudo-oval of $\mathrm{PG}(3n-1,q)$. Pseudo-ovals arising in this way are called **elementary pseudo-ovals**. A pseudo-oval arising from field reduction applied to a conic is called a **pseudo-conic**. All known pseudo-ovals are elemenatry (see Bamberg–Penttila 2006 [12]).

An $n$-dimensional **dual pseudo-oval** of $\mathrm{PG}(3n-1,q)$ is a set $\mathcal{O}$ of $q^n+1$ subspaces of dimension $2n-1$ with the property that any three intersect trivially, together with $q^n+1$ subspaces of dimension $n-1$, called the **tangents** to $\mathcal{O}$, with the property that each element $X$ of $\mathcal{O}$ lies on a unique tangent meeting no other element of $\mathcal{O}$. The following construction demonstrates how to obtain an elation Laguerre plane from a dual pseudo-oval.

**Example 3.3.4** (Steinke 1991 [142], Löwen 1994 [99]) Let $\mathcal{O}$ be an $n$-dimensional dual pseudo-oval of $\mathrm{PG}(3n-1,q)$. Embed $\mathrm{PG}(3n-1,q)$ as a hyperplane $\mathcal{H}$ in $\mathrm{PG}(3n,q)$ and let $L(\mathcal{O})$ be the incidence structure defined as follows. The points of $L(\mathcal{O})$ are the $(2n)$-subspaces of $\mathrm{PG}(3n,q)$ meeting $\mathcal{H}$ in an elements of $\mathcal{O}$, the lines of $L(\mathcal{O})$ are the elements of $\mathcal{O}$, the circles of $L(\mathcal{O})$ are the points of $\mathrm{PG}(3n,q)$ not on $\mathcal{H}$, with the natural incidence. Then $L(\mathcal{O})$ is an elation Laguerre plane of order $q^n$.

In fact, every elation Laguerre plane arises from this construction.

**Theorem 3.3.5** (Steinke 1991 [142]) *A Laguerre plane $L$ is an elation Laguerre plane if and only if $L \cong L(\mathcal{O})$ for some dual pseudo-oval $\mathcal{O}$.*

Finally, we state some results on the geometric properties of elation Laguerre planes. A Laguerre plane is **weakly Miquelian** if it satisfies **condition M2** – whenever distinct points $P_1, P_2, P_3, P_4, Q_1, Q_2, Q_3, Q_4$ are given such that $P_i$ and $Q_i$ are collinear for $i = 1 \dots 4$, and the sets $\{P_1, P_2, P_3, P_4\}$, $\{P_1, P_2, Q_3, Q_4\}$, $\{P_3, P_4, Q_1, Q_2\}$, are contained in a circle, then $\{Q_1, Q_2, Q_3, Q_4\}$ is also contained in a circle. Note that M2 is obtained from M1 by replacing the concircular sets $\{P_2, P_3, Q_2, Q_3\}$, $\{P_4, P_1, Q_4, Q_1\}$ with pairs of collinear points. Schroth

1999 [133] proved that egglike Laguerre planes satisfy condition M2 (see Schroth 1999 [132] for a simpler proof of this result along with a partial converse). The following theorem of Knarr gives a geometric characterization of elation Laguerre planes.

**Theorem 3.3.6** (Knarr 2002 [96]) *A Laguerre plane $L$ satisfies condition* M2 *if and only if $L$ is an elation Laguerre plane.*

## 3.4 Symmetries of Laguerre planes

The most important open problem about Laguerre planes of finite order is whether or not they are all egglike. The difficulty of addressing this problem directly leads naturally to the development of results under suitable symmetry hypotheses. The conclusions of such results may vary – for example, the plane may be an elation Laguerre plane, egglike or Miquelian. The stronger conclusions naturally arise from stronger symmetry hypotheses. Unsurprisingly, the hypothesis of a large group acting nicely forces the plane to be Miquelian, but the proof involves a lot of group theory, and ultimately depends upon the classification of finite simple groups.

The following result is fundamental to our approach.

**Theorem 3.4.1** (Löwen 1994 [99]) *Let $\Delta$ be the elation group of an elation Laguerre plane $L(\mathcal{O})$. Then* $\mathrm{Aut}\, L(\mathcal{O}) = \Delta \rtimes \Gamma\mathrm{L}(3n, q)_{\mathcal{O}}$.

A permutation group is said to be **quasiprimitive** if each of its nontrivial normal subgroups is transitive. A primitive group is quasiprimitive but not conversely.

**Theorem 3.4.2** *Let $L$ be a Laguerre plane with automorphism group $G$. If $G$ acts quasiprimitively on the circles of $L$, and contains an elation of $L$, then $L$ is an elation Laguerre plane.*

**Proof** By Steinke 1991 [142], $\Delta$ is a non-trivial normal subgroup of $G$. By quasiprimitivity, $\Delta$ acts transitively and hence regularly on circles. $\square$

A Laguerre plane is **flag-transitive** its automorphism group acts transitively on (point,circle) flags. A (dual) psuedo-oval $\mathcal{O}$ is **transitive** if its automorphism group acts transitively on $\mathcal{O}$.

**Theorem 3.4.3** *$L(\mathcal{O})$ is flag-transitive if and only if $\mathcal{O}$ is transitive.*

**Proof** Let $\mathcal{H}$ be the hyperplane at infinity. Suppose $L(\mathcal{O})$ is flag-transitive and let $\mathcal{O}_1$, $\mathcal{O}_2 \in \mathcal{O}$. There exists flags $F_i = (P_i, C)$, $i = 1, 2$, of $L(\mathcal{O})$ and $g \in \mathrm{Aut}\, L(\mathcal{O})$ such that $P_i \cap \mathcal{H} = \mathcal{O}_i$ and $gF_1 = F_2$. Then $g\mathcal{O}_1 = \mathcal{O}_2$, and by Theorem 3.4.1, $g$ restricted to $\mathcal{H}$ is in $\mathrm{P\Gamma L}(3n, q)$. Conversely, suppose $\mathcal{O}$ is transitive and $F_i = (P_i, C_i)$, $i = 1, 2$, are flags of $L(\mathcal{O})$ with $P_i \cap \mathcal{H} = \mathcal{O}_i$. Then there exists $g \in \mathrm{P\Gamma L}(3n, q)_{\mathcal{O}}$ with $g\mathcal{O}_1 = \mathcal{O}_2$ and an elation of $\mathrm{PG}(3n, q)$ with centre $C_1C_2 \cap \mathcal{H}$ and axis $\mathcal{H}$ such that $hC_1 = C_2$. If $g$ induces $\overline{g} \in \mathrm{P\Gamma L}(3n+1, q)$, then $\overline{g}hF_1 = F_2$. $\square$

The preceding two theorems have reduced our problem to a problem about subgroups of semi-linear groups, which makes it tractable.

**Theorem 3.4.4** (Bamberg–Penttila 2006 [12]) *A Laguerre plane $L$ arising from a transitive dual pseudo-oval $\mathcal{O}$ of $\mathrm{PG}(3n-1, q)$, $q$ odd, is Miquelian or the full automorphism group $G$ of the pseudo-oval acts reducibly on $\mathrm{PG}(3n-1, q)$.*

**Proof** By Bamberg–Penttila 2006 [12, Theorem 3.1], if $L$ is not Miquelian then $G$ is soluble. By [12, Remark 4.2], $G \leq \Gamma\mathrm{L}(1, q^b)$ for some $b$. We claim that $b = 2n$ and the $G$ fixes a $\mathrm{PG}(2n-1, q)$. Suppose $n = 1$. Then $\Gamma\mathrm{L}(1, q^b) \leq \mathrm{P\Gamma L}(3, q)$, and so $b \leq 2$. Since $|\mathcal{O}| = q + 1 \mid \left|\Gamma\mathrm{L}(1, q^b)\right|$, it follows that $b = 2$. But then $\Gamma\mathrm{L}(1, q^2)$ fixes a line of $\mathrm{PG}(2, q)$. Now suppose $n \geq 2$. Let $\ell$ be a primitive prime divisor of $q^{2n} - 1$. Then $\ell \mid |G|$ as $G$ is transitive on $\mathcal{O}$, so $\ell \mid \left|\Gamma\mathrm{L}(1, q^b)\right|$ and the primitive part $\Phi^*_{2n}(q)$ of $q^{2n} - 1$ divides $\left|\Gamma\mathrm{L}(1, q^b)\right|$. By Hering 1974 [77] and Hering 1985 [78], we can deduce that $2n \mid b$. Since $\Gamma\mathrm{L}(1, q^b) \leq \mathrm{P\Gamma L}(3n, q)$, it follows that $b < 3n$, and hence $b = 2n$. Let $S \in \mathrm{Syl}_\ell(G)$, and let $S_1 = S \cap \mathrm{GL}(1, q^b)$. Since $|L_1| \mid |\mathrm{GL}(1, q^{2n})|$ and $|L_1| \nmid |\mathrm{GL}(1, q^m)|$ for any $m < 2n$, it follows that every non-trivial irreducible representation for $S_1$ is 1-dimensional over $\mathrm{GF}(q^{2n})$, and hence $2n$-dimensional over $\mathrm{GF}(q)$. It follows that as an $S_1$-module, $\mathrm{GF}(q)^{3n} = \bigoplus_{i=1}^{n} 1 \oplus W$ for some $W$ with $\dim W = 2n$. Since $S_1$ is normal in $G$, it follows that $G$ fixes $W$. $\square$

**Theorem 3.4.5** *A Laguerre plane $L$ with automorphism group $G$ containing a non-trivial elation and acting flag-transitively and quasiprimitively on circles is Miquelian of odd order $q$. Conversely, let $L$ be a Miquelian Laguerre plane of odd order $q$ and $G \leq \mathrm{Aut}\, L$. Then $G$ contains a non-trivial elation and acts flag-transitively and quasiprimitvely on circles if and only if $G \geq \Delta \rtimes \Omega(3, q)$.*

**Proof** To prove the first statement, notice that by Theorem 3.4.2, $L$ is an elation Laguerre plane. By Theorem 3.3.5, $L \cong L(\mathcal{O})$ for some dual pseudo-oval $\mathcal{O}$, which is transitive by Theorem 3.4.3. If $q$ is odd and $L$ is not Miquelian, then by Theorem 3.4.4, $G$ is not quasiprimitive on circles since $G$ is of affine type and acts reducibly on $\mathrm{PG}(3n-1, q)$ (see [59]). If $q$ is even then by [146], $\mathcal{O}$ can be extended to a pseudo-hyperoval by the addition of a nuclear element, giving rise to a system of imprimitivity.

To prove the second statement, let $L$ be Miquelian of odd order $q$, and $G \leq \mathrm{Aut}\, L$. If $G \geq \Delta \rtimes \Omega(3, q)$ then clearly $G$ contains a non-trivial elation elation. Since $\Delta \rtimes \Omega(3, q)$ is transitive on the conic, it is flag-transitive on $L$ by Theorem 3.4.3. The orbits of $\Omega(3, q)$ on $\mathrm{PG}(2, q)$ are the conic, internal and external points, all of which span $\mathrm{PG}(2, q)$. Therefore $\Omega(3, q)$, and hence $G$, acts irreducibly on $\mathrm{PG}(2, q)$, and thus $G$ acts quasiprimitively on circles. Now suppose that $G \leq \mathrm{Aut}\, L$ contains a non-trivial elation, and acts flag-transitively and quasiprimitively on circles. Since $G$ contains a non-trivial elation, it contains all elations by quasiprimitivity on circles. Let $\mathcal{H}$ be the hyperplane at infinity. Then the group $H$ induced by $G$ on $\mathcal{H}$ is a subgroup of $\mathrm{P\Gamma O}(3, q)$ acting transitively on the conic, and it follows from [58] that either $H \leq \Gamma\mathrm{L}(1, q^2)$ or $H \geq \mathrm{P}\Omega(3, q)$. The first case cannot arise by the proof of Theorem 3.4.4. Hence $H \geq \mathrm{P}\Omega(3, q) \cong \Omega(3, q)$ (since $q$ is odd). $\square$

Our methods can also be used to characterize all Miquelian Laguerre planes of finite order. Since the automorphism group of a Miquelian Laguerre plane of even order does not act quasiprimitively on circles, we must remove this hypothesis and substitute another to eliminate the one dimensional semilinear case of Bamberg–Penttila 2006 [12].

**Theorem 3.4.6** *A Laguerre plane $L$ with an insoluble automorphism group $G$ containing a non-trivial elation and acting flag-transitively is Miquelian. Conversely, let $L$ be a Miquelian Laguerre plane of order $q$ and $G \leq \mathrm{Aut}\, L$. Then $G$ contains a non-trivial elation, is insoluble, and acts flag-transitively if and only if $G \geq \Delta \rtimes \Omega(3, q)$.*

## 3.5 Generalized quadrangles and eggs

Recall from Section 1.5 that a (finite) **generalized quadrangle** of order $(s, t)$ $(s, t \geq 1)$ is an incidence structure of points and lines with a symmetric incidence relation such that each point is incidenct with $t + 1$ lines, each line is incident with $s + 1$ points, two distinct points lie on at most one line, two distint lines meet in at most one point, and given a line $\ell$ and a point $P$ not on $\ell$, there exists a unique point $Q$ on $\ell$ such that $Q$ is collinear with $P$. If $s = t$ then we say the generalized quadrangel has order $s$. Classical examples of generalized quadrangles arise from non-degenerate quadrics of $\mathrm{PG}(d, q)$. Let $\mathcal{Q}$ be a non-degenerate quadric of $\mathrm{PG}(d, q)$, $d > 3$. The **polar space** $\Pi(\mathcal{Q})$ arising from $\mathcal{Q}$ is the incidence structure with points the points of $\mathcal{Q}$, and lines the lines of $\mathrm{PG}(d, q)$ contained in $\mathcal{Q}$ (with natural incidence). For example, if $\mathcal{Q}$ is a parabolic quadric of $\mathrm{PG}(4, q)$ then $\Pi(\mathcal{Q}) = \mathrm{Q}(4, q)$ is a generalized quadrangle of order $q$. If $\mathcal{Q}$ is an elliptic quadric of $\mathrm{PG}(5, q)$ then $\Pi(\mathcal{Q}) = \mathrm{Q}^-(5, q)$ is a generalized quadrangle of order $(q, q^2)$. See Example 1.5.5 for the complete list of classical generalized quadrangles.

This section is concerned with a certain class of generalized quadrangles related to elation Laguerre planes. A generalized quadrangle $\mathcal{S}$ of order $(s, t)$ $(s, t > 1)$ is a **translation generalized quadrangle** based at $x$ if there is an abelian group $G$ of automorphisms fixing $x$ linewise and acting regularly on points not collinear with $x$. The group $G$ is the **translation group** of $\mathcal{S}$, and $x$ is the **translation point** or base point. The classical examples given above are all translation generalized quadrangles.

When studying translation generalized quadrangles the following combinatorial structure plays an important role. An **egg** $\mathscr{E}$ of $\mathrm{PG}(2n+m-1,q)$ is a set of $q^m+1$ $(n-1)$-spaces of $\mathrm{PG}(2n+m-1,q)$ such that any three distinct elements of $\mathscr{E}$ span a $(3n-1)$-space, and each element $E$ of $\mathscr{E}$ is contained in an $(n+m-1)$-space $T_E$ of $\mathrm{PG}(2n+m-1,q)$, such that $T_E$ is skew from any element of $\mathscr{E} \setminus \{E\}$. $T_E$ is the **tangent space** of $\mathscr{E}$ at $E$.

**Example 3.5.1** Ovals of $\mathrm{PG}(2,q)$ are eggs with $m=n=1$, and pseudo-ovals are eggs with $m=n$. Ovoids of $\mathrm{PG}(3,q)$ are eggs with $m=2$, $n=1$, and hence an egg with $m=2n$ is called a **pseudo-ovoid**. In even characteristic all known pseudo-ovoids are elementary, but this is not true in odd characteristic, with Kantor's bad eggs 1986 [92] providing a counterexample (see also Payne 1985 [117] and Payne 1989 [119]).

We can construct a translation generalized quadrangle from an egg in the following way.

**Example 3.5.2** Let $\mathscr{E}$ be an egg of $\mathrm{PG}(2n+m-1,q)$. Embed $\mathrm{PG}(2n+m-1,q)$ in $\mathrm{PG}(2n+m,q)$, and define the incidence structure $T(\mathscr{E})$ as follows. Points of $T(\mathscr{E})$ are of three types: (i) points of $\mathrm{PG}(2n+m,q) \setminus \mathrm{PG}(2n+m-1,q)$; (ii) $(n+m)$-spaces of $\mathrm{PG}(2n+m,q)$ intersecting $\mathrm{PG}(2n+m-1,q)$ in a tangent space; (iii) the symbol $(\infty)$. Lines of $T(\mathscr{E})$ are of two types: (a) $n$-spaces of $\mathrm{PG}(2n+m,q)$ intersecting $\mathrm{PG}(2n+m-1,q)$ in an element of $\mathscr{E}$; (b) elements of $\mathscr{E}$. Incidence is defined as follows: lines of type (b) are incident with points of type (ii) which contain them, and with $(\infty)$; lines of type (a) are incident with points of type (i) contained in them, and with points of type (ii) which contain them. Then $T(\mathscr{E})$ is a TGQ based at $(\infty)$ of order $(q^n,q^m)$. This generalizes the familiar constructions $T_2(\mathcal{O})$, for an oval $\mathcal{O}$ of $\mathrm{PG}(2,q)$, and $T_3(\Omega)$, for an ovoid $\Omega$ of $\mathrm{PG}(3,q)$, due to Dembowski 1968 [55]. See Example 1.5.10 and Example 1.5.13.

The following theorem shows that the study of translation generalized quadrangles is equivalent to the study of eggs.

**Theorem 3.5.3** (Payne–Thas 1984 [121], see also Payne–Thas 1980 [158]) *A generalized quadrangle $\mathcal{S}$ is a translation generalized quadrangle if and only if $\mathcal{S} \cong T(\mathscr{E})$ for some egg $\mathscr{E}$ of* $\mathrm{PG}(2n-m+1,q)$.

We remark that a pseudo-oval of $\mathrm{PG}(3n-1,q)$ gives rise to a translation generalized quadrangle of order $(q^n,q^n)$ via this construction. We are naturally interested in when translation generalized quadrangles constructed from a pseudo-oval give classical translation generalized quadrangles. Applying field reduction to an egg $\mathscr{E}$ of $\mathrm{PG}(2n+m-1,q^h)$ gives an egg $\overline{\mathscr{E}}$ of $\mathrm{PG}(h(2n+m)-1,q)$, and $T(\mathscr{E}) \cong T(\overline{\mathscr{E}})$ as translation generalized quadrangles. This observation along with the fact that for eggs $\mathscr{E}_1$, $\mathscr{E}_2$ of $\mathrm{PG}(2n+m-1,q)$, $T(\mathscr{E}_1) \cong T(\mathscr{E}_2)$ if and only if $\mathscr{E}_1 \cong \mathscr{E}_2$ (see Thas–Thas–Van Maldeghem 2006 [160]), leads to the following result.

**Theorem 3.5.4** *Let $\mathcal{O}$ be a pseudo-oval of $\mathrm{PG}(3n-1,q)$. Then $T(\mathcal{O}) \cong \mathrm{Q}(4,q^n)$ if and only if $\mathcal{O}$ is a pseudo-conic. $T(\mathcal{O}) \cong \mathrm{Q}^-(5,q^n)$ if and only if $\mathcal{O}$ is obtained from an elliptic quadric by field reduction.*

In order to show that the correspondence of the next section between translation ovoids of $T(\mathcal{O})$ and translations flocks of $L(\mathcal{O}^*)$ is functorial (that is, that equivalent ovoids correspond to equivalent flocks) we must pin down the automorphism group of $T(\mathcal{O})$, for $\mathcal{O}$ a pseudo-oval. While this is an easy consequence of results appearing in the literature, apparently by an oversight it does not appear to be explicitly stated anywhere. The reason for this is that in the literature $T(\mathscr{E})$, for $\mathscr{E}$ an egg, is the centre of attention. There exist eggs $\mathscr{E}$ for which $T(\mathscr{E})$ is not classical but where $\mathrm{Aut}\,T(\mathscr{E})$ does not fix $(\infty)$. However, there do not exist pseudo-ovals with this property, thus simplifying the treatment of $\mathrm{Aut}\,T(\mathcal{O})$ compared to $\mathrm{Aut}\,T(\mathscr{E})$.

**Theorem 3.5.5** (Thas–Thas–Van Maldeghem 2006 [160]) *Let $\mathcal{O}$ be a pseudo-oval of $\mathcal{H} = \mathrm{PG}(3n-1,q)$ and let $T$ be the group of elations of $\mathrm{PG}(3n,q)$ with axis $\mathcal{H}$. Then $\mathrm{Aut}\,T(\mathcal{O})_{(\infty)} = T \rtimes \Gamma\mathrm{L}(3n,q)_{\mathcal{O}}$.*

**Theorem 3.5.6** *Let $T$ be the group of elations of $\mathrm{PG}(3n,q)$ with axis $H$. If $\mathcal{O}$ is a pseudo-conic of $\mathrm{PG}(3n-1,q)$ then $\mathrm{Aut}\,T(\mathcal{O}) = \mathrm{P\Gamma O}(5,q^n)$ and $\mathrm{Aut}\,T(\mathcal{O})_{(\infty)} = T \rtimes \Gamma\mathrm{L}(3n,q)_{\mathcal{O}}$. If $\mathcal{O}$ is not a pseudo-conic of $\mathrm{PG}(3n-1,q)$ then $\mathrm{Aut}\,T(\mathcal{O})_{(\infty)} = \mathrm{Aut}\,T(\mathcal{O}) = T \rtimes \Gamma\mathrm{L}(3n,q)_{\mathcal{O}}$.*

**Proof** If $\mathcal{O}$ is a pseudo-conic, then the result follows from Theorem 3.5.4. If $\mathcal{O}$ is not a pseudo-conic, then by Theorem 3.5.5 it suffices to show that every automorphism of $T(\mathcal{O})$ fixes $(\infty)$. Suppose not. Then $T(\mathcal{O})$ contains at least two distinct translation points $x, y$. Since the orbit of $y$ under the translation group about $x$ consists of translation points not collinear with $x$, we can assume $x$ and $y$ are collinear. By Thas 2002 [161, Theorem 3], $T(\mathcal{O}) \cong \mathrm{Q}(4, q^n)$, contradicting Theorem 3.5.4. □

## 3.6 Ovoids of TGQ and flocks of ELP

An **ovoid** $\Omega$ of a generalized quadrangle is a set of points such that every line contains a unique point of $\Omega$. A **translation ovoid** based at $x$ of a generalized quadrangle is an ovoid $\Omega$ such that there is an abelian group $G$ of automorphisms fixing $\Omega$, fixing $x$ linewise, and acting regularly on $\Omega \setminus \{x\}$. The group $G$ is the **translation group** of $\Omega$, and $x$ is the **translation point** or basepoint. Given an ovoid $\Omega$ of $\mathrm{PG}(3, q)$ containing an oval $\mathcal{O}$ of $\mathrm{PG}(2, q)$, then $\overline{\Omega} = (\Omega \setminus \mathcal{O}) \cup \{\pi_P : P \in \mathcal{O}\}$ is an ovoid of $T_2(\mathcal{O})$, where $\pi_P$ is the tangent plane to $\Omega$ at $P$ (see Brown 2000 [27]). Such an ovoid is called a **projective ovoid**. If $\pi_\infty$ is the plane on $\mathcal{O}$ and $\pi$ is another plane of $\mathrm{PG}(3, q)$ then $\{(\infty)\} \cup \pi \setminus (\pi \cap \pi_\infty)$ is also an ovoid of $T_2(\mathcal{O})$, called a **planar ovoid**.

Let $\mathcal{O}$ be a pseudo-oval of $\mathrm{PG}(3n-1, q)$ and $\Omega$ be a translation ovoid of $T(\mathcal{O})$. If $\mathcal{O}$ is a pseudo-conic then since $\mathrm{Aut}\, T(\mathcal{O})$ is transitive on the points of $T(\mathcal{O})$, we can assume without loss of generality that a translation ovoid $\Omega$ of $T(\mathcal{O})$ has translation point $(\infty)$. On the other hand, suppose $\mathcal{O}$ is not a pseudo-conic. If $(\infty) \notin \Omega$, then $|\Omega| = q^{2n} + 1$ and $\left|(\infty)^\perp \cap \Omega\right| = q^n + 1$. However, $(\infty)$ is fixed by $\mathrm{Aut}\, T(\mathcal{O})$ by Theorem 3.5.6, contrary to $\Omega$ being a translation ovoid. Hence $(\infty) \in \Omega$. If there is a translation point $x \neq (\infty)$ of $\Omega$, then $\Omega \setminus \{x\}$ is an orbit containing $(\infty)$, a contradiction. Hence, without loss of generality we can assume that a $\Omega$ has translation point $(\infty)$. We also remark here that since applying field reduction to a pseudo-oval $\mathcal{O}$ of $\mathrm{PG}(3n-1, p^h)$ gives a pseudo-oval $\overline{\mathcal{O}}$ of $\mathrm{PG}(3hn-1, p)$, and $T(\mathcal{O}) \cong T(\overline{\mathcal{O}})$ as translation generalized quadrangles, we can assume without loss of generality that $q$ is prime.

**Theorem 3.6.1** *Let $\mathcal{S}$ be a translation generalized quadrangle of order $s$. Then every translation ovoid $\Omega$ based at $(\infty)$ corresponds to a subspace $\mathcal{S}(\Omega)$ of projective space over the prime field disjoint from the pseudo-oval $\mathcal{O}$ (after field reduction).*

**Proof** By applying Theorem 3.5.3 and field reduction, $\mathcal{S} \cong T(\mathcal{O})$ for some pseudo-oval of $\mathrm{PG}(3n-1,p)$ for some prime $p$. Let $\mathcal{H}$ be the hyperplane at infinity. Let $P_1$ and $P_2$ be points of $T(\mathcal{O})$ not collinear with $(\infty)$. A routine calculation shows that $P_1$ and $P_2$ are not collinear in $T(\mathcal{O})$ if and only if $P_1P_2 \cap \mathcal{H}$ is disjoint from $\mathcal{O}$. Identify $\mathrm{PG}(3n-1,p) \setminus \mathcal{H}$ with $\mathrm{GF}(p)^{3n}$ and let $G$ be the translation group of $\Omega$. By Theorem 3.5.6, $G \leq T \rtimes \Gamma\mathrm{L}(3n,p)_{\mathcal{O}}$, and it follows that $G \leq T$ with $G$ acting regularly on $\Omega \setminus (\infty)$ over $\mathrm{GF}(p)$. Thus $\Omega \setminus (\infty)$ forms a subspace of $\mathrm{GF}(p)^{3n}$. We therefore have a $\Sigma \cong \mathrm{PG}(2n,p)$ such that $\Sigma \cap \mathcal{H} \cong \mathrm{PG}(2n-1,p)$ is disjoint from $\mathcal{O}$. $\square$

Recall that a flock of a Laguerre plane of order $n$ is a partition of the points into $n$ circles. Flocks of Laguerre planes were surveyed in Section 3.2.3. A **translation flock** of a Laguerre plane is a flock with an abelian group of automorphisms acting regularly on the circles of the flock.

**Theorem 3.6.2** *Every translation flock $\mathcal{F}$ of an elation Laguerre plane $L$ corresponds to a subspace $\mathcal{S}(\mathcal{F})$ of projective space over the prime field disjoint from the dual pseudo-oval $\mathcal{O}$ (after field reduction).*

**Proof** By applying field reduction and Theorem 3.3.5, $L \cong L(\mathcal{O})$ for some dual pseudo-oval of $\mathrm{PG}(3n-1,p)$ for some prime $p$. Let $\mathcal{H}$ be the hyperplane at infinity. A routine calculation shows that two circles $C_1, C_2$ of $L(\mathcal{O})$ are disjoint in $L(\mathcal{O})$ if and only if $C_1C_2 \cap \mathcal{H}$ is disjoint from $\mathcal{O}$. Identify $\mathrm{PG}(3n-1,p) \setminus \mathcal{H}$ with $\mathrm{GF}(p)^{3n}$ and let $G$ be the translation group of $\mathcal{F}$. Then $G \leq \Delta \rtimes \Gamma\mathrm{L}(3n,p)_{\mathcal{O}}$ by Theorem 3.4.1, and thus $G \leq \Delta$ with $G$ acting regularly on $\mathcal{F}$ over $\mathrm{GF}(p)$. Thus $\mathcal{F}$ forms a subspace of $\mathrm{GF}(p)^{3n}$. We obtain a $\Sigma \cong \mathrm{PG}(n,p)$ such that $\Sigma \cap \mathcal{H} \cong \mathrm{PG}(n-1,p)$ is disjoint from $\mathcal{O}$. $\square$

The natural correspondence between Theorem 3.6.1 and Theorem 3.6.2 can be made explicit with the following result.

**Theorem 3.6.3** *Let $\mathcal{O}$ be a pseudo-oval of* $\mathrm{PG}(3n-1,q)$. *To every translation ovoid* $\Omega$ *of* $T(\mathcal{O})$ *there corresponds a translation flock* $\mathcal{F}$ *of* $L(\mathcal{O}^*)$ *and conversely. Two translation ovoids are isomorphic if and only if their corresponding translation flocks are isomorphic.*

**Proof** Apply field reduction so that without loss of generality $q$ is prime. If $\mathcal{O}$ is a pseudo-conic then without loss of generality $\Omega$ is based at $(\infty)$. Applying the standard duality gives $\mathcal{S}(\Omega)^* = \mathcal{S}(\mathcal{F})$ and $\mathcal{S}(\mathcal{F})^* = \mathcal{S}(\Omega)$. By Theorem 3.4.1 and Theorem 3.5.6, $\Omega_1 \cong \Omega_2$ if and only if $\mathcal{S}(\Omega_2)$ and $\mathcal{S}(\Omega_2)$ are in the same orbit of $\mathrm{P\Gamma L}(3n+1,q)_{\mathcal{O}}$, if and only if $\mathcal{S}(\mathcal{F}_1) = \mathcal{S}(\Omega_1)^*$ and $\mathcal{S}(\mathcal{F}_2) = \mathcal{S}(\Omega_2)^*$ are in the same orbit of $\mathrm{P\Gamma L}(3n+1,q)_{\mathcal{O}^*}$, if and only if $\mathcal{F}_1 \cong \mathcal{F}_2$. □

We remark that under this correspondence planar ovoids of $T_2(\mathcal{O})$ correspond to linear flocks of $L(\mathcal{O}^*)$.

Much of the difficulty in phrasing in the latter sections of this paper is concerned with how best to make precise the vague notion that elation Laguerre planes and translation generalized quadrangles with $s = t$ are dual objects. Theorem 3.3.5 and Theorem 3.5.3 focus attention on pseudo-ovals and their duals. In terms of the constructions ($T(\mathcal{O})$ and $L(\mathcal{O}^*)$) the action takes place *at infinity*. The original proofs of the corollary below used a self-duality (which necessitated the hypothesis that $q$ was odd), but in fact the pseudo oval $\mathcal{O}$ and its dual $\mathcal{O}^*$ lie in different projective spaces – it is not advantageous to identify them. We obtain the following theorems as corollaries of our approach.

**Corollary 3.6.4** (Thas 1997 [155], Lunardon 1997 [100]) *To each semifield flock of* $\mathrm{Q}(4,q)$*, $q$ odd, there corresponds a translation ovoid of* $\mathrm{Q}(4,q)$ *and conversely.*

**Corollary 3.6.5** (Johnson 1987 [87], Glynn 1984 [68]) *Semifield flocks of the quadratic cone are linear in characteristic 2 and translation ovoids of* $\mathrm{W}(q)$ *(and hence of* $\mathrm{PG}(3,q)$*), $q$ even, are elliptic quadrics, and are equivalent.*

Finally, the generalization to non-classical generalized quadrangles and non-Miquelian Laguerre planes involves non-trivial examples. There is a non-linear translation flock of $L(\mathcal{O})$, where $\mathcal{O}$ is the Segre-Bartocci oval in $\mathrm{PG}(2,32)$ constructed by Oscar Jenkins, mentioned in Penttila 2005 [124]. There is also a non-linear translation flock of $L(\mathcal{O})$, where $\mathcal{O}$ is the Lunelli–Sce oval in $\mathrm{PG}(2,16)$ [102].

# Chapter 4

# Hemisystems of polar spaces

## 4.1 Introduction

A **hemisystem** $\mathcal{H}$ of a polar space is a set of maximals such that for every point $P$, exactly half the maximals on $P$ are in $\mathcal{H}$. Hemisystems were first introduced by Segre in 1965, in his monumental 201 page memoir [138]. Segre was studying **regular systems** of order $m$ of $\mathrm{H}(3,q^2)$ – sets $\mathcal{R}$ of lines of $\mathrm{H}(3,q^2)$ such that every point lies on exactly $m$ lines of $\mathcal{R}$, with $0 < m < q+1$. He proved that when $q$ is odd, such a system must have $m = (q+1)/2$, and he called a regular system of $\mathrm{H}(3,q^2)$ of order $(q+1)/2$ a hemisystem. He also constructed a hemisystem of $\mathrm{H}(3,3^2)$ admitting $\mathrm{PSL}(3,4)$, and proved that this hemisystem is unique. He raised the following question.

**Problem 4.1.1** (Segre 1965 [138]) *Do hemisystems exist in* $\mathrm{H}(2r-1,q^2)$ *for* $r > 2$*,* $q > 3$*?*

We will completely resolve this problem in the following sections.

Bruen and Hirschfield 1978 [33] proved the nonexistence of regular systems of $\mathrm{H}(3,q^2)$, for $q$ even. Thas 1995 [154] proved that a regular system of $\mathrm{H}(3,q^2)$ is a hemisystem, and hence $q$ is odd, by showing that the complement of the concurrency graph of the lines of a regular system of $\mathrm{H}(3,q^2)$ of order $m$ is a strongly regular graph with $v = (q^3+1)(q+1-m)$, $k = (q^2+1)(q-m)$, $\lambda = q-m-1$, $\mu = q^2+1-m(q+1)$, and applying the fact that in a strongly regular graph we have $\mu(v-k-1) = k(k-\lambda-1)$.

Cameron, Goethals and Seidel 1978 [40], extended Segre's original definition of a hemisystem to also cover any generalized quadrangle of order $(s,s^2)$, $s$ odd. They defined a hemisystem to be a set of points meeting every line in $(s+1)/2$ points, and showed that the collinearity graph of such a set is strongly regular. They also gave a simple construction of Segre's example in the dual setting of $\mathrm{Q}^-(5,q)$. The set of 56 points that arises is the **cap** usually attributed to Hill 1976 [81].

Much of the motivation for the early study of hemisystems comes from their connection to **partial quadrangles**, first introduced by Cameron 1975 [38]. Recall, a partial quadrangle is an incidence structure of points and lines such that any two points are incident with at most one line, every point is incident with $t+1$ lines, every line is incident with $s+1$ points, two non-collinear points are jointly collinear with exactly $\mu$ points, and for any line $\ell$ and point $P$ not on $\ell$, there is at most one point $Q$ on $\ell$ collinear with $P$. Partial quadrangles were introduced in Section 1.5.3. It follows directly from these conditions that the point graph of a partial quadrangle is a strongly reguar graph with parameters $v = 1 + s(t+1)(\mu + st)/\mu$, $k = s(t+1)$, $\lambda = s-1$, $\mu = \mu$.

A **generalized quadrangle** is a partial quadrangle with $\mu = t+1$. Partial quadrangles that are not generalized quadrangles are quite rare – most arise from deleting a point $P$, all lines on $P$, and all points collinear with $P$, from a generalized quadrangle of order $(s, s^2)$. This construction gives a partial quadrangle of order $(s-1, s^2, s(s-1))$, see Theorem 1.5.18. Examples of partial quadrangles that do not come from this construction either arise from one of the seven known triangle free strongly regular graphs, or from caps of projective spaces (see Theorem 1.5.19), or from a hemisystem of a generalized quadrangle of order $(s, s^2)$ in a way that we describe below.

**Example 4.1.2** (Cameron–Delsarte–Goethals 1979 [39]) We can construct a partial quadrangle from a hemisystem of a generalized quadrangle of order $(s, s^2)$ by defining the points of the partial quadrangle to be the lines of the hemisystem, and the lines of the partial quadrangle to be the lines of the generalized quadrangle. The resulting partial quadrangle has order $((s-1)/2, s^2, (s-1)^2/2)$, and therefore does not arise from deleting points and lines from a generalized quadrangle as above. Since the complement of a hemisystem is also a hemisystem, and partial quadrangles give strongly regular graphs, any hemisystem of a GQ$(s, s^2)$ leads to two stongly regular graphs, which may not be isomorphic (see Bamberg–De Clerck–Durante 2009 [10] for an example where this occurs).

Finally, hemisystems are related to combinatorial structures known as association schemes. A $d$-class **association scheme** is a set $X$, together with $d+1$ symmetric relations $R_i$ on $X$ such that $\{R_0, \ldots, R_d\}$ partitions $X \times X$, the identity relation on $X \times X$ is $R_0$, and for any $(x, y) \in R_k$, the numbers $p_{ij}^k = \{z \in X : (x, z) \in R_i \text{ and } (z, y) \in R_j\}$ depend only on $i, j, k$ (and not on $x$ and $y$). Association schemes were first defined by Bose and Shimamoto 1952 [25]. A strongly regular graph gives a 2-class association scheme by defining $(x, y) \in R_1$ if $x$ is adjacent to $y$, and $(x, y) \in R_2$ if $x$ and $y$ are distinct and non-adjacent. Any 2-class association scheme can be viewed as coming from a strongly regular graph. in this way. Similarly, a distance regular graph with diameter $i$ gives an $i$-class association scheme by defining $(x, y) \in R_i$ if $d(x, y) = i$. Association schemes can be also be constructed from permutation groups. For example a generously transitive group $G$ of rank $d+1$ acting on a set $X$ gives a $d$-class association scheme by defining $\{R_1, \ldots, R_d\}$ to be the orbitals of $G$ on $X$. For more information on association schemes see Brouwer–Cohen–Neumaier 1989 [26]. The following example demonstrates the relationship between hemisystems and association schemes.

**Example 4.1.3** (van Dam–Martin–Muzychuk 2010 [168]) A hemisystem $\mathcal{H}$ of a polar space $X$ gives a 4-class association scheme via the following construction. We say that $x, y \in X$ are in the **same half** of $X$ if either $x$ and $y$ are both in $\mathcal{H}$ or both in $\mathcal{H}^c$. We say $x$ and $y$ are in **opposite halves** otherwise. Then define $(x, y) \in R_1$ if $x$ and $y$ are incident and in the same half, $(x, y) \in R_2$ if $x$ and $y$ are incident and in opposite halves, $(x, y) \in R_3$ if $x$ and $y$ are not incident and in the same half, $(x, y) \in R_4$ if $x$ and $y$ are not incident and in opposite halves. This construction is of some interest because the resulting association scheme is cometric but not metric (equivalently, $Q$-polynomial but not $P$ polynomial), and such association schemes are quite rare in the literature. See Martin–Muzychuk–Williford 2007 [103] for definitions of these terms and a survey of cometric but not metric association schemes.

## 4.2 Recent work

Recall, the first hemisystem of $\mathrm{H}(3, q^2)$ was found by Segre in 1965. Thirty years later, no new hemisystems had been found, and Thas conjectured that Segre's example was the only hemisystem in a hermitian space.

**Conjecture 4.2.1** (Thas 1995 [154]) *There are no hemisystems of* $\mathrm{H}(3, q^2)$*, for* $q > 3$.

This conjecture was shown to be false ten years later, with the first new construction of hemisystems since Segre's 1965 example. Cossidente and Penttila constructed an infinite family of hemisystems of $\mathrm{H}(3, q^2)$, $q$ odd, and a sporadic example in $\mathrm{H}(3, 5^2)$.

**Theorem 4.2.2** (Cossidente–Penttila 2005 [49]) *There exists a hemisystem of* $\mathrm{H}(3, q^2)$*, for each odd prime power* $q$*, admitting* $\mathrm{P}\Omega^-(4, q^2)$*. There exists a hemisystem of* $\mathrm{H}(3, 5^2)$ *admitting* $3 \,.\, A_5$.

The resulting partial quadrangles and strongly regular graphs arising from these hemisystems are new for $q > 3$. This construction lead to renewed interest in hemisystems (see for example, Thas 2007 [156]). Four years later, the same authors used a similar construction to get three new families of hemisystems in $\mathrm{H}(5, q^2)$.

**Theorem 4.2.3** (Cossidente–Penttila 2009 [50]) *There exists a hemisystem of* $\mathrm{H}(5, q^2)$*, for each odd prime power* $q$*, admitting* $\mathrm{P}\Omega^-(6, q^2)$*. There exists a hemisystem of* $\mathrm{H}(5, q^2)$ *for each odd prime power* $q$*, admitting* $\mathrm{P}\Omega^+(6, q^2)$*. There exists a hemisystem of* $\mathrm{H}(5, q^2)$*, for each odd prime power* $q$*, admitting* $\mathrm{P}\Omega(5, q^2)$.

The main goal of this work is to generalize the results of Theorem 4.2.2 and Theorem 4.2.3 to obtain hemisystems of $\mathrm{H}(2r-1, q^2)$, for each odd prime power $q$, and each $r > 2$.

The existence of hemisystems of hermitian polar spaces lead to the renewed interest in hemisystems of generalized quadrangles. As we noted earlier, the generalized quadrangles are the only polar spaces that admit non-classical examples. The Fisher–Thas–Walker–Kantor–Betten generalized quadrangle is an example of a non-classical generalized quadrangle (see Example 2.2.26 for the associated $q$-clan). In 2009, a hemisystem of this non-classical generalized quadrangle was constructed.

**Theorem 4.2.4** (Bamberg–De Clerck–Durante 2009 [10]) *There is a hemisystem of the Fisher–Thas–Walker–Kantor–Betten generalized quadrangle of order* $(5, 5^2)$.

Recall, a **flock** of a quadratic cone $\mathcal{K}$ with vertex $V$ in $\mathrm{PG}(3,q)$ is a partition of $\mathcal{K}\setminus V$ into $q$ disjoint conics. Flocks were discussed in Section 3.2.3. Thas 1987 [151] proved that a flock of a quadratic cone leads to a generalized quadrangle – these are the so called **flock generalized quadrangles**. The Fisher–Thas–Walker–Kantor–Betten generalized quadrangle is an example of a flock generalized quadrangle, and indeed, every known $\mathrm{GQ}(s^2,s)$ arises from a flock. Since Theorem 4.2.4 proves that the existence of a hemisystem in this particular flock generalized quadrangle, it is natural to ask if every flock generalized quadrangle contains a hemisystem. The following theorem shows that this is true in odd characteristic.

**Theorem 4.2.5** (Bamberg–Guidici–Royle 2010 [11]) *Every flock generalized quadrangle of order $(s^2,s)$, $s$ odd, contains a hemisystem.*

It appears that after a long period where hemisystems were thought to be extremely rare, we may in fact have an embarrassment of riches. Theorem 4.2.5, in principle, gives rise to a large number of hemisystems of generalized quadrangles (the construction involves a choice, which means that it is possible that each flock generalized quadrangle contains a number of hemisystems; it is not clear at this stage how many of these hemisystems are inequivalent). However, the construction given in Bamberg–Guidici–Royle 2010 [11] is quite complicated, and it appears that it will take some time to gain insight into hemisystems obtained from this model. However, a hemisystem equivalent to the Cossidente–Penttila hemisystems of $\mathrm{H}(3,q^2)$ was constructed in Bamberg–Guidici–Royle 2010 [11], so it is possible that using this model may be useful in the construction of new hemisystems. We will be interested in constructing hemisystems in hermitian polar spaces rather than generalized quadrangles, so this is not an approach that we will consider in this paper.

## 4.3 The Cossidente–Penttila examples

Our goal is to generalize the hemisystems construted in Cossidente–Penttila 2005 [49] and Cossidente–Penttila 2009 [50]. Both of these papers involve a particular embedding of $\mathrm{Q}^\epsilon(d,q) \subset \mathrm{H}(d,q^2)$, and so we will first summarize the key properties of this embedding.

In Cossidente–Penttila 2005 [49] and Cossidente–Penttila 2009 [50], the authors present the embedding in terms of **commuting polarities**. These were first introduced by Tits 1955 [162]. Ten years later, Segre 1965 [138] developed the theory of polarities commuting with a non-degenerate unitary polarity in $\mathrm{PG}(3,q^2)$ in the context of studying the geometry of the hermitian surface $\mathrm{H}(3,q^2)$. The theory of commuting polarities also seems to be of great importance in understanding the structure of certain maximal subgroups of finite classical groups. This is apparent, for example, in the works of Aschbacher 1984 [4] and Cossidente–King 2004 [47].

The particular setting we are interested in is as follows. Let $\mathcal{U}$ be the unitary polarity assoicated with $\mathrm{H}(d,q^2)$. Let $\mathcal{B}$ be an orthogonal polarity commuting with $\mathcal{U}$. Let $\mathcal{V}=\mathcal{B}\mathcal{U}=\mathcal{U}\mathcal{B}$. Then by Segre 1965 [138], $\mathcal{V}$ is a non-linear collineation of $\mathrm{PG}(d,q^2)$, and $\mathscr{Q}=\mathcal{V}\cap\mathrm{H}(d,q^2)$ is a non-degenerate quadric. In fact, $\mathscr{Q}=\mathrm{H}(d,q^2)\cap\Sigma_0$, where $\Sigma_0$ is a **Baer subgeometry** of $\mathrm{PG}(d,q^2)$ isomorphic to $\mathrm{PG}(d,q)$. The type of $\mathscr{Q}$ matches the type of $\mathcal{B}$. Thus, we have $\mathrm{Q}^\epsilon(d,q)\subset\mathrm{H}(d,q^2)$, and

$$\mathrm{P\Omega}^\epsilon(d+1,q)\leq\mathrm{PO}^\epsilon(d+1,q)\leq\mathrm{PU}(d+1,q^2),$$

for $\epsilon=\pm$. This embedding is illustrated in Figure 4.1.

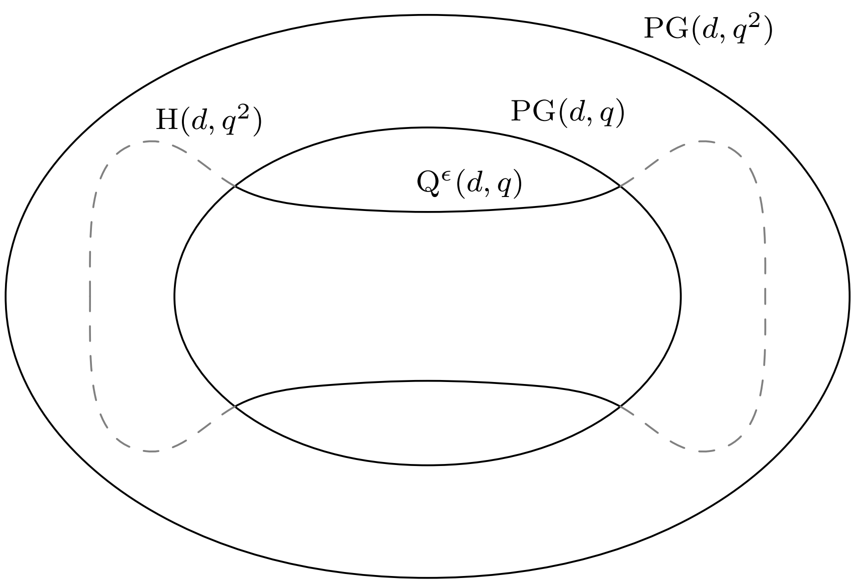


Figure 4.1: The embedding $\mathrm{Q}^\epsilon(d,q)\subset\mathrm{H}(d,q^2)$.

It is perhaps easier to consider this embedding in terms of Gram matrices. Let $\beta$ be the polarization of a quadratic form $Q$ over $\mathrm{GF}(q)^{d+1}$. Then $\beta(x,y) = x^t A y$, for some symmetric matrix $A \in \mathrm{GL}(d+1,q)$. Define a new form $\widetilde{\beta}$ on $\mathrm{GF}(q^2)^{d+1}$ by $\widetilde{\beta}(x,y) = x^t A \overline{y}$, where $^{-} \in \mathrm{Aut}\,\mathrm{GF}(q^2)$ is defined by $\overline{x} = x^q$. Then $^{-}$ is an involution in $\mathrm{Aut}\,\mathrm{GF}(q^2)$ (a **Baer involution**), and $A$ is hermitian with respect to $^{-}$ as a matrix in $\mathrm{GL}(d+1,q^2)$. Hence, $\widetilde{\beta}$ is a hermitian form over $\mathrm{GF}(q^2)^{d+1}$. Clearly, any totally singular subspace with respect to $Q$ is totally isotropic with respect to $\widetilde{\beta}$. This gives the embedding $\mathrm{Q}^\epsilon(d,q) \subset \mathrm{H}(d,q^2)$. Now any isometry $B \in \mathrm{GL}(d+1,q)$ of $\beta$ satisfies $B^t A B = A$, and hence $B^t A \overline{B} = A$, and so $B$ is an isometry of $\widetilde{\beta}$. This gives the chain of subgroups

$$\Omega^\epsilon(d+1,q) \leq \mathrm{O}^\epsilon(d+1,q) \leq \mathrm{U}(d+1,q^2),$$

and so on for the similarities, semisimilarites etc.

Since we have $\mathrm{GF}(q)$ as a subfield of $\mathrm{GF}(q^2)$, $\mathrm{PG}(d,q)$ as a subgeometry of $\mathrm{PG}(d,q^2)$, and an involution acting trivially on the subfield (subgeometry), we borrow language from analysis, and call subspaces in $\mathrm{PG}(d,q^2)$ **real** if they meet $\mathrm{PG}(d,q)$ in a subspace of $\mathrm{PG}(d,q)$, and **imaginary** otherwise. The following theorem is fundamental to the approach in the Cossidente–Penttila papers.

**Theorem 4.3.1** (Sved 1983 [144]) *Every imaginary point of* $\mathrm{H}(d,q^2)$ *lies on a unique real line of* $\mathrm{PG}(d,q^2)$.

Theorem 4.3.1 gives us a way of distinguishing the points of $\mathrm{H}(d,q^2)$. Take a real line $\ell$, and consider $\widetilde{\beta} = \beta|_\ell$. If $\dim \mathrm{rad}(\widetilde{\beta}) = 2$, then $\widetilde{\beta}$ is the zero form, and hence $|\ell \cap \mathrm{H}(d,q^2)| = q^2+1$, $|\ell \cap \mathrm{Q}^\epsilon(d,q)| = q+1$, and $\ell$ is **totally isotropic**. If $\dim \mathrm{rad}(\widetilde{\beta}) = 1$, then $\widetilde{\beta}$ is equivalent to $\widetilde{\beta}(x,y) = x_1\overline{y_1}$, and hence $|\ell \cap \mathrm{H}(d,q^2)| = |\ell \cap \mathrm{Q}^\epsilon(d,q)| = 1$. In this case we say that $\ell$ is a **tangent** line. If $\dim \mathrm{rad}(\widetilde{\beta}) = 0$, then $\widetilde{\beta}$ is non-degenerate, $\widetilde{\beta}$ is equivalent to $\widetilde{\beta}(x,y) = x_1\overline{y_1} + x_2\overline{y_2}$, and hence $|\ell \cap \mathrm{H}(d,q^2)| = q+1$. If $\widetilde{Q} = Q|_{\ell\cap\mathrm{PG}(d,q)}$ has plus type, then $\widetilde{Q}$ is equivalent to $\widetilde{Q}(x) = x_1x_2$, and hence $|\ell \cap \mathrm{Q}^\epsilon(d,q)| = 2$, and $\ell$ is **secant**. If $\widetilde{Q}$ has minus type, then $\widetilde{Q}$ is equivalent to $\widetilde{Q}(x) = x_1^2 + ax_1x_2 + bx_2^2$ with $x^2+ax+b$ irreducible over $\mathrm{GF}(q)$, and hence $|\ell \cap \mathrm{Q}^\epsilon(d,q)| = 0$ and $\ell$ is **external**. The four classes real lines and the structure of their totally isotropic points is shown in Figure 4.2. The points of $\mathrm{H}(d, q^2)$ thus fall into four classes:

- real totally isotropic points
- imaginary totally isotropic points on a real totally isotropic line
- imaginary totally isotropic points on real secant line
- imaginary totally isotropic points on a real external line.

Notice that an imaginary totally isotropic point of $\mathrm{H}(d, q^2)$ cannot lie on a real tangent line, since the point of tangency is real. Now returning to the papers of Cossidente–Penttila, we can start to see how thinking of points in terms of these classes is useful. Define $G = \mathrm{PSU}(4, q^2)_{\mathrm{Q}^-(3,q)}$. By Cossidente–King 2004 [47, Proposition 2.2], $G = \mathrm{PGO}^-(4, q) \cap \mathrm{PSU}(4, q^2)$.

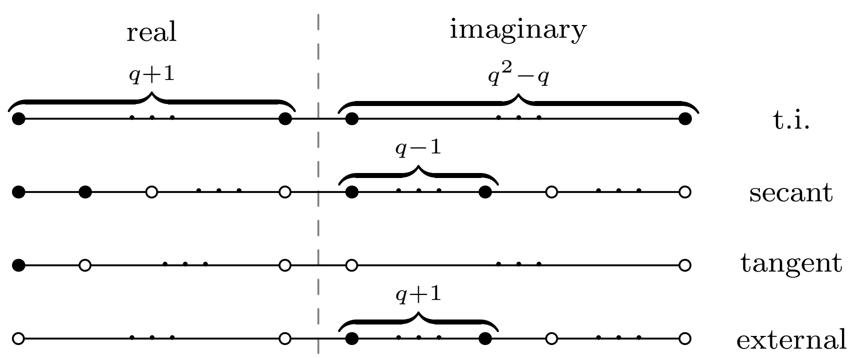


Figure 4.2: The four classes of real lines. Totally isotropic points are denoted by a filled in circle, non-totally isotropic points are denoted by open circles.

**Proposition 4.3.2** ([49, Proposition 2.2]) *The group $G$ has three orbits on the points of* $\mathrm{H}(3, q^2)$ *– real totally isotropic points, imaginary totally isotropic points on a real secant line, and imaginary totally isotropic points on a real external line.*

**Proposition 4.3.3** ([49, Proposition 2.3]) *The group $G$ has two orbits on the lines of* $\mathrm{H}(3, q^2)$ *– the secant lines, and the external lines.*

So the classification of points and lines of the hermitian surface we have considered is compatible with a group of automorphisms. This means that we can bring the extensive theory of the subgroup structure of the classical groups to bear on the problem. The key insight of Cossidente–Penttila 2005 [49] is the existence of a subgroup of $H = \mathrm{P}\Omega^-(4, q)$ of $G$ with the property that $G$ and $H$ have the same orbits on the points of $\mathrm{H}(3, q^2)$, but each $G$-orbit on lines splits into two $H$-orbits. Labeling the point orbits of $H$ as $\{\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3\}$ and the line orbits of $H$ as $\{\mathcal{O}_1, \mathcal{O}_2, \mathcal{O}_3, \mathcal{O}_4\}$, the authors then go on to calculate the intersection numbers $b_{ij} = |\{P \in \mathcal{P}_i : P\, I\, \ell_j$, for a fixed $\ell_j \in \mathcal{O}_j\}|$, and $a_{ij} = |\{\ell \in \mathcal{O}_j : P_i\, I\, \ell$, for a fixed $P_i \in \mathcal{P}_i\}|$. The matrix $B = [b_{ij}]$ is the **block-tactical** decomposition matrix, and the matrix $A = [a_{ij}]$ is the **point-tactical** decomposition matrix.

It turns out that the block-tactical decomposition matrix with respect to the $H$-orbits is

$$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & \frac{q^2+1}{2} & \frac{q^2+1}{2} \\ q^2 & q^2 & \frac{q^2+1}{2} & \frac{q^2+1}{2} \end{bmatrix},$$

and the point-tactical decomposition matrix is

$$\begin{bmatrix} \frac{q+1}{2} & \frac{q+1}{2} & 0 & 0 \\ 0 & 0 & \frac{q+1}{2} & \frac{q+1}{2} \\ 1 & 1 & \frac{q-1}{2} & \frac{q-1}{2} \end{bmatrix}.$$

Notice that each colum in the point-tactical decomposition matrix is repeated. It follows immediately that $\{\mathcal{O}_1, \mathcal{O}_3\}$ and $\{\mathcal{O}_2, \mathcal{O}_4\}$ are hemisystems of $\mathrm{H}(3, q^2)$. Of course, the difficult part of this approach is the calculations of the entries of the decomposition matrices, each of which is highly non-trivial.

The approach in [50] is similar. Note that the maximals in $\mathrm{H}(5, q^2)$ are planes. Define $G^\epsilon = \mathrm{PSU}(6, q^2)_{\mathrm{Q}^\epsilon(5,q)}$. By [47], $G_\epsilon = \mathrm{PGO}^\epsilon(6, q) \cap \mathrm{PSU}(6, q^2)$, for $\epsilon = \pm$. We have the following propositions about the orbits of $G^\epsilon$ on $\mathrm{H}(5, q^2)$.

**Proposition 4.3.4** ([50, Proposition 2.2, Proposition 2.4]) *The group $G^\epsilon$ has four orbits on the points of $\mathrm{H}(5, q^2)$ for $\epsilon = \pm$ – real totally isotropic points of $\mathrm{H}(5, q^2)$, imaginary points on a real totally isotropic line, imaginary points on a real secant line, imaginary points on a real external line.*

**Proposition 4.3.5** ([50, Proposition 2.3, Proposition 2.5]) *The group $G^-$ has three orbits on planes of* $\mathrm{H}(5,q^2)$*. The group $G^+$ has four orbits on planes of* $\mathrm{H}(5,q^2)$*.*

Again, there are subgroups $H^\epsilon = \mathrm{P}\Omega^\epsilon(6,q)$ of $G^\epsilon$ with the same point orbits, and having the property that every $G^\epsilon$-orbit on planes splits into two $H^\epsilon$-orbits. The block-tactical and point-tactical intersection numbers with respect to the $H^\epsilon$ orbits were calculated in [50]. In the elliptic case the block tactical decomposition matrix is

$$\begin{bmatrix} q+1 & q+1 & 1 & 1 & 0 & 0 \\ q^2-q & q^2-q & 0 & 0 & q^2+1 & q^2+1 \\ 0 & 0 & \frac{q^4+q^2}{2} & \frac{q^4+q^2}{2} & \frac{q^4-q^2}{2} & \frac{q^4-q^2}{2} \\ q^4 & q^4 & \frac{q^4+q^2}{2} & \frac{q^4+q^2}{2} & \frac{q^4+q^2}{2} & \frac{q^4+q^2}{2} \end{bmatrix},$$

and the point-tactical decomposition matrix is

$$\begin{bmatrix} \frac{q^3+q^2+q+1}{2} & \frac{q^3+q^2+q+1}{2} & \frac{q^4-q^2}{2} & \frac{q^4-q^2}{2} & 0 & 0 \\ \frac{q+1}{2} & \frac{q+1}{2} & 0 & 0 & \frac{q^4+q^3}{2} & \frac{q^4+q^3}{2} \\ 0 & 0 & \frac{q^3+q^2+q+1}{2} & \frac{q^3+q^2+q+1}{2} & \frac{q^4-q^2}{2} & \frac{q^4-q^2}{2} \\ q+1 & q+1 & \frac{(q^2-1)(q+1)}{2} & \frac{(q^2-1)(q+1)}{2} & \frac{q^4-q^2}{2} & \frac{q^4-q^2}{2} \end{bmatrix}.$$

Again, since columns of the point-tactical decomposition matrix occur in pairs, amalgamation of the first, third, and fifth plane orbits under $\mathrm{P}\Omega^-(6,q)$ gives a hemisystem of $\mathrm{H}(5,q^2)$. In the hyperbolic case the block tactical decomposition matrix is

$$\begin{bmatrix} q^2+q+1 & q^2+q+1 & q+1 & q+1 & 1 & 1 & 0 & 0 \\ q^4-q & q^4-q & q^2-q & q^2-q & 2q^2 & 2q^2 & q^2+1 & q^2+1 \\ 0 & 0 & 0 & 0 & \frac{q^4-q^2}{2} & \frac{q^4-q^2}{2} & \frac{q^4-q^2}{2} & \frac{q^4-q^2}{2} \\ 0 & 0 & q^4 & q^4 & \frac{q^4-q^2}{2} & \frac{q^4-q^2}{2} & \frac{q^4+q^2}{2} & \frac{q^4+q^2}{2} \end{bmatrix},$$

and the point-tactical decomposition matrix is

$$\begin{bmatrix} q+1 & q+1 & \frac{(q^2-1)(q+1)}{2} & \frac{(q^2-1)(q+1)}{2} & \frac{q^4-q^2}{2} & \frac{q^4-q^2}{2} & 0 & 0 \\ 1 & 1 & 1 & 1 & \frac{q^4+q^3+q-1}{2} & \frac{q^4+q^3+q-1}{2} & \frac{q^4+q^3+q-3}{2} & \frac{q^4+q^3+q-3}{2} \\ 0 & 0 & 0 & 0 & \frac{q^3+q^2+q+1}{2} & \frac{q^3+q^2+q+1}{2} & \frac{q^4-q^2}{2} & \frac{q^4-q^2}{2} \\ 0 & 0 & q+1 & q+1 & \frac{(q^2-1)(q+1)}{2} & \frac{(q^2-1)(q+1)}{2} & \frac{q^4-q^2}{2} & \frac{q^4-q^2}{2} \end{bmatrix}.$$

Here, the union of the first, third, fifth, and seventh plane orbits of $\mathrm{Q}^+(6,q)$ gives a hemisystem of $\mathrm{H}(5,q^2)$. In the next section we will look at how to generalize these constructions.

## 4.4 A class of hemisystems in $\mathrm{H}(2r-1, q^2)$

Our goal here is to generalize the construction outlined in Section 4.3. Each hemisystem arose by taking the union of orbits on maximal totally isotropic subspaces under a suitable group, and the fact that these orbits formed a hemisystem was apparent from the fact that each column of the point-tactical decomposition matrix was repeated. However, there is an obvious problem with continuing with this approach. The number of orbits of $\mathrm{P}\Omega^{\epsilon}(d+1, q)$ on totally isotropic points of $\mathrm{H}(d, q^2)$ looks like it will remain constant, but the number of orbits on maximals appears to be growing with the rank. The action of $\mathrm{P}\Omega^{+}(6, q)$ on $\mathrm{H}(5, q^2)$ already has four orbits on totally isotropic points and eight orbits on totally isotropic planes, and so calculating the tactical decomposition matrices requires 32 non-trivial calculations. Trying to calculate these matrices for larger rank seems foolish.

We need to somehow argue that the columns of the point-tactical decomposition are repeated *without having to calculate the matrices.* The insight that was minimized in [49] and [50] is that there are in fact *two* groups involved in the construction of each hemisystem. In each case there were groups $A, B \leq \mathrm{P\Gamma U}(d+1, q^2)$ such that:

- $B$ is a normal subgroup of $A$
- $A$ and $B$ have the same orbits on totally isotropic points of $\mathrm{H}(d, q^2)$
- each $A$-orbit on maximal totally isotropic subspaces of $\mathrm{H}(d, q^2)$ splits into two $B$-orbtis.

As stated above, the authors then proceeded to compute the intersection numbers with respect to the $B$-orbits on points and maximals. However, as the next lemma shows, this is unnecessary.

**Lemma 4.4.1** (The $AB$-Lemma) *Let $\mathscr{I} = (\mathcal{P}, \mathcal{M}, I)$ be an incidence structure with two types, which we call points and maximals. Let $A$ and $B$ be two subgroups of $\mathrm{Aut}\,\mathscr{I}$ such that (i) $B$ is a normal subgroup of $A$, (ii) $A$ and $B$ have the same orbits on $\mathcal{P}$, (iii) each $A$-orbit on $\mathcal{M}$ splits into two $B$-orbits. Then there are $2^n$ hemisystems admitting $B$, where $n$ is the number of $A$-oribts on maximals.*

**Proof** Let $\mathcal{H}$ be a union of $B$-orbits on maximals, one from each $A$-orbit. Let $P$ be a point and $M$ be a maximal in $\mathcal{H}$. Let $\mathcal{O}$ be the $B$-orbit of $M$, and $\mathcal{O}'$ be the complement of $\mathcal{O}$ in the $A$-orbit of $M$. Then $A$ acts transitively on $\{\mathcal{O}, \mathcal{O}'\}$, since $B$ is normal in $A$. It follows that the number of maximals in $\mathcal{O}$ on $P$ equals the number of maximals in $\mathcal{O}'$ on $P$, since $P$ has the same orbit under both $A$ and $B$. Let $\mathcal{H}'$ be the complement of $\mathcal{H}$ in the set of all maximals. It follows that the number of maximals in $\mathcal{H}$ on $P$ equals the numbers of maximals in $\mathcal{H}'$ on $P$, and so this number is half the number of maximals on $P$. Thus $\mathcal{H}$ is a hemisystem. □

The advantage to working abstractly with the two groups instead of concretely with one group is that *we are using that fact that each column of the point-tactical decomposition matrix is repeated without having to know the entries in each column.* So all we need to do is find a pair of subgroups satisfying the hypotheses of the $AB$–Lemma. We will use Lemma 4.4.1 with $\mathscr{I} = \mathrm{H}(2r-1, q^2)$, $A = \mathrm{PO}^-(2r, q)$, $B = \mathrm{PSO}^-(2r, q)$.

**Lemma 4.4.2** *For $r > 1$, $q$ odd,* $\mathrm{PO}^-(2r,q)$ *and* $\mathrm{PSO}^-(2r,q)$ *each have 4 orbits on totally isotropic points of* $\mathrm{H}(2r-1,q^2)$ *– real points, imaginary points on a real secant line, imaginary points on a real external line, and imaginary points on a real line of* $\mathrm{Q}^-(2r,q)$.

**Proof** First we show that $\mathrm{PO}^-(2r,q)$ has the stated orbits. By the classification of quadrics, any two external lines are isometric, as are any two secant lines, as are any two lines of the quadric, as are any two points of the quadric. Hence $\mathrm{PO}^-(2r,q)$ is transitive on real points, and to get the desired result for imaginary points, we may assume that we have two imaginary points on the same real line $\ell$, and that $\ell$ is not tangent to $\mathrm{Q}^-(2r-1,q)$, as such lines are tangent to $\mathrm{H}(2r-1,q^2)$, so contain no imaginary totally isotropic points. By Witt's theorem, the group induced on $\ell$ by the stabiliser of $\ell$ in $\mathrm{O}^-(2r,q)$ is the isometry group of $\ell$. If $\ell$ is a line of the quadric, this is $\mathrm{GL}(2,q)$, which is clearly transitive on $\mathrm{PG}(1,q^2) \setminus \mathrm{PG}(1,q)$. By [94, Proposition 2.9.1 (iii)], if $\ell$ is external then the group $\mathrm{O}^-(2,q)$ induced on $\ell$ by $\mathrm{O}^-(2r,q)$ is dihedral of order $2(q+1)$; in this case, $\ell$ is a hyperbolic line of $\mathrm{H}(2r-1,q^2)$, containing $q+1$ totally isotropic points, and the group is again transitive on the totally isotropic points on $\ell$. By [94, Proposition 2.9.1(iii)], if $\ell$ is secant then the group $O^+(2, q)$ induced on $\ell$ is dihedral of order $2(q-1)$; in this case, $\ell$ is a hyperbolic line of $H(2r-1, q^2)$, containing $q-1$ imaginary totally isotropic points, and the group is yet again transitive on the imaginary totally isotropic points on $\ell$. Hence $PO^-(2r, q)$ has the required point orbits. But since we can apply Witt's theorem with special isometries in place of isometries, it follows that $PSO^-(2r, q)$ has the same point orbits. □

In order to compute the orbits of $PO^-(2r, q)$ and $PSO^-(2r, q)$ on maximal totally isotropic subspaces of $H(2r-1, q^2)$, the following geometric perspective on the field extension $GF(q) \subset GF(q^2)$, and the embedding $PG(2r-1, q) \subset PG(2r-1, q^2)$ is useful. This perspective goes back to Bruen 1972 [31] (see also Bruen 1975 [32]).

Take an $(r-1)$-space $M$ disjoint from $PG(2r-1, q)$. Then $\overline{M}$ is also disjoint from $PG(2r-1, q^2)$. By Casse–O'Keefe 1990 [41], a subspace of $PG(2r-1, q^2)$ of dimension $r$ is fixed by $^-$ if and only if it intersects the subgeometry $PG(2n-1, q)$ in a subspace in dimension $r$. For every point $P \in M$, consider the line $\ell_P$ joining $P$ to $\overline{P}$. This line is fixed by $^-$, and so intersects $PG(2r-1, q)$ in a line. Consider the set $\mathcal{S} = \{\ell_P : P \in M\}$. Since $M$ is skew to $PG(2r-1, q)$, distinct elements of $\mathcal{S}$ are disjoint. Hence, $\mathcal{S}$ is a partition of the points of $PG(2r-1, q)$ into lines. Such a set is called a 1-**spread** of $PG(2r-1, q)$. This construction is illustrated in Figure 4.3. Spreads are connected to many objects of interest in combinatorics. The following example shows that spreads can be used to construct translation planes.

**Example 4.4.3** (Andre 1954 [3], Bruck–Bose 1964 [30]) From a 1-spread $\mathcal{S}$ we construct an affine plane $\mathcal{A}(\mathcal{S})$ as follows. Embed $PG(2r-1, q)$ as a hyperplane in $PG(2r, q)$. Define the points of $\mathcal{A}(\mathcal{S})$ to be the points in $PG(2r, q) \setminus PG(2r-1, q)$, and define the lines of $\mathcal{A}(\mathcal{S})$ to be the planes of $PG(2r, q)$ meeting $PG(2r-1, q)$ in an element of $\mathcal{S}$, with incidence inherited from $PG(2r, q)$. The resulting incidence structure is a $2-(q^{2r}, q^2, 1)$ design, and when $r = 2$, $\mathcal{A}(\mathcal{S})$ is a **translation plane**. For any $n \geq 2$, if $\mathcal{A}(\mathcal{S})$ is isomorphic to the point/line design of some $AG(r, q^2)$, then the spread $\mathcal{S}$ is called **Desarguesian**. It turns out that every Desarguesian spread can be constructed in this way (see Lunardo 1999 [101], Segre 1964 [137]).

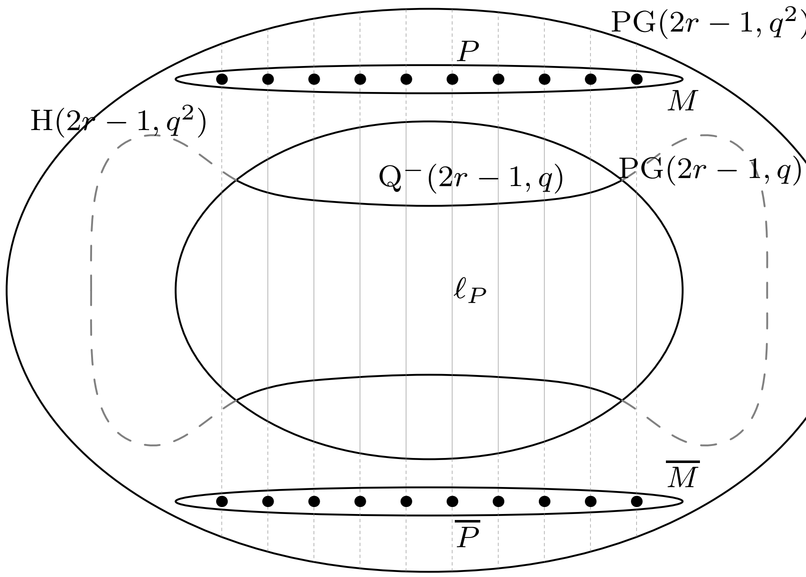


Figure 4.3: The construction of a line spread of PG$(2r-1,q)$ from an $(r-1)$-space $M$ of PG$(2r-1,q^2)$ disjoint from PG$(2r-1,q)$.

Thinking about field extensions in terms of spreads is useful in part because certain results about maximality of orthogonal groups are most naturally stated in terms of stabilizers of spreads. In particular, the work of Cossidente–King 2006 [48] contains very explicit geometric descriptions of subgroups that are suitable for computing orbits, and are therefore convenient for our purposes.

**Lemma 4.4.4** *For $r > 1$, $q$ odd, every maxmial totally isotropic subspace of* H$(2r-1,q^2)$ *disjoint from* PG$(2r-1,q)$ *corresponds to a spread $\mathcal{S}$ of* PG$(2r-1,q)$ *whose stabilizer in* O$^-(2r,q)$ *has the structure* O$^-(r,q^2)\cdot 2$.

**Proof** Firstly, $\overline{M}$ is disjoint from PG$(2r-1,q)$, since otherwise there would be a point $P \in M \cap \overline{M}$, and $\ell = \langle P, \overline{P}\rangle$ would be a real line contained in $M$, a contradiction. For each $P \in M$, define $\ell_P = \langle P, \overline{P}\rangle$. By Bruen 1972 [31], $\mathcal{S} = \{\ell_P : P \in M\}$ is a spread of PG$(2r-1,q)$. Let $\pi$ be the orthogonal polarity of minus type on PG$(2r-1,q^2)$. Define the polarity $\alpha$ on $M$ by $P^\alpha = P^\pi \cap M$. It is easy to see that $P^\pi$ contains $\overline{M}$ and $\overline{P}^\pi$ contains $M$, and so both $P^\pi$ and $\overline{P}^\pi$ contain $\langle P^\alpha, \overline{P}^\alpha\rangle$. Hence, $\langle P^\alpha, \overline{P}^\alpha\rangle = P^\pi \cap \overline{P}^\pi = \ell_P^\pi$. It follows that $\alpha$ is an orthogonal polarity of minus type. Any isometry of the associated quadratic form on

$M$ induces an isometry of $\mathrm{PG}(2r-1,q)$, and by Cossidente–King 2006 [48], the stabilizer of $\mathcal{S}$ is generated by these induced isometries together with the Baer involution. □

**Lemma 4.4.5** *For $r>1$, $q$ odd, two maximal totally isotropic subspaces of $\mathrm{H}(2r-1,q^2)$ lie in the same orbit of $\mathrm{PO}^-(2r-1,q)$ if and only if they have the same number of real points.*

**Proof** Let $M$ be a maximal totally isotropic subspace of $\mathrm{H}(2r-1,q^2)$. Let $N = M \cap \mathrm{Q}^-(2r-1,q)$ have algebraic dimension $n$. Let $\Sigma = N^{\perp}/N \cong \mathrm{H}(2(r-n)-1,q^2)$. Then $M/N$ is a maximal totally isotropic subspace of $\Sigma$ disjoint from $\mathrm{Q}^-(2(r-n)-1,q)$. For $r>1$, $\mathrm{PO}^-(2r,q)$ is transitive on singular subspaces of fixed algebraic dimension, so it suffices to show that for $r>1$, $\mathrm{PO}^-(2r-1,q)$ is transitive on maximals disjoint from $\mathrm{Q}^-(2r-1,q)$. By [94], we know that $\mathrm{PO}^-(2r-1,q)$ is transitive on pairs $\{M,\overline{M}\}$, and by [48] there exists an element in $\mathrm{PO}^-(2r-1,q)$ interchanging $M$ and $\overline{M}$. □

**Lemma 4.4.6** *For $r>2$, $q$ odd, each $\mathrm{PO}^-(2r,q^2)$-orbit on maximal totally isotropic subspaces of $\mathrm{H}(2r-1,q^2)$ disjoint from $\mathrm{PG}(2r-1,q)$ splits into two $\mathrm{PSO}^-(2r,q^2)$-orbits.*

**Proof** Let $M$ be a maximal totally isotropic subspace of $\mathrm{H}(2r-1,q^2)$. Since $\mathrm{PSO}^-(2r,q)$ has index 2 in $\mathrm{PO}^-(2r,q)$, it follows that $\mathrm{PSO}^-(2r,q)_M$ has index 1 or 2 in $\mathrm{PO}^-(2r,q)_M$. We wish to show that the index is 1. By Lemma 4.4.4, we known that $M$ corresponds to a spread $\mathcal{S}$. By Cossidente–King 2006 [48], unless $r$ is odd and $q \equiv 3 \pmod 4$, the stabilizer of the spread $\mathcal{S}$ corresponding to $M$ lies in $\mathrm{PSO}^-(2r,q)$, and the result follows. In the case where $r$ is odd and $q \equiv 3 \pmod 4$, a simple determinant calculation shows that the Baer involution is not in $\mathrm{PSO}^-(2r,q)$, and so even though $\mathrm{PSO}^-(2r,q)_{\mathcal{S}}$ has index 2 in $\mathrm{PO}^-(2r,q)_{\mathcal{S}}$, it is still the case that $\mathrm{PSO}^-(2r,q)_M = \mathrm{PO}^-(2r,q)_M$. □

**Lemma 4.4.7** *For $r>2$, $q$ odd, each $\mathrm{PO}^-(2r,q^2)$-orbit on maximal totally isotropic subspaces of $\mathrm{H}(2r-1,q^2)$ splits into two $\mathrm{PSO}^-(2r,q^2)$-orbits.*

**Proof** Let $M$ be a totally isotropic subspace of $\mathrm{H}(2r-1,q^2)$, and let $N = M \cap \mathrm{Q}^-(2r-1,q)$ have algebraic dimension $n$. By Lemma 4.4.5 and the fact that $\mathrm{PO}^-(2r,q)$ is transitive on totally singular subspaces of fixed aglebraic dimension, we may assume that every maximal in the $\mathrm{PO}^-(2r-1,q)$-orbit meets $\mathrm{Q}^-(2r-1,q)$ in $N$. Let $\Sigma = N^\perp/N \cong \mathrm{H}(2(r-n)-1,q^2)$. Then $M/N$ is a maximal totally isotropic subspace of $\Sigma$ disjoint from $\mathrm{Q}^-(2(r-n)-1,q)$. By Lemma 4.4.6, each $\mathrm{PO}^-(2r-1,q)_N^\Sigma$-orbit on $M/N$ splits into two orbits under $\mathrm{PSO}^-(2r-1,q)_N^\Sigma$, and the result follows. □

**Theorem 4.4.8** *For $r > 2$, $q$ odd, there exists a hemisystem of* $\mathrm{H}(2r-1,q^2)$ *admitting* $\mathrm{PSO}^-(2r,q)$.

**Proof** This follows from Lemma 4.4.1, Lemma 4.4.2, and Lemma 4.4.7. □

We remark that we have completely solved the problem of the existence of hemisystems in hermitian spaces first raised by Segre in 1965.

# Index

# References


[1] *L'oeuvre mathématique de G. Desargues. Textes publiés et commentés avec une introduction biographique et historique par René Taton.* Presses Universitaires de France, Paris, 1951.

[2] *The geometry of René Descartes. (With a facsimile of the first edition, 1637.).* Dover Publications Inc., New York, N. Y., 1954. Translated by David Eugene Smith and Marcia L. Latham.

[3] J. André. Über nicht-Desarguessche Ebenen mit transitiver Translationsgruppe. *Math. Z.*, 60:156–186, 1954.

[4] M. Aschbacher. On the maximal subgroups of the finite classical groups. *Invent. Math.*, 76(3):469–514, 1984.

[5] L. Bader. Some new examples of flocks of $Q^+(3, q)$. *Geom. Dedicata*, 27(2):213–218, 1988.

[6] L. Bader and G. Lunardon. On the flocks of $Q^+(3, q)$. *Geom. Dedicata*, 29(2):177–183, 1989.

[7] R. Baer. Homogeneity of projective planes. *Amer. J. Math.*, 64:137–152, 1942.

[8] R. Baer. Polarities in finite projective planes. *Bull. Amer. Math. Soc.*, 52:77–93, 1946.

[9] R. D. Baker and G. L. Ebert. A nonlinear flock in the Minkowski plane of order 11. *Congr. Numer.*, 58:75–81, 1987. Eighteenth Southeastern International Conference on Combinatorics, Graph Theory, and Computing (Boca Raton, Fla., 1987).

[10] J. Bamberg, F. De Clerck, and N. Durante. A hemisystem of a nonclassical generalised quadrangle. *Des. Codes Cryptogr.*, 51(2):157–165, 2009.

[11] J. Bamberg, M. Giudici, and G. F. Royle. Every flock generalized quadrangle has a hemisystem. *Bull. Lond. Math. Soc.*, 42(5):795–810, 2010.

[12] J. Bamberg and T. Penttila. Transitive eggs. *Innov. Incidence Geom.*, 4:1–12, 2006.

[13] A. Barlotti. Un'estensione del teorema di Segre-Kustaanheimo. *Boll. Un. Mat. Ital. (3)*, 10:498–506, 1955.

[14] L. M. Batten and J. M. Dover. Some sets of type $(m, n)$ in cubic order planes. *Des. Codes Cryptogr.*, 16(3):211–213, 1999.

[15] L. Bayens, W. Cherowitzo, and T. Penttila. Groups of hyperovals in Desarguesian planes. *Innov. Incidence Geom.*, 6/7:37–51, 2007/08.

[16] C. T. Benson. On the structure of generalized quadrangles. *J. Algebra*, 15:443–454, 1970.

[17] D. Betten. 4-dimensionale Translationsebenen mit 8-dimensionaler Kollineationsgruppe. *Geometriae Dedicata*, 2:327–339, 1973.

[18] A. Beutelspacher. Blocking sets and partial spreads in finite projective spaces. *Geom. Dedicata*, 9(4):425–449, 1980.

[19] M. Biliotti and G. Korchmáros. Hyperovals with a transitive collineation group. *Geom. Dedicata*, 24(3):269–281, 1987.

[20] G. Birkhoff and J. von Neumann. The logic of quantum mechanics. *Ann. of Math. (2)*, 37(4):823–843, 1936.

[21] A. Bonisoli. On the sharply 1-transitive subsets of $\mathrm{PGL}(2, p^m)$. *J. Geom.*, 31(1-2):32–41, 1988.

[22] A. Bonisoli and G. Korchmáros. Irreducible collineation groups fixing a hyperoval. *J. Algebra*, 252(2):431–448, 2002.

[23] R. C. Bose. Mathematical theory of the symmetrical factorial design. *Sankhyā*, 8:107–166, 1947.

[24] R. C. Bose. Strongly regular graphs, partial geometries and partially balanced designs. *Pacific J. Math.*, 13:389–419, 1963.

[25] R. C. Bose and T. Shimamoto. Classification and analysis of partially balanced incomplete block designs with two associate classes. *J. Amer. Statist. Assoc.*, 47:151–184, 1952.

[26] A. E. Brouwer, A. M. Cohen, and A. Neumaier. *Distance-regular graphs*, volume 18 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1989.

[27] M. R. Brown. Ovoids of $\mathrm{PG}(3, q), q$ even, with a conic section. *J. London Math. Soc. (2)*, 62(2):569–582, 2000.

[28] M. R. Brown, C. M. O'Keefe, S. E. Payne, T. Penttila, and G. F. Royle. The classification of spreads of $T_2(\mathscr{O})$ and $\alpha$-flocks over small fields. *Innov. Incidence Geom.*, 6/7:111–126, 2007/08.

[29] R. H. Bruck. Finite nets. II. Uniqueness and imbedding. *Pacific J. Math.*, 13:421–457, 1963.

[30] R. H. Bruck and R. C. Bose. The construction of translation planes from projective spaces. *J. Algebra*, 1:85–102, 1964.

[31] A. Bruen. Spreads and a conjecture of Bruck and Bose. *J. Algebra*, 23:519–537, 1972.

[32] A. Bruen. Subregular spreads and indicator sets. *Canad. J. Math.*, 27(5):1141–1148 (1976), 1975.

[33] A. A. Bruen and J. W. P. Hirschfeld. Applications of line geometry over finite fields. II. The Hermitian surface. *Geom. Dedicata*, 7(3):333–353, 1978.

[34] F. Buekenhout. Existence of unitals in finite translation planes of order $q^2$ with a kernel of order $q$. *Geometriae Dedicata*, 5(2):189–194, 1976.

[35] F. Buekenhout, A. Delandtsheer, J. Doyen, P. B. Kleidman, M. W. Liebeck, and J. Saxl. Linear spaces with flag-transitive automorphism groups. *Geom. Dedicata*, 36(1):89–94, 1990.

[36] F. Buekenhout and E. Shult. On the foundations of polar geometry. *Geometriae Dedicata*, 3:155–170, 1974.

[37] R. Calderbank and W. M. Kantor. The geometry of two-weight codes. *Bull. London Math. Soc.*, 18(2):97–122, 1986.

[38] P. J. Cameron. Partial quadrangles. *Quart. J. Math. Oxford Ser. (2)*, 26:61–73, 1975.

[39] P. J. Cameron, P. Delsarte, and J.-M. Goethals. Hemisystems, orthogonal configurations, and dissipative conference matrices. *Philips J. Res.*, 34(3-4):147–162, 1979.

[40] P. J. Cameron, J.-M. Goethals, and J. J. Seidel. Strongly regular graphs having strongly regular subconstituents. *J. Algebra*, 55(2):257–280, 1978.

[41] L. R. A. Casse and C. M. O'Keefe. Indicator sets for $t$-spreads of $\mathrm{PG}((s+1)(t+1)-1,\ q)$. *Boll. Un. Mat. Ital. B (7)*, 4(1):13–33, 1990.

[42] Y. Chen and G. Kaerlein. Eine Bemerkung über endliche Laguerre- und Minkowski-Ebenen. *Geometriae Dedicata*, 2:193–194, 1973.

[43] W. Cherowitzo. $\alpha$-flocks and hyperovals. *Geom. Dedicata*, 72(3):221–246, 1998.

[44] W. Cherowitzo, T. Penttila, I. Pinneri, and G. F. Royle. Flocks and ovals. *Geom. Dedicata*, 60(1):17–37, 1996.

[45] W. E. Cherowitzo, C. M. O'Keefe, and T. Penttila. A unified construction of finite geometries associated with $q$-clans in characteristic 2. *Adv. Geom.*, 3(1):1–21, 2003.

[46] W. E. Cherowitzo and L. Storme. $\alpha$-flocks with oval herds and monomial hyperovals. *Finite Fields Appl.*, 4(2):185–199, 1998.

[47] A. Cossidente and O. H. King. Maximal orthogonal subgroups of finite unitary groups. *J. Group Theory*, 7(4):447–462, 2004.

[48] A. Cossidente and O. H. King. Maximal subgroups of finite orthogonal groups stabilizing spreads of lines. *Comm. Algebra*, 34(12):4291–4309, 2006.

[49] A. Cossidente and T. Penttila. Hemisystems on the Hermitian surface. *J. London Math. Soc. (2)*, 72(3):731–741, 2005.

[50] A. Cossidente and T. Penttila. On $m$-regular systems on $\mathscr{H}(5, q^2)$. *J. Algebraic Combin.*, 29(4):437–445, 2009.

[51] H. S. M. Coxeter. Twelve points in PG(5, 3) with 95040 self-transformations. *Proc. Roy. Soc. London. Ser. A*, 247:279–293, 1958.

[52] H. De Clerck, F.and Van Maldeghem. Some classes of rank 2 geometries. In *Handbook of incidence geometry*, pages 433–475. North-Holland, Amsterdam, 1995.

[53] I. Debroey and J. A. Thas. On semipartial geometries. *J. Combin. Theory Ser. A*, 25(3):242–250, 1978.

[54] P. Dembowski. Möbiusebenen gerader Ordnung. *Math. Ann.*, 157:179–205, 1964.

[55] P. Dembowski. *Finite geometries*. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44. Springer-Verlag, Berlin, 1968.

[56] R. H. F. Denniston. Some maximal arcs in finite projective planes. *J. Combinatorial Theory*, 6:317–319, 1969.

[57] L. E. Dickson. On finite algebras. *Nachr. Ges. Wiss. Göttingen*, pages 358–393, 1905.

[58] L. E. Dickson. *Linear groups: With an exposition of the Galois field theory*. with an introduction by W. Magnus. Dover Publications Inc., New York, 1958.

[59] J. D. Dixon and B. Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

[60] M. M. Eich and S. E. Payne. Nonisomorphic symmetric block designs derived from generalized quadrangles. *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8)*, 52:893–902 (1973), 1972.

[61] Euclid. *Euclid's Elements*. Green Lion Press, Santa Fe, NM, 2002. All thirteen books complete in one volume, The Thomas L. Heath translation, Edited by Dana Densmore.

[62] W. Feit and G. Higman. The nonexistence of certain generalized polygons. *J. Algebra*, 1:114–131, 1964.

[63] W. Feit and J. G. Thompson. Solvability of groups of odd order. *Pacific J. Math.*, 13:775–1029, 1963.

[64] J. C. Fisher and J. A. Thas. Flocks in PG(3, $q$). *Math. Z.*, 169(1):1–11, 1979.

[65] M. J. Ganley. Central weak nucleus semifields. *European J. Combin.*, 2(4):339–347, 1981.

[66] H. Gevaert and N. L. Johnson. Flocks of quadratic cones, generalized quadrangles and translation planes. *Geom. Dedicata*, 27(3):301–317, 1988.

[67] D. G. Glynn. Two new sequences of ovals in finite Desarguesian planes of even order. In *Combinatorial mathematics, X (Adelaide, 1982)*, volume 1036 of *Lecture Notes in Math.*, pages 217–229. Springer, Berlin, 1983.

[68] D. G. Glynn. The Hering classification for inversive planes of even order. *Simon Stevin*, 58(4):319–353, 1984.

[69] D. G. Glynn. A condition for the existence of ovals in $\mathrm{PG}(2, q), q$ even. *Geom. Dedicata*, 32(2):247–252, 1989.

[70] J.-M. Goethals and J. J. Seidel. Quasisymmetric block designs. In *Combinatorial Structures and their Applications (Proc. Calgary Internat. Conf., Calgary, Alta., 1969)*, pages 111–116. Gordon and Breach, New York, 1970.

[71] K. Grüning. A class of unitals of order $q$ which can be embedded in two different planes of order $q^2$. *J. Geom.*, 29(1):61–77, 1987.

[72] M. Hall, Jr. Affine generalized quadrilaterals. In *Studies in Pure Mathematics (Presented to Richard Rado)*, pages 113–116. Academic Press, London, 1971.

[73] N. Hamilton. Some inherited maximal arcs in derived dual translation planes. *Geom. Dedicata*, 55(2):165–173, 1995.

[74] N. Hamilton and R. Mathon. More maximal arcs in Desarguesian projective planes and their geometric structure. *Adv. Geom.*, 3(3):251–261, 2003.

[75] R. W. Hartley. Determination of the ternary collineation groups whose coefficients lie in the $\mathrm{GF}(2^n)$. *Ann. of Math. (2)*, 27(2):140–158, 1925.

[76] W. Heise. Minkowski-Ebenen gerader Ordnung. *J. Geometry*, 5:83, 1974.

[77] C. Hering. Transitive linear groups and linear groups which contain irreducible subgroups of prime order. *Geometriae Dedicata*, 2:425–460, 1974.

[78] C. Hering. Transitive linear groups and linear groups which contain irreducible subgroups of prime order. II. *J. Algebra*, 93(1):151–164, 1985.

[79] D. G. Higman. Invariant relations, coherent configurations and generalized polygons. In *Combinatorics (Proc. Advanced Study Inst., Breukelen, 1974), Part 3: Combinatorial group theory*, pages 27–43. Math. Centre Tracts, No. 57. Math. Centrum, Amsterdam, 1974.

[80] D. Hilbert. *Grundlagen der Geometrie*, volume 6 of *Teubner-Archiv zur Mathematik. Supplement [Teubner Archive on Mathematics. Supplement]*. B. G. Teubner Verlagsgesellschaft mbH, Stuttgart, fourteenth edition, 1999. With supplementary material by Paul Bernays, With contributions by Michael Toepell, Hubert Kiechle, Alexander Kreuzer and Heinrich Wefelscheid, Edited and with appendices by Toepell.

[81] R. Hill. Caps and groups. In *Colloquio Internazionale sulle Teorie Combinatorie (Rome, 1973), Tomo II*, pages 389–394. Atti dei Convegni Lincei, No. 17. Accad. Naz. Lincei, Rome, 1976.

[82] J. W. P. Hirschfeld. Ovals in desarguesian planes of even order. *Ann. Mat. Pura Appl. (4)*, 102:79–89, 1975.

[83] J. W. P. Hirschfeld. *Finite projective spaces of three dimensions*. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, 1985. Oxford Science Publications.

[84] X. L. Hubaut. Strongly regular graphs. *Discrete Math.*, 13(4):357–381, 1975.

[85] D. R. Hughes. Generalized incidence matrices over group algebras. *Illinois J. Math.*, 1:545–551, 1957.

[86] G. Järnefelt and P. Kustaanheimo. An observation on finite geometries. In *Den 11te Skandinaviske Matematikerkongress, Trondheim, 1949*, pages 166–182. Johan Grundt Tanums Forlag, Oslo, 1952.

[87] N. L. Johnson. Semifield flocks of quadratic cones. *Simon Stevin*, 61(3-4):313–326, 1987.

[88] N. L. Johnson. Translation planes admitting Baer groups and partial flocks of quadric sets. *Simon Stevin*, 63(2):167–188, 1989.

[89] J. Kahn. Locally projective-planar lattices which satisfy the bundle theorem. *Math. Z.*, 175(3):219–247, 1980.

[90] W. M. Kantor. Generalized quadrangles associated with $G_2(q)$. *J. Combin. Theory Ser. A*, 29(2):212–219, 1980.

[91] W. M. Kantor. Ovoids and translation planes. *Canad. J. Math.*, 34(5):1195–1207, 1982.

[92] W. M. Kantor. Some generalized quadrangles with parameters $q^2$, $q$. *Math. Z.*, 192(1):45–50, 1986.

[93] W. M. Kantor. 2-transitive and flag-transitive designs. In *Coding theory, design theory, group theory (Burlington, VT, 1990)*, Wiley-Intersci. Publ., pages 13–30. Wiley, New York, 1993.

[94] P. Kleidman and M. Liebeck. *The subgroup structure of the finite classical groups*, volume 129 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1990.

[95] F. Klein. Vergleichende Betrachtungen über neuere geometrische Forschungen. *Math. Ann.*, 43(1):63–100, 1893.

[96] N. Knarr. A geometric characterization of elation Laguerre planes. *Arch. Math. (Basel)*, 78(2):162–165, 2002.

[97] M. Law and T. Penttila. Some flocks in characteristic 3. *J. Combin. Theory Ser. A*, 94(2):387–392, 2001.

[98] M. Law and T. Penttila. Classification of flocks of the quadratic cone over fields of order at most 29. *Adv. Geom.*, (suppl.):S232–S244, 2003. Special issue dedicated to Adriano Barlotti.

[99] R. Löwen. Topological pseudo-ovals, elation Laguerre planes, and elation generalized quadrangles. *Math. Z.*, 216(3):347–369, 1994.

[100] G. Lunardon. Flocks, ovoids of $Q(4, q)$ and designs. *Geom. Dedicata*, 66(2):163–173, 1997.

[101] G. Lunardon. Normal spreads. *Geom. Dedicata*, 75(3):245–261, 1999.

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

[103] W. J. Martin, M. Muzychuk, and J. Williford. Imprimitive cometric association schemes: constructions and analysis. *J. Algebraic Combin.*, 25(4):399–415, 2007.

[104] R. Metz. On a class of unitals. *Geom. Dedicata*, 8(1):125–126, 1979.

[105] H. Mitchell. Determination of the ordinary and modular ternary linear groups. *Trans. Amer. Math. Soc.*, 12(2):207–242, 1911.

[106] E. H. Moore. The subgroups of the generalized finite modular group. In *The decennial publications of the University of Chicago*, pages 141–190. University of Chicago Press, 1903.

[107] Pappus of Alexandria. *Book 7 of the Collection*, volume 8 of *Sources in the History of Mathematics and Physical Sciences*. Springer-Verlag, New York, 1986. Part 1. Introduction, text, and translation, Part 2. Commentary, index, and figures, Edited and with translation and commentary by Alexander Jones.

[108] C. M. O'Keefe and T. Penttila. Polynomials for hyperovals of Desarguesian planes. *J. Austral. Math. Soc. Ser. A*, 51(3):436–447, 1991.

[109] C. M. O'Keefe and T. Penttila. A new hyperoval in $PG(2, 32)$. *J. Geom.*, 44(1-2):117–139, 1992.

[110] C. M. O'Keefe and T. Penttila. Symmetries of arcs. *J. Combin. Theory Ser. A*, 66(1):53–67, 1994.

[111] C. M. O'Keefe and T. Penttila. Automorphism groups of generalized quadrangles via an unusual action of $P\Gamma L(2, 2^h)$. *European J. Combin.*, 23(2):213–232, 2002.

[112] C. M. O'Keefe and J. A. Thas. Collineations of Subiaco and Cherowitzo hyperovals. *Bull. Belg. Math. Soc. Simon Stevin*, 3(2):177–192, 1996.

[113] W. F. Orr. *The Miquelian inversive-plane IP(q) and the associative projective-planes.* ProQuest LLC, Ann Arbor, MI, 1973. Thesis (Ph.D.)–The University of Wisconsin - Madison.

[114] G. Panella. Caratterizzazione delle quadriche di uno spazio (tridimensionale) lineare sopra un corpo finito. *Boll. Un. Mat. Ital. (3)*, 10:507–513, 1955.

[115] S. E. Payne. A complete determination of translation ovoids in finite Desarguian planes. *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8)*, 51:328–331 (1972), 1971.

[116] S. E. Payne. Nonisomorphic generalized quadrangles. *J. Algebra*, 18:201–212, 1971.

[117] S. E. Payne. A garden of generalized quadrangles. In *Proceedings of the conference on groups and geometry, Part A (Madison, Wis., 1985)*, volume 2, pages 323–354, 1985.

[118] S. E. Payne. A new infinite family of generalized quadrangles. In *Proceedings of the sixteenth Southeastern international conference on combinatorics, graph theory and computing (Boca Raton, Fla., 1985)*, volume 49, pages 115–128, 1985.

[119] S. E. Payne. An essay on skew translation generalized quadrangles. *Geom. Dedicata*, 32(1):93–118, 1989.

[120] S. E. Payne, T. Penttila, and I. Pinneri. Isomorphisms between Subiaco $q$-clan geometries. *Bull. Belg. Math. Soc. Simon Stevin*, 2(2):197–222, 1995.

[121] S. E. Payne and J. A. Thas. *Finite generalized quadrangles*, volume 110 of *Research Notes in Mathematics*. Pitman (Advanced Publishing Program), Boston, MA, 1984.

[122] S. E. Payne and J. A. Thas. The stabilizer of the Adelaide oval. *Discrete Math.*, 294(1-2):161–173, 2005.

[123] Giuseppe Pellegrino. Su una interpretazione geometrica dei gruppi $M_{11}$ ed $M_{12}$ di Mathieu e su alcuni $t-(v, k, \lambda)$-disegni-deducibili da una $(12)^4_{5,3}$ calotta completa. *Atti Sem. Mat. Fis. Univ. Modena*, 23(1):103–117 (1975), 1974.

[124] T. Penttila. Flocks of circle planes. In *Surveys in combinatorics 2005*, volume 327 of *London Math. Soc. Lecture Note Ser.*, pages 83–93. Cambridge Univ. Press, Cambridge, 2005.

[125] T. Penttila and I. Pinneri. Irregular hyperovals in $\mathrm{PG}(2, 64)$. *J. Geom.*, 51(1-2):89–100, 1994.

[126] T. Penttila and I. Pinneri. Hyperovals. *Australas. J. Combin.*, 19:101–114, 1999.

[127] T. Penttila and G. F. Royle. On hyperovals in small projective planes. *J. Geom.*, 54(1-2):91–104, 1995.

[128] T. Penttila and G. F. Royle. Sets of type $(m, n)$ in the affine and projective planes of order nine. *Des. Codes Cryptogr.*, 6(3):229–245, 1995.

[129] M. Percsy. A characterization of classical Minkowski planes over a perfect field of characteristic two. *J. Geometry*, 5:191–204, 1974.

[130] B. Qvist. Some remarks concerning curves of the second degree in a finite plane. *Ann. Acad. Sci. Fennicae. Ser. A. I. Math.-Phys.*, 1952(134):27, 1952.

[131] M. Sce. Preliminari ad una teoria aritmetico-gruppale dei $k$-archi. *Rend. Mat. e Appl. (5)*, 19:241–291, 1960.

[132] A. E. Schroth. Flat weakly Miquelian Laguerre planes are ovoidal. *Abh. Math. Sem. Univ. Hamburg*, 69:211–227, 1999.

[133] A. E. Schroth. Ovoidal Laguerre planes are weakly Miquelian. *Arch. Math. (Basel)*, 72(1):77–80, 1999.

[134] B. Segre. Ovals in a finite projective plane. *Canad. J. Math.*, 7:414–416, 1955.

[135] B. Segre. Sui $k$-archi nei piani finiti di caratteristica due. *Rev. Math. Pures Appl.*, 2:289–300, 1957.

[136] B. Segre. Ovali e curve $\sigma$ nei piani di Galois di caratteristica due. *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat. (8)*, 32:785–790, 1962.

[137] B. Segre. Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane. *Ann. Mat. Pura Appl. (4)*, 64:1–76, 1964.

[138] B. Segre. Forme e geometrie hermitiane, con particolare riguardo al caso finito. *Ann. Mat. Pura Appl. (4)*, 70:1–201, 1965.

[139] B. Segre. *Istituzioni di geometria superiore. Vol. III: Complessi, reti, disegni.* Lezioni raccolte da Pier Vittorio Ceccherini. Universitâ degli Studi, Roma. Anno accademico 1963–64. Istituto Matematico "Guido Castelnuovo", Rome, 1965.

[140] B. Segre and U. Bartocci. Ovali ed altre curve nei piani di Galois di caratteristica due. *Acta Arith.*, 18:423–449, 1971.

[141] M. Seib. Unitäre Polaritäten endlicher projektiver Ebenen. *Arch. Math. (Basel)*, 21:103–112, 1970.

[142] G. F. Steinke. On the structure of finite elation Laguerre planes. *J. Geom.*, 41(1-2):162–179, 1991.

[143] G. F. Steinke. Topological circle geometries. In *Handbook of incidence geometry*, pages 1325–1354. North-Holland, Amsterdam, 1995.

[144] M. Sved. Baer subspaces in the $n$-dimensional projective space. In *Combinatorial mathematics, X (Adelaide, 1982)*, volume 1036 of *Lecture Notes in Math.*, pages 375–391. Springer, Berlin, 1983.

[145] M. Tallini Scafati. $\{k, n\}$-archi di un piano grafico finito, con particolare riguardo a quelli con due caratteri. II. *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8)*, 40:1020–1025, 1966.

[146] J. A. Thas. The $m$-dimensional projective space $S_m(M_n(\mathrm{GF}(q)))$ over the total matrix algebra $M_n(\mathrm{GF}(q))$ of the $n \times n$-matrices with elements in the Galois field $\mathrm{GF}(q)$. *Rend. Mat. (6)*, 4:459–532, 1971.

[147] J. A. Thas. Flocks of finite egglike inversive planes. In *Finite geometric structures and their applications (C.I.M.E., II Ciclo, Bressanone, 1972)*, pages 189–191. Edizioni Cremonese, Rome, 1973.

[148] J. A. Thas. Construction of maximal arcs and partial geometries. *Geometriae Dedicata*, 3:61–64, 1974.

[149] J. A. Thas. Flocks of non-singular ruled quadrics in $\mathrm{PG}(3, q)$. *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8)*, 59(1-2):83–85 (1976), 1975.

[150] J. A. Thas. Construction of maximal arcs and dual ovals in translation planes. *European J. Combin.*, 1(2):189–192, 1980.

[151] J. A. Thas. Generalized quadrangles and flocks of cones. *European J. Combin.*, 8(4):441–452, 1987.

[152] J. A. Thas. Flocks, maximal exterior sets, and inversive planes. In *Finite geometries and combinatorial designs (Lincoln, NE, 1987)*, volume 111 of *Contemp. Math.*, pages 187–218. Amer. Math. Soc., Providence, RI, 1990.

[153] J. A. Thas. Solution of a classical problem on finite inversive planes. In *Finite geometries, buildings, and related topics (Pingree Park, CO, 1988)*, Oxford Sci. Publ., pages 145–159. Oxford Univ. Press, New York, 1990.

[154] J. A. Thas. Projective geometry over a finite field. In *Handbook of incidence geometry*, pages 295–347. North-Holland, Amsterdam, 1995.

[155] J. A. Thas. Symplectic spreads in $\mathrm{PG}(3, q)$, inversive planes and projective planes. *Discrete Math.*, 174(1-3):329–336, 1997. Combinatorics (Rome and Montesilvano, 1994).

[156] J. A. Thas. Finite geometries: classical problems and recent developments. *Rend. Mat. Appl. (7)*, 27(1):49–60, 2007.

[157] J. A. Thas, C. Herssens, and F. De Clerck. Flocks and partial flocks of the quadratic cone in $\mathrm{PG}(3, q)$. In *Finite geometry and combinatorics (Deinze, 1992)*, volume 191 of *London Math. Soc. Lecture Note Ser.*, pages 379–393. Cambridge Univ. Press, Cambridge, 1993.

[158] J. A. Thas and S. E. Payne. Moufang conditions for finite generalized quadrangles. In *Combinatorics '81 (Rome, 1981)*, volume 78 of *North-Holland Math. Stud.*, pages 745–751. North-Holland, Amsterdam, 1983.

[159] J. A. Thas, S. E. Payne, and H. Gevaert. A family of ovals with few collineations. *European J. Combin.*, 9(4):353–362, 1988.

[160] J. A. Thas, K. Thas, and H. Van Maldeghem. *Translation generalized quadrangles*, volume 26 of *Series in Pure Mathematics*. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2006.

[161] K. Thas. The classification of generalized quadrangles with two translation points. *Beiträge Algebra Geom.*, 43(2):365–398, 2002.

[162] J. Tits. Sur certaines classes d'espaces homogènes de groupes de Lie. *Acad. Roy. Belg. Cl. Sci. Mém. Coll. in* 8°, 29(3):268, 1955.

[163] J. Tits. Les groupes de Lie exceptionnels et leur interprétation géométrique. *Bull. Soc. Math. Belg.*, 8:48–81, 1956.

[164] J. Tits. Sur la trialité et certains groupes qui s'en déduisent. *Inst. Hautes Études Sci. Publ. Math.*, (2):13–60, 1959.

[165] J. Tits. Ovoïdes et groupes de Suzuki. *Arch. Math.*, 13:187–198, 1962.

[166] J. Tits. *Buildings of spherical type and finite BN-pairs*. Lecture Notes in Mathematics, Vol. 386. Springer-Verlag, Berlin, 1974.

[167] N. Tzanakis and J. Wolfskill. The Diophantine equation $x^2 = 4q^{a/2} + 4q + 1$, with an application to coding theory. *J. Number Theory*, 26(1):96–116, 1987.

[168] E. R. van Dam, W. J. Martin, and M. E. Muzychuk. Uniformity in association schemes and coherent configurations: cometric $Q$-antipodal schemes and linked systems. 2010.

[169] B. L. van der Waerden and L. J. Smid. Eine Axiomatik der Kreisgeometrie und der Laguerregeometrie. *Math. Ann.*, 110(1):753–776, 1935.

[170] H. van Maldeghem. *Generalized polygons*, volume 93 of *Monographs in Mathematics*. Birkhäuser Verlag, Basel, 1998.

[171] O. Veblen and J. W. Young. A Set of Assumptions for Projective Geometry. *Amer. J. Math.*, 30(4):347–380, 1908.

[172] O. Veblen and J. W. Young. *Projective geometry. Vol. 1.* Blaisdell Publishing Co. Ginn and Co. New York-Toronto-London, 1965.

[173] O. Veblen and J. W. Young. *Projective geometry. Vol. 2 (by Oswald Veblen)*. Blaisdell Publishing Co. Ginn and Co. New York-Toronto-London, 1965.

[174] F. D. Veldkamp. Polar geometry. I, II, III, IV, V. *Nederl. Akad. Wetensch. Proc. Ser. A 62; 63 = Indag. Math. 21 (1959), 512-551*, 22:207–212, 1959.

[175] F. D. Veldkamp. An axiomatic treatment of polar geometry. In *Algebraical and Topological Foundations of Geometry (Proc. Colloq., Utrecht, 1959)*, pages 193–198. Pergamon, Oxford, 1962.

[176] T. L. Vis. *Monomial hyperovals in Desarguesian planes*. ProQuest LLC, Ann Arbor, MI, 2010. Thesis (Ph.D.)–University of Colorado at Denver.

[177] M. Walker. A class of translation planes. *Geometriae Dedicata*, 5(2):135–146, 1976.

[178] W. D. Wallis. Configurations arising from maximal arcs. *J. Combinatorial Theory Ser. A*, 15:115–119, 1973.

[179] J. H. Wedderburn. A theorem on finite algebras. *Trans. Amer. Math. Soc.*, 6(3):349–352, 1905.

[180] A. Wiman. *Bestimmung aller Untergruppen einer doppelt unendlichen Reihe von einfachen Gruppen*. K. Svenska Vetenskaps-Akademiens Handlingar. Bihang.

[181] E. Witt. Theorie der quadratischen Formen in beliebigen Körpern. *J. reine angew. Math.*, 176:31–44, 1936.