Symplectic translation planes, pseudo-ovals, and maximal 4-arcs

Sylvia Morris
Bachelor of Mathematical & Computer Sciences (Honours)
University of Adelaide

This thesis is presented for the degree of
Master of Philosophy (Research) of
The University of Western Australia

Mathematics and Statistics

August, 2013

Summary

This thesis is comprised of the study of three distinct problems: the construction of symplectic translation planes, the characterisation of pseudo-ovals, and the classification of maximal arcs.

Non-Desarguesian planes are the only finite projective spaces not to be governed by a finite field and, as such, hold a certain interest for finite geometers. In the '50s and '60s, André, Bruck and Bose, and Segre developed a method — now commonly referred to as the *André/Bruck-Bose construction* — to create translation planes, a subset of projective planes that includes many non-Desarguesian planes, from spreads of higher dimensional projective spaces. In Chapter 4, we outline previous computational work in this area, the linear programming methods we have used, and present eight new examples of translation planes. These examples correspond to spreads of $W(5,5)$ and $W(5,7)$. Appendix A contains the details required to reconstruct each of these spreads.

Examples of pseudo-ovals can be constructed from ovals, using field reduction, and the existence of other types of pseudo-oval is unknown. Pseudo-ovals are represented, via geometric passages, as ovals in translation planes, as elements of translation generalised quadrangles, and, in some cases, as special sets in the Hermitian space $H(3,q^2)$. In Chapter 5 we go through relevant theorems in each situation and summarise the current status of the problem.

The Mathon maximal arcs, generalised from the Denniston maximal arcs, are each formed by taking a union of regular hyperovals on a common nucleus. In Chapter 6 we prove that all maximal 4-arcs, in the Desarguesian plane $PG(2,q)$, that are a union of regular hyperovals or that contain two conics that share exactly one point, are Mathon maximal 4-arcs. This is joint work with Nicola Durante from the Universitá degli Studi di Napoli Federico II.

Background information on projective spaces and polar spaces is contained in Chapter 2. Chapter 3 describes, in more detail, the geometric passages between spaces that will be most useful for the remainder of the thesis and is, in particular, a prelude to Chapter 4. Chapters 4, 5 and 6 can be read independently of each other.

Acknowledgements

From beginning to end, this thesis has only come about as a result of the help, advice and ideas of my supervisors, John Bamberg and Michael Giudici. John, thanks for your boundless enthusiasm and faith. Michael, thanks for keeping us on track and providing an often needed sense of perspective. Thanks to you both for your patience and numerous explanations.

I would also like to thank the rest of the CMSC research group at UWA for fascinating seminars and fun soccer games. In particular, I want to thank Cheryl Praegar for her encouragement in my decision to come to Perth. My fellow students: thanks for making me laugh, encouraging me when things were difficult, and taking time out to sit and talk.

I am very grateful to Nicola Durante for allowing me to visit him in Ischia. The trip is one of the highlights of the past two years. Thank you for teaching me a lot about research and thanks to Emilia for teaching me a lot about Italy.

To the friends I made at conferences: thanks for all the adventures. I will forever enjoy referring to each of you as "my friend from the conference in X, who lives in Y, and comes from Z."

Dear friends and family back in Adelaide: thank you for sending presents, letters, emails, and sometimes yourselves, all the way over to Perth. Especial thanks to my parents for solving emergencies from 2,600km away and for inspiring me to care about maths in the first place.

The most thanks of all must go to Peter, for keeping me sane.

Contents

Chapter 1

Introduction

1.1 Symplectic translation planes

Hessenberg and Vahlen separately proved, in the early 1900s [50, 85], that all finite projective spaces of dimension three or higher, are Desarguesian. It was already known that this could not extend to projective planes — MacLagan-Wedderburn and Young had constructed a non-Desarguesian plane in 1907 [86] — and the construction of non-Desarguesian planes became a major theme of finite projective geometry.

In 1954, André [6] published a paper that gave a group theoretic construction of a large class of projective planes, called translation planes, from spreads of higher dimensional spaces and proved that all translation planes could be constructed using this method. In 1964, Segre [75] built on the work of André to create these translation planes geometrically. Independently, and also in 1964, Bruck and Bose [22] came to the same results as Segre. This construction is now called the *André/Bruck-Bose construction.*

A spread of a $(2e-1)$-dimensional projective space $\mathrm{PG}(2e-1,q)$ is a set of $(e-1)$-spaces that partitions the points of $\mathrm{PG}(2e-1,q)$. The André/Bruck-Bose construction of a translation plane of order q^e uses a spread of $\Sigma' = \mathrm{PG}(2e-1,q)$, such that Σ' is embedded as a hyperplane in a $2e$-dimensional projective space $\Sigma = \mathrm{PG}(2e,q)$. The translation plane has as its points the set $\mathcal{P}$, and the set $\mathcal{L}$ as its lines, defined below. The elements of $\mathcal{P}$ are

- the elements of the spread, and
- the points of $\Sigma \setminus \Sigma'$,

and the elements of $\mathcal{L}$ are

- the planes of Σ that meet Σ' exactly in an element of the spread, and
- the $(2e-1)$-space Σ' itself.

Thus, the classification of translation planes of a certain order is equivalent to the classification of all spreads that satisfy certain parameters. Computational methods for classifying planes were not new when Bruck and Bose published their paper — Hall, Swift and Walker relied on computation to determine, in 1959 [45], that all projective planes of order eight are isomorphic to PG$(2, 8)$ — but their paper introduced a way of describing spreads that would prove to be useful for computation in the future. Dempwolff began using computation to classify spreads of projective spaces in 1982 [36] and he, along with many others, has used computation to aid in the construction of infinite families of translation planes. Translation planes of order q are classified for $q \leq 49$ [31, 68]. In 2002, Kantor showed that there exists a correspondence between commutative semifield planes and symplectic semifield planes [58]. Later, in 2004, he wrote

" . . . it is surprising that there has not yet been an enumeration of all semifields of order at most 256 . . . " [59].

This correspondence has since been studied by Lunardon [63], providing fundamental results on the nuclei, and allowing for further investigation. We, however, broaden the problem and consider all symplectic planes. Symplectic planes of order q are classified for $q < 125$ (see Williams [90] and Ball, Govaerts and Storme [15]). Symplectic planes of order 125 correspond to symplectic spreads in PG$(5, 5)$ and we have contributed to this area by finding all symplectic spreads in PG$(5, 5)$ with non-trivial stabiliser in the isometry group of W$(5, 5)$. These results are contained in Table 1.1 and all the spreads that do not belong to a family are new.

Table 1.1 – Spreads of W$(5, 5)$.

Type	Stabiliser	Orbit lengths	#	Family
Field	$(\mathrm{PSL}(2, 125) : C_2) : C_3$	126	1	Desarguesian
Semi	$C_5^3 : (C_4 \times (C_{31} : C_3))$	$125 + 1$	1	Gen. twisted
Non-semi	$C_2 \times ((C_{31} : C_3) \rtimes C_2)$	$124 + 2$	1	Suetake
Non-semi	D_{14}	14^9	2	-
Non-semi	D_{30}	$30^4 + 6$	1	-
Non-semi	C_{10}	$10^{12} + 2^2 + 1^2$	1	-
Non-semi	D_{18}	18^7	1	-
Non-semi	A_4	$12^8 + 6 + 4^6$	1	-
Non-semi	C_6	$6^{20} + 2^2 + 1^2$	1	-

A normal $(e-1)$-spread of a projective space PG$(en-1, q)$ is a partition of the points of the space into $(e-1)$-spaces, such that the restriction of the $(e-1)$-spread to the space spanned by any two of its elements is a spread. While the André/Bruck-Bose construction uses a spread of PG$(2e-1, q)$ to create a translation plane of order q^e, there is also a way to create a projective space PG$(n-1, q^e)$ from the elements of a normal $(e-1)$-spread of PG$(en-1, q)$ due to Baer [10, 18]. This correspondence, when restricted to PG$(3e-1, q)$, is another way of representing the André/Bruck-Bose construction of Desarguesian planes. Field reduction goes the other way, taking the points of PG$(n-1, q^e)$ to a normal $(e-1)$-spread of PG$(en-1, q)$. Field reduction, the André/Bruck-Bose construction, and the Baer correspondence, transfer objects between different projective spaces and, as such, can reveal important information.

1.2 Pseudo-ovals

An oval is the combinatorial generalisation of an ellipse: a set of points such that no three lie on a line. The field reduction of an oval gives a set of $q^e + 1$ spaces of dimension $e-1$ in $\mathrm{PG}(3e-1, q)$ such that any three span the whole space, and all are contained within a normal $(e-1)$-spread. A set of q^e+1 $(e-1)$-spaces such that any three span $\mathrm{PG}(3e-1, q)$ is referred to as a *pseudo-oval*, and called *classical* if it is contained in a normal $(e-1)$-spread. The existence of non-classical pseudo-ovals is still unknown.

In 1984, Payne and Thas proved that the theory of pseudo-ovals is equivalent to that of translation generalised quadrangles [71]. Thus, if there exists a pseudo-oval that is not classical, it will create a new translation generalised quadrangle and, from that, a new Laguerre plane. A *finite generalised quadrangle* is a geometric structure of points and lines such that

- each point is incident with $t+1$ lines and two distinct points are incident with at most one line,
- each line is incident with $s+1$ lines and two distinct lines are incident with at most one point, and
- if X is a point, not on the line ℓ, then X is collinear with exactly one point on ℓ.

Translation generalised quadrangles are generalised quadrangles that obey certain symmetry properties. In 1985, Casse, Thas and Wild showed that, if a spread induced by a pseudo-oval in a $(2e-1)$-space is regular, then the pseudo-oval is classical [29]. In doing this, they construct a translation plane from the induced spread in which the pseudo-oval is represented by a pencil of ovals. We construct an $(e-1)$-spread arising from a pseudo-oval in $\mathrm{PG}(3e-1, q)$ and prove that a pseudo-oval is classical if and only if this spread is normal.

Shult in *"Problems by the Wayside"* [76], published in 2005, poses the question of the existence of non-classical special sets in the Hermitian polar space $\mathrm{H}(3, q^2)$. *Special sets* in $\mathrm{H}(3, q^2)$ are sets of q^2+1 points such that any three span a non-degenerate plane. Under the Klein correspondence, which takes lines of $\mathrm{PG}(3, q^2)$ to points of $\mathrm{Q}^+(5, q^2)$, a special set becomes a set of q^2+1 lines in $\mathrm{Q}^-(5, q)$. That is, it is a pseudo-oval contained in a quadric. If a pseudo-oval is created from a special set, that is, it's contained within a quadric, then the translation plane constructed by Casse, Thas and Wild contains a parabolic orthogonal-Buekenhout-Metz unital and this unital contains the oval induced by the pseudo-oval. If this translation plane is Desarguesian, then the pseudo-oval and special set are classical.

1.3 Maximal arcs

Maximal arcs were introduced by Barlotti in 1956 [17], and were studied as combinatorial extremal problems. In the early 70s, Thas [81] and Wallis [89] used maximal arcs to create partial geometries and, since then, they have been shown to have links with many other geometric objects.

A *maximal n-arc* is a non-empty set of points in $\mathrm{PG}(2,q)$ such that all lines contain zero or n points of the set. Thas [83] constructed maximal arcs using the André/Bruck-Bose construction applied to a symplectic spread in $\mathrm{PG}(2d-1,q)$. Given one point x, in $\mathrm{PG}(2d,q) \setminus \mathrm{PG}(2d-1,q)$, and an elliptic quadric $\mathrm{Q}^-(2d-1,q)$ in $\mathrm{PG}(2e-1,q)$, the points of the maximal arc are the points of $\mathrm{PG}(2d,q) \setminus \mathrm{PG}(2d-1,q)$ that lie on a line joining x to a point of the quadric.

In 1969, Denniston [38] used the structure of Galois fields to construct maximal n-arcs by taking unions of regular hyperovals. Mathon extended this construction to a much larger family in 2002 [67]. In the situation that Thas' symplectic spread is Desarguesian, the Denniston, Mathon and Thas maximal 4-arcs are all equivalent [83, 67]. The only known maximal 4-arcs in Desarguesian planes are the Denniston arcs, the dual arcs of hyperovals in $\mathrm{PG}(2,8)$, and the dual arcs of Mathon 2^k-arcs in $\mathrm{PG}(2,2^{k+2})$.

In 2008, Aguglia, Giuzzi and Korchmáros [3] used algebraic curves to put limitations on how maximal 4-arcs can be constructed from regular hyperovals. We follow the ideas in Aguglia, Giuzzi and Korchmáros' paper to extend their results. Nicola Durante and I determine all possible arrangements of regular hyperovals that could result in a maximal 4-arc, and determine which are infeasible.

Theorem 1.3.1. *There are no maximal* 4*-arcs that are a union of regular hyperovals, other than those of Mathon, in* $\mathrm{PG}(2,q)$.

Chapter 2

Preliminaries

This chapter forms a foundation for the remainder of the thesis and contains within it necessary background information relating to projective and polar spaces. Many results will be stated without proof. For more detail on this background material, and for proofs of these results, see *"Projective Planes"* by Hughes and Piper [55], *"Translation Planes"* by Lüneburg [65], *"Finite Geometries"* by Dembowski [34], or *"Projective Geometries over Finite Fields"* by Hirschfeld [52], for instance. This thesis deals solely with finite geometry and we will not specify the situations in which results generalise to infinite cases.

2.1 Projective planes

A *projective plane* is a set of points and lines such that

P1 Any two points span a unique line,

P2 Any two lines meet in a unique point,and

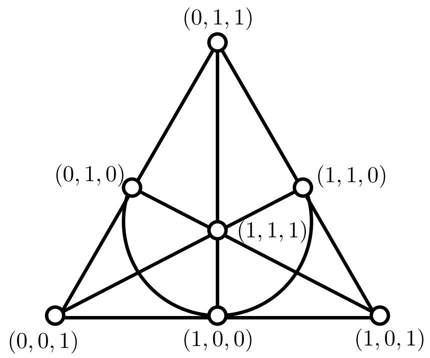
P3 There exist four points (a *quadrangle*) such that no line meets three of them.

We say that a point P is on a line ℓ, or that ℓ contains P if P, and ℓ are incident.

Given a point P and a line ℓ disjoint from P, we know that, for each point of ℓ, there exists a line containing P and that point. We also know that every line through P must meet ℓ in a point. As this is true for all pairs P and ℓ, there are the same number of lines through a point as there are points on a line. If this number is $q + 1$, we say a plane has *order* q.

Example 2.1.1. *The smallest projective plane is the* Fano plane*. It has seven points, seven lines and its order is two. We give* homogeneous *coordinates to the Fano plane using the field of two elements* GF(2)*, as shown in Figure 2.1.*

Figure 2.1 – PG(2, 2): The Fano plane.



In fact, we can use these homogeneous coordinates to create projective planes of all prime power orders. Let $\mathrm{GF}(q)$ denote the finite field of q elements, q a prime power, then the unique plane that is coordinatised by the field $\mathrm{GF}(q)$ is denoted $\mathrm{PG}(2, q)$.

A point in $\mathrm{PG}(2, q)$ will be described by its *homogeneous coordinates* (X_0, X_1, X_2), where $X_i \in \mathrm{GF}(q)$, not all zero. Each point (X_0, X_1, X_2) represents the set of vectors $\{\rho(X_0, X_1, X_2) \mid \rho \in \mathrm{GF}(q) \setminus \{0\}\}$, and thus the coordinates (X_0, X_1, X_2) and $\rho(X_0, X_1, X_2)$ describe the same point. There are two ways to describe lines. First, we can describe a line as the span $\lambda(a, b, c) + \mu(x, y, z)$ of any two distinct points (a, b, c) and (x, y, z) of the line. Alternatively, if ℓ is the line containing all points (X_0, X_1, X_2) such that

$$Y_0X_0 + Y_1X_1 + Y_2X_2 = 0,$$

for some Y_0, Y_1, Y_2 then we say $\ell = [Y_0, Y_1, Y_2]$. We will most often use the first notation and will make it clear when we are using the second. A set of points is called *collinear* if they lie on a common line, and a set of lines is *concurrent* if they contain a common point.

Let us now create a configuration, known as the *Desargues configuration*, in a projective plane π.

A plane is called *Desarguesian* if, for every pair of triangles ABC and abc in π,

- the lines Aa, Bb, and Cc are concurrent if and only if the points $AB \cap ab$, $AC \cap ac$ and $BC \cap bc$ are collinear.

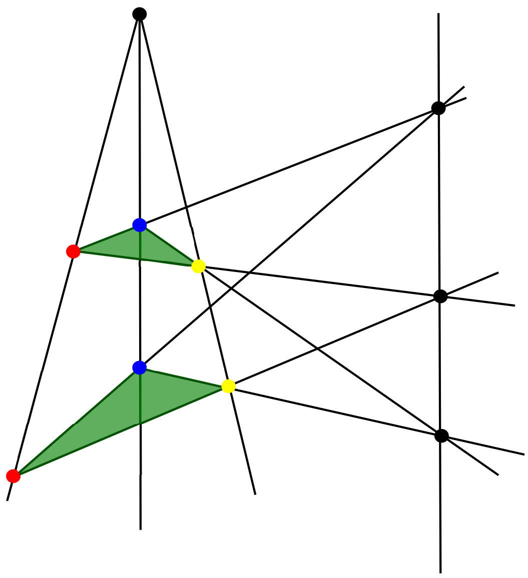
Figure 2.2 provides an illustration.

Theorem 2.1.2 (Hilbert [51], Chapter 5)**.** *A finite projective plane is Desarguesian if and only if it can be coordinatised by a field.*

Let π_1 and π_2 be projective planes. A bijective map $\sigma : \pi_1 \mapsto \pi_2$ is called a *collineation* if it preserves incidence and type. That is, for all P incident with ℓ in π_1 we know that $\sigma(P)$ is incident with $\sigma(\ell)$ in π_2 and if P is a point, or line, in π_1 then $\sigma(P)$ is a point, or line, respectively, in π_2. Two projective planes are *isomorphic* if there is a collineation mapping one to the other. The set of all collineations from a projective plane π_1 onto itself forms a group, called the *collineation group* and we refer to elements of that group as *collineations of* π_1.

A collineation of π, not the identity map, is called an *elation* if it fixes all the points on some line ℓ and all the lines through some point $P \in \ell$. We call ℓ the *axis*, and P the *centre*, of the elation.

Figure 2.2 – The Desargues configuration.



Example 2.1.3 (The Fano plane)**.** *In Figure 2.3 we give an example of an elation of the Fano plane. The line joining* $(0, 0, 1)$ *and* $(1, 1, 0)$ *is its axis and* $(1, 1, 0)$ *is its centre.*

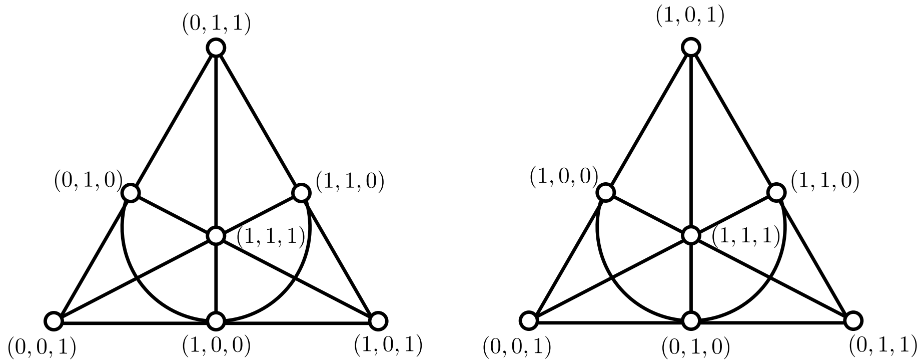


Figure 2.3 – An elation on the Fano plane.

A *translation plane* π is a projective plane with the condition that there exists a line $\ell \in \pi$ such that the group of elations with axis ℓ is transitive on the points of $\pi \setminus \ell$.

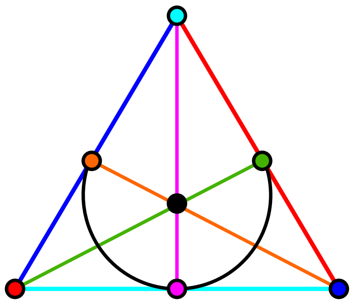
Consider the effect of the axioms of a projective plane on the points and lines of the plane. Now **(i)** demands the same behaviour of points and lines as does **(ii)** of lines and points. Suppose we take a projective plane $\pi = (\mathcal{P}, \mathcal{L}, \mathcal{I})$, and use it to construct another geometry: $\pi^D = (\mathcal{L}, \mathcal{P}, \mathcal{I}^D)$ where incidence is induced by π. That is, any two points X and Y in π^D lie on the line Z in π^D if and only if the two lines X and Y meet at the point Z in π. Given a projective plane $\pi = (\mathcal{P}, \mathcal{L}, \mathcal{I})$, we call $\pi^D = (\mathcal{L}, \mathcal{P}, \mathcal{I}^D)$ the *dual*, of π, and note that π^D must also be a projective plane.

A *duality* is a bijection taking π to π^D that preserves incidence. That is, P is in ℓ if and only if ℓ^D is in P^D. The *standard duality* of $\mathrm{PG}(2, q)$ is that which takes the point $x = (x_0, x_1, x_2)$ to the line with coordinates $[x_0, x_1, x_2]$.

A projective plane is called *self-dual* if it is isomorphic to its dual plane. A *polarity* is a duality of order two acting on a self-dual projective plane.

Example 2.1.4 (The Fano plane)**.** *Figure 2.4 shows a polarity acting on the Fano plane. The polarity takes points of a given colour to lines of the same colour, and vice versa.*

Figure 2.4 – A polarity of the Fano plane.



Any statement regarding points, lines and incidence has a *dual statement* which can be constructed by swapping the words 'point' and 'line' and making any grammatical changes required.

For example, the statement 'there are $q+1$ points on every line' has dual statement 'there are $q+1$ lines through every point'.

If a statement is true for all projective planes then its dual statement must also be true for all projective planes. If we have only proved a statement for one particular projective plane we know only that the dual statement is true for the dual of that plane.

Theorem 2.1.5 (Hirschfeld [52], pg. 31)**.** *The Desarguesian plane* $\mathrm{PG}(2,q)$ *is* self-dual*.*

The set of bijections from a projective plane to itself that preserve incidence, but not necessarily type, are called *correlations*. Every correlation of $\mathrm{PG}(2,q)$ that is not a collineation is the composition of a collineation and the standard duality.

The projective planes of order 9 provide the smallest examples of non-Desarguesian planes.

Example 2.1.6. *There are four projective planes of order 9.*

Name	*Translation plane*	*Self-dual*
$\mathrm{PG}(2,9)$	*yes*	*yes*
Hall	*yes*	*no*
Dual Hall	*no*	*no*
Hughes	*no*	*yes*

Two of the biggest open conjectures in projective geometry are that all finite projective planes of prime order are Desarguesian and that all finite projective planes have prime power order. Both conjectures have been settled, in the affirmative, for finite translation planes, see Lüneburg [65] pg. 4,6.

2.2 Projective spaces

In this section we generalise many of the concepts of Section 2.1 to higher dimensions.

A *projective space* is a set of points and lines such that

(i) each pair of distinct points p and q is contained in exactly one common line,

(ii) Veblen's axiom: if a, b, c and d are distinct points and the lines through ab and cd meet, then so do the lines through ac and bd,

(iii) every line has at least three points on it, and

(iv) there exist three non-collinear points.

Let $K = \{p_1, \ldots, p_n\}$ be a set of points in a projective space Π. Let K_1 be the set of all points on the lines joining pairs of points of K. That is, $K_1 = \{x \mid x \in p_i p_j \text{ for some } i, j\}$. Recursively define K_m to be the set of all points on the lines joining pairs of points of K_{m-1} until $K_{m+1} = K_m$ for some m. Then $K \subseteq K_1 \subseteq \cdots \subseteq K_m$ and we call K_m the *span* of K. If K' is the span of any set of points in K' then we refer to K' as a *subspace* of Π. If, for instance, $K = \{p_1, p_2\}$ then K' is the line p_1p_2. If $K = \{p_1, p_2, p_3\}$ then the span of K is the line p_1p_2 when $p_3 \in p_1p_2$ and a plane if $p_3 \notin p_1p_2$.

Similarly, the *span* of two subspaces X and Y is defined as the span of the points of $X \cup Y$ and we denote this span by $\langle X, Y \rangle$. Let $K \setminus \{p\}$ denote the set K with the element p removed. If K' is the span of $K = \{p_1, \ldots, p_n\}$ and, for all p_i, K' is not the span of $K \setminus \{p_i\}$, we say K has *projective dimension*, or simply *dimension* $n - 1$. That is, a point itself has dimension zero, a line has dimension one, and a plane has dimension two. We refer to subspaces of $\mathrm{PG}(n, q)$ of dimension $3, d$ and $n - 1$ as solids, d-spaces and hyperplanes, respectively. Let $\dim X$ be the dimension of the subspace X and denote the intersection of two subspaces X and Y by $X \cap Y$. If $X \cap Y$ contains a set of points K then K' is also in $X \cap Y$ and, therefore, $X \cap Y$ is also a subspace of Π for all subspaces X and Y. If two subspaces do not meet we say they are *skew* or *disjoint*.

If a subspace X is spanned by the points $\{p_1, \ldots, p_n\}$ we write $X = [P]$, where the i^{th} row of P is p_i.

Theorem 2.2.1 (Grassmann's Dimension Theorem (Dembowski [34] pg. 25))**.** *Let X and Y be two subspaces of Π. Then*

$$\dim X + \dim Y = \dim\langle X, Y \rangle + \dim X \cap Y,$$

Note that $\dim\langle X, Y \rangle \leq \dim \Pi$ and, therefore, in a projective space of dimension 3, there may exist pairs of skew lines, however all plane-line pairs must meet in at least a point.

Let X and Y be subspaces of $\mathrm{PG}(n, q)$, such that X and Y are disjoint, and let $\mathcal{K}$ be a subset of points of Y. A *cone* of a projective space with base $\mathcal{K}$ and vertex X is the union of the set of points on the lines joining a point of X to a point of $\mathcal{K}$.

Collineations are defined for projective spaces in the same way that they are for projective planes. That is, a collineation is a bijection from one projective space to another that preserves incidence and type. Two projective spaces are *isomorphic* if there is a collineation mapping one to the other.

Theorem 2.2.2 (Hessenberg [50], Vahlen [85] Theorems 136 and 137 (first published in 1905))**.** *Every projective space of dimension 3 or higher is isomorphic to the Desarguesian projective space of the same dimension and order.*

We will denote the unique projective space of order q and dimension $n \geq 3$ by $\mathrm{PG}(n, q)$. Every point of $\mathrm{PG}(n, q)$ is of the form $(x_0, \ldots, x_n)$ where x_i is an element of $\mathrm{GF}(q)$ for all i. This space is, therefore, contained in the higher order space $\mathrm{PG}(n, q^a)$, by allowing the coordinates to take values in $\mathrm{GF}(q^a)$.

Given a subspace X of dimension $e-1$ in $\mathrm{PG}(n, q)$ we can find e points $\{x_1, \ldots, x_e\}$ that span X. That is, all points of X have the form $\alpha_1 x_1 + \cdots + \alpha_e x_e$, where $\alpha_i \in \mathrm{GF}(q)$. Consider $\mathrm{PG}(n, q)$ embedded in $\mathrm{PG}(n, q^a)$. We now allow $\alpha_i \in \mathrm{GF}(q^a)$ call the resulting subspace the *extension* of X to $\mathrm{PG}(n, q^a)$.

In $\mathrm{PG}(n, q)$, a space of dimension $n-1$ is called a *hyperplane*. If X is the hyperplane containing all points $(X_0, X_1, \ldots, X_n)$ such that

$$Y_0 X_0 + Y_1 X_1 + \cdots + Y_n X_n = 0,$$

for some $Y_0, Y_1, \ldots, Y_n$ then we say $X = [Y_0, Y_1, \ldots, Y_n]$. Recall that in Section 2.1 we used this notation for lines.

Theorem 2.2.3 (The Fundamental Theorem of Projective Geometry (Dembowski [34] pg. 31))**.** *The set of all collineations of a projective space* $\mathrm{PG}(n, q)$ *onto itself forms the group* $\mathrm{P\Gamma L}(n+1, q)$*, called the* collineation group *of* $\mathrm{PG}(n, q)$*. Every collineation of* $\mathrm{PG}(n, q)$ *is given by*

$$x \mapsto x^{\sigma} A, \ \forall\, x \in \mathcal{P}$$

for some $(n+1) \times (n+1)$ *matrix* A *over* $\mathrm{GF}(q)$ *and some automorphism* σ *of* $\mathrm{GF}(q)$*, where* $x^{\sigma} = (x_0^{\sigma}, x_1^{\sigma}, \ldots, x_n^{\sigma})$*. We will denote this collineation by* (σ, A)*. Note that* $(\rho x)A = \rho(xA)$ *and* $(\rho x)^{\sigma} = \rho^{\sigma} x^{\sigma}$*. Therefore, two coordinates for the same point are mapped to the same image.*

The points $E_0 = (1, 0, \ldots, 0), \ldots, E_n = (0, \ldots, 0, 1), U = (1, 1, \ldots, 1)$ of $\mathrm{PG}(n, q)$ are called the *fundamental frame* of the projective space. Note that $E_0 + \ldots + E_n = U$.

Here we mention a well known result, which allows us to choose nice coordinates when proving general results.

Theorem 2.2.4 (Hirschfeld [52], pg. 31)**.** *In a projective space* $\mathrm{PG}(n, q)$ *there is a unique e* $(n+1) \times (n+1)$ *matrix* M *over* $\mathrm{GF}(q)$ *taking the* fundamental frame $E_0, \ldots, E_n, U$ *to any other ordered set of* $n+2$ *points, no* $n+1$ *in a hyperplane.*

Proof. We prove this by constructing the element M that takes the fundamental frame to the ordered set of points $P_0, \ldots, P_{n+1}$, where $P_i = (p_{i,1}, p_{i,2}, \ldots, p_{i,n+1})$. Note that there exists a set of non-zero scalars λ_i such that $P_{n+1} = \lambda_0 P_0 + \cdots + \lambda_n P_n$. None of these λ_i can be zero or there would be a set of $n+1$ points of the frame contained in a hyperplane. We define a matrix M whose j^{th} row is $\lambda_j P_j$, for all $0 \leq j \leq n$. Then $E_i M = \lambda_i P_i \equiv P_i$ and $UM = P_{n+1}$. Now M is invertible because the points $P_0, \ldots, P_n$ are linearly independent and the λ_i are non-zero.

We know that M is unique, up to a scalar multiple, because any matrix fixing all the E_i and U must be the identity. To see this note that the i^{th} row of such a matrix must have form $\lambda_i E_i$ and, if $\sum_i \lambda_i E_i = U$, then all the λ_i must be equal. □

Let $\Sigma_1, \Sigma_2, \Sigma_3$ be three skew $(e-1)$-spaces in $\mathrm{PG}(2e-1,q)$, $q>2$. Then a *transversal* is a line that meets all three of these $(e-1)$-spaces.

Suppose A and B are $e \times e$ matrices over $\mathrm{GF}(q)$. We use the notation $[\mathrm{A},\mathrm{B}]$ to denote the $(e-1)$-space of $\mathrm{PG}(2e-1,q)$ spanned by the points $(a_{k,1}, a_{k,2}, \ldots, a_{k,e}, b_{k,1}, b_{k,2}, \ldots, b_{k,e})$, that is, the rows of the matrix [AB]. We use I and 0 to refer to the $e \times e$ identity and zero matrices respectively.

Theorem 2.2.5 (Hirschfeld [52], pg. 31)**.** *Any set of three skew* $(e-1)$*-spaces in* $\mathrm{PG}(2e-1,q)$ *can be mapped to* $[\mathrm{I}\,0]$*,* $[0\,\mathrm{I}]$*, and* $[\mathrm{I}\,\mathrm{I}]$*.*

Proof. Let Σ_1, Σ_2 and Σ_3 be three skew $(e-1)$-spaces, and, for all $i \in \{1, \ldots, e+1\}$, let m_i be a transversal to these $(e-1)$-spaces. By Theorem 2.2.4, we may map any set of $2e+1$ points in $\mathrm{PG}(2e-1,q)$, no $2e$ in a hyperplane, to the fundamental frame. Therefore, without loss of generality we let $\Sigma_1 \cap m_i = E_{i-1}$, $\Sigma_2 \cap m_i = E_{e+i}$, for $i \in \{1, \ldots, n\}$, and let $\Sigma_3 \cap m_{n+1} = U$. It can then be determined that $\Sigma_1 = [\mathrm{I}\,0]$, $\Sigma_2 = [0\,\mathrm{I}]$, and $\Sigma_3 = [\mathrm{I}\,\mathrm{I}]$. □

The *dual* of a projective space $\mathrm{PG}(n,q)$ is the geometry in which the subspaces of dimension r are interchanged with those of dimension $n-r-1$, for all $0 \le r \le n-1$ and incidence is retained. A *duality* is a bijection that takes a projective space to its dual.

Theorem 2.2.6 (Hirschfeld [52], pg. 31)**.** *All projective spaces* $\mathrm{PG}(n,q)$*,* $n \geq 2$ *are self dual.*

The ability to count the number of subspaces of a given dimension incident with a subspace of another dimension will be useful at several points in the rest of this work.

Theorem 2.2.7 (Dembowski [34], pg. 28)**.** *The number of subspaces of dimension* k *in* $\mathrm{PG}(n,q)$ *is*

$$\begin{bmatrix} n+1 \\ k+1 \end{bmatrix}_q = \frac{\displaystyle\prod_{i=n-k+1}^{n+1} (q^i - 1)}{\displaystyle\prod_{i=1}^{k+1} (q^i - 1)}$$

and the number of k*-spaces through an* r*-space of* $\mathrm{PG}(n,q)$ *is*

$$\begin{bmatrix} n-r+1 \\ n-k+1 \end{bmatrix}_q = \frac{\displaystyle\prod_{i=k-r+1}^{n-r} (q^i - 1)}{\displaystyle\prod_{i=1}^{n-k} (q^i - 1)}.$$

2.2.1 Polarities and forms

The definition of a *polarity* extends to projective spaces. That is, it is a duality of order two acting on a self-dual projective space.

Example 2.2.8 (The standard duality)**.** *Let τ act on every subspace W of* $\mathrm{PG}(n,q)$ *by*

$$W^{\tau} = \{v \in V \mid vw^T = 0, \forall\, w \in W\}.$$

Then we say τ is the standard duality *of* $\mathrm{PG}(n,q)$*.*

In general, let the polarity ω be denoted by (σ, A, τ), where (σ, A) is a collineation and τ is the standard duality. Let U be a subspace of $\mathrm{PG}(n,q)$. Then

$$\begin{aligned}\omega(U) &= U^{\tau\sigma A}\\ &= A(U^{\tau\sigma})\\ &= \{v \in V \mid vA(u^{\sigma})^T = 0, \forall\, u \in U\}.\end{aligned}$$

Let $u_1, u_2, u, v \in V(n,q)$ and $a, b \in \mathrm{GF}(q)$. A *σ-sesquilinear form* on $\mathrm{GF}(q)$ is a map $\beta : V \times V \to \mathrm{GF}(q)$ such that

- σ is an automorphism of $\mathrm{GF}(q)$,
- $\beta(u_1 + u_2, v) = \beta(u_1, v) + \beta(u_2, v)$ and $\beta(v, u_1 + u_2) = \beta(v, u_1) + \beta(v, u_2)$, and
- $\beta(au, bv) = a\sigma(b)\beta(u, v)$.

Two vectors $u, v \in V$ are called *orthogonal* with respect to a form β if $\beta(u,v) = 0$.

Given an arbitrary, σ-sesquilinear form β, such that

$$\beta(x,y) \coloneqq xA(y^{\sigma})^T,$$

we see that β defines a map $\omega(X) = \{v \in V \mid \beta(v,x) = 0, \text{ for all } x \in X\}$, which is equivalent to the map (σ, A, τ) for some matrix A and automorphism σ. We now determine when ω is a polarity. For ω to be a polarity we require $\omega(\omega(X)) = X$. Now

$$\omega(\omega(X)) = \{v \in V \mid \beta(v,y) = 0, \text{ for all } y \in \omega(X)\},$$

is equal to X if and only if $\beta(v,x) = 0$ exactly when $\beta(x,v) = 0$, for all $x \in X$. This condition must be true for all $u, v \in V$, in which case we say β is *reflexive*. Thus, the only σ-sesquilinear forms that define polarities are reflexive σ-sesquilinear forms.

The polarity $\omega = (\sigma, A\tau)$ defines a form β such that

$$\beta(x,y) \coloneqq xA(y^{\sigma})^T.$$

Theorem 2.2.9 (Birkhoff and von Neumann [19])**.** *Let (σ, A) denote the polarity ω where $x^{\omega} = A(x^{\sigma})^{\tau}$. The four types of polarity of* $\mathrm{PG}(n,q)$ *are*

Orthogonal: $(1, A)$ *such that $A^T = A$, and q odd*

Pseudo: $(1, A)$*, such that $A^T = A$, not all $a_{i,i} = 0$, and q even*

Symplectic: $(1, A)$*, $A^T = -A$, $a_{i,i} = 0$ for all i, n even, and*

Hermitian: (σ, A)*, $\sigma \neq 1$, $\sigma = \sqrt{q}$ such that $(A^T)^{\sqrt{q}} = A$ and q is a square.*

Example 2.2.10 (Hermitian polarity). *Consider the projective space* $\mathrm{PG}(2,q^2)$. *Define a Hermitian polarity* $\omega = (\sigma, A, \tau)$, *with* τ *the standard duality, such that*

$$\sigma : x \mapsto x^q$$

and A *is the* 3×3 *identity matrix. Then* $\omega((X_0, X_1, X_2)) = [X_0^q, X_1^q, X_2^q]$.

The σ*-sesquilinear form* β *induced by* ω *is*

$$\begin{aligned}\beta(x,y) &= xA(y^q)^T \\ &= X_0Y_0^q + X_1Y_1^q + X_2Y_2^q.\end{aligned}$$

2.3 Objects in projective spaces

There are several projective space objects that will be used throughout the rest of this thesis. We define these objects, and mention some of their basic properties, in this section.

A set of d-spaces, $d \geq 1$, that partitions the points of $\mathrm{PG}(n,q)$ is called a *d-spread.* If $2d+1 = n$, then we simply refer to it as a *spread*.

We use the terminology *line spread* and *plane spread* for 1-spreads and 2-spreads, respectively.

Theorem 2.3.1 (Segre (see Dembowski [34], pg. 29)). *A d-spread of* $\mathrm{PG}(n,q)$ *can only exist if* $d+1$ *divides* $n+1$.

Therefore, the smallest dimensional space that can contain a spread is $\mathrm{PG}(3,q)$, there are no spreads of $\mathrm{PG}(4,q)$ and there may exist both line and plane spreads of $\mathrm{PG}(5,q)$, for example.

A *partial d-spread* is a set of mutually disjoint d-spaces.

Thus, a d-spread is a set of subspaces so that every point is contained in exactly one subspace. Next we consider sets of points that have interesting intersections with higher dimensional subspaces.

An *oval* of a projective plane π is a set of $q+1$ points such that no three are collinear.

Given a point P in an oval $\mathcal{O}$, there are exactly q lines through P that also contain another element of $\mathcal{O}$. Therefore there is one line through P that contains no other points of $\mathcal{O}$. We call this line a *tangent line* of $\mathcal{O}$ at P. The lines of π that pass through two points of $\mathcal{O}$ are called *secant lines* and those that are disjoint from the oval are called *external lines.*

A set of ovals $O_1, \ldots, O_n$ is said to be *in perspective* with *axis* ℓ and *centre* P if

- $P \in O_i$ for all i,
- for any $x \in O_i$ there exists a $y \in O_j$ such that x, y and P are collinear, and
- if $x_1, x_2 \in O_i$ and $y_1, y_2 \in O_j$ such that x_1, y_1 and P are collinear and x_2, y_2 and P are collinear then the lines x_1x_2 and y_1y_2 meet at a point of ℓ.

A *conic* in $\mathrm{PG}(2,q)$ is a set of points, each of the form (X,Y,Z) satisfying the equation

$$aX^2 + bY^2 + cZ^2 + dXY + eXZ + fYZ = 0$$

for some set of constants a, b, c, d, e, f not all zero.

We say that a conic is *non-degenerate* if it contains $q + 1$ points, not all in a line, and *degenerate* otherwise. Every non-degenerate conic is a set of $q + 1$ lines, no three collinear, and is therefore an oval.

Lemma 2.3.2 (Hirschfeld [52], pg. 141)**.** *There is a unique non-degenerate conic containing any set of five points of* $\mathrm{PG}(2, q)$*,* $q \geq 4$*, no three collinear.*

That is, any two distinct, non-degenerate, conics can share at most four points.

In order to discuss ovals in greater detail we need to consider q even and odd separately.

If q is odd, an oval is the largest set of points such that no three are collinear [20]. Let $\mathcal{O}$ be an oval. For all R not in $\mathcal{O}$, R lies on either $(q + 1)/2$ secants and $(q + 1)/2$ external lines, in which case it is called an *internal* point, or it lies on $(q - 1)/2$ secants, two tangents, $(q - 1)/2$ external lines, and is called an *external* point of $\mathcal{O}$.

A *dual oval* is a set of $q + 1$ lines such that no three are concurrent.

Each line ℓ in a dual oval meets the other q lines of the dual oval in distinct points. Therefore there is exactly one point of each line that is not contained in any other line of the dual oval. We call these points *tangent points* to a dual oval. Any oval in a projective plane of order q, q odd, defines a dual oval by taking the set of tangent lines to it and any dual oval defines an oval by taking the set of tangent points on it.

Theorem 2.3.3 (Segre [74])**.** *Every oval in* $\mathrm{PG}(2, q)$*, with* q *odd, is a conic.*

If q is even, the largest set of points in a projective plane π such that no three are collinear has size $q + 2$ and is called a *hyperoval*. Every oval in π can be extended to a hyperoval by adding the intersection point of all the tangent lines, called the *nucleus*. By Qvist [73], the nucleus always exists for q even. A hyperoval that comprises of a conic and its nucleus is called a *regular hyperoval*. The nucleus of a non-degenerate conic

$$C : aX^2 + bY^2 + cZ^2 + dXY + eXZ + fYZ = 0$$

is the point (f, e, d).

Lemma 2.3.4 (Hirschfeld [52], pg. 140)**.** *Let* q *be even and let* $C : aX^2 + bY^2 + cZ^2 + dXY + eXZ + fYZ = 0$ *be a conic of* $\mathrm{PG}(2, q)$*. Then* C *is degenerate exactly when* $(f, e, d) = (0, 0, 0)$ *or* (f, e, d) *is a point of the conic.*

A *quadric* is a set of points in $\mathrm{PG}(n, q)$ satisfying an equation

$$\sum_{i,j=0, i \leq j}^{n} a_{i,j} X_i X_j = 0,$$

for some set of constants a_{ij} not all zero. The quadrics of $\mathrm{PG}(2, q)$ are exactly the conics of $\mathrm{PG}(2, q)$. A quadric is called *singular* if it can be reduced to an equation in n or fewer variables via a coordinate change and *non-singular* otherwise.

The concept of nucleus also generalises to higher dimensions. A quadric in $\mathrm{PG}(2n, q)$, q even, has a point, called the *nucleus* such that all lines through the nucleus meet the quadric in exactly one point.

When n is even all the quadrics are equivalent to the quadric with equation

$$X_0^2 + X_1X_2 + \cdots + X_{n-1}X_n = 0$$

but when n is odd we have the *hyperbolic* quadrics, that are equivalent to,

$$X_0X_1 + \cdots + X_{n-1}X_n = 0$$

and the *elliptic* quadrics, equivalent to,

$$f(X_0, X_1) + X_2X_3 + \cdots + X_{n-1}X_n = 0$$

where f is an irreducible quadratic form over $\mathrm{GF}(q)$. That is, where f is a quadratic form that does not factor over $\mathrm{GF}(q)$.

Let us recall polarities for a moment and consider the quadric $\mathcal{Q}$ with equation

$$\sum_{i,j=0, i\leq j}^{n} a_{i,j}X_iX_j = 0.$$

For q odd, define a matrix $B = (b_{ij})$ such that

$$b_{ij} = b_{ji} = \frac{a_{i,j}}{2}$$

for $i < j$, and $b_{ii} = a_{i,i}$. Then B is the matrix of an orthogonal polarity with absolute points the points of $\mathcal{Q}$ (see Theorem 2.2.9). For q even and n odd, define $B = (b_{ij})$ such that $b_{ii} = 0$ and $b_{ij} = b_{ji} = a_{i,j}$ for $i < j$. Then B is the matrix of a symplectic polarity and all points of $\mathrm{PG}(n, q)$ are absolute. If n and q are both even there is no polarity associated to the quadric.

We now examine the type of object associated with a Hermitian polarity. The equation

$$\sum_{i,j=0}^{n} a_{i,j}X_iX_j^q$$

is that described by the Hermitian polarity $XA(X^T)^q$ where $A = (a_{i,j})$. We call the zeroes of this equation the points of a *Hermitian variety.*

A *unital* U in a projective plane π of order q^2 is a set of $q^3 + 1$ points such that any line of π meets U in one or $q + 1$ points.

Example 2.3.5 (Hermitian polarity)**.** *Consider the Hermitian polarity ω sending the point $x = (X_0, X_1, X_2)$ to $[X_0^q, X_1^q, X_2^q]$, discussed in Example 2.2.10, and its corresponding form β*

$$\beta(x, y) = X_0Y_0^q + X_1Y_1^q + X_2Y_2^q.$$

The set of points of $\mathrm{PG}(2, q^2)$ *such that $\beta(x, x) = 0$ or, equivalently, such that $x \in x^\omega$, form a unital.*

An *ovoid* in $\mathrm{PG}(3, q)$ is a set of $q^2 + 1$ points such that no three are collinear.

Example 2.3.6 ($Q^-(3,3)$)**.** *In the projective space* $PG(3,3)$*, the set of points satisfying the equation*

$$X_0^2 + X_1^2 + X_2X_3 = 0$$

forms an ovoid. This equation, and ovoid, are induced by the orthogonal polarity sending the point (X_0, X_1, X_2, X_3) *to the plane defined by all points orthogonal to* $[X_0, X_1, -X_3, -X_2]$*. These points are:*

$$(0,0,1,0), (0,0,0,1), (1,0,1,2), (1,0,2,1), (0,1,1,2),$$
$$(0,1,2,1), (1,1,1,1), (1,2,1,1), (2,1,1,1), (2,2,1,1).$$

2.4 Linear representation

Let $\Pi_\infty = PG(n-1,q)$ be embedded in $PG(n,q)$. The *linear representation* $T^*_{n-1}(K_\infty)$ of a set $K_\infty \subseteq \Pi_\infty$ is the geometric structure whose

- points are the points of $PG(n,q) \setminus \Pi_\infty$,
- lines are the lines of $PG(n,q)$ that meet Π_∞ in a point of K_∞, and
- which has incidence induced by $PG(n,q)$.

We call the points in $PG(n,q) \setminus \Pi_\infty$ *affine points* and the lines of $PG(n,q) \setminus \Pi_\infty$, that meet Π_∞ in a point of K_∞, *affine lines.*

Example 2.4.1 ($T_2^*(\mathcal{O})$, Ahrens-Szekeres [4], Hall Jr. [44])**.** *Let* $\Pi_\infty = PG(2,q)$*, q even, be embedded in* $PG(3,q)$ *and consider* $\mathcal{O}$ *a hyperoval in* Π_∞*. For each affine point P there are* $q+2$ *lines containing P and a point of* $\mathcal{O}$*. Each affine line contains one point of* $\mathcal{O}$ *and q affine points. Therefore, in the linear representation* $T_2^*(\mathcal{O})$*, each point lies on* $q+2$ *lines and each line contains q points.*

There are many similar ways to construct geometries using elements of a projective space embedded in a larger dimensional projective space.

2.5 Polar spaces

Polar spaces were first introduced by Veldkamp in 1959 [88] however we will use an equivalent definition due to Buekenhout and Shult, published in 1974 [27]. Polar spaces bring together several important concepts we have already discussed, including conics, quadrics and polarities.

A *polar space* is a set of points and lines obeying the axioms that

A1 there are at least three points on every line,

A2 any pair of points spans at most one line,

A3 any two lines meet in at most one point,

A4 no point is collinear with every other point, and

A5 given a point P and a line ℓ, with P not on ℓ, there is either one line through P that meets ℓ or all lines through P meet ℓ.

Example 2.5.1 ($T_2^*(\mathcal{O})$). *We can show that $T_2^*(\mathcal{O})$, described in Section 2.4, is an example of a polar space. It satisfies the first three axioms trivially. In* $\mathrm{PG}(3,q)$ *consider the line joining any point P to a point in $\Pi_\infty \setminus \mathcal{O}$. The affine points not on that line are not collinear with P, and $T_2^*(\mathcal{O})$ satisfies the fourth axiom. It remains to check the fifth axiom. Consider an affine point P and an affine line ℓ in* $\mathrm{PG}(3,q)$ *such that P is not a point of ℓ. Then the plane $\langle P,\ell\rangle$ contains all affine lines on P, that meet a point of ℓ, and it meets Π_∞ in a line m. Now m contains the point $\ell \cap \Pi_\infty \in \mathcal{O}$ and therefore meets $\mathcal{O}$ in another point R. The line $\langle P,R\rangle$ is the unique affine line through P that meets ℓ.*

Let $x_0,\dots x_n$ be a set of points in a polar space. If the span $\langle x_0,\dots x_n\rangle$ is a projective space we say that the subspace is in the polar space. A polar space has rank r, if the highest dimensional subspace it contains has dimension $r-1$. We call these subspaces *maximals*. A *d-spread* of a polar space is a set of d-spaces in the polar space that partition the points of the polar space.

A polar space is called *classical* if it is one of the following examples.

- The Hermitian polar spaces, denoted $\mathrm{H}(n,q^2)$, are the geometries containing the subspaces of non-singular Hermitian varieties. They exist for $\mathrm{PG}(n,q^2)$ for both odd and even n and q. These have rank $n/2$ if n is even and $(n+1)/2$ if n is odd.
- The *symplectic* polar spaces, denoted $\mathrm{W}(n,q)$, contain all the points of $\mathrm{PG}(n,q)$ and all the subspaces of a symplectic polarity. They exist only for odd n and have rank $(n+1)/2$.
- The *parabolic quadrics*, denoted $\mathrm{Q}(n,q)$ for n even, have rank $n/2$.
- The *elliptic quadrics*, denoted $\mathrm{Q}^-(n,q)$, for n odd, have rank $(n-1)/2$.
- The *hyperbolic quadrics*, denoted $\mathrm{Q}^+(n,q)$, for n odd, have rank $(n+1)/2$.

We have already discussed the fact that projective spaces of dimension three or higher can always be coordinatised by a finite field. There is a corresponding result by Tits from 1974.

Theorem 2.5.2 (Tits [84] Section 8.21). *All polar spaces of rank $r \geq 3$ are classical.*

In Table 2.1, we list important information for the classical polar spaces.

Let P be a point of a classical polar space Π and let $P^\perp$ denote the image of P under the polarity. Then $P^\perp$ is a hyperplane containing P and all the points of $P^\perp \cap \Pi$ must necessarily be collinear with P.

Theorem 2.5.3 (Cameron [28], pg. 90). *Let Π be a classical polar space of rank r and let P be a point of Π. Then $\Pi \cap P^\perp$ is a cone with vertex P and base a polar space of rank $r-1$ of the same type as Π. The* quotient space *of a point $P \in \Pi$ is the set of all subspaces through P where the lines through P are considered as points, the planes through P as lines, and so on. The quotient space is a polar space of rank $r-1$ and of the same type as Π.*

Table 2.1 – The classical polar spaces.

Type	Rank	# points	# maximals	# spread elements
$\mathrm{W}(2n-1,q)$	n	$\dfrac{q^{2n}-1}{q-1}$	$(q+1)(q^2+1)\cdots(q^n+1)$	q^n+1
$\mathrm{H}(2n-1,q^2)$	n	$(q^{2n-1}+1)\dfrac{q^{2n}-1}{q^2-1}$	$(q+1)(q^3+1)\cdots(q^{2n-1}+1)$	$q^{2n-1}+1$
$\mathrm{H}(2n,q^2)$	n	$(q^{2n+1}+1)\dfrac{q^{2n}-1}{q^2-1}$	$(q^3+1)(q^5+1)\cdots(q^{2n+1}+1)$	$q^{2n+1}+1$
$\mathrm{Q}^-(2n+1,q)$	n	$(q^{n+1}+1)\dfrac{q^n-1}{q-1}$	$(q^2+1)(q^3+1)\cdots(q^{n+1}+1)$	$q^{n+1}+1$
$\mathrm{Q}(2n,q)$	n	$(q^n+1)\dfrac{q^n-1}{q-1}$	$(q+1)(q^2+1)\cdots(q^n+1)$	q^n+1
$\mathrm{Q}^+(2n-1,q)$	n	$(q^{n-1}+1)\dfrac{q^n-1}{q-1}$	$2(q+1)(q^2+1)\cdots(q^{n-1}+1)$	$q^{n-1}+1$

Example 2.5.4 ($\mathrm{W}(3,q)$)**.** *Consider a point P in $\mathrm{W}(3,q)$. Then $P^\perp$ is a plane, containing P, and $\mathrm{W}(3,q)\cap P^\perp$ is the set of $q+1$ lines through P in $P^\perp$. Each line ℓ of $\mathrm{PG}(3,q)$ in $P^\perp$, such that $P\notin\ell$, has all its points in $\mathrm{W}(3,q)$ but is not in $\mathrm{W}(3,q)$ itself. That is, it is isomorphic to the polar space $\mathrm{W}(1,q)$.*

In the hyperbolic quadric $\mathrm{Q}^+(2n-1,q)$, there are two classes of maximals, called *Latins* and *Greeks*. These classes are defined by their intersections with one another. If n is odd then two maximals belong to the same class if and only if their intersection is a subspace with odd dimension, and if n is even then two maximals belong to the same class if and only if their intersection is a subspace with even dimension.

Remark 2.5.5 (The Klein Correspondence)**.** *The* Klein correspondence*, introduced by Klein in his PhD thesis [61], maps the set of lines of $\mathrm{PG}(3,q)$ to the set of points of $\mathrm{Q}^+(5,q)$.*

Let ℓ be a line of $\mathrm{PG}(3,q)$ containing the points $X=(x_0,x_1,x_2,x_3)$ and $Y=(y_0,y_1,y_2,y_3)$. Then define a coordinate vector *L by*

$$L=(\ell_{0,1},\ell_{0,2},\ell_{0,3},\ell_{1,2},\ell_{3,1},\ell_{2,3}),$$

where $\ell_{i,j}=x_iy_j-x_jy_i$.

We use this notation to define the Klein correspondence on $\mathrm{Q}^+(5,q)$, where the form of the polar space is $x_0x_5+x_1x_4+x_2x_3$, and $(x_0,x_1,x_2,x_3,x_4,x_5)=(\ell_{0,1},\ell_{0,2},\ell_{0,3},\ell_{1,2},\ell_{3,1},\ell_{2,3})$. Table 2.2 gives some of the most useful correspondences.

Table 2.2 – Some Klein correspondences.

$\mathrm{PG}(3,q)$	$\mathrm{Q}^+(5,q)$
lines	points
points	Latins
planes	Greeks
lines of $\mathrm{H}(3,q)$	points of $\mathrm{Q}^-(5,\sqrt{q})$, when $\sqrt{q}$ a prime power
lines of $\mathrm{W}(3,q)$	points of $\mathrm{Q}(4,q)$

A *finite generalised quadrangle* is a geometric structure of points and lines such that

- each line is incident with $s+1$ points and two distinct lines are incident with at most one point,
- each point is incident with $t+1$ lines and two distinct points are incident with at most one line, and
- if X is a point, not on the line ℓ, then X is collinear with exactly one point on ℓ.

That is, a generalised quadrangle is exactly a polar space of rank 2 and its maximals are lines. We say that a generalised quadrangle has order (s,t) if it has $s+1$ points on a line and $t+1$ lines through a point, or, if $s=t$, that it has order s. So $T_2^*(\mathcal{O})$ is a generalised quadrangle of order $(q-1,q+1)$. The *dual* of a generalised quadrangle of order (s,t) is a generalised quadrangle of order (t,s).

Definition 2.5.6. *Let* Π *be a finite generalised quadrangle and let* K *be the set of points of* Π. *If a collineation* θ *of* Π *fixes all the lines through some point* P *and* θ *is either the identity or fixes no point of* $K-P^\perp$ *then* θ *is an* elation *of* Π *about* P *and* P *is the* centre *of* θ.

Let Π be a generalised quadrangle, let P be a point of Π and let G be the group of elations with centre P. If, for every pair of points X and Y of $\Pi\setminus\{P\}$, there is a unique element $g\in G$ such that $gX=Y$, then we say Π is a *translation generalised quadrangle* with respect to P.

Just as there are Desarguesian planes, there are also classical generalised quadrangles. These are: $\mathrm{W}(3,q)$ and its dual $\mathrm{Q}(4,q)$, $\mathrm{H}(3,q^2)$ and its dual $\mathrm{Q}^-(5,q)$, $\mathrm{H}(4,q^2)$, and $\mathrm{Q}^+(3,q)$. In order to discuss different generalised quadrangles, we extract some properties from these classical examples.

If x and y are collinear in a generalised quadrangle $\mathcal{T}=(\mathcal{P},\mathcal{L},\mathcal{I}\}$ we write $x\sim y$ and define $x^\perp=\{z\in\mathcal{P}\mid x\sim z\}$. Let x and y be noncollinear points in a generalised quadrangle $\mathcal{T}$ and let $\{x,y\}^{\perp\perp}$ be the set of all points z such that all points of $z^\perp$ are in both $x^\perp$ and $y^\perp$, that is, $\{x,y\}^{\perp\perp}=\{z\in\mathcal{P}\mid z\in u^\perp,\forall\, u\in x^\perp\cap y^\perp\}$, as illustrated in Figure 2.5. We call $\{x,y\}^{\perp\perp}$ the *hyperbolic line* containing x and y. If x and y are collinear, or if $\{x,y\}^{\perp\perp}$ contains $t+1$ points,

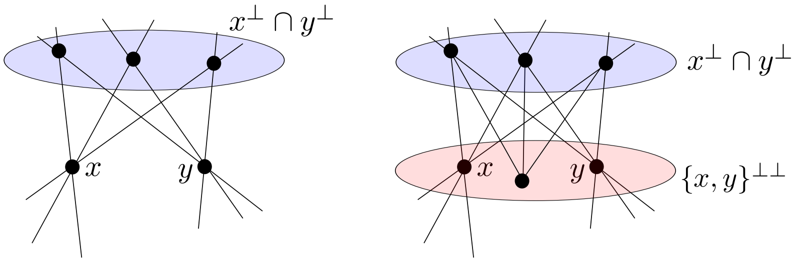


Figure 2.5 – $\{x,y\}^{\perp\perp}$.

then we say the pair $\{x,y\}$ is *regular*. A point x is called *regular* if, for all other points y in $\mathcal{T}$, the pair $\{x,y\}$ is regular.

Example 2.5.7 ($\mathrm{W}(3,q)$)**.** *The order of* $\mathrm{W}(3,q)$ *is* q *and we shall show that each point of* $\mathrm{W}(3,q)$ *is regular. Consider any pair of non-collinear points* $x,y\in\mathrm{W}(3,q)$. *The* $q+1$ *lines through* x *must each contain exactly one point collinear with* y. *Therefore* $x^\perp\cap y^\perp$ *has* $q+1$ *elements, which we* *will denote* $u_0, \ldots, u_q$. *For each* u_i, $u_i^\perp$ *is a plane containing* u_i, x *and* y *and all points of* $\mathrm{W}(3,q)$ *in this plane must be collinear with* u_i. *Now every point of* $\mathrm{PG}(3,q)$ *is also in* $\mathrm{W}(3,q)$ *so the* $q+1$ *points of the line* xy *must be collinear with* u_i *for all* i. *Thus, all pairs* $\{x,y\}$ *are regular and all points are regular.*

Theorem 2.5.8 (Payne and Thas [71], pg. 29)**.** *The dual of* $\mathrm{Q}(4,q)$ *is* $\mathrm{W}(3,q)$.

Proof. By the Klein correspondence (see Remark 2.5.5), we can find a map between lines of $\mathrm{PG}(3,q)$ and points of $\mathrm{Q}^+(5,q)$. The image of $\mathrm{W}(3,q)$ on $\mathrm{Q}^+(5,q)$ is the intersection of a non-tangent hyperplane with $\mathrm{Q}^+(5,q)$, that is, a $\mathrm{Q}(4,q)$. Thus, we can find a map taking the lines of $\mathrm{W}(3,q)$ to the points of $\mathrm{Q}(4,q)$. Now the perp of each point of $\mathrm{W}(3,q)$ is a pencil of lines in a plane. This pencil is mapped to a line of $\mathrm{Q}(4,q)$, completing the correspondence. □

For more details regarding generalised quadrangles see *Finite Generalised Quadrangles* by Payne and Thas [71].

Let β be the form of a classical polar space $\Pi(n,q)$ and let σ be a collineation on the projective space $\mathrm{PG}(n,q)$. Then, if $\beta(u,v) = \beta(\sigma(u), \sigma(v))$, for all u, v in $\mathrm{PG}(n,q)$, we say that σ *preserves the form* and call σ an *isometry*. The set of these collineations is called the *isometry group* of the polar space. If there exists $\lambda \in \mathrm{GF}(q)$ such that $\beta(u,v) = \lambda\beta(\sigma(u), \sigma(v))$ for all u and v, we say that λ preserves the form *up to a scalar* and call λ a *similarity*. This set of collineations is called the similarity group of the polar space.

We can also adapt the definitions of objects in projective spaces so they generalise to objects in polar spaces.

Recall that a *d-spread* of a polar space is a set of d-spaces in the polar space that partition the points of the polar space.

Any d-spread of $\mathrm{W}(n,q)$ will also be a d-spread of $\mathrm{PG}(n,q)$. This relation between spreads of the projective space and symplectic space is a catalyst for the work of Chapter 4.

An *ovoid* $\mathcal{O}$ of a polar space Π is a set of points such that every maximal of Π meets $\mathcal{O}$ in exactly one point.

The number of elements in an ovoid is the same as the number of elements in a spread and we call this the *ovoid number*. Recall that in $\mathrm{Q}^+(2n-1,q)$, if n is odd then two maximals belong to the same class if and only if their intersection is a subspace with odd dimension, and if n is even then two maximals belong to the same class if and only if their intersection is a subspace with even dimension. That is, there can only exist spreads of $\mathrm{Q}^+(2n-1,q)$ when n is even and, in that case, each spread is entirely formed from elements of one class.

Remark 2.5.9. *In* $\mathrm{Q}^+(7,q)$ *we can obtain spreads from ovoids and vice versa. Denote the points, lines, Latins and Greeks of* $\mathrm{Q}^+(7,q)$ *by* $\mathcal{P}, \mathcal{L}, \mathcal{M}_1$ *and* $\mathcal{M}_2$, *respectively. Then a* triality τ *of* $\mathrm{Q}^+(7,q)$ *preserves incidence, fixes* $\mathcal{L}$ *and*

$$\tau : \mathcal{P} \mapsto \mathcal{M}_1 \mapsto \mathcal{M}_2 \mapsto \mathcal{P},$$

is a bijective map at each step.

Let τ *be a triality of* $\mathrm{Q}^+(7,q)$*. Then*

- *if* $\mathcal{O}$ *is an ovoid then* $\mathcal{O}^\tau$ *and* $\mathcal{O}^{\tau^2}$ *are spreads, and*
- *if* $\mathcal{S}$ *is a spread then either* $\mathcal{S}^\tau$ *or* $\mathcal{S}^{\tau^2}$ *is an ovoid, and the other is a spread.*

Chapter 3

Spreads and translation planes

In this chapter we will consider the André/Bruck-Bose construction, the Baer correspodence and field reduction: all of which are methods of representing projective space objects in different projective spaces.

The *André/Bruck-Bose construction* creates translation planes of order q^e from spreads in $\mathrm{PG}(2e-1, q)$. The construction was independently published by André in 1954 [6], Segre [75] in 1964 and Bruck and Bose [22] in 1964. Historically, it has been important in bringing together two previously separate fields of finite geometry: Desarguesian spaces and non-Desarguesian planes.

The *Baer correspondence* [10] creates a Desarguesian space $\mathrm{PG}(n-1, q^e)$, $n-1 > 2$, from a normal $(e-1)$-spread in $\mathrm{PG}(en-1, q)$ and, from this, we show that a non-Desarguesian spread of $\mathrm{PG}(2e-1, q)$ cannot be contained within a normal $(e-1)$-spread of $\mathrm{PG}(en-1, q)$.

Field reduction takes the points of $\mathrm{PG}(n-1, q^e)$, $n-1 \geq 1$, to an $(e-1)$-spread of $\mathrm{PG}(en-1, q)$ and we use this, together with the André/Bruck-Bose construction, to give geometric properties of Desarguesian spreads.

3.1 The André/Bruck-Bose construction

The methods André, Segre, and Bruck and Bose use to construct translation planes from spreads are different — André uses group partitions while Segre, and Bruck and Bose, work with projective spaces — but, given the same spread, each method constructs the same translation plane. We will follow the methods of Segre, and Bruck and Bose. For more details on André's method, see *"The Handbook of Finite Translation Planes"* [56], Sections 2.2 and 4.5.

Theorem 3.1.1 (André/Bruck-Bose [22] pg. 88, see Figure 3.1)**.** *Let $\mathcal{S}$ be a spread of $\Sigma' = \mathrm{PG}(2e-1, q)$, $e \geq 2$, and let Σ' be embedded in $\Sigma = \mathrm{PG}(2e, q)$ as a hyperplane. Define a geometry $\pi = (\mathcal{P}, \mathcal{L}, \mathcal{I})$, with $\mathcal{P}$ given by*

- *the elements of $\mathcal{S}$, and*
- *the points of $\Sigma \setminus \Sigma'$,*

$\mathcal{L}$ given by

- *the $(2e-1)$-space Σ', and*
- *the e-spaces of Σ that meet Σ' in an element of $\mathcal{S}$,*

and $\mathcal{I}$ induced. Then π is a projective plane of order q^e.

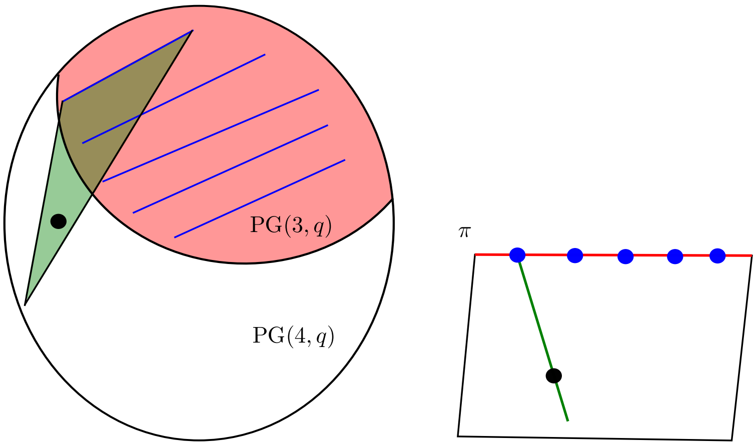


Figure 3.1 – The André/Bruck-Bose construction for a translation plane of order q^2.

Proof. Recall that a projective plane is a set of points and lines such that

P1 any two points span a unique line,

P2 any two lines meet in a unique point, and

P3 there exist four points such that no line meets three of them.

First, consider **(P1)**:

- If $X, Y \in \mathcal{S}$ then they span Σ' and the unique element of $\mathcal{L}$ they span is Σ'.
- Suppose $X \in \mathcal{S}$ and $Y \in \Sigma \setminus \Sigma'$. Then the unique element of $\mathcal{L}$ they span is the e-space spanned by X and Y.
- Suppose $X, Y \in \Sigma \setminus \Sigma'$, then the line XY must meet Σ' in a point contained in a spread element J. Then the unique element of $\mathcal{L}$ spanned by X and Y is the e-space XJ.

Next, we prove that $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ satisfies **(P2)**. By definition, every affine e-space meets Σ' in a spread element. Now we consider the more interesting case, where s and t are affine e-spaces in Σ. If these both meet Σ' in the same spread element we are finished. Thus, suppose they do not. However, the intersection of two e-spaces in a $2e$-space must contain a point P, and P is not in Σ', therefore it belongs to $\mathcal{P}$.

Finally, we find an example of four elements of $\mathcal{P}$ such that no element of $\mathcal{L}$ contains three of them. There exist $q^e + 1 > 2$ spread elements in Σ'. Let X, Y and Z be any three spread elements and choose a point $P \in \Sigma \setminus \Sigma'$. Let R be any point in $PZ \setminus Z$ such that $R \neq P$. Then there is no element of $\mathcal{L}$ passing through three of the points X, Y, R, P.

Thus, π satisfies all the axioms of a projective plane. □

In fact, André proved that this construction always gives a translation plane, and that all translation planes can be constructed in this way.

Let $\mathcal{S}$ be a spread of $\mathrm{PG}(2e-1,q)$. Consider the elements of $\mathcal{S}$ as e-spaces over the vector space $V(2e,q)$. These e-spaces will only intersect at the zero vector.

Given A, B, C in $\mathcal{S}$ there is a unique linear transformation L from A to B, such that $B = \{aL \mid a \in A\}$ and $C = \{a + aL \mid a \in A\}$. This can be seen by recalling Theorem 2.2.5 and noting that if $L : [\mathrm{I}, 0] \to [0, \mathrm{I}]$, such that $[\mathrm{I}, \mathrm{I}] = a + aL$, for $a \in [\mathrm{I}0]$, then L is unique and must map E_i to E_{e+i}, where E_i is the i^{th} point of the fundamental frame.

We define other e-spaces $J(X)$, by linear transformations $X + L$, where X maps A into A, and define $\mathcal{C}(A, B, C) = \{X \mid J(X) \in \mathcal{S}\}$. That is, $J(0)$ is B, $J(\mathrm{I})$ is C and $J(X) = \{aX + aL \mid a \in A\}$. We denote A by $J(\infty)$. Note that these linear transformations can be seen as $e \times e$ matrices, whereby $J(X) = B + AX$, and that $\mathcal{C}$ contains 0 and I, has q^e elements, and for all $X, Y \in \mathcal{C}$, $\det(X - Y) \neq 0$.

This set of linear representations can be seen as a collection of matrices, called a *spreadset*.

Every e-spread $\mathcal{S}$ in $\mathrm{PG}(2e-1,q)$ can be described by a *spreadset* $\mathcal{C}$ is a set of $e \times e$ matrices, with entries in $\mathrm{GF}(q)$, satisfying the following properties.

- $|\mathcal{C}| = q^e$,
- $0, I \in \mathcal{C}$, and
- $\forall\, X \neq Y \in \mathcal{C}$ then $\det(X - Y) \neq 0$,

such that $\mathcal{S} = \{S_M \mid M \in \mathcal{C} \cup \{\infty\}\}$, where

- $S_M = \{(x, xM) \mid \forall\, x \in V(2e,q)\}$ for $M \in \mathcal{C}$, and
- $S_\infty = \{(0, x) \mid \forall\, x \in V(2e,q)\}$.

Spreadsets can be found by mapping three elements of the spread to $[\mathrm{I}, 0], [0, \mathrm{I}], [\mathrm{I}, \mathrm{I}]$, and are not unique.

Example 3.1.2 (A spread in $\mathrm{PG}(3,3)$)**.** *The nine matrices*

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$
$$\begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix},$$

are a spreadset, defining a spread of $\mathrm{PG}(3,3)$.

Lemma 3.1.3 (Bruck and Bose [23] pg. 156)**.** *Let $\mathcal{S}$ be a spread of* $\mathrm{PG}(2e-1,q)$. *and let $\mathcal{C} = \mathcal{C}(A, B, C)$ be a spreadset of $\mathcal{S}$. Then the spreadsets $\mathcal{C}^{-1} = \{X^{-1} \mid X \in \mathcal{C}\}$ and $(T - S)^{-1}(\mathcal{C} - S) = \{(T - S)^{-1}(X - S) \mid X \in \mathcal{C}\}$, where $T, S \in \mathcal{C}, T \neq S$, define translation planes isomorphic to that described by $\mathcal{C}$.*

Proof. Let P be a one-to-one linear transformation from A to A', where A' is an e-space of $\mathrm{PG}(2e-1,q)$, and let $\mathcal{S}'$ denote the spread $P^{-1}\mathcal{S}P$. Then $\mathcal{S}$ and $\mathcal{S}'$ define isomorphic translation planes and $\mathcal{C}' = P^{-1}\mathcal{C}P$ is a spreadset of $\mathcal{S}'$.

Let L be the unique linear transformation from A to B, such that $B = \{aL \mid a \in A\}$ and $C = \{a + aL \mid a \in A\}$. Define a linear transformation ω on the vector space such that

$$a\omega = aL \text{ and } aL\omega = a, \text{ for all } a \in A = J(\infty).$$

Then $\omega^2 = 1$ and we define $\mathcal{C}^* = C(J(0), J(\infty), J(\mathrm{I}))$. That is, $X \in \mathcal{C}^*$ when

$$\{aLX + a \mid a \in A = J(\infty)\} \in \mathcal{S}.$$

Note that $\mathcal{C}^*$ is also a spreadset of $\mathcal{S}$. Now suppose $Y \in \omega\mathcal{C}^*\omega$, so $Y = \omega X\omega$ for some $X \in \mathcal{S}$. Then $X = \omega Y\omega$ and

$$\begin{aligned}
&\{aL(\omega Y\omega) + a \mid a \in A\} \in \mathcal{S},\\
&\{aY\omega + a \mid a \in A\} \in \mathcal{S},\\
&\{aYL + a \mid a \in A\} \in \mathcal{S},\\
&\{bL + bY^{-1} \mid b \in A\} \in \mathcal{S}.
\end{aligned}$$

Then $Y^{-1} \in \mathcal{C}$ and, therefore, $\omega\mathcal{C}^*\omega = \mathcal{C}^{-1}$. Now $\mathcal{C}^*$ is a spreadset of $\mathcal{S}$ and therefore any conjugate of $\mathcal{C}^*$ must describe a translation plane that is isomorphic to the one described by any spreadset of $\mathcal{S}$, including $\mathcal{C}$.

Now, consider taking a spreadset from $C(J(\infty), J(0), J(\mathrm{I}))$ to $\mathcal{C}^* = C(J(\infty), J(Q), J(R))$. We attempt to find a linear transformation ϕ that satisfies

$$\begin{aligned}
&a\phi = a,\\
&aL\phi = aMQ + aLM, \text{ and}\\
&(a + aL)\phi = aNR + aLN,
\end{aligned}$$

for all $a \in A = J(\infty)$,where M, N are linear transformations of A into A. This implies $M = N$, $I + MQ = NR$ and, therefore, $M = N = (R-Q)^{-1}$. Now consider $X' = (T-S)^{-1}(X-S)$. Then, if $b = aM$,

$$(aX' + aL)\phi = a(X' + MQ) + aML = bX + bL$$

and therefore $J(X')\phi = J(X)$. Note that $L\phi$ is the unique linear transformation from $J(\infty)$ to $J(Q)$ such that $J(R) = \{a + aL\phi \mid a \in J(\infty)\}$. Therefore, $X \in \mathcal{C}^*$ when $\{aX + aL\phi \mid a \in J(\infty)\} \in \mathcal{S}$ and $X \in \phi\mathcal{C}\phi^{-1}$ whenever $\phi^{-1}X\phi \in \mathcal{C}^*$, that is, $\{a\phi^{-1}X\phi + aL\phi \mid a \in J(\infty)\} \in \mathcal{S}$. Consider

$X' = (R-Q)^{-1}(X-Q)$, where $X \in \mathcal{C}$. We want to show $X' \in \phi\mathcal{C}^*\phi^{-1}$. We know

$$\begin{aligned}
&\{a\phi^{-1}X'\phi + aL\phi \mid a \in J(\infty)\} \in \mathcal{S}\\
&\{bX'\phi + b\phi L\phi \mid b \in J(\infty)\} \in \mathcal{S}\\
&\{bX'\phi + bL\phi \mid b \in J(\infty)\} \in \mathcal{S}\\
&\{bX'\phi + b(R-Q)Q + b(R-Q)L \mid b \in J(\infty)\} \in \mathcal{S}\\
&\{c(R-Q)X' + c(Q+L) \mid c \in J(\infty)\} \in \mathcal{S}\\
&\{c(X-Q) + c(Q+L) \mid c \in J(\infty)\} \in \mathcal{S}\\
&\{cX + cL \mid c \in J(\infty)\} \in \mathcal{S}.
\end{aligned}$$

Thus, $X' \in \phi\mathcal{C}^*\phi^{-1}$ for $X \in \mathcal{C}$ and the transformation $\mathcal{C} \mapsto (T-S)^{-1}(\mathcal{C}-S)$, where $T, S \in \mathcal{C}, T \neq S$ gives an isomorphic translation plane to $\mathcal{C}$. □

By Bruck and Bose [22], we can form a coordinate ring $(A, \cdot, +)$, of the translation plane π, from any corresponding spreadset.

Multiplication in $(A, \cdot, +)$ is determined by choosing an identity element $I \in A$. Then for each $b \in A$, we have $b = IX$ for some $X \in \mathcal{C}$, and $ab = a(IX) = aX$. Addition is given by vector addition.

Bruck and Bose proved that $(A, \cdot, +)$ is always a right quasifield. That is

- $(A \setminus \{0\}, \cdot)$ has identity I,
- for all $a, b \in A \setminus \{0\}$, there exist unique elements x and y such that $ax = b$ and $ya = b$,

so $(A \setminus \{0\}, \cdot)$ is a loop, and

- $(A, +)$ is an abelian group, with zero 0,
- $(x+y)z = (xz + yz), \forall\, x, y, z \in A$, and
- if $a, b, c \in A$, such that $a \neq b$, then there is a unique $x \in A$ such that $xa = xb + c$.

When A is a field, the plane it coordinatises must be Desarguesian [34].

A spread is called *Desarguesian* if, under the André/Bruck-Bose construction, it creates a Desarguesian plane.

We wish to determine when $(A, \cdot, +)$ has more than just a right quasifield structure.

Theorem 3.1.4 (Bruck and Bose [**?**], Section 11)**.** *Let π be the translation plane constructed from $\mathcal{S}$ by the André/Bruck-Bose construction and let $(A, \cdot, +)$ be the coordinate ring of π formed from the set of linear transformations $\mathcal{C}$. Then $(A, \cdot, +)$ is a field, and hence π a Desarguesian plane, if $\mathcal{C}$ is closed under addition and multiplication.*

Proof. The *Artin-Zorn Theorem* [91] states that every finite alternative division ring is a finite field. We already know that multiplication is right distributive, addition is commutative and that all elements have a multiplicative inverse because it is a quasifield.

Thus, to prove this theorem we show that $(A, \cdot, +)$ has left distributive and associative multiplication, when $\mathcal{C}$ is closed under addition and multiplication.

Let $b = IX$, $c = IY$, and $b + c = IS$, for $X, Y, S \in \mathcal{C}$. Now

$$\begin{aligned} a(b+c) &= a(IX + IY) \\ &= a(IS) \\ &= aS, \end{aligned}$$

and

$$\begin{aligned} ab + ac &= a(IX) + a(IY) \\ &= aX + aY \\ &= a(X+Y). \end{aligned}$$

Therefore, left multiplication is distributive over addition in $(A, \cdot, +)$ if $X + Y \in \mathcal{C}$ for all $X, Y \in \mathcal{C}$. Note that if $X + Y \in \mathcal{C}$ then $X + Y = S$ because $aZ = b$ must have a unique solution.

Similarly, $\mathcal{C}$ is closed under multiplication if $(A, \cdot, +)$ has associative multiplication. □

Theorem 3.1.5 (Bruck and Bose [**?**], Section 11)**.** *If a spreadset $\mathcal{C}$ is closed under addition and inversion then it describes a Desarguesian plane π.*

Proof. Let $b \in (A, \cdot, +)$ and let b^{-1} be the unique element of A such that $bb^{-1} = I$. If $b = IX$ and $b^{-1} = IX'$ then $IXX' = I$ for $X, X' \neq 0$. Also, for any $X \in \mathcal{C} \setminus \{0\}$, the equation $IXX' = I$ holds for a unique element X'. Therefore $(ab)b^{-1} = aXX'$ and this is equal to a if and only if $X^{-1} \in \mathcal{C}$ and A has the right inverse property and thus is an alternative division ring. By the Artin-Zorn theorem [91] we know that every finite division ring is a field, therefore A is a field and π is Desarguesian. □

Remark 3.1.6 (Coordinates for the translation plane)**.** *Let π be a translation plane described by a spread $\mathcal{S}$. Define $J(\infty), J(0)$ and $J(\mathrm{I})$ as above, so that $J(\infty)$ has basis $\{b_1, \ldots, b_e\}$, $J(0)$ has basis $\{b'_1, \ldots, b'_e\}$ and $J(\mathrm{I})$ has basis $\{b_1 + b'_1, \ldots, b_e + b'_e\}$. Then, define b^* such that $\{b'_1, \ldots, b'_e, b_1, \ldots, b_e, b^*\}$ is a basis for $V(2e+1, q)$. Any point of $\mathrm{PG}(2e, q) \setminus \mathrm{PG}(2e-1, q)$ can be described by $y + x' + b^*$ for some $x, y \in J(\infty)$ and we give it the coordinates $(x, y, 1)$. If a point on the line at infinity comes from the spread element $J(X)$ we give it the coordinate $(1, X, 0)$ or, in the case of $J(\infty)$, the coordinate $(0, 1, 0)$.*

3.2 Normal spreads

The André/Bruck-Bose construction creates planes from spreads of $\mathrm{PG}(2e-1, q)$. Baer, in 1963 [10], used normal $(e-1)$-spreads of $\mathrm{PG}(en-1, q)$ to create spaces of smaller dimension and, in 1974, Barlotti and Cofman [18] followed up on, and extended the theory of, this method. The Baer correspondence creates a projective plane of order q^e from a normal $(e-1)$-spread in $\mathrm{PG}(3e-1, q)$ and we prove that this projective plane is Desarguesian. From this, we prove that the restriction of a normal $(e-1)$-spread, to a $(2e-1)$-space spanned by two of its elements, must be a Desarguesian spread.

An $(e-1)$-spread of $\mathrm{PG}(en-1,q)$, is called *normal* if it induces a spread in any subspace generated by two of its elements. Note that $(e-1)$-spreads of $\mathrm{PG}(2e-1,q)$ are trivially normal.

3.2.1 The Baer correspondence

In Section 3.1, we showed how to construct a translation plane of order q^e from spreads of $\mathrm{PG}(2e-1,q)$. In this section we will discuss how to create projective spaces of dimension $n-1$, from $(e-1)$-spreads of $\mathrm{PG}(en-1,q)$. See Bader and Lunardon [9] for more detail.

Theorem 3.2.1 (Baer [10], Barlotti and Cofman [18] pg. 232)**.** *An $(e-1)$-spread $\mathcal{S}$ of $\mathrm{PG}(en-1,q)$, $n>2$, is normal if and only if the elements of $\mathcal{S}$ form the points, and the $(2e-1)$-spaces spanned by pairs of distinct spread elements form the lines, of a projective space π with dimension $n-1$ and order q^e.*

Proof. Let $\pi=(\mathcal{S},\mathcal{L},\mathcal{I})$ where $\mathcal{L}$ is the set of $(2e-1)$-spaces spanned by pairs of distinct elements of $\mathcal{S}$ and incidence is inherited from $\mathrm{PG}(en-1,q)$.

Any two elements of $\mathcal{S}$ span exactly one element of $\mathcal{L}$, by the definition of $\mathcal{L}$, and every element of $\mathcal{L}$ contains q^e+1 elements of $\mathcal{S}$, because $\mathcal{S}$ is normal. Thus, to prove π is a projective space, it remains to prove that there exist three non-collinear points and check Veblen's axiom: If A,B,C,D are distinct points such that the lines AB and CD meet, then the lines AC and BD also meet.

Let A,B,C,D be elements of $\mathcal{S}$ such that the elements $AB,CD\in\mathcal{L}$ meet in an element of $\mathcal{S}$. Then A,B,C,D are contained in a $(3e-1)$-space by Grassmann's Dimension Theorem (Theorem 2.2.1). Therefore AC and BD are also contained in this $(3e-1)$-space and must also meet in an $(e-1)$-space. This $(e-1)$-space must be an element of $\mathcal{S}$ because AC and BD are both partitioned by the elements of $\mathcal{S}$.

To see that there exist three non-collinear points, take two spread elements X,Y, and choose a third spread element Z that does not meet the $(2e-1)$-space that they span. Now, Z must exist because there are points in $\mathrm{PG}(en-1,q)\setminus\langle X,Y\rangle$ and if Z contains any point outside of $\langle X,Y\rangle$, then Z is disjoint from $\langle X,Y\rangle$.

The dimension and order of π can be calculated to be $n-1$ and q^e, respectively, by noting that each element of $\mathcal{L}$ contains q^e+1 elements of $\mathcal{S}$ and that $\mathcal{S}$ contains $(q^{en}-1)/(q^e-1)$ elements in total.

Conversely, suppose $(\mathcal{S},\mathcal{L},\mathcal{I})$ satisfy the axioms of an $(n-1)$-dimensional projective space of order q^e. Then two elements $A,B\in\mathcal{S}$ span a unique element of $\mathcal{L}$ containing q^e+1 elements of $\mathcal{S}$ and hence we have satisfied the conditions for $\mathcal{S}$ to be a normal $(e-1)$-spread. □

Therefore, we can use normal spreads to create projective spaces. In particular, a normal $(e-1)$-spread in $\mathrm{PG}(3e-1,q)$ forms a projective plane of order q^e. We will call this the *Baer correspondence*.

Lemma 3.2.2 (Segre [75]). *Let $\mathcal{S}$ be a normal $(e-1)$-spread of* $\mathrm{PG}(3e-1,q)$*. The plane π constructed according to Theorem 3.2.1 is isomorphic to the plane created by restricting $\mathcal{S}$ to any subspace spanned by two elements of $\mathcal{S}$ and applying the André/Bruck-Bose construction to the induced spread.*

Proof. Let $\mathcal{S}'$ denote the set of spread elements contained in a $(2e-1)$-space Σ' generated by two elements of $\mathcal{S}$. Let Σ be a $2e$-space containing Σ'.

Let $\pi = (\mathcal{S}, \mathcal{L}_\pi, \mathcal{I}_\pi)$, where $\mathcal{L}_\pi$ is the set of $(2e-1)$-spaces spanned by two elements of $\mathcal{S}$ and incidence is induced, and let $\gamma = (\mathcal{P}_\gamma, \mathcal{L}_\gamma, \mathcal{I}_\gamma)$, where $\mathcal{P}_\gamma = \{s \cap \Sigma \mid s \in \mathcal{S}\}$, $\mathcal{L}_\gamma$ is as per the André/Bruck-Bose construction, and incidence is induced.

To show that γ is a translation plane we need only determine that $\mathcal{P}_\gamma$ is equal to the set of points of $(\Sigma \setminus \Sigma') \cup \mathcal{S}'$. The elements of $\mathcal{S}'$ are common to both sets. Now $\mathcal{S}$ is a spread so each point of $\Sigma \setminus \Sigma'$ is covered by an element of $\mathcal{S} \setminus \mathcal{S}'$ and, if any element $s \in \mathcal{S} \setminus \mathcal{S}'$ were to meet Σ in a line, it must meet Σ' in a point, a contradiction. So $\mathcal{P}_\gamma$ contains the set of points of $\Sigma \setminus \Sigma'$. Also, each element of $\mathcal{S}$ must meet Σ in at least a point, by Grassmann's Dimension Theorem (Theorem 2.2.1), so the set of points of $(\Sigma \setminus \Sigma') \cup \mathcal{S}'$ contains $\mathcal{P}_\gamma$. See Figure 3.2.

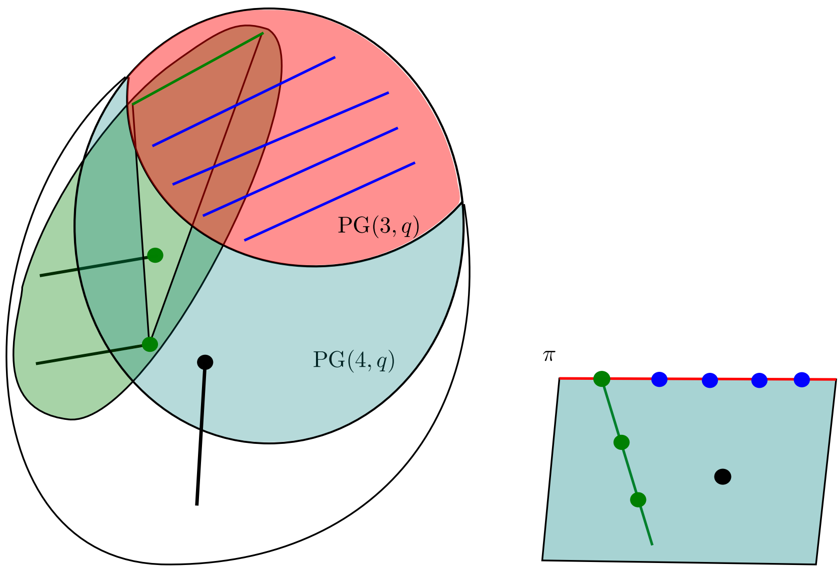


Figure 3.2 – Restriction of a normal spread in $\mathrm{PG}(3,q)$ to the André/Bruck-Bose construction on two spread elements.

Therefore, γ is a translation plane, and there is a one-to-one correspondence between the points of π and the points of γ. Now, we wish to show that the map taking each point to its corresponding point is a collineation, that is, that it preserves incidence. To do this we show that, for all $x, y \in \pi$, the line $\langle x \cap \Sigma, y \cap \Sigma \rangle$ contains $a \cap \Sigma$ in γ if and only if $a \in xy$ in π. In fact, as both planes have the same number of points in each line we need only show that if $a \in xy$ in π then $a \cap \Sigma \in \langle x \cap \Sigma, y \cap \Sigma \rangle$ in γ.

We know that Σ' is a line in both π and γ and that it contains the same points in both. Consider $x, y \in \mathcal{S}$ and let $M = \langle x, y \rangle$. As each line of π contains a point of Σ', we let y be an element of Σ'

without loss of generality. Let $\mathcal{S}|_M$ denote the spread of M. Thus, in π, the points of M are the elements of $\mathcal{S}|_M$.

The element of $\mathcal{L}_\gamma$ spanned by $x \cap \Sigma$ and $y \cap \Sigma$ is an e-space M'. As $x \cap \Sigma$ and $y \cap \Sigma$ are both in M, we know that M' is contained within M and, therefore, is equal to the e-space $M \cap \Sigma$. Now, each $(e-1)$-space in M must meet M' in at least a point. Therefore each element a of $\mathcal{S}|_M$ meets M' in a point. Note that $a \cap M' \in \Sigma$ and, therefore, $a \cap M' = a \cap \Sigma$. Therefore, if $a \in xy$ in π, we see that $a \in \langle x \cap \Sigma, y \cap \Sigma \rangle$ in γ, as required. □

So we see that the overlap between the Baer correspondence and the André/Bruck-Bose construction occurs exactly when we have a normal $(e-1)$-spread in $\mathrm{PG}(3e-1, q)$ or, equivalently, when we have a spread in $\mathrm{PG}(2e-1, q)$ that can be extended to a normal $(e-1)$-spread in $\mathrm{PG}(3e-1, q)$.

Corollary 3.2.3 (Bader and Lunardon [9])**.** *If an $(e-1)$-spread $\mathcal{S}$ of $\mathrm{PG}(en-1, q)$, with $n-1 > 2$, is normal, then for any two elements X, Y of $\mathcal{S}$, the elements of $\mathcal{S}$ in $\langle X, Y \rangle$ form a Desarguesian spread of $\langle X, Y \rangle$. We say this is the spread spanned by X and Y.*

Proof. Theorem 3.2.1 tells us that the spread elements of $\mathcal{S}$ correspond to the points of a projective space π with dimension $n-1$ and order q^e. Now π is Desarguesian because it has dimension greater than two [87] and therefore any plane $\Pi \in \pi$ must also be Desarguesian.

Let X and Y be any two elements of $\mathcal{S}$ and let the spread induced by $\mathcal{S}$ in $\Sigma' = \langle X, Y \rangle$ be denoted $\mathcal{S}'$. Let Z be a spread element outside of Σ' and let $\Sigma = \langle \Sigma', Z \rangle$. We know that restricting $\mathcal{S}$ to Σ gives a Desarguesian plane under the Baer correspondence. By Lemma 3.2.2, therefore, the plane constructed by applying the André/Bruck-Bose construction to $\mathcal{S}'$ is also Desarguesian. □

Therefore, non-Desarguesian spreads in $\mathrm{PG}(2e-1, q)$ do not extend to normal $(e-1)$-spreads in $\mathrm{PG}(en-1, q)$ where $n-1 > 2$.

Example 3.2.4 (Translation planes created from 2-spreads of $\mathrm{PG}(5, q)$)**.** *In* $\mathrm{PG}(5, q)$

Baer: *a normal line spread is equivalent to a Desarguesian plane of order q^2,*

André/Bruck-Bose: *the restriction of this normal line spread to a solid can be used to construct the same Desarguesian plane, and*

André/Bruck-Bose: *a plane spread can be used to construct a translation plane of order q^3, by embedding* $\mathrm{PG}(5, q)$ *as a hyperplane in* $\mathrm{PG}(6, q)$.

3.3 Creating spreads from projective spaces

In the previous sections we constructed projective spaces from spreads in higher dimensional projective spaces, by both the André/Bruck-Bose construction and the Baer correspondence. We now construct spreads from the points of lower dimensional projective spaces by field reduction.

3.3.1 Segre's spread

Let ζ act on $\mathrm{PG}(en-1, q^e)$ by

$$\zeta((X_0, \ldots, X_{en})) \coloneqq (X_0^q, \ldots, X_{en}^q) = X^q.$$

So ζ fixes all subspaces of $\mathrm{PG}(en-1, q)$ and preserves incidence and type in $\mathrm{PG}(en-1, q^e)$. In fact, a d-space of $\mathrm{PG}(en-1, q^e)$ is fixed by ζ if and only if it is an extension of a d-space of $\mathrm{PG}(en-1, q)$ (see Section 2.2).

Lemma 3.3.1 (Segre [75], (Bader and Lunardon [9])). *There exists an $(n-1)$-space X in $\mathrm{PG}(en-1, q^e)$ such that X is disjoint from $\mathrm{PG}(en-1, q)$ and the set of $(n-1)$-spaces $\{X, X^q, X^{q^2}, \ldots, X^{q^{e-1}}\}$ are mututally disjoint.*

Theorem 3.3.2 (Segre [75], (Bader and Lunardon [9])). *Consider an $(n-1)$-space X in $\mathrm{PG}(en-1, q^e)$ such that X is disjoint from $\mathrm{PG}(en-1, q)$. Let P be a point of X and denote the span of $\{P, P^q, \ldots, P^{q^{e-1}}\}$ by $\hat{P}$. The set of $(e-1)$-spaces $\{\hat{P}_0, \ldots, \hat{P}_{\frac{q^n-1}{q-1}}\}$, where $P_i \in X$, forms a normal spread of $\mathrm{PG}(en-1, q)$.*

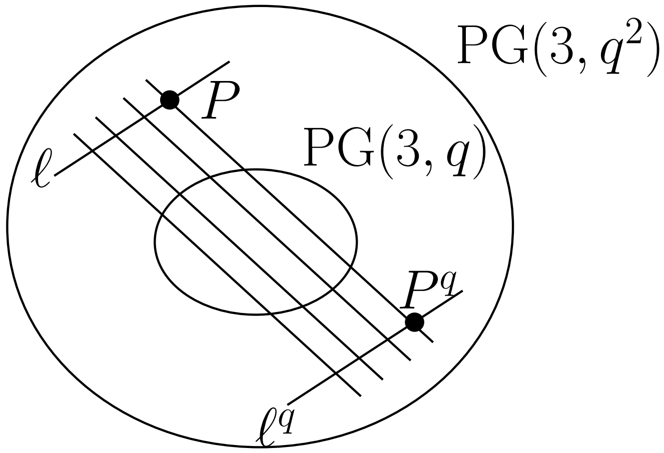
Proof. Suppose, by way of contradiction, that two of the $(e-1)$-spaces, $\hat{P}_i$ and $\hat{P}_j$, meet in a point R. The lines $\langle P_i, R\rangle$ and $\langle P_j, R\rangle$ are extensions of lines of $\mathrm{PG}(en-1, q)$. As such, the plane π containing P_i, P_j and R spans a plane in $\mathrm{PG}(en-1, q)$ and all the lines of π must meet $\mathrm{PG}(en-1, q)$ in a line. But the line $\langle P_i, P_j\rangle$ is contained in X, which is disjoint from $\mathrm{PG}(en-1, q)$. Therefore, the set of $(e-1)$-spaces are mutually disjoint and form a spread. Consider the span of two $(e-1)$-spaces $\langle \hat{P}_i, \hat{P}_j\rangle$. For all P_k in the line $\langle P_i, P_j\rangle$, the $(e-1)$-space $\hat{P}_k$ is contained in $\langle \hat{P}_i, \hat{P}_j\rangle$, and so the spread is normal. □

We will call this spread *Segre's spread.*

Example 3.3.3 (Segre's spread in $\mathrm{PG}(3, q)$ [75]). *In this example we will construct a spread in $\mathrm{PG}(3, q)$ from lines in $\mathrm{PG}(3, q^2)$.*

Let ℓ be a line of $\mathrm{PG}(3, q^2)$ disjoint from $\mathrm{PG}(3, q)$. Then ℓ and ℓ^q are disjoint. Let P and R be points of ℓ. The line PP^q is fixed by ζ and therefore meets $\mathrm{PG}(3, q)$ in a line. Suppose PP^q and RR^q meet in a point Y, by way of contradiction. Then PP^q and RR^q span a plane. This plane contains the lines $PR = \ell$ and $P^qR^q = \ell^q$ and therefore ℓ^q and ℓ must meet in a point, which is a contradiction. Thus, the set of lines $\{PP^q \mid P \in \ell\}$ are mutually disjoint and all meet $\mathrm{PG}(3, q)$ in a line. That is, they cover $(q^2+1)(q+1) = q^3+q^2+q+1$ points of $\mathrm{PG}(3, q)$ and, therefore, form a spread. This is illustrated in Figure 3.3.

Figure 3.3 – Segre's spread.



3.3.2 Field reduction

Let $\mathrm{PG}(n-1, q^e)$ be a projective space over the field $\mathrm{GF}(q^e)$. The points in $\mathrm{PG}(n-1, q^e)$ are 1-dimensional vector spaces over $\mathrm{GF}(q^e)$. These spaces can also be considered as e-dimensional spaces over $\mathrm{GF}(q)$, that is, as $(e-1)$-spaces in $\mathrm{PG}(en-1, q)$. The image of $\mathrm{PG}(n-1, q^e)$ in $\mathrm{PG}(en-1, q)$ by this process is called *field reduction*.

Example 3.3.4. *Consider the space* $\mathrm{PG}(1, q^2)$ *and let* $\{1, \alpha\}$ *be a basis for* $\mathrm{GF}(q^2)$*. Let* (x, y) *be a point of* $\mathrm{PG}(1, q^2)$ *such that* $x = x_1 + \alpha x_2$ *and* $y = y_1 + \alpha y_2$*. Define a map* θ *such that*

$$\theta : (x, y) \mapsto (x_1, x_2, y_1, y_2).$$

Next, consider the point $(1, 0) \equiv (\rho, 0)$ *where* $\rho \in \mathrm{GF}(q^2)$*. Then*

$$\theta((1, 0)) = (1, 0, 0, 0)$$
$$\theta((\alpha, 0)) = (0, 1, 0, 0)$$

and we see that the point $(1, 0) \in \mathrm{PG}(1, q^2)$ *is mapped to the line* $\{(1, \lambda, 0, 0) \mid \lambda \in \mathrm{GF}(q)\} \cup \{(0, 1, 0, 0)\} \in \mathrm{PG}(3, q)$*.*

Let $\{1, \alpha, \ldots, \alpha^{e-1}\}$ be a basis for $\mathrm{GF}(q^e)$. In general, define $\hat{\theta} : \mathrm{GF}(q^e) \to \mathrm{GF}(q)^e$ such that, if $x = x_0 + x_1\alpha + \cdots + x_{e-1}\alpha^{e-1}$ then

$$\hat{\theta}(x) = (x_0, x_1, \ldots, x_{e-1}).$$

We then define $\theta : \mathrm{PG}(n-1, q^e) \to \mathrm{PG}(en-1, q)$ such that $\theta((y_0, \ldots, y_{n-1}))$ is the span of the set of $e-1$ points

$$\{(\hat{\theta}(\alpha^i y_0), \ldots, \hat{\theta}(\alpha^i y_{n-1})) \mid 0 \le i \le e-1\}.$$

Then $\theta((y_0, \ldots, y_{n-1}))$ is the field reduction of $(y_0, \ldots, y_{n-1})$ into $\mathrm{PG}(en-1, q)$.

Theorem 3.3.5 (Shult and Thas [78] pg. 426)**.** *Let* X *and* Y *be subspaces of* $\mathrm{PG}(n-1, q^e)$*. Then*

$$\theta(\langle X, Y \rangle) = \langle \theta(X), \theta(Y) \rangle,$$

and

$$\theta(X \cap Y) = \theta(X) \cap \theta(Y).$$

In order to use field reduction we first prove a useful lemma.

Lemma 3.3.6. *Let* $\{1, \alpha, \dots, \alpha^{e-1}\}$ *be a basis for* $\mathrm{GF}(q^e)$ *such that* $\alpha^e = k_0 + k_1\alpha + \cdots + k_{e-1}\alpha^{e-1}$. *Denote the coefficient of* α^i *for* $y \in \mathrm{GF}(q^e)$ *by* $\sigma_i(y)$ *and suppose* $y = y_0 + y_1\alpha + \cdots + y_{e-1}\alpha^{e-1}$, *so* $\sigma_i(y) = y_i$. *Then, for* $m \le e-1$,

$$\sigma_s(\alpha^{e+m}) = \begin{cases} k_{s-m} + \sum_{j=0}^{m-1} k_{e-m+j}\sigma_s(\alpha^{e+j}) & \text{, when } m \le s, \text{ and} \\ \sum_{j=0}^{m-1} k_{e-m+j}\sigma_s(\alpha^{e+j}) & \text{, when } m > s, \end{cases}$$

and

$$\sigma_r(\alpha^i y) = \sum_{j=0}^{e-1} y_j \sigma_r(\alpha^{i+j}).$$

Proof. We write

$$\alpha^{e+m} = k_0\alpha^m + \cdots + k_{e-1}\alpha^{e+m-1},$$

and therefore

$$\sigma_s(\alpha^{e+m}) = \sigma_s(k_0\alpha^m) + \cdots + \sigma_s(k_{e-1}\alpha^{e+m-1}).$$

For all α^i such that $i < e$, the only term for which $\sigma_s(k_{i-m}\alpha^i)$ is not equal to zero is for $i = s$, in which case $\sigma_s(k_{s-m}\alpha^s) = k_{s-m}$. The remaining cases $i \ge e$ each have the form $k_{e-m+j}\alpha^{e+j}$, where $0 \le j \le m-1$ and we note that $\sigma_s(k_{e-m+j}\alpha^{e+j}) = k_{e-m+j}\sigma_s(\alpha^{e+j})$.

For the second equation, note that

$$\alpha^i y = y_0\alpha^i + y_1\alpha\alpha^i + \cdots + y_{e-1}\alpha^{e-1}\alpha^i,$$

and recall that $y_j \in \mathrm{GF}(q)$ so $\sigma_r(y_j\alpha^k) = y_j\sigma_r(\alpha^k)$. □

Theorem 3.3.7 (Segre [75])**.** *The field reduction of* $\mathrm{PG}(n-1, q^e)$ *into* $\mathrm{PG}(en-1, q)$ *is equivalent to Segre's spread.*

Proof. Let $\{1, \alpha, \dots, \alpha^{e-1}\}$ be a basis for $\mathrm{GF}(q^e)$ and, let $\alpha^e = k_0 + k_1\alpha + \cdots + k_{e-1}\alpha^{e-1}$, for $k_i \in \mathrm{GF}(q)$.

The $(n-1)$-space

$$\Pi = \begin{pmatrix} 1\ \mu_1 \cdots \mu_{e-1} & 0 & \cdots & 0 \\ 0 & 1\ \mu_1 \cdots \mu_{e-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1\ \mu \cdots \mu_{e-1} \end{pmatrix}$$

where

$$\mu_i = \frac{\alpha^{e-i} - \sum_{z=1}^{e-i-1} \alpha^z k_{i+z}}{k_0} \tag{3.1}$$

is a subspace of PG$(en-1,q^e)$.

Let $\delta : \text{PG}(n-1,q^e) \to \Pi$, such that

$(x_0, x_1, \dots, x_{n-1}) \mapsto (x_0, x\mu_1 x_0, \dots, \mu_{e-1}x_0, x_1, \mu x_1, \dots, \mu_{e-1}x_1, \dots, x_{n-1}, \mu_1 x_{n-1}, \dots, \mu_{e-1}x_{n-1})$.

Then δ gives a one-to-one correspondence between points of PG$(n-1,q^e)$ and Π.

For the remainder of this proof, we apply field reduction to an arbitrary point $P = (x_0, x_1, .., x_n)$ and show that $\delta(P)$ is in the extension, to PG$(en-1,q^e)$, of $\theta(P)$, the field reduction of P. Then, $\theta(P)$ will be the unique $(e-1)$-space containing $\delta(P), \delta(P)^q, \dots, \delta(P)^{q^{e-1}}$.

The field reduction of P is

$$\theta(P) = \begin{pmatrix} \sigma_0(x_0) & \sigma_1(x_0) & \cdots & \sigma_{e-1}(x_0) & \sigma_0(x_1) & \cdots & \sigma_{e-1}(x_1) & \cdots \\ \sigma_0(\alpha x_0) & \sigma_1(\alpha x_0) & \cdots & \sigma_{e-1}(\alpha x_0) & \sigma_0(\alpha x_1) & \cdots & \sigma_{e-1}(\alpha x_1) & \cdots \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ \sigma_0(\alpha^{e-1}x_0) & \sigma_1(\alpha^{e-1}x_0) & \cdots & \sigma_{e-1}(\alpha^{e-1}x_0) & \sigma_0(\alpha^{e-1}x_1) & \cdots & \sigma_{e-1}(\alpha^{e-1}x_1) & \cdots \end{pmatrix}.$$

Therefore every point in $\theta(P)$ has form

$$(\sum_{i=0}^{e-1} \lambda_i \sigma_0(\alpha^i x_0), \dots, \sum_{i=0}^{e-1} \lambda_i \sigma_{e-1}(\alpha^i x_0), \sum_{i=0}^{e-1} \lambda_i \sigma_0(\alpha^i x_1), \dots, \sum_{i=0}^{e-1} \lambda_i \sigma_{e-1}(\alpha^i x_1), \sum_{i=0}^{e-1} \lambda_i \sigma_0(\alpha^i x_2) \dots)$$

for some $\lambda_i \in \text{GF}(q)$. By allowing $\lambda_i \in \text{GF}(q^e)$, we extend these $(e-1)$-spaces into PG$(en-1,q^e)$.

We now choose $\lambda_i = \mu_i$ and show that

$$\sum_{i=0}^{e-1} \lambda_i \sigma_s(\alpha^i x_r) = \mu_s x_r$$

for all $0 \le r, s \le e-1$. That is, we will show that $\delta(P) \in \theta(P)$.

At this point, x_r is simply an element of GF(q^e). Therefore, to simplify notation, in the remainder of this proof, we let $y = y_0 + y_1\alpha + \cdots + y_{e-1}\alpha^{e-1}$ and prove that, for all $y \in \text{GF}(q^e)$,

$$\sum_{i=0}^{e-1} \lambda_i \sigma_s(\alpha^i y) = \mu_s y.$$

To do this we will show that the coefficient of $y_z \alpha^t$ is the same on both sides of the equation, for all $0 \le z, t \le e-1$.

To begin, we consider the right hand side of the equation: $\mu_s y$. By Equation 3.1, the coefficient of y_z in $\mu_s y$ is

$$\alpha^{e+(z-s)} - \sum_{j=1}^{e-s-1} k_{s+j}\alpha^{j+z}. \tag{3.2}$$

In order to determine the coefficient of $y_z\alpha^t$ we will consider the cases $z \ge s$ and $z < s$ separately.

We start with the case $z \ge s$, that is, $\alpha^{e+(z-s)}$ is not a basis element. The coefficient of α^t of $\alpha^{e+(z-s)}$, the first part of Equation 3.2, is

$$\sigma_t(\alpha^{e+(z-s)}) = k_{t-(z-s)} + \sum_{n=0}^{z-s-1} k_{e-(z-s)+n}\sigma_t(\alpha^{e+n}) \tag{3.3}$$

The second half of Equation 3.2, $\sum_{j=1}^{e-s-1} k_{s+j}\alpha^{j+z}$, can be split into one part made up of basis elements and another without any, giving

$$-\sum_{n=1}^{e-z-1} k_{s+n}\alpha^{n+z} - \sum_{n=e-z}^{e-s-1} k_{s+n}\alpha^{n+z},$$

which can be rewritten as

$$-\sum_{n=z+1}^{e-1} k_{s+n-z}\alpha^{n} - \sum_{n=0}^{z-s-1} k_{e-(z-s)+n}\alpha^{e+n}.$$

We take the α^t coefficients of these

$$-\sum_{n=z+1}^{e-1} k_{s+n-z}\sigma_t(\alpha^{n}) - \sum_{n=0}^{z-s-1} k_{e-(z-s)+n}\sigma_t(\alpha^{e+n}),$$

to get

$$\begin{cases} -k_{s+(t-z)} - \sum_{n=0}^{z-s-1} k_{e-(z-s)+n}\sigma_t(\alpha^{e+n}) & \text{if } t \geq z+1, \\ -\sum_{n=0}^{z-s-1} k_{e-(z-s)+n}\sigma_t(\alpha^{e+n}) & \text{otherwise.} \end{cases}$$

By joining this information with Equation 3.3 we determine that, for $z \geq s$,

$$\text{the coefficient of } x_z\alpha^t \text{ in } \mu_s x \text{ is } \begin{cases} 0 & \text{if } t \geq z+1, \\ k_{t-z+s} & \text{otherwise.} \end{cases}$$

Next, we consider the coefficient of $y_z\alpha^t$ in Equation 3.2 when $s > z$, that is, when $\alpha^{e+(z-s)}$ is a basis element.

The first part of Equation 3.2, $\alpha^{e+(z-s)}$, has a coefficient of α^t as 1 in the case $t = e - s + z$ ($\Rightarrow z = t + s - e$) and 0 otherwise.

The second part of Equation 3.2, $\sum_{j=1}^{e-s-1} k_{s+j}\alpha^{j+z}$, contributes a coefficient of α^t exactly when $z < t \leq e - s + z - 1$.

Thus, we now have a complete list of coefficients for $y_z\alpha^t$, for the right hand side of the equation.

$$\text{The coefficient of } y_z\alpha^t \text{ in } \mu_s x \text{ is } \begin{cases} 1 & \text{if } t = e-s+z \text{ and } z < s, \\ k_{s+t-z} & \text{if } t \leq z \text{ and } z-t \leq s \leq z, \\ -k_{s+t-z} & \text{if } z < t < e-s+z \text{ and } z < s, \\ 0 & \text{otherwise.} \end{cases}$$

We repeat the above process for $\sum_{i=0}^{e-1} \mu_i\sigma_s(\alpha^i y)$.

Noting that $\mu_0 = 1$, we see that the coefficient of y_z, in $\sum_{i=0}^{e-1} \mu_i\sigma_s(\alpha^i y)$, is

$$\sigma_s(\alpha^z) + \sum_{i=1}^{e-1} \mu_i\sigma_s(\alpha^{i+z}). \tag{3.4}$$

This can be separated out to give

$$\sigma_s(\alpha^z) + \sum_{i=1}^{e-1} \alpha^{e-i}\sigma_s(\alpha^{i+z}) - \sum_{i=1}^{e-1}\sum_{j=1}^{e-i-1} \alpha^j k_{i+j}\sigma_s(\alpha^{i+z}).$$

The only part of the above equation that can contribute a constant term, therefore giving a coefficient of α^0, is $\sigma_s(\alpha^z)$.

The coefficients of α^t, for $t > 0$, are

$$\sigma_s(\alpha^{e-t+z}) - \sum_{i=1}^{e-t-1} k_{i+t}\sigma_s(\alpha^{i+z}). \tag{3.5}$$

We now consider this over differing values of s, t, z.

If $z < t$ then

$$\text{the coefficient of } y_z\alpha^t \text{ is } \begin{cases} 1 & \text{if } s = e-(t-z) \\ -k_{s-z+t} & \text{if } z < s \leq e-t-1+z \\ 0 & \text{otherwise} \end{cases}$$

Next consider $z \geq t$. If $t = 0$, then the coefficient of α^t is k_0 when $s = z$ and 0 otherwise. If $t \neq 0$ then we separate out Equation 3.5 and apply Lemma 3.3.6 to get

$$\begin{aligned} k_{s-z-t} &+ \sum_{j=0}^{z-t-1} k_{e-(z-t)+j}\sigma_s(\alpha^{e+j}) \\ &- \sum_{i=1}^{e-z-1} k_{i+t}\sigma_s(\alpha^{i+z}) - \sum_{i=e-z}^{e-t-1} k_{i+t}\sigma_s(\alpha^{i+z}). \end{aligned}$$

By changing the summation indices on the last sum so that it cancels with the second sum we can simplify this to

$$k_{s-(z-t)} - \sum_{i=1}^{e-z-1} k_{i+t}\sigma_s(\alpha^{i+z}).$$

Finally, we consider the different possible values of s in relation to z and determine that

$$\text{the coefficient of } y_z\alpha^t \text{ is } \left\{ \begin{array}{ll} 0 & \text{if } s > z, \\ k_{s-(z-t)} & \text{if } z-t \leq s \leq z, \\ 0 & \text{otherwise.} \end{array} \right\}$$

This is the same result as determined for the lefthand side of the equation. Thus we have shown that the image of a point of $\mathrm{PG}(n-1, q^e)$, under field reduction, is the same $(e-1)$-space created by embedding an $(n-1)$-space in $\mathrm{PG}(en-1, q^e)$ and taking the span of a point with its conjugates. Thus, we have proved that the field reduction of $\mathrm{PG}(n-1, q^e)$ is equivalent to Segre's spread. □

Therefore, the field reduction of a projective space $\mathrm{PG}(n-1, q^e)$ is a normal $(e-1)$-spread in $\mathrm{PG}(en-1, q)$. Note that this is a trivial statement for $n = 2$.

3.4 Desarguesian spreads

In the previous sections of this chapter we left a few questions unanswered. Regarding the André/Bruck-Bose construction, we are yet to determine, geometrically, when a spread is Desarguesian. Regarding field reduction, we have not determined the geometric properties of the image of $\mathrm{PG}(1, q^e)$. These questions are the subject of this section, but first we will go through some necessary background.

A *regulus* in $\mathrm{PG}(2e-1, q)$, $q > 2$ is a set of $q+1$ pairwise disjoint $(e-1)$-spaces such that any line that meets three of them meets them all.

Let $\Sigma_1, \Sigma_2, \Sigma_3$ be three skew $(e-1)$-spaces in $\mathrm{PG}(2e-1, q)$, $q > 2$. Recall that a *transversal* is a line that meets all three of these $(e-1)$-spaces.

The following results for reguli and transversals are well known.

Lemma 3.4.1 (Hirschfeld and Thas [54], pg. 199)**.** *Any collection of three skew $(e-1)$-spaces $\Sigma_1, \Sigma_2, \Sigma_3$, in $\mathrm{PG}(2e-1, q)$, $q > 2$ defines a unique set of $(q^e-1)/(q-1)$ transversals of $\Sigma_1, \Sigma_2, \Sigma_3$.*

Proof. Let point P lie on Σ_1 and consider the e-spaces, $P \oplus \Sigma_2$ and $P \oplus \Sigma_3$. By Grassmann's Dimension Theorem (Theorem2.2.1), these e-spaces must meet in a subspace with dimension at least one. Suppose their intersection contains a plane. Then $\dim(P \oplus \Sigma_2 \oplus \Sigma_3) \leq 2e-2$, contradicting the fact that $P \oplus \Sigma_2 \oplus \Sigma_3$ contains the two disjoint $(e-1)$-spaces Σ_1 and Σ_2. Thus, for every point $P \in \Sigma_1$ there is a unique line through P that meets both Σ_2 and Σ_3. □

Theorem 3.4.2 (Hirschfeld and Thas [54], pg. 200)**.** *Any collection of three skew $(e-1)$-spaces $\Sigma_1, \Sigma_2, \Sigma_3$, in $\mathrm{PG}(2e-1, q)$, $q > 2$ defines a unique regulus.*

Proof. By Theorem 2.2.5 we need only consider the $(e-1)$-spaces $\Sigma_1 = [\mathrm{I}\,0]$, $\Sigma_2 = [0\,\mathrm{I}]$, and $\Sigma_3 = [\mathrm{I}\,\mathrm{I}]$.

For each $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_e)$, with $\lambda_i \in \mathrm{GF}(q)$, we consider the line

$$t_\lambda = \langle (0, 0, \ldots, 0, \lambda_1, \lambda_2, \ldots, \lambda_e), (\lambda_1, \lambda_2, \ldots, \lambda_e, 0, 0, \ldots, 0) \rangle.$$

These lines will pass through Σ_1 when $\mu = 0$, Σ_2 at the point $(0, 0, \ldots, 0, \lambda_1, \lambda_2, \ldots, \lambda_e)$, and Σ_3 when $\mu = 1$. Thus, they are transversals of $\Sigma_1, \Sigma_2, \Sigma_3$. Moreover, by Lemma 3.4.1, they are the unique set of $(q^e-1)/(q-1)$ transversals for $\Sigma_1, \Sigma_2, \Sigma_3$.

Each of these transversals will also pass through the $(e-1)$-spaces

$$X_\mu = \{[\mathrm{I}\,\mu\mathrm{I}]\}$$

for each $\mu \in \mathrm{GF}(q)$ and the set $\{X_\mu \mid \mu \in \mathrm{GF}(q)\} \cup \{\Sigma_2\}$ is a regulus.

By Lemma 3.4.1 these transversals are unique and so the regulus must also be unique. □

We call the unique regulus through three spaces $\Sigma_1, \Sigma_2, \Sigma_3$, the regulus *generated* by $\Sigma_1, \Sigma_2, \Sigma_3$ and denote it $\mathcal{R}(\Sigma_1, \Sigma_2, \Sigma_3)$.

Our work so far has been leading to the following definition.

A spread is called *regular* if it contains the regulus generated by any three spread elements. An $(e-1)$-spread in $\mathrm{PG}(en-1,q)$ is called *regulus closed* if the spread it induces on the span of any two of its elements is regular.

Every regulus-closed spread is, therefore, defined to be normal.

Theorem 3.4.3 (Bruck [21] Theorem 5.3)**.** *The spread formed in* $\mathrm{PG}(2e-1,q)$ *by the field reduction of* $\mathrm{PG}(1,q^e)$ *is regular.*

Proof. This proof is directly from the field reduction of $\mathrm{PG}(1,q^e)$. See Bruck [21] for a proof using Segre's spread construction. Let $\{1,\alpha,\ldots,\alpha^{e-1}\}$ be a basis for $\mathrm{GF}(q^e)$ and when

$$y = y_1 + y_2\alpha + \cdots + y_e\alpha^{e-1}$$

denote

$$\hat{y} = (y_1, y_2, \ldots, y_e).$$

Let $(\hat{x},\hat{y})$ denote the vector of length $2e$, where the first e entries are given by $\hat{x}$ and the next e by $\hat{y}$. Then the field reduction of (x,y) is given by

$$\theta((x,y)) = (\hat{x},\hat{y}) + \gamma_1(\hat{\alpha}\hat{x},\hat{\alpha}\hat{y}) + \cdots + \gamma_{e-1}(\hat{\alpha}^{e-1}\hat{x},\hat{\alpha}^{e-1}\hat{y}),$$

where $\gamma_i \in \mathrm{GF}(q)$. Note that if $\lambda \in \mathrm{GF}(q)$, then $\hat{\alpha}^i\hat{\lambda} = \lambda E_i$. So $\theta((1,0)) = [\mathrm{I}\,0]$, $\theta((0,1)) = [0\,\mathrm{I}]$, $\theta((1,1)) = [\mathrm{I}\,\mathrm{I}]$, which we will refer to as $\Sigma_1,\Sigma_2,\Sigma_3$ respectively, and $\theta((1,\mu)) = X_\mu$, where $\mu \in \mathrm{GF}(q)$. The X_μ are the elements of $\mathcal{R}(\Sigma_1,\Sigma_2,\Sigma_3)$ and they are also in the field reduction of $\mathrm{PG}(1,q^e)$, and thus we have proved that one regulus is contained within the spread.

Any other set of three points $(a_1,a_2),(b_1,b_2),(c_1,c_2)$, of $\mathrm{PG}(1,q^e)$, where $a_i,b_i,c_i \in \mathrm{GF}(q^e)$, satisfies the equation

$$(a_1,a_2) + (v_1 + v_2\alpha + \cdots + v_e\alpha^{e-1})(b_1,b_2) = \rho_1(c_1,c_2),$$

for some $v_i \in \mathrm{GF}(q)$, and defines a subline

$$\{(b_1,b_2)\} \cup \{(a_1,a_2) + \lambda(v_1 + v_2\alpha + \cdots + v_e\alpha^{e-1})(b_1,b_2) \mid \lambda \in \mathrm{GF}(q)\}.$$

Thus the map taking $(a_1,a_2),(b_1,b_2),(c_1,c_2)$ to $(1,0),(0,1),(1,1)$ takes the rest of the subline to $(1,\lambda)$, where $\lambda \in \mathrm{GF}(q)$.

This means that, in the field reduced setting, lines of the form

$$t_i = [\mathrm{A}_1\,\mathrm{A}_2]_i + \lambda\left(v_1[\mathrm{B}_1\,\mathrm{B}_2]_i + v_2[\mathrm{B}_1\,\mathrm{B}_2]_{i+1} + \cdots + v_e[\mathrm{B}_1\,\mathrm{B}_2]_{i+e-1}\right),$$

with subscript addition modulo e, will meet each of $[\mathrm{A}_1\,\mathrm{A}_2],[\mathrm{B}_1\,\mathrm{B}_2]$ and $[\mathrm{C}_1\,\mathrm{C}_2]$ and the field reduction of the subline defined by $(a_1,a_2),(b_1,b_2)$, and (c_1,c_2). □

The field reduction of a line gives a regular spread. Therefore, the field reduction of a projective space gives a normal spread that generates a regular spread in the space spanned by any two of its elements.

We can embed $\mathrm{PG}(2e-1,q)$ in $\mathrm{PG}(2e,q)$ and use the André/Bruck-Bose construction to construct a plane of order q^e. We now wish to show that this plane is Desarguesian if and only if the spread is regular.

Theorem 3.4.4 (Bruck and Bose [23] pg. 164)**.** *A spread of* $\mathrm{PG}(n,q)$*,* $q>2$*, is regular if and only if it is Desarguesian.*

Proof. We start with a regular spread and show that the translation plane it describes is Desarguesian. Without loss of generality, consider a regular spread containing $A=[\mathrm{I}\,0], B=[0\,\mathrm{I}], C=[\mathrm{I}\,\mathrm{I}]$. The transversals joining A,B,C, as defined earlier, have equation $T_\mu=\lambda a_\mu+a_\mu L$, where $B=\{aL \mid a\in A\}$, $\lambda\in\mathrm{GF}(q)$. So the remaining regulus elements of $\mathcal{R}(A,B,C)$ are defined by the linear transformations $\lambda\mathrm{I}$ and have equation $J(\lambda)=\lambda A+B$, $\lambda\in\mathrm{GF}(q)$.

Every equivalent spreadset $\mathcal{C}^*$ must also contain $0,\mathrm{I}$ and therefore $\lambda\mathrm{I}\in\mathcal{C}^*$. Let $T,S\in\mathcal{C}$ such that $T\neq S$ and let $\mathcal{C}^*=(T-S)^{-1}(\mathcal{C}-S)$. Therefore, for each $\lambda\in\mathrm{GF}(q)$ there exists some $X\in\mathcal{C}$ such that $(T-S)^{-1}(X-S)=\lambda\mathrm{I}$. We rearrange this to get $X=(1-\lambda)S+\lambda T$. We choose S to be zero and note that $\mathcal{C}$ is closed under scalar multiplication. Now $q\neq 2$, and therefore we take $\lambda=\omega(1-\lambda)$ where $\omega\in\mathrm{GF}(q)$, $\omega\neq 1$. Because $\omega S\in\mathcal{C}$, $\mathcal{C}$ must contain $(1-\lambda)(\omega S)+\lambda T=\lambda(S+T)$, for all $S\neq T$, and is closed under addition. This proof did not rely on any information regarding the spreadset chosen so we know that all the spreadsets of $\mathcal{S}$ are closed under addition.

Next we show that $\mathcal{C}$ is closed under inverses by taking $\mathcal{C}^*=\mathcal{C}^{-1}$. Let $\mathrm{I},Y,Z\in\mathcal{C}$ such that $\mathrm{I}\neq Y, \mathrm{I}-Y=Z$. Then $W=\mathrm{I}+Z^{-1}\in\mathcal{C}^*$. Now $\mathrm{I}WZ=Z+I=Y$ so $W=YZ^{-1}$ and, as $W\neq 0$, $W^{-1}\in\mathcal{C}^*$. But $W^{-1}=ZY^{-1}=I-Y^{-1}$ and thus $Y^{-1}\in\mathcal{C}$.

By Theorem 3.1.5 we know that the plane created by a spreadset that is closed under addition and inversion is Desarguesian.

Conversely, let $\mathcal{S}$ be Desarguesian. Then $\mathcal{C}$ is closed under addition and multiplication, forming the field $\mathrm{GF}(q^e)$, and $\mathcal{S}$ is isomorphic to the spread containing the elements

- $S_M=\{(x,xM)\mid \forall\, x\in V(2n,q)\}$, $M\in\mathcal{C}$, and
- $S_\infty=\{(0,x)\mid \forall\, x\in V(2n,q)\}$.

This is the same spread as that generated by the field reduction of a line and therefore, by Theorem 3.4.3, is regular. □

Corollary 3.4.5 (Bader and Lunardon [9] pg. 25)**.** *If an* $(e-1)$*-spread* $\mathcal{S}$ *of* $\mathrm{PG}(3e-1,q)$ *is normal then the spread spanned by any two of its elements is Desarguesian.*

Proof. Let $X,Y\in\mathcal{S}$ and let $\mathcal{S}'$ be the restriction of $\mathcal{S}$ to $\Sigma'=\langle X,Y\rangle$. Suppose the translation plane γ, created by applying the André/Bruck-Bose construction to $\mathcal{S}'$, is not Desarguesian. By Lemma 3.2.2, γ is unchanged regardless of which $(2e-1)$-subspace we use for the André/Bruck-Bose construction, so $\mathcal{S}$ cannot contain any Desarguesian subspreads. Also, $\mathcal{S}'$ cannot be contained in any $(e-1)$-spread of $\mathrm{PG}(3e-1,q)$ that also contains a Desarguesian subspread.

Let $\mathcal{R}$ be a regulus-closed $(e-1)$-spread of $\mathrm{PG}(3e-1,q)$. We can choose $\mathcal{R}$ to contain X and Y by Theorem 2.2.5 and we let $\mathcal{R}'$ be the spread induced by $\mathcal{R}$ in Σ'. Note that $\mathcal{R}'$ is Desarguesian, by Theorem 3.4.4. Because $\mathcal{R}$ is normal, we can replace $\mathcal{R}'$ by $\mathcal{S}'$ to give a new normal spread $\hat{\mathcal{R}}$. But, for any spread element $Z \in \hat{\mathcal{R}} \setminus \mathcal{S}'$, the spread induced in $\langle Z, X \rangle$ by $\hat{\mathcal{R}}$ is the same as the spread induced in $\langle Z, X \rangle$ by $\mathcal{R}$ and is, therefore, Desarguesian. □

In summary, by Theorem 3.2.1 and Theorem 3.4.4, the following are equivalent conditions on an $(e-1)$-spread $\mathcal{S}$ of $\mathrm{PG}(en-1, q)$, when $n-1 \geq 2$ and $q > 2$:

(a) $\mathcal{S}$ is normal,

(b) $\mathcal{S}$ is regulus-closed, and

(c) the induced spread in every $(2e-1)$-space spanned by two spread elements of $\mathcal{S}$ is Desarguesian.

Field reduction can only be applied to Desarguesian projective spaces and will always generate regulus-closed $(e-1)$-spreads. The Baer correspondence shows the equivalence of normal spreads and Desarguesian projective spaces. The André/Bruck-Bose construction is the only one of these methods that deals with non-Desarguesian spaces and it generates a non-Desarguesian plane for every spread of $\mathrm{PG}(2e-1, q)$ that is not regular.

Chapter 4

Spreads of $\mathrm{W}(5, q)$

This chapter is focused on computational work and gives the details of newly constructed spreads in $\mathrm{W}(5,5)$ and $\mathrm{W}(5,7)$ which, by the André/Bruck-Bose construction, correspond to translation planes of order 125 and 343. We also discuss the history of using computation to find spreads and go through computational methods of finding spreads and determining whether two spreads are equivalent. The information required to recreate the new spreads is contained in Appendices A and B.

4.1 A survey of past methods and results

From our work in Chapter 3 it is clear that spreads are natural objects to study in projective spaces and that they are useful for constructing planes.

Theorem 2.2.2 states that all finite projective spaces of dimension three or higher are coordinatised by fields. This orderliness does not apply to projective planes and there has been much research into the existence of projective planes that cannot be coordinatised by a field, that is, non-Desarguesian planes. In 1907, Veblen and MacLagan-Wedderburn published the construction of a non-Desargeusian plane of order 9 [86].

When the construction of non-Desarguesian planes from spreads was published, it led the way for many new translation planes to be created. Since then, there have been many papers published that contain new non-Desarguesian planes, and families of these planes, using spreads of higher dimensional spaces. The introduction of spreadsets as a way to describe and manipulate spreads aided the enumeration of spreads by making it easier to determine whether two spreads describe isomorphic translation planes.

Starting in 1982, with the paper *"Translation planes of order 16 admitting a Baer 4-group"*, [36] Dempwolff, in collaboration with various others, has published a series of papers containing computational methods and results for calculations of translation planes from spreads. Computation has formed an important part of this section of mathematical research because it is, for the time being, a search: a search for families of spreads that then give families of planes.

In 1983, Dempwolff and Reifart classified the eight translation planes of order 16 [37], in 1992 Czerwinski and Oakden classified the 21 translation planes of order 25 [33], and Dempwolff followed this up in 1994 by classifying the 7 translation planes of order 27 [35]. In 1995, Mathon and Royle computed the 1347 translation planes of order 49 [68] and Charnes and Dempwolff independently corroborated these results via a different computational method in 1998 [31].

A spread of $W(n, q)$ is called a *symplectic spread* and, because all the points of $PG(n, q)$ are also points of $W(n, q)$, it is also a spread of $PG(n, q)$.

"The Handbook of Finite Translation Planes" [56] contains most of the known symplectic spreads of $W(5, q)$, however, more recently the focus has been on constructing semifield spreads, that is, spreads corresponding to translation planes coordinatised by a semifield. At least one family of these newly constructed semifield spreads is symplectic, namely, the Lunardon-Marino-Polverino-Trombetti (LMPT) spreads [64]. The known families of symplectic spreads are listed in Table 4.1.

Table 4.1 – Known families of symplectic spreads. F = field, S = semifield, N = non-semifield.

Name	Type	Conditions on $W(5, q)$
Desarguesian	F	-
Gen. twisted field	S	q odd
Suetake/Hering	N	q odd
Kantor, Kantor-Williams	S,N	$q = 2^t$
LMPT	S	$q = p^6$, p prime

Semifield and symplectic spreads are particularly studied because their associated translation planes have special properties. In particular, two properties of note are that symplectic semifield spreads are related to commutative semifield planes [58], and that if a translation plane is associated with one symplectic spread, then all other spreads that give rise to that plane are also symplectic [60, 63].

The spreads of $W(5, q)$ are classified for $q \leq 4$, giving translation planes of orders 8, 27 and 64. The only spread of $W(5, 2)$ is Desarguesian and this was proved by Hall, Swift and Walker in 1956 [45]. The non-Desarguesian symplectic translation planes are the generalised twisted field plane [5], which is a semifield plane, and the Hering plane [49], which is a non-semifield plane. They are both contained in infinite families of planes, corresponding to infinite families of spreads. The Hering plane was generalised to an infinite family by Suetake [79] and this family was extended, and proved to be symplectic, by Ball, Bamberg, Lavrauw and Penttila [12]. The generalised twisted field planes were proved to be symplectic by Bader, Kantor and Lunardon [8].

Now, we explore the spreads of $W(5, q)$, with q even. First, recall from Section 2.5 that, when q is even, $W(5, q)$ is isomorphic to $Q(6, q)$. Next, note that $Q(6, q)$ can be embedded as a hyperplane section in $Q^+(7, q)$.

Consider $Q(6, q)$ embedded as a hyperplane section in $Q^+(7, q)$ and let $\mathcal{S}$ be a spread of $Q^+(7, q)$.

The maximals of $\mathrm{Q}(6,q)$ are planes, so no elements of $\mathcal{S}$ can be contained in $\mathrm{Q}(6,q)$, and by Grassmann's Dimension Theorem (Theorem 2.2.1) all solids of $\mathrm{Q}^+(7,q)$ must meet a hyperplane in a plane or more. Therefore, each element of $\mathcal{S}$ meets $\mathrm{Q}(6,q)$ in a plane. This set of planes covers the points of $\mathrm{Q}(6,q)$ and is therefore a spread of both $\mathrm{Q}(6,q)$ and $\mathrm{W}(5,q)$.

Each plane of $\mathrm{Q}^+(7,q)$ is contained in one Latin and one Greek, therefore, the extension of a spread in $\mathrm{Q}(6,q)$, by taking a fixed solid type, forms a spread of $\mathrm{Q}^+(7,q)$. Finally, in $\mathrm{Q}^+(7,q)$ there exists a triality automorphism between Latins and Greeks and points. The images of an ovoid under triality are a spread of each type, and a spread of either type maps to an ovoid and another spread (see Remark 2.5.9).

That is, the question of finding spreads in $\mathrm{W}(5,q)$, q even, is equivalent to that of finding ovoids and spreads in $\mathrm{Q}^+(7,q)$.

Gunawardena proved, in 2000 [42], that there is only one ovoid of $\mathrm{Q}^+(7,4)$. This ovoid maps to two Desarguesian spreads in $\mathrm{Q}^+(7,4)$ under triality. By slicing these spreads, Kantor obtained six distinct spreads of $\mathrm{W}(5,4)$ [57], and these are listed in Tables 4.3 and 4.4. This ovoid exists for all q even and, therefore, Kantor's six spreads of $\mathrm{W}(5,4)$ generalise to spreads of $\mathrm{W}(5,q)$, for any even $q \geq 4$.

Table 4.2 – Spreads of $\mathrm{W}(5,3)$.

Name	Stabiliser	Type
Desarguesian	$\mathrm{PSL}(2,27) : C_6$	F
Gen. twisted	$C_3^3 : (C_{13} : C_6)$	S
Hering/Suetake	$\mathrm{PSL}(2,13)$	N

Table 4.3 – Spreads of $\mathrm{W}(5,4)$ induced by one of the spreads of $\mathrm{Q}^+(7,4)$.

Name	Order of stabiliser	Orbit lengths	Type
Desarguesian	$\mathrm{PSL}(2,27) : C_3$	65	F
Kantor	$C_2^2 \times (C_2^4 : C_3)$	64.1	S
Kantor	$C_5 \times (C_{13} : C_3)$	65	N
Kantor	$(C_{63} : C_3) : C_2$	63.2	N

Table 4.4 – Spreads of $\mathrm{W}(5,4)$ induced by one of the spreads of $\mathrm{Q}^+(7,4)$.

Name	Stabiliser	Orbit lengths	Type
Kantor	$((C_7 : C_3) : C_2 \times S_3$	42.21.2	N
Kantor	$(C_{13} : C_4) : C_3$	52.13	N

4.2 Methods

4.2.1 Preliminary theory and notation

The notation introduced in this section will be used throughout the rest of this chapter.

Let G denote the similarity group of $W := \mathrm{W}(2n-1,q)$ and let $\mathcal{S}$ be a spread of W. Then, let $|G_{\mathcal{S}}| = q_1^{\alpha_1} \dots q_m^{\alpha_m}$ denote the unique prime decomposition of $|G_{\mathcal{S}}|$. By Cauchy's Theorem, for each i, there exists an element $g_i \in G_{\mathcal{S}}$ such that $|\langle g_i \rangle| = q_i$. Note that, for all i, $\langle g_i \rangle \leq G$ and $q_i \mid |G|$.

Let $\{p_1, \dots, p_t\}$ be the set of all primes dividing $|G|$ and suppose there are s conjugacy classes of subgroups of order p_i. To find all spreads whose stabiliser has order divisible by p_i we take representatives $\{\langle h_1 \rangle, \dots, \langle h_s \rangle\}$ of the conjugacy classes of subgroups of order p_i, and find all spreads fixed by each $\langle h_j \rangle$. Any remaining spreads of W must have stabilisers whose order is not divisible by p_i. Therefore, if we follow this process for each p_i, then any spread that remains undiscovered must have a trivial stabiliser.

Let h be a representative of a conjugacy class of subgroups of order p. There are several computational methods that can be used to generate all spreads fixed by $H = \langle h \rangle$. In the following sections let $\mathcal{O}_H$ denote the orbits of H on $(e-1)$-spaces and let $\hat{\mathcal{O}}_H$ denote the subset of $\mathcal{O}_H$ containing only those orbits that are partial spreads.

4.2.2 Symmetry breaking

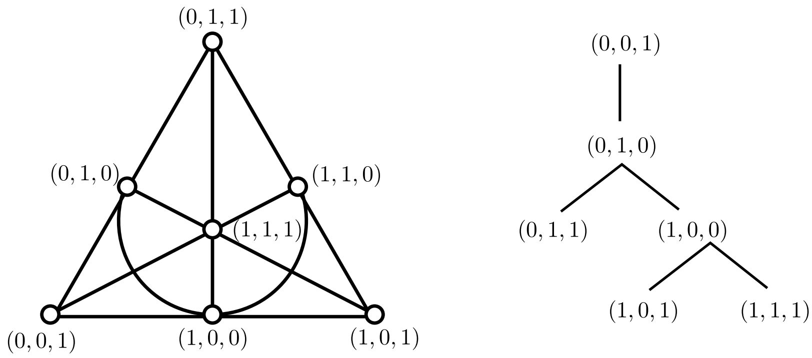
The symmetry of Desarguesian projective spaces can be used to our advantage when searching for spreads. We will go through a small example of symmetry breaking, before providing a full explanation.

Example 4.2.1 (Hyperovals in $\mathrm{PG}(2,q)$)**.** *Suppose we wish to find all the non-equivalent hyperovals in the Fano plane. There exists a collineation mapping any pair of points of the Fano plane to any other pair, so we may choose two points* $(0,0,1)$ *and* $(0,1,0)$ *to be our starter set, without loss of generality. Suppose we wish to choose a third point. Any 3 non-collinear points can be mapped to any other set of 3 non-collinear points, by Theorem 2.2.4, so we now have two options: first, the point* $(0,1,1)$ *collinear with* $(0,0,1)$ *and* $(0,1,0)$ *and second, any other point.*

Thus, any set of three points is either a line, and is equivalent to $\{(0,0,1),(0,1,0),(0,1,1)\}$ *or is an oval, and is equivalent to* $\{(0,0,1),(0,1,0),(1,0,0)\}$*. A line cannot be extended to a hyperoval so we only continue the search down the oval branch. The remaining points fall into two classes: the points that lie on a line joining two points of the oval, and the point* $(1,1,1)$*. So all hyperovals are equivalent to the hyperoval* $\{(0,0,1),(0,1,0),(1,0,0),(1,1,1)\}$ *and our search is complete. The search tree is given in Figure 4.1.*

This method of using group symmetry can be used to find many objects and we need not be restricted to acting on one element at a time, but instead can slightly adapt the method for orbits of elements.

Figure 4.1 – Finding hyperovals in the Fano Plane



Let $N_G(H)$ be the normaliser of H in G and suppose we wish to find all spreads fixed by H, that is, all spreads built up from the orbits of H. If $N_G(H)$ acts transitively on $\hat{\mathcal{O}}_H$ then, without loss of generality, we may start by choosing one partial spread orbit O_1 to build the rest of our spread around because all spreads can be mapped, under the normaliser, to a spread containing O_1. Let $\hat{\mathcal{O}}_H^*$ be the subset of $\hat{\mathcal{O}}_H$ comprising of the orbits disjoint from O_1 and let $N_G(H)_{O_1}$ be the stabiliser of O_1. If $N_G(H)_{O_1}$ is transitive on $\hat{\mathcal{O}}_H^*$ then we may choose another orbit O_2, without loss of generality. That is, each pair of two orbits that can be contained in a spread is equivalent to $\{O_1, O_2\}$. We continue this process.

At some point we will no longer be able to choose another orbit without loss of generality. Then, we may attempt to solve directly from our single chosen set (see Section 4.2.3), or we can build up a tree of starter sets.

We may use the solutions from one starter set to aid in finding all spreads containing another starter set. Suppose we find all spreads containing the orbits $\mathcal{O}_3 = \{O_1, O_2, O_3\}$. Then, when searching for all spreads containing $\mathcal{O}_j = \{O_1, O_2, O_j\}$, we may not only exclude those spreads containing O_3 but also every set $\{O_1^\omega, O_2^\omega, O_3^\omega\}$, for $\omega \in G$.

4.2.3 Linear programming

Suppose we have chosen a starter set $\mathcal{O}$ and wish to find all spreads, fixed by H, containing $\mathcal{O}$. Let O_i denote the i^{th} element of $\hat{\mathcal{O}}_H$ and let P_j denote the j^{th} point of W.

We create a matrix $A = (a_{ij})$ such that $a_{ij} = k$ when P_j lies in k planes of O_i. Then, we let x be the orbit inclusion vector for our spread and solve

$$xA = [1, 1, \ldots, 1], \text{ such that } x_i \in \{0, 1\}.$$

with the condition that

$$x_i = 1, \forall\, O_i \in \mathcal{O}.$$

For each solution $\hat{x}$, we add the constraint that $x\hat{x}^T < \mathrm{Sum}(\hat{x})$ before resuming the search. That is, no new spread can contain exactly the same set of orbits as the one just found.

In addition to this, we use a method developed by Royle [16], to deal with computationally heavy cases. This method is described below.

Suppose we have found t inequivalent spreads: $\{\mathcal{S}_0, \ldots, \mathcal{S}_t\}$. For each $\mathcal{S}_i$, and spread $\mathcal{R} \neq \mathcal{S}_i$, let $m_{\mathcal{R},i}$ denote the number of orbits in the intersection of $\mathcal{S}_i$ and $\mathcal{R}$. We maximise $m_{\mathcal{R},i}$ across all spreads $\mathcal{R} \neq \mathcal{S}_i$, denote this maximum M_0, and find all spreads that intersect $\mathcal{S}_i$ in M_0 orbits.

Thus, if a spread meets $\mathcal{S}_i$ in more than M_0 orbits, it's equal to $\mathcal{S}_i$. We repeat the above process for M_1, this time with the condition that $m_{\mathcal{R},i} < M_0$, so that if a spread meets $\mathcal{S}_i$ in more than M_1 orbits then it is either $\mathcal{S}_i$, or one of the spreads that meets $\mathcal{S}_i$ in M_0 orbits. We continue this process, for $m_j < m_{j-1}$ until $m_j < M$, for a specified M. Thus, we know all spreads that meet $\mathcal{S}_i$ in M or more orbits.

In our new search for spreads we add the constraint: $x\hat{x}^T < M$, for each spread we find. If we find a new inequivalent spread we must repeat the original process to find all the spreads that meet the new spread in more than M orbits.

After having found all the solutions containing our starter set $\mathcal{O}$, for a certain set of conditions on x_i, for all future starter sets we add the constraint that $\mathcal{O}^\omega$ cannot be contained in the spread, for all ω in the similarity group.

4.2.4 Invariants

Many of the spreads calculated by the methods above will be equivalent under the similarity group and it is essential that we can determine whether two spreads are equivalent. The simplest method, conceptually, to determine whether two spreads are equivalent is to search in the automorphism group of $\mathrm{W}(2n-1, q)$ for an element that maps between them. This is painfully slow and the fewer times done, the better. If two spreads have non-isomorphic stabilisers in the automorphism group then they cannot be equivalent. Thus, we need only test equivalence for spreads with isomorphic stabilisers. If two spreads do have isomorphic stabilisers then we search for an isomorphism between the spreads in the normaliser of one of the stabilisers.

If, however, two spreads have the same stabiliser and neither can be mapped to the other by elements of the normaliser, there are some more complicated ways to test for equivalence that we will now explore. For more details on the following methods, and for proofs, see Charnes [30].

Let p be an odd prime. We say that a is a *quadratic residue* modulo p if there exists some x such that $x^2 \equiv a \mod p$. Otherwise we say that a is a *quadratic non-residue* modulo p.

Let p be an odd prime number. The *Legendre symbol* is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \mod p \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0 \mod p \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

Let $\mathcal{S} = \{x_0, \ldots, x_{q^n}\}$ be a spreadset. Define

$$[x] = \left(\frac{\det x}{q}\right)$$

Then, define $Q = (a_{i,j})$ where $(a_{i,j})$ is given by

$$a_{i,j} = \left|\sum_{k=0}^{q^n} [x_i - x_k][x_j - x_k] + 1\right|, 0 \leq i, j \leq q^n$$

$$a_{i,q^n+1} = a_{q^n+1,i} = \left|\sum_{k=0}^{q^n} [x_i - x_k]\right|, 0 \leq i \leq q^n$$

$$a_{q^n+1,q^n+1} = q^n + 1.$$

We call Q the *fingerprint* of $\mathcal{S}$. Choosing a different coordinatisation of $\mathcal{S}$ simply permutes the elements of Q and therefore the multiset of the entries of Q is an invariant of equivalence.

Next, consider $\overline{Q} = (\overline{a_{i,j}})$ where

$$\overline{a_{i,j}} = \left|\sum_{k=0}^{q^n} [x_i - x_k][x_j - x_k]\right|, 0 \leq i, j \leq q^n.$$

We call the multiset of entries of $\overline{Q}$ the *weight* of $\mathcal{S}$. The weight is constant for all spreads that have the same spread element represented by $[\mathrm{I}\,0]$. Hence, we calculate the *weightvector* by finding $q^{n+1} + 1$ spreadsets of each spread, each with a different element mapped to $[\mathrm{I}\,0]$. The multiset of entries of the weightvector is an invariant of equivalence.

Finally, let

$$((x)) = \begin{cases} 1 & \text{if} \det x \neq 0 \\ 0 & \text{otherwise.} \end{cases}$$

Then $k(\mathcal{S}) = \sum_{i<j}((x_i + x_j))$ is called the *Kennzahl* of $\mathcal{S}$. The *Kennvector* has $\binom{q^n+1}{2}$ entries: one for each pair of points being mapped to the set $\{[\mathrm{I}, 0], [0, \mathrm{I}]\}$. The Kennvector is another invariant of equivalence.

To check equivalence we also use the `SmallestImageSet` function [62] in GAP [40]. This function takes a set and a permutation group as input and returns the smallest image (lexicographically) of the set under the permutation group.

4.3 Results for $\mathrm{W}(5, 5)$ and $\mathrm{W}(5, 7)$

The calculations contained in this section were carried out using Gurobi [43], a linear optimisation program, and GAP [40]. See Appendices A and B for information on how to construct these spreads in GAP.

Spreads in $\mathrm{W}(5, 5)$ contain 126 planes, chosen from 19656 planes in total. The similarity group of $\mathrm{W}(5, 5)$ has prime factors: $2, 3, 5, 7, 13$ and 31 but it can quickly be determined that the unique conjugacy class of elements of order 13 does not stabilise any spreads. The feasible conjugacy classes are listed in Table 4.5, along with their ATLAS notation [2]. ATLAS notation ranks conjugacy classes of the same order from largest centraliser to smallest centraliser, using letters to denote the position of a conjugacy class in this rank.

Table 4.5 – The feasible conjugacy classes and their centralisers in the similarity group G of $\mathrm{W}(5,5)$.

Conj. Classes	Centraliser order (in G)
31A	124
7A	126
5D	1875000
5E[1]	75000
3B	2268000
3C	86400
2B[2]	4536000
2C	2976000

All the spreads we computed in $\mathrm{W}(5,5)$ are contained in Table 4.6. Any remaining spreads in $\mathrm{W}(5,5)$ have a trivial stabiliser in the isometry group. As such, the automorphism groups of their translation planes contain only translations, and possibly an element of order 2 from the similarity group. We conducted a preliminary search for spreads stabilised by the conjugacy class 2B, which is in the similarity group but not isometry group, and did not find any such spreads, but this search has not been completed.

To the best of our knowledge the new translation planes we have constructed are the only known translation planes, along with the Luneburg-Tits family of translation planes in $\mathrm{W}(3,2^{2t+1})$, that are symplectic, non-semifield and have odd order over their kernel $\mathrm{GF}(q)$ (see *"The Handbook of Finite Translation Planes"* [56]). Although previous results seemed to indicate that such translation planes are rare, we consider this to be largely because many current computational searches for spreads are focused on finding semifield spreads.

Our computation of spreads in $\mathrm{W}(5,7)$ is far from complete, and has only been undertaken in an attempt to generalise the spreads in Table 4.6. While we have been unsuccessful in generalising those spreads so far, we have also discovered a new spread in $\mathrm{W}(5,7)$. The known spreads of $\mathrm{W}(5,7)$ are listed in Table 4.7.

The automorphism groups of the translation planes can be determined by the stabilisers of the spreads.

Theorem 4.3.1 ((Lüneburg [65], pg. 5)). *Let S be a non-Desarguesian spread of $\mathrm{PG}(n,q)$. The automorphism group of the translation plane constructed from S is given by the equation*

$$\mathrm{Aut}(P)_{\ell_\infty} = T \rtimes \Gamma L(n,q)_S,$$

where T is the translation group.

[1]This is one of two conjugacy classes with the same order centraliser in G.
[2]This element is contained in the similarity group of $\mathrm{W}(5,5)$ but not the isometry group.

Table 4.6 – The spreads we computed in W(5, 5). Conjugacy classes are listed in ATLAS notation. Orbit lengths of $X^a + Y^b$, for example, indicate a orbits of length X and b orbits of length Y.

Type	Factors	Stabiliser	Orbit lengths	#	Family
Field	all but 5E	$(\mathrm{PSL}(2,125) : C_2) : C_3$	126	1	Desarguesian
Semi	31A, 5D, 3C, 2C	$C_5^3 : (C_4 \times (C_{31} : C_3))$	$125 + 1$	1	Gen. twisted
Non-semi	31A, 3C, 2B, 2C	$C_2 \times ((C_{31} : C_3) \rtimes C_2)$	$124 + 2$	1	Suetake
Non-semi	7A, 2B	D_{14}	14^9	2	-
Non-semi	5E,3B, 2B	D_{30}	$30^4 + 6$	1	-
Non-semi	5E, 2C	C_{10}	$10^{12} + 2^2 + 1^2$	1	-
Non-semi	3B, 2B	D_{18}	18^7	1	-
Non-semi	3C, 2C	A_4	$12^8 + 6 + 4^6$	1	-
Non-semi	3C, 2C	C_6	$6^{20} + 2^2 + 1^2$	1	-

Table 4.7 – The spreads we computed in W(5, 7). Orbit lengths of $X^a + Y^b$, for example, indicate a orbits of length X and b orbits of length Y.

Type	Stabiliser	Orbit lengths	#	Family
Field	$\mathrm{PSL}(2,343)$	344	1	Desarguesian
Semi	$C_7^3 : ((C_{171} : C_3) : C_2)$	343 + 1	1	Gen. twisted
Non-semi	$(C_{171} : C_3) : C_2$	342 + 2	1	Suetake
Non-semi	$C_2 \times ((C_{19} : C_3) : C_2)$	228 + 76 + 38 + 2	1	-

Chapter 5

Pseudo-ovals in various representations

Psuedo-ovals are a generalisation of ovals to higher dimensional projective spaces and in this chapter we consider the open question of the existence of non-classical pseudo-ovals. We survey the work of Casse, Thas and Wild [29], and provide a new avenue for determining whether a pseudo-oval is classical. In addition to discussing the general case, we also consider the restriction of the problem to the existence of non-classical pseudo-ovals in the elliptic quadric $\mathrm{Q}^-(5,q)$.

5.1 Introduction and definitions

An *egg* $\mathcal{E}_{n,m}$ of $\mathrm{PG}(2n+m-1,q)$ is a set of q^m+1 $(n-1)$-spaces such that

- any three span a $(3n-1)$-space, and
- for all $X \in \mathcal{E}_{n,m}$ there is an $(n+m-1)$-dimensional space containing X that is skew to all the other elements of $\mathcal{E}_{n,m}$, called the *tangent space* at X.

If $n=m$ we refer to $\mathcal{E}_{n,n}$ as a pseudo-oval.

Example 5.1.1. *An oval is a pseudo-oval* $\mathcal{E}_{1,1}$ *in* $\mathrm{PG}(2,q)$*. An ovoid in* $\mathrm{PG}(3,q)$ *is an example of an egg* $\mathcal{E}_{1,2}$ *that is not a pseudo-oval.*

One method of constructing pseudo-ovals is, as might be expected from their name, by using an oval $\mathcal{O}$ of $\mathrm{PG}(2,q^e)$. The field reduction θ of $\mathrm{PG}(2,q^e)$ to $\mathrm{PG}(3e-1,q)$ maps points to $(e-1)$-spaces and, hence, $\theta(\mathcal{O})$ is a set of q^e+1 $(e-1)$-spaces. In $\mathrm{PG}(2,q^e)$ any three points of $\mathcal{O}$ span the entire plane and this condition implies that any three elements of $\theta(\mathcal{O})$ must span the entire $(3e-1)$-space. In addition to this, each tangent line of $\mathcal{O}$ becomes a $(2e-1)$-space that contains one element of $\theta(\mathcal{O})$ and is disjoint from the others. That is, $\theta(\mathcal{O})$ is a pseudo-oval. This construction is due to Thas [80]. We will say that a pseudo-oval is *classical* if it is isomorphic to the field reduction of an oval and that it is a *pseudo-conic* if it is isomorphic to the field reduction of a conic. Note that, by Segre's Theorem (Theorem 2.3.3), all classical pseudo-ovals of $\mathrm{PG}(3e-1,q)$, q odd, are also pseudo-conics.

All known examples of pseudo-ovals are classical and a computer search by Penttila in 2000 [72] has shown there are no non-classical pseudo-ovals for $q^e \leq 16$.

When pseudo-ovals were first introduced by Thas [80], they came about in the context of generalised quadrangles. Recall from Theorem 2.4.1 that ovals can be used to construct examples of translation generalised quadrangles. This construction extends to pseudo-ovals, and eggs in general. We will consider only the pseudo-oval case. Let S be a pseudo-oval in $\mathrm{PG}(3e-1,q)$ and construct from S a translation generalised quadrangle $\mathcal{T}(S) = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ as follows. Embed $\mathrm{PG}(3e-1,q)$ in $\mathrm{PG}(3e,q)$ as a hyperplane.

The elements of $\mathcal{P}$ are

- a symbol P_∞,
- the $2e$-spaces of $\mathrm{PG}(3e,q)$ that meet $\mathrm{PG}(3e-1,q)$ exactly in the tangent space of an element of S, and
- the points of $\mathrm{PG}(3e,q) \setminus \mathrm{PG}(3e-1,q)$.

The elements of $\mathcal{L}$ are

- the elements of S, and
- the e-spaces of $\mathrm{PG}(3e,q)$ that meet $\mathrm{PG}(3e-1,q)$ in exactly one element of S.

Incidence is induced by incidence in $\mathrm{PG}(3e-1,q)$. The order of $\mathcal{T}(S)$ is (q^2,q^2). The dual translation generalised quadrangle $\mathcal{T}(S)^D = (\mathcal{L}, \mathcal{P}, \mathcal{I})$ will also have order (q^2,q^2).

Theorem 5.1.2 (Payne and Thas [71], pg. 30, 116)**.** *The translation generalised quadrangle associated with a pseudo-conic of* $\mathrm{PG}(3e-1,q)$ *is isomorphic to* $\mathrm{Q}(4,q^e)$.

The remainder of this chapter is devoted to exploring possibilities for the characterisation of pseudo-ovals. We will use the notation $S = \{s_y \mid y \in \{0,\ldots,q^e\}\}$, to work with pseudo-ovals of $\mathrm{PG}(3e-1,q)$ throughout this chapter.

5.2 Spreads and their associated translation planes

In Chapter 3 we showed that the field reduction of a projective plane $\mathrm{PG}(2,q^e)$ is a normal $(e-1)$-spread of $\mathrm{PG}(3e-1,q)$ and, therefore, we know that every classical pseudo-oval of $\mathrm{PG}(3e-1,q)$ is contained within a normal $(e-1)$-spread. In this section we investigate spreads described by pseudo-ovals, and their corresponding translation planes.

Theorem 5.2.1 (Casse, Thas and Wild [29], Section 6)**.** *A pseudo-oval S in* $\mathrm{PG}(3e-1,q)$ *is classical if and only if it is contained within a normal* $(e-1)$*-spread.*

Proof. First, suppose the pseudo-oval S in $\mathrm{PG}(3e-1,q^e)$ is classical, that is, it is the field reduction of an oval in the plane $\pi = \mathrm{PG}(2,q^e)$. Then, by Theorem 3.3.2 and Theorem 3.3.7, the points of

π under field reduction form a normal $(e-1)$-spread of $\mathrm{PG}(3e-1,q)$ and it contains S.

Conversely, suppose S is contained within a normal $(e-1)$-spread. Then, by Corollary 3.4.5, the elements of the normal $(e-1)$-spread, and the $(2e-1)$-spaces spanned by any pair of elements of the $(e-1)$-spread, are the points and lines of a Desarguesian plane. Therefore, the elements of the pseudo-oval are a set of q^e+1 points, such that no three are collinear. That is, they form an oval. □

Therefore, in order to prove that a pseudo-oval of $\mathrm{PG}(3e-1,q)$ is classical, it suffices to show that it is contained within a normal $(e-1)$-spread.

First let us go through a few well known results regarding pseudo-ovals that will be required later on.

Let s_y be an element of S. Then, we denote the tangent space at s_y by $T(s_y)$.

Corollary 5.2.2 (Casse, Thas and Wild [29] Section 4)**.** *Let* Π *be a* $(2e-1)$*-space that does not contain* $s_y \in S$*. Then* $T(s_y)$ *meets* Π *in an* $(e-1)$*-space.*

Remark 5.2.3. *The set of* q^e+1 $(2e-1)$*-spaces* $\{\langle s_y, s_x\rangle \mid s_x \in S\setminus\{s_y\}\}\cup\{T(s_y)\}$ *meet exactly in* s_y *and therefore cover*

$$(q^e+1)\left(\frac{q^{2e}-1}{q-1}-\frac{q^e-1}{q-1}\right)+\frac{q^e-1}{q-1}=\frac{q^{3e}-1}{q-1}$$

points of $\mathrm{PG}(3e-1,q)$*. That is, every point of* $\mathrm{PG}(3e-1,q)$ *is covered by the set.*

A *dual pseudo-oval* is defined analogously to a dual oval. That is, it is a set of q^e+1 $(2e-1)$-spaces such that no three share a point.

Lemma 5.2.4 (Payne and Thas [70] Section 8.7)**.** *When* q *is odd, the set of* q^e+1 *tangent spaces to a pseudo-oval of* $\mathrm{PG}(3e-1,q)$ *forms a dual pseudo-oval. When* q *is even, the set of* q^e+1 *tangent spaces meet in a common* $(e-1)$*-space, called the* nucleus*.*

5.2.1 Work of Casse, Thas and Wild

Casse, Thas and Wild [29] outline three methods for creating spreads of $(2e-1)$-spaces from a pseudo-oval. Two of these methods are for q odd, one for q even.

Construction 5.2.5 (Projection spread, q odd)**.** *Given any element* $s_y \in S$*, and a* $(2e-1)$*-space* Π *disjoint from* s_y*, we can define a set of* $(e-1)$*-spaces* $W(s_y)=\{\langle s_y,s_x\rangle\cap\Pi \mid s_x \in S\setminus\{s_y\}\}\cup\{T(s_y)\cap\Pi\}$.

Lemma 5.2.6 (Casse, Thas and Wild [29] pg. 27-28)**.** *The set* $W(s_y)$ *on* Π *forms a spread of* Π.

Proof. For each s_x, $\langle s_y,s_x\rangle\cap\Pi$ contains an $(e-1)$-space by Grassmann's Dimension Theorem (Theorem 2.2.1). Suppose there is an e-space $\pi\subseteq\langle s_y,s_z\rangle\cap\langle s_x,s_w\rangle$. Then the span of s_y,s_z,s_w has dimension

$$\dim(\langle s_y,s_z\rangle)+\dim(\langle s_y,s_w\rangle)-\dim(\langle s_y,s_z\rangle\cap\langle s_y,s_w\rangle)\le 2e-1+2e-1-e=3e-2$$

which is a contradiction to the conditions on S. Thus the intersection of any two $(2e-1)$-spaces $\langle s_y, s_z\rangle, \langle s_y, s_w\rangle$ is exactly the $(e-1)$-space s_y.

Now, Π must meet each $(2e-1)$-space $\langle s_y, s_x\rangle$ in an $(e-1)$-space. Thus, the set of $(2e-1)$-spaces $\{\langle s_y, s_x\rangle \mid s_x \in S \setminus \{s_y\}\}$ meet Π in a set of q^e mutually disjoint $(e-1)$-spaces. This partial $(e-1)$-spread can be uniquely completed to an $(e-1)$-spread [26] and so there is an extra $(e-1)$-space $m \in \Pi$, such that $\langle s_y, m\rangle \cap \Pi$ is disjoint from $\langle s_y, s_x\rangle$, for all s_x. Suppose there is an e-space $X \subseteq \langle s_y, m\rangle \cap \langle s_y, s_x\rangle$. Then X must meet Π in a point, which is a contradiction as $\langle s_y, s_x\rangle$ and $\langle s_y, m\rangle$ are disjoint in Π. Therefore $\langle s_y, m\rangle \cap \langle s_y, s_x\rangle = s_y$, for all s_x. That is, $\langle s_y, m\rangle = T(s_y)$. □

*We will refer to $W(s_y)$ as the s_y-*projection spread *of S on Π.*

Construction 5.2.7 (Tangent spread, q odd)**.** *For any pseudo-oval element $s_y \in S$, we can define a set of q^e+1 elements $W^*(s_y) = \{s_y\} \cup \{T(s_i) \cap T(s) \mid s_i \in S \setminus \{s_y\}\}$*

Theorem 5.2.8 (Casse, Thas and Wild [29], pg. 27-28)**.** *The set $W^*(s_y)$ is a spread of $T(s_y)$.*

Proof. Recall from Lemma 5.2.4 that the intersection of $T(s_i)$ with $T(s_j)$ is an $(e-1)$-space and that no point of $\mathrm{PG}(3e-1,q)$ can be contained in three or more tangent spaces. Therefore, the intersections $T(s_i) \cap T(s_y)$ and $T(s_j) \cap T(s_y)$ are disjoint for all i, j. □

We will refer to $W^*(s_y)$ as the tangent spread *of S on $T(s_y)$.*

Construction 5.2.9 (The spread for q even)**.**

Theorem 5.2.10 (Casse, Thas and Wild [29] pg. 27-28)**.** *Let N be the nucleus of S and let Σ be any $(2e-1)$-space disjoint from N. The set of q^e+1 elements $\hat{W} = \{T(s_y) \cap \Sigma \mid s_y \in S\}$ is a spread of Σ.*

Proof. Every tangent space must meet a mutually disjoint $(2e-1)$-space in an $(e-1)$-space and two tangent spaces can only intersect at N. Therefore we have defined q^e+1 distinct $(e-1)$-spaces in a $(2e-1)$-space. □

We will not use this spread in the following work, but rather focus on the case that q is odd.

Lemma 5.2.11 (Casse, Thas and Wild [29] pg. 37)**.** *If a pseudo-oval S of $\mathrm{PG}(3e-1,q)$, q odd, is contained within a normal spread, then the s_x-projection spread on $T(s_y)$ must be equal to the tangent spread on $T(s_y)$ for all $s_y, s_x \in S$.*

Proof. Suppose S is contained within a normal spread M. Then, the elements $\langle s_i, s_j\rangle \cap \langle s_k, s_l\rangle$ are contained in M for all i, j, k, l.

Now, we fix s_y and s_x and consider $\Pi = \langle s_i, s_j\rangle$, where $s_i, s_j \notin \{s_y, s_x\}$. The elements $\langle s_y, s_k\rangle \cap \Pi$, of the spread $W(s_y)$ on Π, must be elements of M and thus $T(s_y) \cap \Pi$ is also an element of M. This implies that $T(s_y)$ is the span of two elements of M and, hence, that $\langle s_k, s_l\rangle \cap T(s_y)$ is an element of M for all k, l. Therefore, the elements of the spread $W(s_x)$ on $T(s_y)$ are in M and the element $T(s_y) \cap T(s_x)$ is in M.

This holds for all choices of s_y and s_x. That is, all elements of all the s_y-projection spreads on tangent spaces, and all elements of all the tangent spreads belong to M. Therefore, these spreads must be equal on the spaces in which they overlap. $\square$

Consider a spread $\mathcal{S}$ of $\Sigma = \mathrm{PG}(2e-1, q)$ embedded in $\mathrm{PG}(3e-1, q)$. Let Π be an $(e-1)$-space in $\mathrm{PG}(3e-1, q)$ disjoint from Σ, generated by a set of e points $\{z_1, \ldots, z_e\}$, and let $\Sigma_1, \ldots, \Sigma_e$ be the $2e$-spaces where each Σ_j is $\langle \Sigma, z_j \rangle$. Then, for each Σ_j, we have the exact representation required to construct a translation plane from $\mathcal{S}$ using the André-Bruck-Bose construction (see Theorem 3.1.1). Let π_j denote the translation plane constructed from Σ_j. The set of translation planes $\{\pi_1, \ldots, \pi_e\}$, are isomorphic because the collineation fixing Σ pointwise and mapping z_i to z_j defines the equivalence between the corresponding spreads.

We can apply the André/Bruck-Bose construction in this way to both the projection spread and the tangent spread. Figure 5.1 shows an example of one translation plane constructed from a pseudo-oval in $\mathrm{PG}(5, q)$. First, we consider the projection spread.

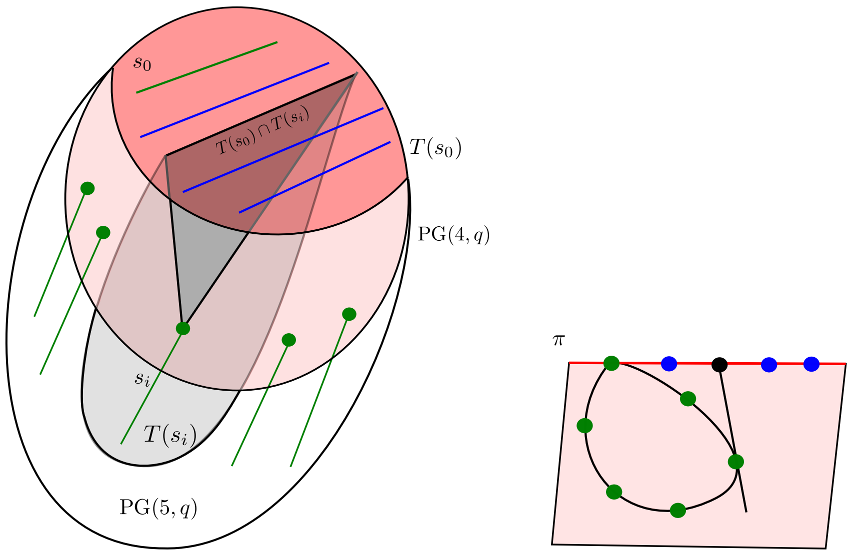


Figure 5.1 – A translation plane created from the tangent spread, via the André/Bruck-Bose construction.

Theorem 5.2.12 (Casse, Thas and Wild [29], Section 5)**.** *Let s_y be an element of S and let Σ be a $(2e-1)$-space in $\mathrm{PG}(3e-1, q)$ such that $s_y \cap \Sigma = \varnothing$. Create the projection spread $W(s_y)$ of Σ, as in Construction 5.2.5. In the corresponding translation planes, let $T(s_y) \cap \Sigma$, and the point of s_y in the plane, have coordinates $(0, 1, 0)$ and $(0, 0, 1)$, respectively (see Remark 3.1.6). Give the same coordinates to each of the elements of $W(s_y)$ in all the π_j. Define a set of isomorphisms from each translation plane onto one chosen plane π, and denote the set of e isomorphisms, by $\omega_1, \ldots, \omega_e$ where ω_1 is the identity. Let $K_1, \ldots, K_e$ denote the e sets of $q^e - 1$ points defined by the pseudo-oval. Then*

(i) each K_x contains $(0, 0, 1)$,

(ii) *if there exists a point t of K_j on the translation line, then all the K_x will contain t, and the line joining $(0, 0, 1)$ to t will contain no other points of any K_x, and*

(iii) *every line through $(0, 0, 1)$ meets no other affine point of K_x, for any x, or it meets each K_x in one other point and those points $(x_j, y_j, 1)$ are such that $x_1, \ldots, x_e$ form a basis for $T(s) \cap \Sigma$.*

Theorem 5.2.13 (Casse, Thas and Wild [29], Section 5)**.** *Let s_y be an element of S and let Σ be a $(2e-1)$-space in $\mathrm{PG}(3e-1, q)$ such that $s_y \cap \Sigma = \varnothing$. Create the projection spread $W(s_y)$ of Σ, as in Construction 5.2.5. In the corresponding translation planes, let $T(s_y) \cap \Sigma$, and the point of s_y in the plane, have coordinates $(0, 1, 0)$ and $(0, 0, 1)$, respectively. Give the same coordinates to each of the elements of $W(s_y)$ in all the π_j. Define a set of isomorphisms from each translation plane onto one chosen plane π, and denote the set of e isomorphisms, by $\omega_1, \ldots, \omega_e$ where ω_1 is the identity. Let $K_1, \ldots K_e$ denote the e sets of $q^e - 1$ points defined by the pseudo-oval.*

If $W(s_y) = W(s_z)$, for all $s_z \in S$ such that $s_z \notin \Sigma$, then, in addition to the results of Theorem 5.2.12, we also know that

(iv) *each K_x is an oval, and*

(v) *$K_1, \ldots, K_e$ are in perspective with axis the translation line and centre $(0, 0, 1)$.*

Next, we consider the tangent spread.

Theorem 5.2.14 (Casse, Thas and Wild [29], Section 5)**.** *Let s_y be an element of S and create the tangent spread W^* of $T(s_y)$, as in Construction 5.2.7. In the corresponding translation planes, let s_y have coordinate $(0, 1, 0)$. Give the same coordinates to each of the elements of W^* in all the π_j. Define a set of isomorphisms from each translation plane onto one chosen plane π, and denote the set of e isomorphisms, by $\omega_1, \ldots, \omega_e$ where ω_1 is the identity. Let $K_1, \ldots K_e$ denote the e sets of $q^e - 1$ points defined by the pseudo-oval. Then*

(a) *Each K_x is an oval,*

(b) *All K_x contain $(0, 1, 0)$ and the translation line is the tangent to K_x at $(0, 1, 0)$, and*

(c) *All K_x contain $(0, 0, 1)$ and the common tangent to K_x at this point meets the translation line at $(1, 0, 0)$.*

The proofs of Theorems 5.2.12, 5.2.13, and 5.2.14 have been omitted because they are quite technical and do not provide relevant insights.

The work so far gives several different representations of a pseudo-oval in a translation plane. We now take one of these representations, that of Theorem 5.2.13, and reconstruct a pseudo-oval from it.

Theorem 5.2.15 (Casse, Thas and Wild [29], Section 5)**.** *If a translation plane π of order q^e, q odd, contains $K_1, \ldots, K_e$ satisfying properties (i),(ii) and (iii) from Theorem 5.2.12 and properties (iv) and (v) from Theorem 5.2.13 then there exists a pseudo-oval S such that π is the plane constructed from the projection spread $W(s)$ for some $s \in S$.*

Proof. Let M be the spread of $\Sigma = \mathrm{PG}(2e-1,q)$ that corresponds to π, and embed Σ in $\mathrm{PG}(3e-1,q)$. Let $\Sigma_1,\ldots,\Sigma_e$ be a set of $2e$-spaces that generate $\mathrm{PG}(3e-1,q)$, such that $\Sigma \subset \Sigma_i$ for all i. Let π_j be the translation plane generated by Σ_j. Also, let ω_j be an isomorphism from π_j to π that fixes the translation line pointwise.

The point $(0,0,1)$ determines e points of $\mathrm{PG}(3e-1,q)$ by determining the point $\omega_j^{-1}((0,0,1))$ in each Σ_j. These points generate an $(e-1)$-space X_0 that is disjoint from Σ. Any point of K_j on the translation line also belongs to all the other K_i and corresponds to an element of M.

A line ℓ, incident with $(0,0,1)$, that contains one point z_j of K_j, will also contain points $z_1,\ldots,z_e$ of each of the other ovals. Therefore, in $\mathrm{PG}(3e-1,q)$, ℓ defines an $(e-1)$-space, skew to Σ, spanned by the points corresponding to $\omega_i^{-1}(z_i)$ in each Σ_i. That is, we have defined q^e+1 $(e-1)$-spaces in $\mathrm{PG}(3e-1,q)$. We now show these $(e-1)$-spaces, denoted $\mathcal{O} = \{X_0,\ldots,X_{q^e}\}$ form a pseudo-oval.

Consider the subspace $\langle X_0, X_j\rangle$. If $X_j \in \Sigma$ then $\langle X_0,X_j\rangle \cap \Sigma = X_j$. Otherwise, by (iii), $\langle X_0,X_j\rangle$ intersects Σ in an $(e-1)$-space generated by the e points corresponding to the linearly independent vectors: $y_1 + x_1', \ldots, y_e + x_e'$ where the points of π corresponding to X_j have coordinates (y_i, x_i). Thus, $\langle X_0, X_j\rangle$ has dimension $2e-1$ and X_0 is skew to all the other X_i. By (iv), the projections $\langle X_0,X_j\rangle \cap \Sigma$ are distinct elements of M and so we know that X_i and X_j are skew for all i,j.

Property (v) tells us that $\langle X_i, X_j\rangle$ intersects Σ in an element of M and, by property (iv), any set of three distinct elements X_i, X_j, X_k, no two in Σ, pairwise determine three distinct elements of M. That is, any set of three distinct elements of $\mathcal{O}$ spans all of $\mathrm{PG}(3e-1,q)$. □

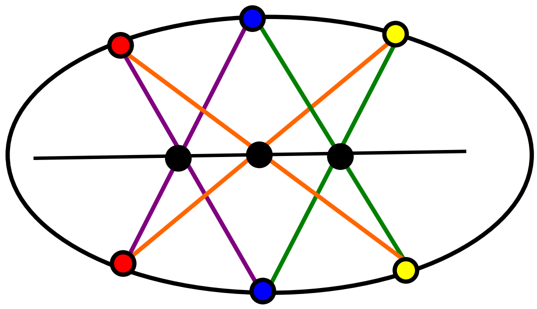
Theorem 5.2.16 (Casse, Thas and Wild [29], Section 7)**.** *Let $\mathcal{S}$ be a pseudo-oval in* $\mathrm{PG}(3e-1,q)$*, with q odd. If, for any element $s_y \in S$ and any $(2e-1)$-space Σ disjoint from s_y, either the spread W, or W^* induced by S in Σ gives rise to a Desarguesian plane then S is a pseudo-conic.*

5.2.2 Pascalian ovals

There are many ways to prove that a plane is Desarguesian. One of the methods that seems most suited to this problem is to use Buekenhout's Pascalian theorem.

Pascal's theorem states that, given six points of a conic $\{a,a',b,b',c,c'\}$, the points defined by $P_{ab} = ab' \cap ba'$, $P_{ac} = ac' \cap ca'$ and $P_{bc} = bc' \cap cb'$ are collinear. See Figure 5.2. Any space in which this theorem holds is called *Pascalian*.

Figure 5.2 – Pascal's Theorem.



Theorem 5.2.17 (Dembowski [34], pg. 151)**.** *The plane* PG$(2, q)$ *is* Pascalian*.*

Therefore all conics in PG$(2, q)$ are *Pascalian*. An oval is called *Pascalian* if Pascal's Theorem holds for every set of six vertices belonging to the oval.

Theorem 5.2.18 (Buekenhout [24] Theorem 5)**.** *Let K be an oval of a finite projective plane π. If K is Pascalian then π is Desarguesian and K is a conic.*

We say that a pseudo-oval $\mathcal{S}$ of PG$(3e-1, q)$ is *Pascalian on s* for some $s \in S$ if, for every set of six elements $\{s_0, s_1, s_2, s_3, s_4, s_5\}$ of $\mathcal{S}$, the $(e-1)$-spaces $s_0s_4 \cap s_1s_3, s_0s_5 \cap s_2s_3, s_1s_5 \cap s_2s_4$ lie in a $(2e-1)$-space that contains $T(s) \cap T(s_i)$ for some i.

Lemma 5.2.19. *A classical pseudo-oval in* PG$(3e-1, q)$*, q odd, is Pascalian.*

Proof. Every oval of PG$(2, q^e)$ is a conic and therefore Pascalian. Let $p_0, p_1, p_2, p_3, p_4, p_5$ be six points of a conic $\mathcal{C}$. Then, the points $p_0p_4 \cap p_1p_3, p_0p_5 \cap p_2p_3, p_1p_5 \cap p_2p_4$ are contained in some line ℓ in PG$(2, q)$. Now, q is odd so the intersection of ℓ and a tangent line m to $\mathcal{C}$ is contained in one other tangent line n. Thus, in PG$(3e-1, q)$ the images of $p_0p_4 \cap p_1p_3, p_0p_5 \cap p_2p_3, p_1p_5 \cap p_2p_4$ are contained within a $(2e-1)$-space and this $(2e-1)$-space contains the intersection of two tangent spaces. This statement holds for any set of six points and, therefore, the pseudo-oval is Pascalian. □

Theorem 5.2.20. *Let S be a pseudo-oval that is Pascalian on s_y. If, for all $s_x \in S \setminus \{s_y\}$, $W(s_x) = W^*(s_y)$, then S is classical.*

Proof. Let Σ be a $2e$-space containing $T(s_y)$ and let π be the translation plane constructed from $W^*(s_y)$. Recall from Theorem 5.2.14, that the image of S in π is an oval. Let $s_0, \ldots, s_5$ be any six elements of the pseudo-oval. Now, S is Pascalian on s_y, so there exists a $(2e-1)$-space L containing $s_0s_4 \cap s_1s_3, s_0s_5 \cap s_2s_3, s_1s_5 \cap s_2s_4$, such that $L \cap T(s_y) \in W^*(s_y)$, for any set of $s_i \in S$, $i \in \{0, \ldots 5\}$. Let p_i denote $s_i \cap \Sigma$, and let ℓ denote $L \cap \Sigma$.

Note that $\langle s_i, s_j \rangle \cap T(s_y) \in W^*(s_y)$, for all $i \neq j$, $i, j \in \{0, \ldots, 5\}$. That is, the unique affine e-space of Σ containing p_i and p_j, that meets $T(s_y)$ in an element of $W^*(s_y)$ is $\langle s_i, s_j \rangle \cap \Sigma$. Let p_ip_j denote this e-space and note that, for all other m, n, p_ip_j contains a point of p_mp_n, by Grassmann's Dimension Theorem.

Thus, ℓ contains the points $p_0p_4 \cap p_1p_3, p_0p_5 \cap p_2p_3, p_1p_5 \cap p_2p_4$, because all these points are contained in both L and Σ.

Therefore, in π, we have a set of points $\{p_0, \ldots, p_5\}$ such that $p_0p_4 \cap p_1p_3, p_0p_5 \cap p_2p_3, p_1p_5 \cap p_2p_4$ are collinear. That is, the hexagon containing $p_0, \ldots, p_5$ is Pascalian. This holds for any set of six points of the oval corresponding to S and, therefore, the oval is Pascalian and π is Desarguesian. Thus, $W^*(s_y)$ is regular and S is classical. □

Note that the spread condition of Theorem 5.2.20 is identical to that of Theorem 5.2.13, requiring that all the projection spreads on a certain tangent space coincide both with each other and with the tangent spread.

5.2.3 An $(e-1)$-spread of $\mathrm{PG}(3e-1,q)$ arising from a pseudo-oval

Another way of considering the problem is to prove directly that S is contained within a normal $(e-1)$-spread. In this section we construct an $(e-1)$-spread and prove that if S is contained in a normal $(e-1)$-spread then it must be equal to the constructed spread.

Theorem 5.2.21. *Let S be a pseudo-oval of* $\mathrm{PG}(3e-1,q)$ *and let $s_i, s_j, s_k \in S$ pairwise distinct. Let $M_{i,j,k}$ consist of the $(e-1)$-spaces*

(i) $s_i, s_j, T(s_i) \cap T(s_j)$

(ii) $T(s_i) \cap \langle s_j, s_x\rangle, T(s_j) \cap \langle s_i, s_x\rangle, \forall\, x \neq i, j$

(iii) $\langle s_i, s_x\rangle \cap \langle s_j, s_y\rangle, \forall\, x, y \neq i, j,\ x \neq y$

(iv) $\langle s_k, s_x\rangle \cap \langle s_i, s_j\rangle, \forall\, x \neq i, j, k$

(v) $T(s_k) \cap \langle s_i, s_j\rangle$

Proof. In order to prove $M_{i,j,k}$ is a spread we will show that all its elements are $(e-1)$-spaces, that there are $\dfrac{q^{3e}-1}{q^e-1} = q^{2e}+q^e+1$ of them, and that they cover the points of $\mathrm{PG}(5,q)$.

In Lemma 5.2.2, we showed that the span of any two elements of the pseudo-oval must meet a tangent space in an $(e-1)$-space. That is, (ii) and (v) contain only $(e-1)$-spaces. Lemma 5.2.4 tells us that $T(s_i) \cap T(s_j)$ is an $(e-1)$-space.

Lastly, two $(2e-1)$-spaces in $\mathrm{PG}(3e-1,q)$ must meet in at least an $(e-1)$-space by Grassmann's Dimension Theorem (Theorem 2.2.1). If $\langle s_i, s_x\rangle \cap \langle s_j, s_y\rangle$ contains an e-space π (for any i, j, x, y) then the span of the two $(2e-1)$-spaces is in a hyperplane containing four pseudo-oval elements, and this is a contradiction because any three elements of the pseudo-oval span all of $\mathrm{PG}(3e-1,q)$. This shows that (iii) and (iv) contain only $(e-1)$-spaces, and thus that all the elements of $M_{i,j,k}$ are $(e-1)$-spaces.

Counting these spaces gives us

$$3 + 2(q^e-1) + (q^e-1)^2 + q^e - 2 + 1 = q^{2e} + q^e + 1$$

$(e-1)$-spaces, which is the correct number of $(e-1)$-spaces for an $(e-1)$-spread of $\mathrm{PG}(3e-1,q)$.

Finally, to show these $(e-1)$-spaces cover the points of $\mathrm{PG}(3e-1,q)$, we consider a few separate cases. First, the pseudo-oval S is contained in $M_{i,j,k}$ by taking the elements s_i, s_j and $\{\langle s_i, s_x\rangle \cap \langle s_j, s_x\rangle \mid x \neq i, j\}$.

Next, by Remark 5.2.3, we recall that every point of $\mathrm{PG}(3e-1,q)$, is contained in either $T(s_i)$ or $\langle s_i, s_x\rangle$, for some x.

Thus, if a point P is not in $\langle s_i, s_j\rangle$ or $T(s_i)$ then P is contained in $\langle s_i, s_x\rangle$ for some $s_x \neq s_j$. Similarly, if P is not in $\langle s_i, s_j\rangle$ or $T(s_j)$ then P is contained in $\langle s_j, s_y\rangle$, for some $s_y \neq s_i$. Thus, if P is not in $\langle s_i, s_j\rangle$, $T(s_i)$ or $T(s_j)$ then P is in $\langle s_i, s_x\rangle \cap \langle s_j, s_y\rangle$ for some $s_x, s_y \in S \setminus \{s_i, s_j\}$.

If a point P is in $T(s_i)$ or $T(s_j)$ then it will be contained in $T(s_i) \cap \langle s_j, s_x\rangle$ or $T(s_j) \cap \langle s_i, s_x\rangle$, respectively, for some x, by Lemma 5.2.6.

Finally, if a point P is in $\langle s_i, s_j \rangle$ then it will be contained in $\langle s_k, s_x \rangle \cap \langle s_i, s_j \rangle$ for some x or in $T(s_k) \cap \langle s_i, s_j \rangle$. □

Lemma 5.2.22. *If there exists a normal spread $\mathcal{M}$ containing S then it must necessarily be $M_{i,j,k}$, as described in Theorem 5.2.21, and $M_{i,j,k} = M_{x,y,z}$ for all i, j, k, x, y, z.*

Proof. The definition of a normal spread requires that, for any four elements $x, y, z, w \in \mathcal{M}$, $\langle x, y \rangle \cap \langle z, w \rangle \in \mathcal{M}$ is in the spread. Thus we know that the elements in (iii) and (iv) must also be elements of $\mathcal{M}$. Now, we know that the only way to complete the spread of $\langle s_i, s_x \rangle$, after projecting over $\mathcal{S}$ from s_j is by adding $T(s_j) \cap \langle s_i, s_x \rangle$. Therefore, $\mathcal{M}$ must contain the elements in (ii) and (v). Finally, the only space remaining uncovered in $\mathrm{PG}(3e-1, q)$ is $T(s_i) \cap T(s_j)$, which must therefore also be an element of $\mathcal{M}$. Thus, all the elements of $M_{i,j,k}$ are contained in $\mathcal{M}$, regardless of i, j, k and, as a result of this, $M_{x,y,z} = M_{i,j,k}$. □

Corollary 5.2.23. *A pseudo-oval S is classical if and only if the $(e-1)$-spread $M_{i,j,k}$ arising from S is normal.*

We conclude this section with an open problem:

Prove that the $(e-1)$-spread $M_{i,j,k}$ is always normal.

5.3 Pseudo-ovals in $\mathrm{Q}^-(5, q)$

In Chapter 2, we mentioned Segre's Theorem (Theorem 2.3.3) — all ovals in $\mathrm{PG}(2, q)$, q odd, are conics — and discussed the fact that conics are the quadrics of $\mathrm{PG}(2, q)$. The 'smallest' field reduction of a conic is to a pseudo-conic of $\mathrm{PG}(5, q)$. Thus, it is natural to consider $\mathrm{PG}(5, q)$ specially when questioning the existence of non-classical pseudo-ovals.

The image of a conic, under field reduction, in $\mathrm{PG}(5, q)$ is contained in either $\mathrm{Q}^+(5, q)$ or $\mathrm{Q}^-(5, q)$ [41]. Therefore, every classical pseudo-oval in $\mathrm{PG}(5, q)$ is contained in either a hyperbolic quadric or an elliptic quadric.

Theorem 5.3.1 (Shult and Thas [77] Theorem 15)**.** *If a pseudo-oval is contained within a hyperbolic quadric $\mathrm{Q}^+(5, q)$, with q odd, it is classical.*

We now turn our attention to pseudo-ovals contained in an elliptic quadric.

Remark 5.3.2. *A* special set *$\mathcal{S}$ of $\mathrm{H}(3, q^2)$, q odd, is a set of q^2+1 points such that any three points of $\mathcal{S}$ span a non-degenerate plane of $\mathrm{H}(3, q^2)$, that is, they span an $\mathrm{H}(2, q^2)$. This is equivalent to the definition of a special set as $q^2 + 1$ points such that, for all points X in $\mathrm{H}(3, q^2) \setminus \mathcal{S}$, X is collinear with 0 or 2 points of $\mathcal{S}$.*

Recall from Remark 2.5.5, that elements of $\mathrm{PG}(3, q^2)$ can be seen in $\mathrm{PG}(5, q^2)$ and, in particular, that the lines of $\mathrm{H}(3, q^2)$ map to points of $\mathrm{Q}^-(5, q)$.

Lemma 5.3.3 (Shult [76] pg. 177)**.** *Special sets of $\mathrm{H}(3, q^2)$ are equivalent to pseudo-ovals of $\mathrm{Q}^-(5, q)$.*

5.3.1 Buekenhout-Metz unitals

In Section 5.2.1, we constructed two different spreads from a given pseudo-oval, for q odd, and proved results regarding the image of the pseudo-oval in the resulting translation planes. Now that our pseudo-oval is embedded in $Q^-(5,q)$, we rework some of these results to include information from the quadric. First, we consider the image of the quadric in the translation plane.

Theorem 5.3.4 (Buekenhout [25], Metz [69], see Figure 5.3)**.** *Let $\mathcal{S}$ be a spread in $\mathrm{PG}(3,q) \subset \mathrm{PG}(4,q)$ and let $\mathcal{O}$ be an ovoid of $\mathrm{PG}(4,q)$, such that $\mathcal{O} \cap \mathrm{PG}(3,q) = X$ for some point X. Let ℓ be the line of $\mathcal{S}$ containing X and define a cone C with vertex Y and base $\mathcal{O}$ for some $Y \in \ell$ and $Y \neq X$. The set of points in $C \setminus \mathrm{PG}(3,q)$, together with the point ℓ, form a unital in the translation plane π_S.*

Note that we have not specified any properties of the spread and therefore we can construct these unitals in any translation plane of order q^2.

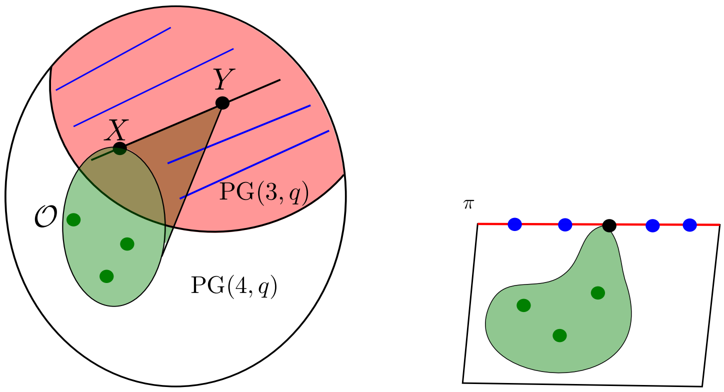


Figure 5.3 – The Buekenhout-Metz unital.

A *Buekenhout-Metz* unital is a unital that can be constructed from an ovoid as described in Theorem 5.3.4. If the ovoid is an *elliptic quadric* we call the unital an *orthogonal* Buekenhout-Metz unital and, if the unital is tangent to the translation line we say it is a *parabolic* Buekenhout-Metz unital.

Corollary 5.3.5. *Let S be a pseudo-oval of $Q^-(5,q)$, let s_0 be a line of S, let $x \in s_0$ and consider the tangent spread on $T(s_0)$. Recall from Section 2.5 that $x^\perp$ is the image of x under the polarity of $Q^-(5,q)$ and that $x \in x^\perp$ if and only if $x \in Q^-(5,q)$. Then $x^\perp$ is a $2e$-space containing $T(s_0)$ and we denote by π_S the translation plane constructed by applying the André/Bruck-Bose construction to $T(s_0)$ in $x^\perp$. The oval of π_S corresponding to the elements of S is contained in a parabolic orthogonal-Buekenhout-Metz unital.*

Proof. The perp of the degenerate point x is a cone with an elliptic quadric $Q^-(3,q)$ as its base. Exactly one line of the cone lies in $T(s_0)$, and therefore we have the conditions required to construct an orthogonal Buekenhout-Metz unital in π_S. All points that are in lines of the pseudo-oval are totally isotropic in $Q^-(5,q)$, and therefore they are in the cone $x^\perp$, and belong to the unital in

π_S. The translation line contains the point corresponding to s_0 and no other points of the unital. Therefore it is a tangent to the unital. □

We now put this information together with the results from Casse, Thas and Wild.

Corollary 5.3.6. *Let s be a line of the pseudo-oval S. For each point $y \in s$, construct a translation plane from $T(s)$ embedded in $y^\perp$. By mapping all these translation planes onto one chosen one we will have all the conditions given in Theorem 5.2.14. That is,*

(a) each K_x is an oval,

(b) all K_x contain $(0,1,0)$ and the translation line is the tangent to K_x at $(0,1,0)$, and

(c) every line through $(0,0,1)$ meets no other affine point of K_x, for any x, or it meets each K_x in one point and those points $(x_j, y_j, 1)$ are such that $x_1, \ldots, x_n$ form a basis for $(0,1,0)$,

and the new condition that

- *there exist $q-1$ parabolic orthogonal Buekenhout-Metz unitals $U_1, \ldots, U_{q-1}$ such that $K_i \in U_i$ for all i.*

5.3.2 The $(e-1)$-spread revisited

In Section 5.2.3 we defined a spread on $\mathrm{PG}(3e-1, q)$ arising from a pseudo-oval S. When we restrict the problem to considering only pseudo-ovals in $\mathrm{Q}^-(5,q)$, we can use the polarity and dimension to provide us with more results about the spread. Define $\mathcal{T} = \{T(s_i) \cap T(s_j) \mid s_i, s_j \in \mathcal{S}\}$ and $\mathcal{U} = \{u = \langle s_i, s_j \rangle \cap \langle s_m, s_n \rangle \mid u \notin \mathcal{S}, \mathcal{T}\}$. Then,

$$\mathcal{S} \cup \mathcal{T} \cup \mathcal{U} = \bigcup_{i,j,k} M_{i,j,k}.$$

Theorem 5.3.7. *Let $\mathcal{S}$ be a pseudo-oval of $\mathrm{Q}^-(5,q)$. Suppose that, for all $s \in \mathcal{S}$, the spread of $T(s)$ given by $\{T(s_k) \cap T(s) \mid s_k \in S\}$ is the same as each spread $X_i = \{T(s_k) \cap \langle s_i, s_j \rangle \mid s_j \in S\}$. Then $M_{i,j,k} = M_{x,y,z}$ for any x, y, z.*

Proof. First we show that $\mathcal{T} \subseteq M_{i,j,k}$.

Let $t_{m,n}$ denote $T(s_m) \cap T(s_n)$. Then, by the assumptions of the lemma, $t_{m,n}$ is in both $\langle s_i, s_x \rangle$ for some x, or in $T(s_i)$, and in $\langle s_j, s_y \rangle$ for some y, or in $T(s_j)$. Therefore $t_{m,n} \in M_{i,j,k}$ for all m, n and $\mathcal{T} \subseteq M_{i,j,k}$.

Let $s_m, s_n \in \mathcal{S}$ and consider the span $\langle s_m, s_n \rangle$. Then, for each $s \in \mathcal{S} \setminus \{s_m, s_n\}$, $\langle s_m, s_n \rangle \cap T(s)$ is an element of $\mathcal{T}$ and therefore of $M_{i,j,k}$. Each of these elements belongs to two tangent spaces and therefore $\mathcal{T}$ covers $(q^2-1)/2$ lines of $\langle s_m, s_n \rangle$.

We focus our attention back to the solids $\{\langle s_i, s \rangle \mid s \in S \setminus \{s_i\}\}$. We know these solids are partitioned by $M_{i,j,k}$ and therefore there are

$$q^2 + 1 - 2 - \frac{q^2-1}{2} = \frac{q^2-1}{2}$$

lines of $M_{i,j,k}$ in each $\langle s_i, s\rangle$ that are not in $\mathcal{S}$ or $\mathcal{T}$, giving $q^2(q^2-1)/2$ lines altogether. These lines must be a subset of $\mathcal{U}$, as $M_{i,j,k} \in \mathcal{S} \cup \mathcal{T} \cup \mathcal{U}$, and we shall denote this subset $\mathcal{U}'$.

Let $u \in \mathcal{U}'$, with $u = \langle s_i, s_x\rangle \cap \langle s_j, s_y\rangle$. Then $u^\perp = \langle t_{i,x}, t_{j,y}\rangle$ contains no lines of S. To determine the average number of elements of $\mathcal{T}$ in $u^\perp$, we double count $(t, u^\perp)$, where $t \in u^\perp$. Let X denote the average number of elements of $\mathcal{T}$ in $u^\perp$, then

$$\frac{q^2(q^2+1)}{2}\frac{q^2-1}{2} = \frac{q^2(q^2-1)}{2}X$$

and

$$X = \frac{q^2+1}{2}.$$

The maximum number of elements of $\mathcal{T}$ that can be contained in any solid, other than a perp space, is $(q^2+1)/2$ because each element of $\mathcal{T}$ is in the perp space of two distinct elements of $\mathcal{S}$ and no solid, other than a perp space, can contain two lines from the same perp space. Thus there are $(q^2+1)/2$ lines of $\mathcal{T}$ in the perp of every element of $\mathcal{U}'$. This means each line of $\mathcal{U}'$ is contained in $(q^2+1)/2$ spans of pairs of lines of $\mathcal{S}$ and therefore, for every $s \in \mathcal{S}$, it belongs to a span $\langle s, s'\rangle$ for some s'.

To show that $M_{i,j,k} = M_{x,y,z}$, for all x, y, z, we need only show that the line $v = \langle s_m, s_n\rangle \cap \langle s_g, s_h\rangle$ is in $M_{i,j,k}$ for any m, n, g, h. If v is not a line of $M_{i,j,k}$, then $v \notin \mathcal{S}$ and $v \notin T(s)$ for any s. Now, there exists $u \in M_{i,j,k}$ such that $u \cap v \neq \varnothing$. We know $u \notin \mathcal{S}$, or else $\dim\langle u, s_g, s_h\rangle = 4$. Suppose $u \in \mathcal{T}$, so $u = T(s) \cap T(s')$. But, we know that the spread $W(s_g)$ on $T(s)$ and the spread $W(s_m)$ on $T(s)$ are identical, so $\langle s_m, s_n\rangle \cap \langle s_g, s_h\rangle$ is either contained within, or disjoint from, $T(s)$ which is a contradiction. Therefore, $u \in \mathcal{U}'$. Recall that for every $s \in \mathcal{S}$, $u \in \langle s, s'\rangle$ for some s'. So, there exists f such that $u \in \langle s_g, s_f\rangle$. But $\langle s_g, s_f\rangle$ and $\langle s_g, s_h\rangle$ must be disjoint unless $f = h$, and thus, this is a contradiction.

$\square$

Remark 5.3.8. *Note that the condition in Theorem 5.3.7 is stronger than that required by Theorem 5.2.13. Theorem 5.2.13 requires only that $W(s) = W(s')$ for all s' on one particular Σ. Theorem 5.3.7 requires that, for all $\Sigma = T(s)$, for some $s \in \mathcal{S}$, we have $W(s') = W^*$ for all s'.*

To conclude this chapter we ask two questions, the answers of which would aid in solving the question of the existence of non-classical pseudo-ovals.

- When is the spread $M_{i,j,k}$ (of Theorem 5.2.21) classical?
- When do parabolic orthogonal Buekenhout-Metz unitals, of non-Desarguesian translation planes, contain ovals?

Chapter 6

Maximal arcs that contain regular hyperovals

This chapter is joint work with Nicola Durante. We investigate maximal n-arcs in $\mathrm{PG}(2,q)$ that are formed by taking unions of regular hyperovals. Let $\mathcal{K}$ be a maximal n-arc, that is a union of regular hyperovals, in $\mathrm{PG}(2,q)$, such that $q > n^2$. The main results we have proved are that

- $\mathcal{K}$ must contain exactly $n-1$ regular hyperovals,
- every point of $\mathcal{K}$ must lie on an odd number of these hyperovals, and
- if $\mathcal{K}$ is a maximal 4-arc, then it is of *Mathon type*.

A *maximal n-arc* is a non-empty set of points in a projective plane such that all lines contain zero or n points of the set. Maximal arcs were introduced by Barlotti in 1956 [17], and were studied as combinatorial extremal problems. In the early 70s, Thas [81] and Wallis [89] used maximal arcs to create partial geometries and, since then, they have been shown to have links with many other geometric objects including partial geometries and 2-weight codes. We will not explore these links but rather focus purely on the maximal arcs.

Trivial examples of maximal n-arcs are a point ($n = 1$), the projective plane minus a line ($n = q$), and the full projective plane($n = q + 1$).

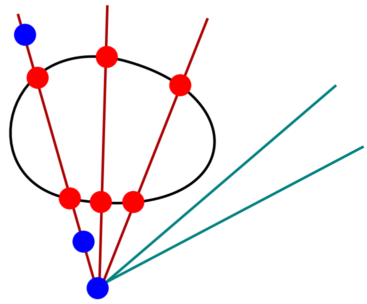
Let P be a point of the maximal n-arc $\mathcal{K}$ in the projective plane π of order q. Every line through P must contain an additional $n-1$ points of $\mathcal{K}$ and there can be no further points of $\mathcal{K}$. Therefore, the number of points in $\mathcal{K}$ is $q(n-1)+n$. We say that a line is *secant* to $\mathcal{K}$ if it contains n points of $\mathcal{K}$ and *external* if it contains zero points of $\mathcal{K}$. Suppose $n \neq q+1$ and let R be a point of $\pi \setminus \mathcal{K}$. Each line through R that contains a point of $\mathcal{K}$ contains n points of $\mathcal{K}$ and every point of $\mathcal{K}$ lies on a line through R. Therefore, there are

$$\frac{q(n-1)+n}{n} = q + 1 - \frac{q}{n}$$

secant lines through R and then n divides q.

Example 6.0.9 (A hyperoval in PG$(2,4)$ (see Section 2.3))**.** *A hyperoval in* PG$(2,4)$ *meets all lines in zero or two points and is, therefore, a maximal* 2*-arc. It has six points in total and its secant lines contain two maximal arc points and three external points. Each external point lies on three secant lines and two external lines.*

Figure 6.1 – A hyperoval in PG$(2,4)$.



We will see, in the rest of this chapter, that there exist maximal arcs in PG$(2,q)$ for all q even. However, the same is not true for q odd. In 1996, Ball, Blokhuis, and Mazzocca [14], proved that maximal arcs do not exist for q odd, settling a 20 year old conjecture of Thas [82].

For the remainder of this chapter, we let q be even and assume $n \notin \{1, q, q+1\}$.

Lemma 6.0.10 (Cossu [32], Faina and Korchmáros [39] Prop. 3.4)**.** *The image, under duality, of a set of lines external to a maximal n-arc in* PG$(2,q)$ *is a maximal (q/n)-arc, called the* dual arc.

Proof. Let $\mathcal{K}'$ be the set of lines external to a maximal n-arc $\mathcal{K}$. No point of $\mathcal{K}$ is incident with a line of $\mathcal{K}'$. Let R be a point of PG$(2,q) \setminus \mathcal{K}$. Then R lies on $q+1-q/n$ lines with n points of $\mathcal{K}$ and, therefore, q/n lines external to $\mathcal{K}$. Therefore all points of PG$(2,q)$ lie on 0 or q/n lines of $\mathcal{K}'$ and so, under duality, all lines of PG$(2,q)$ contain 0 or q/n points of the dual of $\mathcal{K}'$. □

Example 6.0.11 (Hyperovals and their dual arcs)**.** *If a maximal arc contains an oval, then all the lines through the nucleus of the oval are secant lines to the maximal arc. Therefore, the nucleus is also a point of the maximal arc.*

Note that all maximal 2*-arcs are hyperovals and vice-versa: each is a set of $q+2$ points such that every line meets the set in zero or two points. The dual arc of a hyperoval is a set of $(q^2+q)/2-q$ points that form a maximal $q/2$-arc.*

6.1 Known constructions of maximal arcs

In 1969, Denniston [38] constructed maximal d-arcs in PG$(2,q)$ for every d such that GF(q) has an additive subgroup G of order d. Each element λ of the group G defines a conic with equation

$$C_\lambda : x^2 + \alpha xy + y^2 + \lambda z^2 = 0,$$

where α is an element of GF(q) such that $x^2 + \alpha x + 1$ is irreducible. The point $(0,0,1)$ is both the degenerate conic C_0 and the common nucleus of the other, non-degenerate, conics. A *Denniston maximal arc* is the union of all the C_λ for a fixed α.

Abatangelo and Larato [1], in 1989, proved results indicating that the Denniston arcs would not be easily generalised.

Theorem 6.1.1 (Abatangelo and Larato [1] pg. 198)**.** *If A is a subset of* $\mathrm{GF}(q)$ *such that the union of all conics C_λ, $\lambda \in A$, is a maximal arc then A is an additive subgroup of* $\mathrm{GF}(q)$*.*

Theorem 6.1.2 (Abatangelo and Larato [1] pg. 201-202)**.** *The dual of a Denniston maximal arc is also a Denniston maximal arc.*

That is, the Denniston arcs cannot be used to generate other maximal arcs by taking duals or by using other values for λ.

In 1980, Thas [83] constructed maximal arcs using linear representation. We now describe his methods. Let $S^* = \{s_1^*, s_2^* \dots, s_{q^d+1}^*\}$ be a $(d-1)$-spread of a parabolic quadric $\mathrm{Q} = \mathrm{Q}(2d, q)$, $d \geq 2$, and consider a hyperplane $\Sigma = \mathrm{PG}(2d-1, q)$ such that $\Sigma \cap \mathrm{Q}$ is an elliptic quadric $\mathrm{Q}^- = \mathrm{Q}^-(2d-1, q)$. Let N be the nucleus of Q. Then S^* induces a $(d-1)$-spread onto Σ given by

$$S = \{s_i = \langle s_i^*, N\rangle \cap \Sigma \mid i \in \{1, 2, \dots, q^d + 1\}\}$$

, and a $(d-2)$-spread

$$S^- = \{s_i \cap Q^- \mid i \in \{1, 2, \dots, q^d + 1\}\}$$

of $\mathrm{Q}^-(2d-1, q)$.

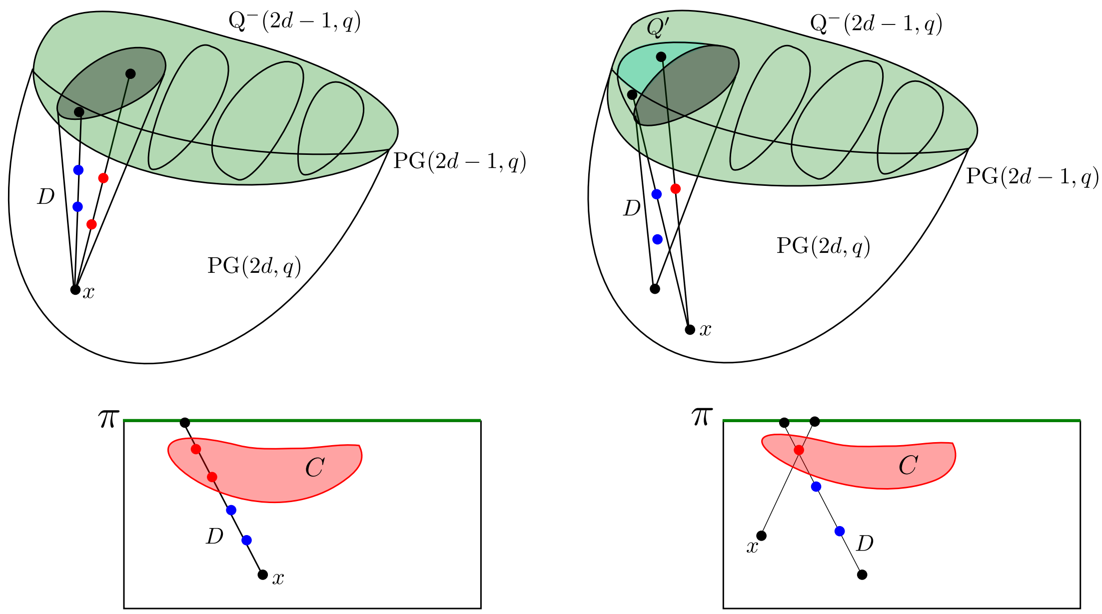


Figure 6.2 – When $x \in D$ and $x \notin D$.

Recall from Chapter 3 that we can create a translation plane π_S, of order q^d, from S. Let x be a point of $\mathrm{PG}(2d, q) \setminus \Sigma$. Consider the set of points C in this translation plane corresponding to the affine points that lie on a line joining x to a point of $\mathrm{Q}^-(2d-1, q)$. That is, x belongs to C, but no point of $\mathrm{Q}^-(2d-1, q)$ belongs to C. Therefore, no point of the translation line belongs to C.

We now show that C is a maximal q^{d-1}-arc. Figure 6.2 shows the types of lines that exist in π, and whether they contain points of C.

Consider an affine d-space D of $\mathrm{PG}(2d, q)$, containing the spread element s_i. If $x \in D$ then all the points in the span of x and $s_i \cap Q^-$ are in C, other than those in Q^-. That is,

$$\begin{aligned}|D \cap C| =& \frac{q^d - 1}{q-1} - \frac{q^{d-1} - 1}{q-1} \\ =& \frac{q^d - q^{d-1}}{q-1} \\ =& q^{d-1}.\end{aligned}$$

Suppose that $x \notin D$ and $\langle x, D\rangle \cap Q^-$ contains no points other than those of D. Then $|D \cap C| = 0$. Finally, suppose $D' := \langle x, D\rangle \cap Q^-$ contains a point z of $Q' := D' \cap Q^-$ such that $z \notin D$. Note that each point of Q' is contained within an element of S^-. Now, Q' contains the $(d-2)$-space $s_i \cap Q^-$ and therefore Q' is a cone with vertex a hyperplane of $s_i \cap Q^-$. Then

$$\begin{aligned}|Q'| =& \frac{q^{d-2} - 1}{q-1}(q-1)(q+1) + \frac{q^{d-2} - 1}{q-1} + q + 1 \\ =& \frac{q^{d-1} - 1}{q-1} + q^{d-1}\end{aligned}$$

where $(q^{d-1} - 1)/(q - 1)$ represents the points of $s_i \cap Q^-$. Each of the lines joining x to one of the remaining q^{d-1} points of Q' intersects D at a point. Therefore $|D \cap S| = q^{d-1}$ and every line of π_S meets C in 0 or q^{d-1} points. We call this maximal arc a *maximal q^{d-1}-arc of Thas type.*

Remark 6.1.3. *In 2010, Bader [7] proved that a translation plane of order q^n, q even, contains a maximal arc of Thas type if and only if it is symplectic. We do not explore this relationship but it is worth noting in context of the previous thesis chapters.*

Theorem 6.1.4 (Hamilton and Penttila [47] pg. 75)**.** *If the translation plane containing a Thas type maximal arc is Desarguesian then the maximal arc itself is Denniston.*

Thus, the Denniston maximal $(d-1)$-arcs in $\mathrm{PG}(2, q^d)$ can be constructed from linear representation and the Thas representation provides no new examples of maximal arcs in $\mathrm{PG}(2, q)$.

Remark 6.1.5. *In 1974, Thas [81] created maximal arcs from* $\mathrm{PG}(3, q)$ *using a similar method to that he used in 1980. Instead of the elliptic quadric, Thas used any ovoid in* $\mathrm{PG}(3, q)$ *such that the symplectic spread was tangent to the ovoid. The only other known ovoid of* $\mathrm{PG}(3, 2^m)$ *is the Suzuki-Tits ovoid [11] which exists only for m odd, and is tangent to the Lüneburg and Desarguesian spreads. The maximal* 2^{2s+1}*-arcs generated in* $\mathrm{PG}(2, 2^{2(2s+1)})$ *by the Suzuki-Tits ovoid are not of Denniston type [47] and are self-dual [46].*

Mathon generalised the Denniston construction of maximal arcs [67] in 2002. To follow Mathon's construction we consider the conics

$$C_{\alpha,\beta,\lambda} : \alpha x^2 + xy + \beta y^2 + \lambda z^2 = 0,$$

where $\alpha x^2 + x + \beta$ is irreducible over $\mathrm{GF}(q)$. All of these conics have nucleus $C_0 = (0, 0, 1)$ and, other than the case $\lambda = 0$, they are non-degenerate.

We define the *composition* of two conics $C_{\alpha,\beta,\lambda} \oplus C_{\alpha',\beta',\lambda'} = C_{\alpha\oplus\alpha',\beta\oplus\beta',\lambda\oplus\lambda'}$, $\lambda \neq \lambda'$, such that

$$\alpha \oplus \alpha' = \frac{\alpha\lambda + \alpha'\lambda'}{\lambda + \lambda'}, \beta \oplus \beta' = \frac{\beta\lambda + \beta'\lambda'}{\lambda + \lambda'}, \lambda \oplus \lambda' = \lambda + \lambda',$$

and

$$C_{\alpha\oplus\alpha',\beta\oplus\beta',\lambda\oplus\lambda'} : (\alpha \oplus \alpha')x^2 + xy + (\beta \oplus \beta')y^2 + (\lambda + \lambda')z^2 = 0.$$

This composition is commutative and, given that $\lambda \neq \lambda'$, it defines a non-degenerate conic.

Lemma 6.1.6 (Mathon [67] pg. 356)**.** *If $C_{\alpha,\beta,\lambda}$ and $C_{\alpha',\beta',\lambda'}$ are two non-degenerate conics, with $\lambda \neq \lambda'$ and $(\alpha \oplus \alpha')x^2 + x + (\beta \oplus \beta')$ is irreducible then $C_{\alpha,\beta,\lambda}, C_{\alpha',\beta',\lambda'}$ and $C_{\alpha\oplus\alpha',\beta\oplus\beta',\lambda\oplus\lambda'}$ are mutually disjoint.*

We say that a set of conics $\mathcal{K}$ is *closed under composition* if, for any pair of conics $C_{\alpha,\beta,\lambda} \neq C_{\alpha',\beta',\lambda'}$ in $\mathcal{K}$, $C_{\alpha\oplus\alpha',\beta\oplus\beta',\lambda\oplus\lambda'}$ is also in $\mathcal{K}$.

Theorem 6.1.7 (Mathon [67] pg. 357)**.** *Let $\mathcal{K}$ be a set of $2^d - 1$ non-degenerate conics in $\mathrm{PG}(2, 2^m)$, of the type $C_{\alpha,\beta,\lambda}$, with $1 \leq d \leq m$, that is closed under composition. Then the union of the points in $\mathcal{K}$, together with their common nucleus $(0, 0, 1)$ forms a maximal 2^d-arc.*

We call these maximal arcs *Mathon arcs.*

Lemma 6.1.8 (Mathon [67] pg. 356)**.** *The Denniston maximal arcs are all of Mathon type and all Mathon 4-arcs are Denniston arcs.*

A *Mathon* maximal n-arc is formed by taking the union of $n - 1$ disjoint conics together with their shared nucleus. That is, every Mathon maximal arc is a union of regular hyperovals.

By Lemma 6.0.10, we know that in $\mathrm{PG}(2, 2^{k+2})$, the dual arc of any maximal 2^k-arc will be a maximal 4-arc.

Theorem 6.1.9 (Hamiton and Mathon [46] pg. 256-257)**.** *If a Mathon maximal arc is not of Denniston type then its dual arc cannot be constructed from a closed set of conics.*

Thus, there exist maximal 4-arcs in $\mathrm{PG}(2, 2^{k+2})$ that are not of Mathon type, whenever there exist maximal 2^k-arcs of Mathon, but not Denniston, type.

The only known maximal 4-arcs in $\mathrm{PG}(2, q)$ are the Denniston 4-arcs, the duals of hyperovals in $\mathrm{PG}(2, 8)$, and the duals of Mathon 2^k-arcs. The maximal arcs of $\mathrm{PG}(2, q)$ have been classified for $q \leq 16$ by Ball and Blokhuis [13].

6.2 Restrictions on maximal arcs that contain regular hyperovals

The motivation for our work stemmed from an excellent result of Maes:

Theorem 6.2.1 (Maes [66] pg. 35S)**.** *A maximal arc consisting of disjoint conics on a common nucleus is a Mathon arc.*

We will not use Maes' condition that the conics are disjoint, and on the same nucleus, but will instead restrict the degree of the maximal arc. First we consider the restrictions on the number of regular hyperovals that can 'fit' in a maximal arc.

Two conics can meet in at most four points, by Lemma 2.3.2, so the minimum number of points covered by j conics is

$$\begin{aligned}\sum_{i=0}^{j-1}(q+1-4i) &= jq+j-4\frac{j(j-1)}{2}\\ &= jq+j-2j(j-1)\\ &= jq-2j^2+3j.\end{aligned}$$

Lemma 6.2.2. *A maximal n-arc can contain n distinct conics only when $q > n^2$.*

Proof. The number of points in a maximal n-arc must be larger than the number of points in n distinct conics. That is,

$$\begin{aligned}|\mathcal{K}| = q(n-1)+n &\geq nq+3n-2n^2\\ \Rightarrow -q+n &\geq -2n^2+3n \qquad (6.1)\\ \Rightarrow q &\leq 2n^2-2n.\end{aligned}$$

Now suppose that $n^2 < q < 2(n^2-n)$. We know also that n divides q and both are powers of two, so if $n = 2^k$ then $n^2 < q$ implies $q \geq 2n^2$, which is a contradiction to Equation 6.1. □

Lemma 6.2.3. *If a maximal n-arc $\mathcal{K}$ in $\mathrm{PG}(2,q)$ is a union of regular hyperovals then, for $q > n^2$, $\mathcal{K}$ contains exactly $n-1$ regular hyperovals.*

Proof. The maximum number of points that $n-2$ regular hyperovals contain is $(n-2)(q+2) < q(n-1)+n$. Thus $\mathcal{K}$ contains at least $n-1$ hyperovals. But if $\mathcal{K}$ contains n regular hyperovals then it must contain n conics, a contradiction. □

If a point lies on t regular hyperovals of $\mathcal{K}$ then we say that point has *multiplicity* $t-1$. That is, the multiplicity tells us the number of times a point is covered, after it has been covered once. We will call the sum of the multiplicities of the points of $\mathcal{K}$ the *intersection multiplicity* of $\mathcal{K}$.

Lemma 6.2.4. *If $\mathcal{K}$ is the union of $n-1$ distinct regular hyperovals then the intersection multiplicity of $\mathcal{K}$ is $n-2$.*

Proof. The number of points covered by the union of the hyperovals is $(q+2)(n-1)-x$, where x is the intersection multiplicity of $\mathcal{K}$. So we can calculate

$$q(n-1)+n = (q+2)(n-1)-x$$

which gives $x = n-2$. □

Lemma 6.2.5. *If a maximal n-arc $\mathcal{K}$ is the union of regular hyperovals then each point of $\mathcal{K}$ lies on an odd number of hyperovals.*

Proof. Suppose there are m hyperovals on the point P. The intersection multiplicity of $\mathcal{K}$ is $n-2$, and the number of lines through P is $q+1 > n-2$. Thus there is a line ℓ through P that does not contain any further intersection points, so ℓ contains $m+1$ points, of $\mathcal{K}$, from the m hyperovals through P. Now ℓ meets all remaining hyperovals of the arc in either 0 or 2 points and hence ℓ contains $m+1+2y$ points of $\mathcal{K}$ for some y. Therefore, m is odd. □

In other words, the multiplicity of every point of $\mathcal{K}$ is odd.

Let us now focus on maximal 4-arcs. We can immediately see from the preceding results that a maximal 4-arc, formed by taking a union of regular hyperovals, must contain exactly three regular hyperovals and one intersection point with multiplicity two.

If three regular hyperovals meet in a point P then either P is a nucleus for at least two hyperovals or P is a point of the conic for at least two hyperovals. Thus the maximal arc extends from either (a) two disjoint conics on a common nucleus, or (b) two conics meeting in a point.

Case (a) — Two disjoint conics on the same nucleus

Theorem 6.2.6 (Aguglia, Giuzzi and Korchmáros [3], Section 5)**.** *Two disjoint conics on the same nucleus can be extended to a unique maximal* 4*-arc of Mathon type.*

Corollary 6.2.7 (Aguglia, Giuzzi and Korchmáros [3], Section 5)**.** *Any maximal* 4*-arc* $\mathcal{K}$ *containing two disjoint conics* C_1, C_2 *on the same nucleus* N *is a Mathon* 4*-arc.*

Proof. Suppose $\mathcal{K}$ is the unique maximal 4-arc of Mathon type containing $K = C_1 \cup C_2 \cup \{N\}$, as per Theorem 6.2.6, and consider the external lines of K. The addition of one extra conic to K is not sufficient to turn any external line into a 4-secant so the external lines to $\mathcal{K}$ must be the same as those to K. Note also that there is no point of $\mathrm{PG}(2,q) \setminus \mathcal{K}$ such that all lines through it meet the maximal arc. Thus the points of $\mathrm{PG}(2,q) \setminus K$ that are on no external lines are exactly the points that, when added, give the unique Mathon-type arc, and there does not exist another set of points that can be added to K to give a maximal arc. □

Case (b) — Two conics that meet in a point

Let us denote the two conics by C_1, C_2 and the nuclei by N_1, N_2. Let $P = C_1 \cap C_2$ and $K = C_1 \cup C_2 \cup \{N_1, N_2\}$.

Theorem 6.2.8 (Aguglia, Giuzzi and Korchmáros [3], Section 5)**.** *If* P, N_1, N_2 *are collinear then there exists a line* s*, through* P*, such that through every point of* s *there is a line, other than* s *itself, containing at least three points of* K*.*

Corollary 6.2.9. *If* P, N_1, N_2 *are collinear then there exists a line* s*, through* P*, such that through every point of* s *there is a line, other than* s *itself, containing at least four points of* K*.*

Proof. Suppose, for $X \in s$, that ℓ is a line containing three points of $C_1 \cup C_2 \cup \{N_1, N_2\}$. Thus, ℓ meets both $C_1 \cup \{N_1\}$ and $C_2 \cup \{N_2\}$, and it must meet each in two points. Because $\ell \neq s$, and therefore $P \notin \ell$, these four points must be distinct. □

Thus, there is no point on s that can be added to K without creating a 5-secant. See Figure 6.3.

So if P, N_1, N_2 are collinear then K cannot be extended to a maximal 4-arc. We follow the same

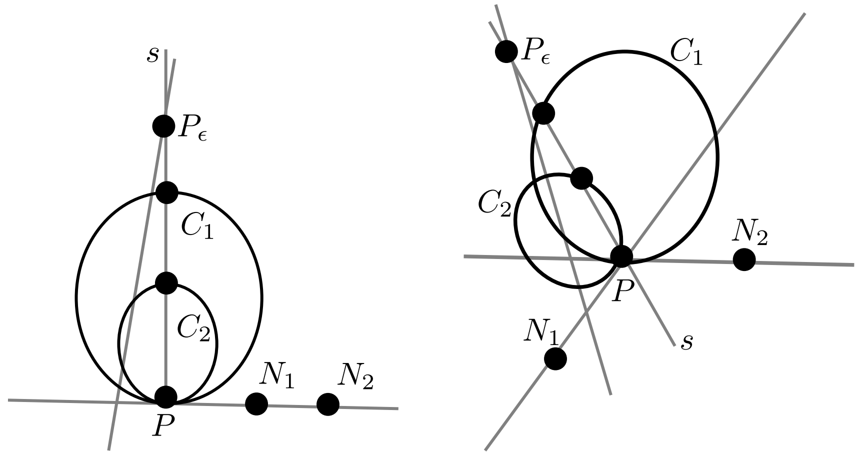


Figure 6.3 – The two arrangements.

methods used by Aguglia, Giuzzi, and Korchmáros [3] to consider the case when the line N_1N_2 does not pass through P. This case is illustrated in Figure 6.3.

Theorem 6.2.10. *Let C_1, C_2 be two distinct conics, sharing the point P, with nuclei N_1, N_2 respectively. Then there exists a line s through P such that every point on s lies on at least one 4-secant to K.*

Proof. We may assume that P, N_1, N_2 are not collinear and we choose our coordinate system such that $P = (0,0,1), N_1 = (\lambda_1, 0, 1), N_2 = (0, \lambda_2, 1)$, $\lambda_1, \lambda_2 \neq 0$. Then

$$C_1 : \alpha_1 x^2 + \beta_1 y^2 + xy + \lambda_1 yz = 0, and$$
$$C_2 : \alpha_2 x^2 + \beta_2 y^2 + xy + \lambda_2 xz = 0$$

with $\alpha_1 \neq 0, \beta_2 \neq 0$. Let s be the line $x = 0$, containing N_2, P and another point $(0, \lambda_1/\beta_1, 1)$ of C_1. Let $P_m \in C_1$ and $P_t \in C_2$, so $P_m = (\lambda_1 m, \lambda_1, \alpha_1 m^2 + \beta_1 + m)$ and $P_t = (\lambda_2, \lambda_2 t, \alpha_2 + \beta_2 t^2 + t)$.

Then for any $\epsilon \in \mathrm{GF}(q) \setminus \{0\}$ such that $P_\epsilon = (0, \epsilon, 1)$ and $\epsilon \notin \{0, \lambda_1/\beta_1, \lambda_2\}$, $P_\epsilon \in s$ we have $P_\epsilon \notin K = C_1 \cup C_2 \cup \{N_1, N_2\}$.

Then the point P_ϵ is on the line $P_m P_t$ if and only if

$$\begin{vmatrix} \lambda_1 m & \lambda_1 & \alpha_1 m^2 + \beta_1 + m \\ \lambda_2 & \lambda_2 t & \alpha_2 + \beta_2 t^2 + t \\ 0 & \epsilon & 1 \end{vmatrix} = 0$$

$$\lambda_1\lambda_2 mt + \lambda_2\epsilon\alpha_1 m^2 + \lambda_2\epsilon m + \lambda_2\epsilon\beta_1 + \lambda_2\lambda_1 + \lambda_1\epsilon\alpha_2 m + \lambda_1\epsilon\beta_2 t^2 m + \lambda_1\epsilon mt = 0. \tag{6.2}$$

Therefore we wish to show that, for any ϵ, Equation 6.2 holds for some value of m and t.

Consider this equation as the affine equation of a cubic curve $\mathcal{D}$ in the indeterminates m and t. The only points at infinity of $\mathcal{D}$ are $X_\infty = (1, 0, 0)$ and $Y_\infty = (0, 1, 0)$.

The homogeneous equation is

$$\mathcal{D} : \lambda_1\lambda_2 mtz + \lambda_2\epsilon\alpha_1 m^2 z + \lambda_2\epsilon m z^2 + \lambda_2\epsilon\beta_1 z^3 + \lambda_2\lambda_1 z^3 + \lambda_1\epsilon\alpha_2 m z^2 + \lambda_1\epsilon\beta_2 t^2 m + \lambda_1\epsilon mtz = 0. \quad (6.3)$$

A singular point on an algebraic plane cubic is a point at which all partial derivatives are zero. Note that $(0, 0, 0)$ is not a projective point and therefore we consider $(m, t, z) \neq (0, 0, 0)$. Now the partial derivatives of $\mathcal{D}$ are

$$\frac{d}{dm} = \lambda_1\lambda_2 tz + \lambda_2\epsilon z^2 + \lambda_1\epsilon z^2 + \lambda_1\epsilon\beta_2 t^2 + \lambda_1\epsilon tz,$$
$$\frac{d}{dz} = \lambda_1\lambda_2 mt + \lambda_2\epsilon m^2 + \lambda_2\epsilon\beta_1 z^2 + \lambda_2\lambda_1 z^2 + \lambda_1\epsilon mt, \text{ and}$$
$$\frac{d}{dt} = \lambda_1\lambda_2 mz + \lambda_1\epsilon mz,$$

and, if neither m nor z are zero, then

$$\frac{d}{dt} = 0 \Rightarrow \lambda_2 = \epsilon \text{ or } \lambda_1 = 0.$$

Neither of these cases are of importance, as they imply $P_\epsilon = N_2$ and $N_1 = P$, respectively. Therefore, we consider the cases $m = 0$ and $z = 0$. If $z = 0$, then

$$\frac{d}{dm} = \epsilon\beta_2 t^2,$$

which is equal to zero exactly when $t = 0$. This requires $m \neq 0$ and that

$$\frac{d}{dz} = \lambda_2\epsilon m^2 = 0,$$

which is a contradiction. Thus, $z \neq 0$ and we consider $m = 0$. This gives

$$\frac{d}{dz} = \lambda_2\epsilon\beta_1 z^2 + \lambda_2\lambda_1 z^2,$$

which is equal to zero exactly when $z = 0$, $\lambda_2 = 0$ or $\epsilon\beta_1 = \lambda_1$, none of which are permitted.

Therefore, $\mathcal{D}$ is a nonsingular plane cubic and, by the *Hasse bound* [48], $\mathcal{D}$ contains at least $q + 1 - 2\sqrt{q}$ points over GF(q) (see Hirschfeld [53]). We know that there are only two points at infinity so, provided that $q \geq 8$, there exists a point (m, t, z) that is not at infinity. This implies that, for any given $\epsilon \in \text{GF}(q) \setminus \{0\}$, there exists a pair of values $\overline{m}, \overline{t} \in \text{GF}(q) \setminus \{0\}$ satisfying Equation (6.2) and that the resulting points will be distinct. Hence, for any point $P_\epsilon \in s$, there exists a line $\ell \neq s$ through P_ϵ, that meets both C_1 and C_2 in a point. Now C_1 and C_2 are both hyperovals, so ℓ must meet $C_1 \cup N_1$ and $C_2 \cup N_2$ in two points each and therefore every point P_ϵ lies on a 4-secant to K. □

No point of s can be added to the partial maximal arc K and s is a 3-secant in K, therefore K cannot be completed to a maximal 4-arc.

Corollary 6.2.11. *No maximal 4-arc can contain two conics that meet in exactly one point.*

Therefore, we have now proved Theorem 1.3.1 of the Introduction. The only maximal 4-arc that is a union of regular hyperovals is the Mathon 4-arc.

Index

Bibliography

[1] V. Abatangelo and B. Larato. A characterization of Denniston's maximal arcs. *Geom. Dedicata*, 30(2):197–203, 1989.

[2] R. Abbott, J. Bray, S. Linton, S. Nickerson, S. Norton, R. Parker, I. Suleiman, J. Tripp, P. Walsh, and R. Wilson. Atlas of finite group representations - version 3, August 2013.

[3] A. Aguglia, L. Giuzzi, and G. Korchmáros. Algebraic curves and maximal arcs. *J. Algebraic Combin.*, 28(4):531–544, 2008.

[4] R. W. Ahrens and G. Szekeres. On a combinatorial generalization of 27 lines associated with a cubic surface. *J. Austral. Math. Soc.*, 10:485–492, 1969.

[5] A. A. Albert. Generalized twisted fields. *Pacific J. Math.*, 11:1–8, 1961.

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

[7] L. Bader. A remark on symplectic spreads. *Ricerche di Matematica*, 59(1):125–128, 2010.

[8] L. Bader, W. M. Kantor, and G. Lunardon. Symplectic spreads from twisted fields. *Boll. Un. Mat. Ital. A (7)*, 8(3):383–389, 1994.

[9] L. Bader and G. Lunardon. Desarguesian spreads. *Ric. Mat.*, 60(1):15–37, 2011.

[10] R. Baer. Partitionen abelscher Gruppen. *Arch. Math. (Basel)*, 14:73–83, 1963.

[11] B. Bagchi and N. S. N. Sastry. Even order inversive planes, generalized quadrangles and codes. *Geo. Dedicata*, 22:137–147.

[12] S. Ball, J. Bamberg, M. Lavrauw, and T. Penttila. Symplectic spreads. *Des. Codes Cryptogr.*, 32(1-3):9–14, 2004.

[13] S. Ball and A. Blokhuis. The classification of maximal arcs in small Desarguesian planes. *Bull. Belg. Math. Soc. Simon Stevin*, 9(3):433–445, 2002.

[14] S. Ball, A. Blokhuis, and F. Mazzocca. Maximal arcs in Desarguesian planes of odd order do not exist. *Combinatorica*, 17(1):31–41, 1997.

[15] S. Ball, P. Govaerts, and L. Storme. On ovoids of parabolic quadrics. *Des. Codes Cryptogr.*, 38(1):131–145, 2006.

[16] J. Bamberg, M. Giudici, and G. F. Royle. Hemisystems of small flock generalized quadrangles. *Des. Codes Cryptogr.*, 67(1):137–157, 2013.

[17] A. Barlotti. Sui $\{k; n\}$-archi di un piano lineare finito. *Boll. Un. Mat. Ital. (3)*, 11:553–556, 1956.

[18] A. Barlotti and J. Cofman. Finite Sperner spaces constructed from projective and affine spaces. *Abh. Math. Sem. Univ. Hamburg*, 40:231–241, 1974.

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

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

[21] R. H. Bruck. Construction problems of finite projective planes. In *Combinatorial Mathematics and its Applications (Proc. Conf., Univ. North Carolina, Chapel Hill, N.C., 1967)*, pages 426–514. Univ. North Carolina Press, Chapel Hill, N.C., 1969.

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

[23] R. H. Bruck and R. C. Bose. Linear representations of projective planes in projective spaces. *J. Algebra*, 4:117–172, 1966.

[24] F. Buekenhout. Plans projectifs à ovoïdes pascaliens. *Arch. Math. (Basel)*, 17:89–93, 1966.

[25] 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.

[26] F. Buekenhout, editor. *Handbook of incidence geometry*. North-Holland, Amsterdam, 1995. Buildings and foundations.

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

[28] P. J. Cameron. *Projective and polar spaces*, volume 13 of *QMW Maths Notes*. Queen Mary and Westfield College School of Mathematical Sciences, London, 199?

[29] L. R. A. Casse, J. A. Thas, and P. R. Wild. $(q^n + 1)$-sets of $\mathrm{PG}(3n-1, q)$, generalized quadrangles and Laguerre planes. *Simon Stevin*, 59(1):21–42, 1985.

[30] C. Charnes. Quadratic matrices and the translation planes of order 5^2. In *Coding theory, design theory, group theory (Burlington, VT, 1990)*, Wiley-Intersci. Publ., pages 155–161. Wiley, New York, 1993.

[31] C. Charnes and U. Dempwolff. The translation planes of order 49 and their automorphism groups. *Math. Comp.*, 67(223):1207–1224, 1998.

[32] A. Cossu. Su alcune proprietà dei $\{k, n\}$-archi di un piano proiettivo sopra un corpo finito. *Rend. Mat. e Appl. (5)*, 20:271–277, 1961.

[33] T. Czerwinski and D. Oakden. The translation planes of order twenty-five. *J. Combin. Theory Ser. A*, 59(2):193–217, 1992.

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

[35] U. Dempwolff. Translation planes of order 27. *Des. Codes Cryptogr.*, 4(2):105–121, 1994.

[36] U. Dempwolff and A. Reifart. Translation planes of order 16 admitting a Baer 4-group. *J. Combin. Theory Ser. A*, 32(1):119–124, 1982.

[37] U. Dempwolff and A. Reifart. The classification of the translation planes of order 16. I. *Geom. Dedicata*, 15(2):137–153, 1983.

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

[39] G. Faina and G. Korchmáros. Aldo Cossu's work in finite geometry. *Mediterr. J. Math.*, 3(3-4):349–361, 2006.

[40] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.6.3*, 2013.

[41] N. Gill. Polar spaces and embeddings of classical groups. *New Zealand J. Math.*, 36:175–184, 2007.

[42] A. Gunawardena. Primitive ovoids in $O_8^+(q)$. *J. Combin. Theory Ser. A*, 89(1):70–76, 2000.

[43] Inc. Gurobi Optimization. Gurobi optimizer reference manual, 2012.

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

[45] M. Hall, Jr., J. D. Swift, and R. J. Walker. Uniqueness of the projective plane of order eight. *Math. Tables Aids Comput.*, 10:186–194, 1956.

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

[47] N. Hamilton and T. Penttila. Groups of maximal arcs. *J. Combin. Theory Ser. A*, 94(1):63–86, 2001.

[48] H. Hasse. Zyklische unverzweigte Erweiterungskörper vom Primzahlgrade p über einem algebraischen Funktionenkörper der Charakteristik p. *Monatsh. Math. Phys.*, 43(1):477–492, 1936.

[49] C. Hering. Eine nicht-desarguessche zweifach transitive affine Ebene der Ordnung 27. *Abh. Math. Sem. Univ. Hamburg*, 34:203–208, 1969/1970.

[50] G. Hessenberg. Über einen geometrischen Calcül (Verknüpfungs-Calcül). *Acta Math.*, 29(1):1–23, 1905.

[51] D. Hilbert. *Grundlagen der Geometrie*. Neunte Auflage, revidiert und ergänzt von Paul Bernays. B. G. Teubner Verlagsgesellschaft, Stuttgart, 1962.

[52] J. W. P. Hirschfeld. *Projective geometries over finite fields.* The Clarendon Press Oxford University Press, New York, 1979. Oxford Mathematical Monographs.

[53] 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.

[54] J. W. P. Hirschfeld and J. A. Thas. *General Galois geometries.* Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, 1991. Oxford Science Publications.

[55] D. R. Hughes and F. C. Piper. *Projective planes.* Springer-Verlag, New York, 1973. Graduate Texts in Mathematics, Vol. 6.

[56] N. L. Johnson, V. Jha, and M. Biliotti. *Handbook of finite translation planes*, volume 289 of *Pure and Applied Mathematics (Boca Raton).* Chapman & Hall/CRC, Boca Raton, FL, 2007.

[57] W. M. Kantor. Spreads, translation planes and Kerdock sets. I. *SIAM J. Algebraic Discrete Methods*, 3(2):151–165, 1982.

[58] W. M. Kantor. Commutative semifields and symplectic spreads. *J. Algebra*, 270(1):96–114, 2003.

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

[60] W. M. Kantor. Isomorphisms of symplectic planes, 2007.

[61] C. F. Klein. *Uber die Transformation der allgemeinen Gleichung des zweiten Grades zwischen Linien-Koordinaten auf eine kanonische Form.* PhD thesis, Friedrich-Wilhelms-Universitat, 1868.

[62] S. Linton. Finding the smallest image of a set. In *ISSAC 2004*, pages 229–234. ACM, New York, 2004.

[63] G. Lunardon. Symplectic spreads and finite semifields. *Des. Codes Cryptogr,*, 44(1-3):39–48, 2007.

[64] G. Lunardon, G. Marino, O. Polverino, and R. Trombetti. Symplectic semifield spreads of pg(5, q) and the veronese surface. *Ricerche di Matematica*, 60(1):125–142, 2011.

[65] H. Lüneburg. *Translation planes.* Springer-Verlag, Berlin, 1980.

[66] T. Maes. *A geometric approach to Mathon maximal arcs.* PhD thesis, Ghent University, 2011.

[67] R. Mathon. New maximal arcs in Desarguesian planes. *J. Combin. Theory Ser. A*, 97(2):353–368, 2002.

[68] R. Mathon and G. F. Royle. The translation planes of order 49. *Des. Codes Cryptogr.*, 5(1):57–72, 1995.

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

[70] S. E. Payne and J. A. Thas. Generalized quadrangles with symmetry. *Simon Stevin*, 49(1/2):3–32, 1975/76.

[71] S. E. Payne and J. A. Thas. *Finite generalized quadrangles*, volume 110 of *Research Notes in Mathematics*. Pitman (Advanced Publishing Program), Boston, MA, 1984.

[72] T. Penttila. Translation generalised quadrangles and elation laguerre planes of order 16. Preprint, 2000.

[73] 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.

[74] B. Segre. Ovals in a finite projective plane. *Canad. J. Math.*, 7:414–416, 1955.

[75] B. Segre. Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane. *Ann. Mat. Pura Appl. (4)*, 64:1–76, 1964.

[76] E. E. Shult. Problems by the wayside. *Discrete Math.*, 294(1-2):175–201, 2005.

[77] E. E. Shult and J. A. Thas. m-systems of polar spaces. *J. Combin. Theory Ser. A*, 68(1):184–204, 1994.

[78] E. E. Shult and J. A. Thas. Constructions of polygons from buildings. *Proc. London Math. Soc. (3)*, 71(2):397–440, 1995.

[79] C. Suetake. A new class of translation planes of order q^3. *Osaka J. Math.*, 22(4):773–786, 1985.

[80] 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.

[81] J. A. Thas. Construction of maximal arcs and partial geometries. *Geometriae Dedicata*, 3:61–64, 1974.

[82] J. A. Thas. Some results concerning $\{(q+1)(n-1); n\}$-arcs and $\{(q+1)\ (n-1)+1; n\}$-arcs in finite projective planes of order q. *J. Combinatorial Theory Ser. A*, 19(2):228–232, 1975.

[83] J. A. Thas. Construction of maximal arcs and dual ovals in translation planes. *European J. Combin.*, 1(2):189–192, 1980.

[84] J. Tits. *Buildings of spherical type and finite BN-pairs.* Lecture Notes in Mathematics, Vol. 386. Springer-Verlag, Berlin, 1974.

[85] T. Vahlen. *Abstrakte Geometrie. Untersuchungen über die Grundlagen der Euklidischen und nicht-Euklidischen Geometrie.* S. Hirzel, Leipzig, 1940. Zweite, neubearbeitete Auflage. Zweites Beiheft zu Deutsche Mathematik.

[86] O. Veblen and J. H. Maclagan-Wedderburn. Non-Desarguesian and non-Pascalian geometries. *Trans. Amer. Math. Soc.*, 8(3):379–388, 1907.

[87] O. Veblen and J. W. Young. *Projective geometry. Vol. 2 (by Oswald Veblen).* Blaisdell Publishing Co. Ginn and Co. New York-Toronto-London, 1965.

[88] 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.

[89] W. D. Wallis. Configurations arising from maximal arcs. *J. Combinatorial Theory Ser. A*, 15:115–119, 1973.

[90] B. Williams. *Ovoids of parabolic and hyperbolic spaces.* PhD thesis, The University of Western Australia, 1999.

[91] M. Zorn. Theorie der alternativen ringe. *Abh. Math. Sem. Hamburg*, 8:123–147, 1930.

Appendix A

Spread data for $\mathrm{W}(5,5)$

Let W be the symplectic space with Gram matrix:

$$\begin{pmatrix} 0 & 0 & 0 & 3 & 0 & 4 \\ 0 & 0 & 0 & 0 & 4 & 1 \\ 0 & 0 & 0 & 4 & 1 & 3 \\ 2 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 4 & 0 & 0 & 0 \\ 1 & 4 & 2 & 0 & 0 & 0 \end{pmatrix}.$$

For each spread S we list elements to generate the stabiliser group S, and one plane from each orbit of the stabiliser on S.

A.1 A_4

2C

$$\begin{pmatrix} 3\mathrm{I} & 0 \\ 0 & 2\mathrm{I} \end{pmatrix}$$

3C

$$\begin{bmatrix} 1 & 0 & 4 & 0 & 2 & 1 \\ 1 & 2 & 4 & 1 & 3 & 1 \\ 4 & 3 & 2 & 4 & 0 & 2 \\ 0 & 4 & 4 & 4 & 3 & 0 \\ 3 & 0 & 3 & 3 & 0 & 0 \\ 1 & 3 & 0 & 2 & 2 & 1 \end{bmatrix}$$

Orbit representatives:

$$\begin{pmatrix} 0&1&0&0&1&2\\ 0&0&1&0&3&0\\ 0&0&0&1&4&4 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&0&1\\ 0&1&0&2&1&0\\ 0&0&1&0&3&2 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&0&2\\ 0&1&0&1&2&1\\ 0&0&1&3&4&3 \end{pmatrix},$$
$$\begin{pmatrix} 1&0&0&0&0&4\\ 0&1&0&0&4&1\\ 0&0&1&4&3&0 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&0&3\\ 0&1&0&3&3&1\\ 0&0&1&3&2&0 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&1&0\\ 0&0&1&0&2&4\\ 0&0&0&1&2&3 \end{pmatrix},$$
$$\begin{pmatrix} 1&0&0&0&1&1\\ 0&1&0&1&2&3\\ 0&0&1&0&1&1 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&1&2\\ 0&1&0&4&4&1\\ 0&0&1&3&4&2 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&2&4\\ 0&1&0&3&3&2\\ 0&0&1&4&2&3 \end{pmatrix},$$
$$\begin{pmatrix} 1&0&0&0&3&2\\ 0&1&0&0&2&1\\ 0&0&1&1&4&4 \end{pmatrix}, \begin{pmatrix} 1&0&0&1&1&0\\ 0&1&0&0&1&1\\ 0&0&1&2&2&1 \end{pmatrix}, \begin{pmatrix} 1&0&0&1&2&1\\ 0&1&0&4&4&3\\ 0&0&1&3&1&0 \end{pmatrix},$$
$$\begin{pmatrix} 1&0&0&1&4&4\\ 0&1&0&3&4&4\\ 0&0&1&3&1&4 \end{pmatrix}, \begin{pmatrix} 1&0&0&2&0&0\\ 0&1&0&4&2&2\\ 0&0&1&3&2&1 \end{pmatrix}, \begin{pmatrix} 1&0&0&2&2&3\\ 0&1&0&2&2&0\\ 0&0&1&2&2&2 \end{pmatrix}.$$

A.2 D_{18}

2B $\qquad\qquad$ $\theta = (3B)^2$

$$\begin{bmatrix} 0&0&4&4&2&0\\ 3&0&0&0&3&2\\ 1&2&2&2&4&3\\ 3&2&0&1&3&4\\ 3&2&1&4&1&1\\ 3&3&0&3&3&1 \end{bmatrix} \qquad \begin{bmatrix} 0&2&0&0&0&3\\ 3&1&3&4&1&4\\ 0&1&4&2&2&4\\ 2&3&1&0&1&1\\ 3&4&4&2&0&2\\ 0&2&4&4&2&0 \end{bmatrix}$$

Orbit representatives:

$$\begin{pmatrix} 0&0&1&0&0&2\\ 0&0&0&1&0&2\\ 0&0&0&0&1&3 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&0&0\\ 0&1&0&0&2&0\\ 0&0&1&0&3&0 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&0&2\\ 0&1&0&3&2&2\\ 0&0&1&2&0&0 \end{pmatrix},$$
$$\begin{pmatrix} 1&0&0&0&0&3\\ 0&1&0&3&3&1\\ 0&0&1&4&0&3 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&1&0\\ 0&1&3&0&4&3\\ 0&0&0&1&4&3 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&1&2\\ 0&1&0&3&3&3\\ 0&0&1&0&4&3 \end{pmatrix},$$
$$\begin{pmatrix} 1&0&0&0&4&2\\ 0&1&4&0&1&2\\ 0&0&0&1&0&3 \end{pmatrix}.$$

A.3 C_6

2C

$$\begin{pmatrix} 3\mathrm{I} & 0 \\ 0 & 2\mathrm{I} \end{pmatrix}$$

3C

$$\begin{pmatrix} \mathrm{A} & 0 \\ 0 & \mathrm{A} \end{pmatrix},$$

with $\mathrm{A} = (1, z^5, z^{10})$, where z is the primitive root of $\mathrm{GF}(q^3)$.

Orbit representatives:

$$\begin{pmatrix} 0&0&0&1&0&0 \\ 0&0&0&0&1&0 \\ 0&0&0&0&0&1 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&0&1 \\ 0&1&0&2&1&0 \\ 0&0&1&2&4&3 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&0&2 \\ 0&1&0&4&4&0 \\ 0&0&1&0&4&4 \end{pmatrix},$$

$$\begin{pmatrix} 1&0&0&0&0&4 \\ 0&1&0&0&1&1 \\ 0&0&1&4&1&0 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&0&3 \\ 0&1&0&1&3&0 \\ 0&0&1&3&3&0 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&1&0 \\ 0&1&0&4&1&3 \\ 0&0&1&2&4&0 \end{pmatrix},$$

$$\begin{pmatrix} 1&0&0&0&1&1 \\ 0&1&0&1&2&3 \\ 0&0&1&1&4&4 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&1&2 \\ 0&1&0&2&0&0 \\ 0&0&1&3&4&2 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&1&4 \\ 0&1&0&3&4&1 \\ 0&0&1&3&2&1 \end{pmatrix},$$

$$\begin{pmatrix} 1&0&0&0&1&3 \\ 0&1&0&4&0&0 \\ 0&0&1&4&1&2 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&2&0 \\ 0&1&0&3&0&1 \\ 0&0&1&0&3&3 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&2&1 \\ 0&1&0&3&2&0 \\ 0&0&1&2&2&1 \end{pmatrix},$$

$$\begin{pmatrix} 1&0&0&0&2&2 \\ 0&1&0&4&0&2 \\ 0&0&1&3&4&1 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&4&1 \\ 0&1&0&1&2&1 \\ 0&0&1&0&4&3 \end{pmatrix}, \begin{pmatrix} 1&0&0&0&4&4 \\ 0&1&0&2&0&1 \\ 0&0&1&0&3&4 \end{pmatrix},$$

$$\begin{pmatrix} 1&0&0&0&3&3 \\ 0&1&0&1&4&3 \\ 0&0&1&4&3&0 \end{pmatrix}, \begin{pmatrix} 1&0&0&1&0&0 \\ 0&1&0&0&1&0 \\ 0&0&1&0&0&1 \end{pmatrix}, \begin{pmatrix} 1&0&0&1&0&2 \\ 0&1&0&3&4&2 \\ 0&0&1&0&3&0 \end{pmatrix},$$

$$\begin{pmatrix} 1&0&0&1&2&0 \\ 0&1&0&4&0&4 \\ 0&0&1&0&1&4 \end{pmatrix}, \begin{pmatrix} 1&0&0&1&4&4 \\ 0&1&0&3&0&4 \\ 0&0&1&1&4&3 \end{pmatrix}, \begin{pmatrix} 1&0&0&2&0&0 \\ 0&1&0&0&2&0 \\ 0&0&1&0&0&2 \end{pmatrix},$$

$$\begin{pmatrix} 1&0&0&2&0&2 \\ 0&1&0&4&2&0 \\ 0&0&1&0&3&1 \end{pmatrix}, \begin{pmatrix} 1&0&0&2&4&2 \\ 0&1&0&4&1&4 \\ 0&0&1&1&1&0 \end{pmatrix}, \begin{pmatrix} 1&0&0&4&0&0 \\ 0&1&0&0&4&0 \\ 0&0&1&0&0&4 \end{pmatrix}.$$

A.4 C_{10}

2C

$$\begin{pmatrix} 3\mathrm{I} & 0 \\ 0 & 2\mathrm{I} \end{pmatrix}$$

5E

$$\begin{pmatrix} A & B \\ B & A \end{pmatrix},$$

where: A = $\begin{pmatrix} 2 & 4 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ and B = $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 4 & 4 & 0 \end{pmatrix}$.

Orbit representatives:

$$\begin{pmatrix} 1 & 0 & 0 & 3 & 0 & 1 \\ 0 & 1 & 0 & 2 & 2 & 0 \\ 0 & 0 & 1 & 4 & 2 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 & 0 & 4 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 2 & 3 & 3 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 4 & 3 & 0 \\ 0 & 0 & 1 & 2 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 4 \\ 0 & 1 & 3 & 0 & 4 & 0 \\ 0 & 0 & 0 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 4 & 3 \\ 0 & 0 & 1 & 4 & 1 & 3 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 2 \\ 0 & 1 & 0 & 4 & 4 & 1 \\ 0 & 0 & 1 & 0 & 0 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 0 \\ 0 & 1 & 2 & 0 & 3 & 3 \\ 0 & 0 & 0 & 1 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 2 \\ 0 & 1 & 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 2 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 3 & 4 \\ 0 & 1 & 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 0 & 4 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 2 & 1 & 0 \\ 0 & 0 & 1 & 0 & 4 & 3 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 3 \\ 0 & 1 & 0 & 2 & 0 & 3 \\ 0 & 0 & 1 & 4 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 2 & 3 & 2 \\ 0 & 1 & 0 & 2 & 4 & 2 \\ 0 & 0 & 1 & 1 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 4 & 0 & 0 \\ 0 & 1 & 0 & 0 & 4 & 0 \\ 0 & 0 & 1 & 0 & 0 & 4 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 0 & 0 & 4 & 2 & 3 \\ 0 & 1 & 0 & 0 & 4 & 4 \\ 0 & 0 & 1 & 2 & 3 & 4 \end{pmatrix}.$$

A.5 D_{30}

2B

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 3 \\ 0 & 3 & 1 & 3 & 3 & 2 \\ 3 & 2 & 4 & 2 & 1 & 2 \\ 3 & 3 & 0 & 1 & 2 & 3 \\ 3 & 1 & 2 & 0 & 3 & 0 \\ 2 & 2 & 1 & 3 & 0 & 4 \end{bmatrix}$$

3B

$$\begin{bmatrix} 0 & 4 & 4 & 0 & 4 & 3 \\ 3 & 0 & 0 & 0 & 1 & 1 \\ 2 & 1 & 4 & 2 & 4 & 3 \\ 1 & 2 & 3 & 1 & 0 & 1 \\ 0 & 4 & 4 & 2 & 2 & 1 \\ 3 & 3 & 4 & 3 & 2 & 1 \end{bmatrix}$$

5E has matrix $\begin{pmatrix} A & B \\ B & A \end{pmatrix}$, where: A = $\begin{pmatrix} 2 & 4 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ and B = $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 4 & 4 & 0 \end{pmatrix}$.

Orbit representatives:

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 4 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 3 & 2 & 4 \\ 0 & 0 & 1 & 3 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 1 & 3 & 1 \\ 0 & 0 & 1 & 2 & 0 & 0 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 3 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 4 & 4 \\ 0 & 0 & 1 & 2 & 3 & 4 \end{pmatrix}.$$

A.6 D_{14}

2B

$$\begin{bmatrix} 3 & 0 & 2 & 3 & 3 & 2 \\ 4 & 2 & 0 & 4 & 2 & 3 \\ 0 & 4 & 2 & 1 & 0 & 2 \\ 2 & 3 & 1 & 2 & 0 & 3 \\ 2 & 4 & 3 & 1 & 3 & 0 \\ 1 & 3 & 4 & 0 & 1 & 3 \end{bmatrix}$$

7A

$$\begin{bmatrix} 0 & 1 & 2 & 2 & 3 & 0 \\ 4 & 4 & 1 & 0 & 2 & 3 \\ 2 & 1 & 4 & 1 & 1 & 2 \\ 0 & 1 & 0 & 0 & 2 & 4 \\ 0 & 0 & 1 & 3 & 3 & 2 \\ 2 & 2 & 0 & 4 & 2 & 3 \end{bmatrix}$$

Orbit representatives:

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 3 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 4 & 4 & 1 \\ 0 & 0 & 1 & 2 & 0 & 3 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 4 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 4 \\ 0 & 1 & 0 & 2 & 0 & 2 \\ 0 & 0 & 1 & 4 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 3 \\ 0 & 1 & 0 & 3 & 0 & 1 \\ 0 & 0 & 1 & 3 & 0 & 0 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 4 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 & 0 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 2 \\ 0 & 1 & 3 & 0 & 0 & 3 \\ 0 & 0 & 0 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 4 & 3 \\ 0 & 1 & 0 & 0 & 4 & 1 \\ 0 & 0 & 1 & 2 & 1 & 3 \end{pmatrix}.$$

Appendix B

Spread data for $\mathrm{W}(5,7)$

Let W be the symplectic space with Gram matrix:

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & 0 \end{pmatrix}.$$

The group elements to generate the stabiliser of the spread S are listed below.

Order 3:

$$\begin{bmatrix} 6 & 6 & 0 & 4 & 4 & 4 \\ 0 & 3 & 6 & 0 & 6 & 6 \\ 4 & 1 & 1 & 0 & 4 & 6 \\ 3 & 2 & 1 & 6 & 3 & 2 \\ 2 & 5 & 3 & 6 & 2 & 4 \\ 1 & 2 & 4 & 5 & 4 & 3 \end{bmatrix}$$

Order 6:

$$\begin{bmatrix} 6 & 2 & 6 & 1 & 2 & 3 \\ 0 & 0 & 5 & 5 & 5 & 1 \\ 2 & 2 & 4 & 2 & 5 & 3 \\ 1 & 1 & 4 & 1 & 3 & 5 \\ 4 & 2 & 6 & 3 & 2 & 2 \\ 5 & 2 & 6 & 5 & 0 & 1 \end{bmatrix}$$

Order 6:

$$\begin{bmatrix} 3 & 1 & 6 & 4 & 5 & 1 \\ 0 & 6 & 3 & 0 & 1 & 5 \\ 3 & 5 & 3 & 2 & 4 & 4 \\ 4 & 3 & 1 & 4 & 2 & 1 \\ 6 & 5 & 1 & 2 & 5 & 6 \\ 5 & 1 & 2 & 1 & 3 & 0 \end{bmatrix}$$

One plane from each orbit of the stabiliser on S is listed below.

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 4 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 4 \\ 0 & 1 & 0 & 0 & 2 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 3 & 0 & 0 \\ 0 & 1 & 0 & 0 & 4 & 0 \\ 0 & 0 & 1 & 1 & 2 & 0 \end{pmatrix}.$$