Michel Lavrauw

Scattered Spaces with respect to Spreads,

and

Eggs in Finite Projective Spaces

Scattered Spaces with respect to Spreads,

and

Eggs in Finite Projective Spaces

PROEFSCHRIFT

ter verkrijging van de graad van doctor aan
de Technische Universiteit Eindhoven, op gezag van de
Rector Magnificus, prof.dr. M. Rem, voor een
commissie aangewezen door het College voor
Promoties in het openbaar te verdedigen
op vrijdag 23 mei 2001 om 16.00 uur

door

Michel Lavrauw

geboren te Izegem

Dit proefschrift is goedgekeurd door de promotoren:

prof.dr. A. Blokhuis

en

prof.dr. A. E. Brouwer

Preface

This dissertation is a report of the research that I performed during my years as a PhD student. The work can be seen as consisting of two main parts, which can be read separately. The first part, the second chapter, treats the so-called *scattered subspaces with respect to a spread in a finite projective space.* The second part, the third chapter, is situated in the theory of *finite generalized quadrangles*, in particular *translation generalized quadrangles* and the equivalent so-called *eggs in finite projective spaces.*

However, the discussed subjects in both of these parts are substructures of *Galois spaces*, and in this setting they are very much related. *Galois geometry* started around 1950 with the work of the celebrated Italian mathematician Beniamino Segre who studied n-dimensional projective spaces over Galois fields and substructures of these spaces. His research led to what in the past years has been called the fundamental problems of finite geometry: (1) the determination of the maximal and/or minimal number of points belonging to a substructure satisfying specific geometric conditions, (2) the classification of those substructures having the optimal minimal or maximal number of elements, and (3) when the minimal number or maximal number of elements of such a substructure is known, the determination of the cardinality of the second smallest or second largest such substructure. The problems treated in this thesis are of this kind.

In Chapter 1 an overview is given of the definitions and fundamental results concerning incidence structures and projective spaces over finite fields. However, it is not intended to be a first introduction to the theory of Galois geometry. At the end of the chapter we turn our attention to spreads in finite projective spaces and present a representation of spreads in the tensor product of two vector spaces, which will be used in the next chapter.

With Chapter 2 we enter the world of scattered spaces. A subspace is called *scattered with respect to a spread* in a finite projective space if it intersects every element of the spread in at most a point. This world is only recently created (or discovered) and has its origin in the theory of blocking sets in finite projective spaces. At first we consider scattered spaces with respect to arbitrary spreads, yielding an upper bound on the dimension of a scattered space. If a scattered subspace attains the upper bound, then it is called *maximum*. An attempt to construct such a maximum scattered subspace results in a lower bound on its dimension. From then on we restrict ourselves to Desarguesian spreads, and improve the upper and lower bounds on the dimension of a maximum scattered subspace. In the case where the elements of the spread have even dimension and the projective space has odd dimension the obtained bound is tight. Moreover, it turns out that a maximum scattered subspace with respect to a Desarguesian spread in a projective space of odd dimension yields a two-intersection set with respect to hyperplanes in a projective space of lower dimension over an extension field, and we are able to prove that these two-intersection sets are new. Next we apply the theory of scattered spaces to blocking sets and give some constructions of linear blocking sets of various sizes. At the end of the chapter we give two explicit constructions of a multiple blocking set in a projective plane, one using the technique of polynomials in finite geometry and one using the representation of spreads in the tensor product of two vector spaces introduced in Chapter 1. The obtained blocking sets are of importance when compared to a theorem of Aart Blokhuis, Leo Storme and Tamás Szőnyi.

In the third chapter we allow ourselves a taste of the very popular subject of finite generalized quadrangles. Generalized quadrangles were introduced by Tits in 1959 in order to understand better the structure of the semisimple algebraic groups (including the groups of Lie-type and the Chevalley groups) of relative rank two. Since the book *Finite Generalized Quadrangles* by Payne and Thas, this subject has received a lot of attention from many researchers in geometry, not surprising considering the numerous connections with other branches of geometry. Here, we restrict ourselves to translation generalized quadrangles. After given the necessary introduction we delve into to theory of eggs in finite projective spaces, which is equivalent to the theory of translation generalized quadrangles. We present a new model for eggs, allowing a uniform representation of good eggs, and their dual eggs, in projective spaces over a finite field of odd order, i.e., the eggs corresponding with a semifield flock of a quadratic cone in a three-dimensional projective space over a finite field of odd order. Using this model we are able to give a short proof for an important result of Joseph A. Thas (proved in a more general context). In the second half of the chapter we turn our attention to ovoids of the classical generalized quadrangle corresponding with a non-degenerate quadric in a four-dimensional projective space over a finite field of odd order. The prove of the main result of that section leads to an interesting new method of constructing the good egg from the semifield flock, yielding a characterization of the eggs of Kantor type. In the next section we give a very recent result of great significance in the classification of semifield flocks. We conclude the chapter with the classification of eggs in seven-dimensional projective space over the field of order two.

Contents

Chapter 1

Preliminaries

In this chapter we give the necessary definitions and results that provide a background for the following chapters.

1.1 Incidence structures

An excellent reference on incidence geometry is the book *Handbook of Incidence Geometry*, edited by Buekenhout [25]. An *incidence structure* or a *geometry of rank 2*, S, is a triple $(\mathcal{P}, \mathcal{L}, \mathrm{I})$, where $\mathcal{P}$ is a set of elements called *points*, $\mathcal{L}$ is a set of elements called *blocks* or *lines*, and $\mathrm{I} \subset \mathcal{P} \times \mathcal{L} \cup \mathcal{L} \times \mathcal{P}$, called the *incidence relation*. If $(P, \ell) \in \mathrm{I}$, then we say that P *is incident with* ℓ, or ℓ *is incident with* P, denoted by $P \mathrm{~I~} \ell$. If the blocks are sets of points, then we also say that P *is on* ℓ, ℓ *is on* P, or ℓ *contains* P. An incident point-line pair is called a *flag*. A non-incident point-line pair is called an *antiflag*. The (*point-line*) *dual* of an incidence structure $S = (\mathcal{P}, \mathcal{L}, \mathrm{I})$ is the incidence structure $S^D = (\mathcal{L}, \mathcal{P}, \mathrm{I})$. If two points P and Q are on the same line ℓ, then we say that they are *collinear*. The line ℓ is called the line *joining* P *and* Q. If two lines m and n are on the same point P then we say that they are *concurrent*. The point P is called the *intersection of* m *and* n. A *substructure* $S' = (\mathcal{P}', \mathcal{L}', \mathrm{I}')$ of an incidence structure $S = (\mathcal{P}, \mathcal{L}, \mathrm{I})$ is an incidence structure with $\mathcal{P}' \subseteq \mathcal{P}$, $\mathcal{L}' \subseteq \mathcal{L}$, and $\mathrm{I}' = \mathrm{I} \cap (\mathcal{P}' \times \mathcal{L}' \cup \mathcal{L}' \times \mathcal{P}')$. If every point is incident with the same number of lines, $t+1$, and if every line is incident with the same number of points, $s+1$, then we say that the incidence structure has *order* (s, t). The incidence structure is *finite* if $\mathcal{P}$ and $\mathcal{L}$ are finite sets.

An *isomorphism* or a *collineation* of an incidence structure $S = (\mathcal{P}, \mathcal{L}, \mathrm{I})$ onto an incidence structure $S' = (\mathcal{P}', \mathcal{L}', \mathrm{I}')$ is a pair of bijections $(\alpha : \mathcal{P} \to \mathcal{P}', \beta : \mathcal{L} \to \mathcal{L}')$ preserving incidence and non-incidence, i.e., $(P, \ell) \in \mathrm{I} \Leftrightarrow$

$(P^\alpha, \ell^\beta) \in \mathrm{I}'$. If there exists such an isomorphism then we say that S and S' are *isomorphic*, and we write $S \cong S'$. Here we will only consider incidence structures where the lines are completely determined by the set of points that they contain, which implies that β is completely determined by α. An isomorphism may then simply be defined by a bijection $\alpha : \mathcal{P} \rightarrow \mathcal{P}'$, preserving incidence and non-incidence, inducing a bijection $\mathcal{L} \rightarrow \mathcal{L}'$. An *anti-isomorphism* of an incidence structure S onto an incidence structure S' is a collineation of S onto the dual ${S'}^D$ of S'. A *duality* of S is an anti-isomorphism of S onto itself. A *polarity* is a duality of order 2. All isomorphisms of an incidence structure S onto itself form a group $\mathrm{Aut}\, S$, the *automorphism group* or *collineation group* of S.

Let α be a collineation of the incidence structure S. If there exists a point P of S, such that all lines on P are fixed by α, then P is called a *center* of α and α is called a *central collineation*. Dually an *axis* of α is a line of S for which all points are fixed by α, and in this case α is called an *axial collineation*.

A $t-(v,k,\lambda)$ *design* is an incidence structure such that the set of points has cardinality v, every block contains k points, and every set of t points is contained in exactly λ blocks. A *parallelism* of a design S is an equivalence relation among the blocks of the design, satisfying the following property. For any point P and any block B there exists a unique block C such that P is incident with C, and C and B belong to the same equivalence class. In this case we say that B is *parallel* with C and S is called a *design with parallelism*.

1.2 Projective spaces over finite fields

Standard works on Finite Geometry are the books *Finite Geometries* by Dembowski [32], *Projective Geometries over Finite Fields* by Hirschfeld [37], *Finite Projective Spaces of Three Dimensions* by Hirschfeld [39], and *General Galois Geometries*, by Hirschfeld and Thas [38]. A good introduction to the theory of projective and polar spaces is *Projective and Polar spaces* by Cameron [26]. Projective spaces can be defined over arbitrary fields. Here we restrict ourselves to finite fields.

Let $\mathrm{V}(n,q)$ be the n-dimensional vector space over the finite field of order q, $\mathrm{GF}(q)$, where $q = p^h$, p prime, $h \geq 1$. We define the $(n-1)$*-dimensional Desarguesian projective space over* $\mathrm{GF}(q)$ ($\mathrm{PG}(n-1,q)$) as follows. The 0-dimensional subspaces of $\mathrm{PG}(n-1,q)$ are the one-dimensional subspaces of $\mathrm{V}(n,q)$, the one-dimensional subspaces of $\mathrm{PG}(n-1,q)$ are the two-dimensional subspaces of $\mathrm{V}(n,q)$, ..., the $(n-2)$-dimensional subspaces of $\mathrm{PG}(n-1,q)$ are the $(n-1)$-dimensional subspaces of $\mathrm{V}(n,q)$. The *dimension of* $\mathrm{PG}(n-1,q)$

is $n-1$. To avoid confusion, we use the word *rank* (sometimes abbreviated as *rk*) for the dimension of a vector space and *dimension* (sometimes abbreviated as *dim*) for the dimension of the corresponding projective space. So we say that a subspace of $\mathrm{PG}(n-1,q)$ has rank t and dimension $t-1$. The *codimension* (sometimes abbreviated as *codim*) of a subspace of dimension $n-k-1$ of $\mathrm{PG}(n-1,q)$ is k. A subspace of $\mathrm{PG}(n-1,q)$ of dimension 0, 1, 2, 3, $n-2$ is called a *point*, a *line*, a *plane*, a *solid*, and a *hyperplane*, respectively. Sometimes we will use the term t*-space* or t*-subspace* of $\mathrm{PG}(n-1,q)$ instead of t-dimensional subspace of $\mathrm{PG}(n-1,q)$. We also say that $\mathrm{PG}(n-1,q)$ is an $(n-1)$*-dimensional projective space* or short a *projective space*.

If H is a hyperplane of $\mathrm{PG}(n-1,q)$, then $\mathrm{AG}(n-1,q) = \mathrm{PG}(n-1,q) \setminus H$ is an $(n-1)$*-dimensional Desarguesian affine space over* $\mathrm{GF}(q)$. The *subspaces of* $\mathrm{AG}(n-1,q)$ are $U \setminus H$ where U is a subspace of $\mathrm{PG}(n-1,q)$. We say that H is the *hyperplane at infinity of* $\mathrm{AG}(n-1,q)$.

Every non-zero vector $v \in \mathrm{V}(n,q)$ determines a projective point $P(v)$ of $\mathrm{PG}(n-1,q)$. The vector v is called a *coordinate vector* of $P(v)$ or v is a vector *representing* the point $P(v)$. If v has coordinates $(x_1, x_2, \ldots, x_n)$ with respect to a fixed basis, then we denote the point $P(v)$ by $\langle x_1, x_2, \ldots, x_n \rangle$. If U is a subspace of $\mathrm{V}(n,q)$ then we denote the corresponding subspace of $\mathrm{PG}(n-1,q)$ with $P(U)$. If a subspace W is contained in a subspace U, then we say that W *is incident with* U, U *is incident with* W, U *is on* W, or W *is on* U, denoted by $W \subset U$. The *intersection* of two subspaces U and W, written $U \cap W$, is the subspace containing the points common to U and W. The *span* of two subspaces U and W, or the *subspace spanned by* U *and* W, written $\langle U, W \rangle$, is the smallest subspace of $\mathrm{PG}(n-1,q)$ containing the points of U and the points of W.

If we denote the number of points of $\mathrm{PG}(n-1,q)$ by $\theta_{n-1}(q)$ then

$$\theta_{n-1}(q) = \frac{q^n - 1}{q - 1} = q^{n-1} + q^{n-2} + \cdots + q + 1.$$

The *Gaussian coefficient*

$$\begin{aligned} \begin{bmatrix} n \\ k \end{bmatrix}_q &= \frac{(q^n-1)(q^n-q)\ldots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\ldots(q^k-q^{k-1})} \\ &= \frac{(q^n-1)(q^{n-1}-1)\ldots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\ldots(q-1)}, \end{aligned}$$

counts the number of subspaces of rank k in $\mathrm{V}(n,q)$. Let U be a subspace of rank r in $\mathrm{V}(n,q)$. Then the number of subspaces of rank k containing U in

V(n,q), with $r \leq k$, is equal to

$$\begin{bmatrix} n-r \\ k-r \end{bmatrix}_q .$$

Let $2 \leq t \leq n-2$, let $\mathcal{P}$ be the set of points of PG$(n-1,q)$, and let $\mathcal{L}$ be the set of $(t-1)$-dimensional subspaces of PG$(n-1,q)$. If we define the incidence relation I between elements of $\mathcal{P}$ and $\mathcal{L}$ as symmetric containment, then $(\mathcal{P},\mathcal{L},\mathrm{I})$ is a

$$2-(\theta_{n-1}(q),\theta_{t-1}(q),\begin{bmatrix} n-2 \\ t-2 \end{bmatrix}_q)$$

design, denoted by PG$_{t-1}(n-1,q)$. In the same way the set of points and the set of $(t-1)$-dimensional subspaces of AG$(n-1,q)$ form a

$$2-(q^{n-1},q^{t-1},\begin{bmatrix} n-2 \\ t-2 \end{bmatrix}_q)$$

design, with the following parallelism. Two blocks belong to the same equivalence class of the parallelism, if they intersect the hyperplane at infinity in the same $(t-2)$-dimensional subspace. The design is denoted by AG$_{t-1}(n-1,q)$.

Let U and W be two $(n-1)$-dimensional Desarguesian projective spaces over GF(q), $n \geq 3$. A *collineation of U onto W* is a bijection α between the set of points of U and the set of points of W, preserving incidence. We denote the collineation induced by the bijection α also by α. Note that the definition of a collineation between projective spaces is a special case of the definition of a collineation between two incidence structures which we have already defined in Section 1.1. A collineation between two lines L and M is a bijection between the set of points of L and M, which can be extended to a collineation of a plane containing L onto a plane containing M. A collineation of a projective space U onto itself is called a *collineation of U*.

Let A be a non-singular $(n \times n)$-matrix over GF(q). The bijection between the points of U and the points of W induced by the map (with respect to a fixed basis)

$$x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \mapsto Ax = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$$

induces a collineation of U onto W, called a *projectivity* of U onto W. The collineation induced by A is also denoted by A. If $\sigma : x \mapsto x^\sigma$ is an automorphism of GF(q), then the map $\langle x_1,x_2,\dots,x_n\rangle \mapsto \langle x_1^\sigma,x_2^\sigma,\dots,x_n^\sigma\rangle$ defines a collineation of PG$(n-1,q)$, called an *automorphic collineation of* PG$(n-1,q)$.

Theorem 1.2.1 (The Fundamental Theorem of Projective Geometry)

1. *The set of projectivities of* $\mathrm{PG}(n-1,q)$ *and the set of collineations of* $\mathrm{PG}(n-1,q)$*, form a group with the composition as operator.*

2. *If* α *is a collineation of* $\mathrm{PG}(n-1,q)$*, then* α *is the composition of an automorphic collineation* σ *and a projectivity* A*. We write* $\alpha = (A, \sigma)$*.*

3. *If* $\{P_1, P_2, \ldots, P_n\}$ *and* $\{Q_1, Q_2, \ldots, Q_n\}$*, are sets of points of* $\mathrm{PG}(n-1,q)$ *such that the subspace spanned by each of these sets is* $\mathrm{PG}(n-1,q)$*, then there exists a unique projectivity* α *such that* $P_i^\alpha = Q_i$*,* $i = 1, 2, \ldots, n$*.*

The group $\mathrm{P\Gamma L}(n,q)$ of collineations of $\mathrm{PG}(n-1,q)$ is called the *collineation group of* $\mathrm{PG}(n-1,q)$. The group $\mathrm{PGL}(n,q)$ of projectivities of $\mathrm{PG}(n-1,q)$ is called the *projective general linear group of* $\mathrm{PG}(n-1,q)$.

The definitions for the dual of an incidence structure, and for dualities and polarities, can be specialised in the case of projective spaces. Given a finite projective space S, the *dual space* S^D, is the incidence structure whose points and hyperplanes are respectively the hyperplanes and points of S. Consider a function $\delta : S \rightarrow S^D$. If δ is a collineation, then it is called a *duality of* S. If δ is a projectivity then it is called a *correlation of* S. In either case, if δ has order 2, then it is called a *polarity of* S. Let δ be a polarity of $\mathrm{PG}(n-1,q)$. If U is a subspace of $\mathrm{PG}(n-1,q)$ then we say that U^δ is the *polar space of* U (*with respect to the polarity* δ). If a point P is contained in its polar space, then we say that P is an *absolute point* (*with respect to* δ). By Theorem 1.2.1, there exists a non-singular matrix $A = (a_{ij})_{i,j}$ and an automorphism σ of $\mathrm{GF}(q)$ such that $\delta = (A, \sigma) \in \mathrm{P\Gamma L}(n,q)$. We list the five types of polarities.

- If $\sigma = 1$, q odd, $A = A^T$, the polarity δ is called an *ordinary polarity*, or *orthogonal polarity*, or also a *polarity with respect to a quadric.*

- If $\sigma = 1$, $A = -A^T$, and all $a_{ii} = 0$, then every point is an absolute point and n should be even (since A is non-singular and skew-symmetric). We call the polarity δ a *symplectic polarity*, a *null polarity*, or a *polarity with respect to a linear complex.*

- If $\sigma = 1$, q even, $A = A^T$, and $a_{ii} \neq 0$ for some i, then the polarity δ is called a *pseudo-polarity.*

- If $\sigma \neq 1$, then q must be a square and $x^\sigma = x^{\sqrt{q}}$. In this case the polarity δ is called a *unitary polarity*, or a *Hermitian polarity.*

A projective plane $\mathrm{PG}(2,q)$ is an example of an incidence structure, where a point P is incident with a line L if $P \subset L$. Remember that an incidence structure is also called a geometry of rank 2. The reason for this is that there are two types of elements, which we called points and lines. One can define a *geometry of rank* n in a similar way. Then we have n types of elements of the geometry. We do not want to go in detail here. For more on this subject we refer to [25]. An example of such a geometry of rank $n-1$ is induced by the subspaces of $\mathrm{PG}(n-1,q)$. One can define sets $S_1, S_2, \ldots, S_{n-1}$, as follows. S_1 is the set of points of $\mathrm{PG}(n-1,q)$, S_2 is the set of lines of $\mathrm{PG}(n-1,q)$, ..., S_{n-1} is the set of hyperplanes of $\mathrm{PG}(n-1,q)$. An element x is incident with an element y if x is contained in y or y is contained in x. The definitions of a collineation between incidence structures and of isomorphic incidence structures can easily be extended to geometries of rank n.

Let U be a subspace of $\mathrm{PG}(n-1,q)$ of dimension $k-1$ $(0 \geq k \geq n)$. We define the following geometry $\mathcal{G}$. The elements of type (1), called *points*, of $\mathcal{G}$ are the k-dimensional subspaces of $\mathrm{PG}(n-1,q)$ containing U; the elements of type (2) of $\mathcal{G}$ are the $(k+1)$-dimensional subspaces of $\mathrm{PG}(n-1,q)$ containing U; ...; the elements of type $(n-k)$ are the hyperplanes of $\mathrm{PG}(n-1,q)$ containing U. This defines a geometry of rank $n-k$, with the incidence relation induced by symmetric containment. One can prove that this geometry $\mathcal{G}$ is isomorphic with the geometry of rank $n-k$ induced by the $(n-k-1)$-dimensional projective space $\mathrm{PG}(n-k-1,q)$. It is called the *quotient geometry of* U *in* $\mathrm{PG}(n-1,q)$.

If we restrict the coordinates of the points of $\mathrm{PG}(n-1,q)$ with respect to a fixed basis to a subfield of $\mathrm{GF}(q)$, then we obtain a *subgeometry* of $\mathrm{PG}(n-1,q)$. With respect to a fixed basis this subgeometry is called *canonical*. If $q = q_1^2$, then a subgeometry isomorphic to $\mathrm{PG}(n-1,q_1)$ is called a *Baer subgeometry*.

We say that a projective space P_2 is an *embedding* of a projective space P_1 in a projective space P_3 if

- P_2 is isomorphic to P_1,
- the pointset of P_2 is a subset of the pointset of P_3 and
- the lines of P_2 are the lines of P_3 induced by the points of P_2.

1.3 The projective plane

Consider the Desarguesian projective plane $\mathrm{PG}(2,q)$. Then the following properties are satisfied.

1. Any two distinct lines are incident with exactly one point.
2. Any two distinct points are incident with exactly one line.

3. There exists a set of 4 points, no three of which are collinear.

An incidence structure $(\mathcal{P}, \mathcal{L}, \mathrm{I})$ is called a *projective plane* if it satisfies the conditions 1, 2, and 3. A projective plane π is *Desarguesian* if the plane satisfies the theorem of Desargues, see [32], or equivalently, if there exists a prime power q such that the plane π is isomorphic with $\mathrm{PG}(2, q)$. A collineation of a projective plane π has an axis ℓ if and only if it has a center P, see [32]. If the center of a central collineation is incident with the axis then the collineation is called an *elation*. If the center and the axis of a central collineation are not incident, then the collineation is called a *homology*.

An *affine plane* is an incidence structure that is obtained by deleting a line ℓ and the points incident with ℓ of a projective plane. The line ℓ is called the *line at infinity* of the affine plane. Consider an affine plane π_ℓ with corresponding projective plane π and line at infinity ℓ. A collineation of π_ℓ is called a *dilatation* if it has axis ℓ when regarded as a collineation of π. A *translation* of π_ℓ is either the identity or a dilatation without fixed points. The translations of an affine plane form a group, called the *translation group of* π_ℓ. We say that π_ℓ is a *translation plane* if its translation group acts transitively on the points of π_ℓ.

1.4 Subsets of projective spaces

Let $\mathcal{A}$ and $\mathcal{B}$ be two sets of subspaces of $\mathrm{PG}(n-1, q)$. We say that $\mathcal{A}$ is *isomorphic* to $\mathcal{B}$, denoted $\mathcal{A} \cong \mathcal{B}$, if there exists a collineation of $\mathrm{PG}(n-1, q)$ mapping $\mathcal{A}$ onto $\mathcal{B}$.

Let $Q = \sum_{i,j=1, i \leq j}^{n} a_{ij} X_i X_j$ be a quadratic form over $\mathrm{GF}(q)$. A *quadric* $\mathcal{Q}$ in $\mathrm{PG}(n-1, q)$ is a set of points whose coordinates, with respect to a fixed basis, satisfy $Q = 0$. We denote such a quadric with $Q(n-1, q)$. Let q be a square and let $H = \sum_{i,j=1}^{n} a_{ij} X_i X_j^{\sqrt{q}}$, with $a_{ij} = a_{ji}^{\sqrt{q}}$, a Hermitian form over $\mathrm{GF}(q)$. A *Hermitian variety in* $\mathrm{PG}(n-1, q)$, denoted by $H(n-1, q)$, is a set of points whose coordinates, with respect to a fixed basis, satisfy $H = 0$. A quadric or Hermitian variety of $\mathrm{PG}(n-1, q)$ is called *degenerate* if there exists a coordinate transformation which reduces the form to one in fewer variables; otherwise, the quadric or Hermitian variety is called *non-degenerate*.

Theorem 1.4.1 (Projective classification of quadrics)
The number of orbits on the set of non-degenerate quadrics in $\mathrm{PG}(n-1, q)$ *under the action of* $\mathrm{PGL}(n, q)$ *is one if* n *is odd and two if* n *is even. They have canonical forms as follows.*

- *n is odd:*

$$X_1^2 + X_2X_3 + \cdots + X_{n-1}X_n, \tag{1.1}$$

- *n is even:*

$$X_1X_2 + X_3X_4 + \cdots + X_{n-1}X_n, \tag{1.2}$$

  or

$$f(X_1, X_2) + X_3X_4 + \cdots + X_{n-1}X_n, \tag{1.3}$$

  where f is an irreducible binary quadratic form.

Quadrics with form (1.1), (1.2), and (1.3), are called *parabolic*, *hyperbolic*, and *elliptic*, respectively, and are denoted by $Q(n-1,q)$, $Q^+(n-1,q)$, and $Q^-(n-1,q)$. A quadric of $\mathrm{PG}(2,q)$ is called a *conic of* $\mathrm{PG}(2,q)$. The *projective index* of a quadric is the maximum dimension of subspaces contained in the quadric. The *Witt index* of a quadric is the rank of the maximal subspace, i.e., the projective index plus one. If q is odd, respectively q is even, then the absolute points of an orthogonal polarity, respectively of a pseudo-polarity, form a quadric $\mathcal{Q}$ in $\mathrm{PG}(n-1,q)$. If q is a square, then the absolute points of a Hermitian polarity form a Hermitian variety $\mathcal{H}$ in $\mathrm{PG}(n-1,q)$. If the polar space of a point P on the quadric $\mathcal{Q}$, respectively on the Hermitian variety $\mathcal{H}$, intersects the quadric $\mathcal{Q}$, respectively the Hermitian variety $\mathcal{H}$, in P, then it is called the tangent space of $\mathcal{Q}$, respectively $\mathcal{H}$, at the point P.

Consider the projective plane $\mathrm{PG}(2,q)$. A set of k points with the property that no three points are collinear is called a *k-arc*. A k-arc is *complete* if it is not contained in a $(k+1)$-arc.

Theorem 1.4.2 (Bose [20])
Let $\mathcal{K}$ be a k-arc in $\mathrm{PG}(2,q)$. If q is odd then $k \leq q+1$. If q is even then $k \leq q+2$.

A $(q+1)$-arc is called an *oval*, a $(q+2)$-arc is called a *hyperoval*. A line intersecting $\mathcal{K}$ in exactly one point is called a *tangent* or a *tangent line*. A line intersecting $\mathcal{K}$ in two points is called a *secant* or a *secant line*. A line not meeting $\mathcal{K}$ is called an *external line*. The $q+1$ tangent lines of an oval in $\mathrm{PG}(2,q)$, q even, are concurrent. The intersection point is called the *nucleus* of the oval. Adding the nucleus to the oval we get a hyperoval of $\mathrm{PG}(2,q)$. For q odd, ovals are classified by the following theorem.

Theorem 1.4.3 (Segre [68], [69])
In $\mathrm{PG}(2,q)$, q odd, every oval is a conic.

Dually a set of $q+1$ lines no three concurrent is called a *dual oval*. If q is odd, then the tangents to an oval of $\mathrm{PG}(2,q)$ form a dual oval. As we already mentioned the tangents to an oval of $\mathrm{PG}(2,q)$, q even, all contain the nucleus. Hence they do not form a dual oval. If q is odd then every point P not on a conic $\mathcal{C}$ is either on no tangent line to $\mathcal{C}$, in which case P is called an *internal point*, or on exactly two tangent lines to $\mathcal{C}$, in which case P is called an *external point*. For more on ovals and hyperovals we refer to the lecture notes of Brown [24]. A lot of information on hyperovals can also be found on *Bill Cherowitzo's Hyperovals page* [30].

Consider the projective 3-dimensional space $\mathrm{PG}(3,q)$. Let P be a point of $\mathrm{PG}(3,q)$ and $\mathcal{C}$ a conic in a plane of $\mathrm{PG}(3,q)$ not containing P. A *quadratic cone* $\mathcal{K}$ of $\mathrm{PG}(3,q)$ is the set of points on the lines $\langle P,Q\rangle$, $Q\in\mathcal{C}$. P is called the *vertex* of $\mathcal{K}$ and $\mathcal{C}$ is called the *base* of $\mathcal{K}$.

A *k-cap* of $\mathrm{PG}(3,q)$ is a set of k points of $\mathrm{PG}(3,q)$ no three collinear.

Theorem 1.4.4 (Bose [20] for q odd, Seiden [71] for $q=4$, Qvist [66] for q even)
If $\mathcal{O}$ is a k-cap in $\mathrm{PG}(3,q)$ and $q>2$ then $k\le q^2+1$.

When $q=2$, then the affine points of $\mathrm{PG}(3,2)$ with respect to a hyperplane form an 8-cap. An *ovoid* of $\mathrm{PG}(3,q)$ is a (q^2+1)-cap of $\mathrm{PG}(3,q)$.

Theorem 1.4.5 (Barlotti [10])
If $\mathcal{O}$ is an ovoid of $\mathrm{PG}(3,q)$, q odd, then $\mathcal{O}$ is an elliptic quadric of $\mathrm{PG}(3,q)$.

If q is an odd power of 2, then there is one more example of an ovoid of $\mathrm{PG}(3,q)$ known, the so-called *Tits ovoid*, Tits [85]. Ovoids in $\mathrm{PG}(3,q)$ are classified for $q\le 32$. In 1990 O'Keefe and Penttila [53] have shown that all ovoids of $\mathrm{PG}(3,16)$ are elliptic quadrics (a computer search). A computer-free proof was given in 1992 [54]. In 1994 O'Keefe, Penttila and Royle [55] have shown that all ovoids of $\mathrm{PG}(3,32)$ are elliptic quadrics or Tits ovoids. For more on ovoids in $\mathrm{PG}(3,q)$ we refer to the lecture notes of Brown [24], for a published survey we refer to O'Keefe [52].

A plane meeting an ovoid in one point is called a *tangent plane*. If a plane of $\mathrm{PG}(3,q)$ meets an ovoid in more than one point then it meets the ovoid in an oval. Hence any plane of $\mathrm{PG}(3,q)$ meets an ovoid in 1 or $q+1$ points. Such a set is called a *two-intersection set with respect to planes of* $\mathrm{PG}(3,q)$. More generally, a *two-intersection set with respect to hyperplanes in* $\mathrm{PG}(n-1,q)$ is a set T of points for which there exist integers m_1 and m_2, such that every hyperplane of $\mathrm{PG}(n-1,q)$ meets T in m_1 or m_2 points. The numbers m_1 and m_2 are called the *intersection numbers of T*.

1.5 Spreads

A *partial spread* (*partial* $(t-1)$*-spread*) of $\mathrm{PG}(n-1,q)$ is a set of mutually disjoint subspaces of the same dimension $(t-1)$. Let $\mathcal{S}$ be a set of $(t-1)$-dimensional subspaces of $\mathrm{PG}(n-1,q)$. Then $\mathcal{S}$ is called a *spread* or $(t-1)$*-spread* of $\mathrm{PG}(n-1,q)$ if every point of $\mathrm{PG}(n-1,q)$ is contained in exactly one element of $\mathcal{S}$. Let $\mathcal{S}$ be a $(t-1)$-spread of $\mathrm{PG}(n-1,q)$. The *deficiency* of a partial $(t-1)$-spread $\mathcal{S}_p$ of $\mathrm{PG}(n-1,q)$ equals $|\mathcal{S}|-|\mathcal{S}_p|$. If $t=1$ then $\mathcal{S}$ is just the set of points of $\mathrm{PG}(n-1,q)$. If $t=2$ then $\mathcal{S}$ is called a *line spread* or a *spread of lines*. If $t=3$ then $\mathcal{S}$ is called a *plane spread* or a *spread of planes*.

If $\mathcal{S}$ is a set of subspaces of $\mathrm{V}(n,q)$ of rank t, then $\mathcal{S}$ is called a t*-spread* of $\mathrm{V}(n,q)$ if every vector of $\mathrm{V}(n,q)-\{0\}$ is contained in exactly one element of $\mathcal{S}$. Note that spreads of $\mathrm{V}(n,q)$ are in one-to-one correspondence with spreads of $\mathrm{PG}(n-1,q)$, and from now on we will consider these two spreads as one object $\mathcal{S}$.

Lemma 1.5.1 *If there exists a* $(t-1)$*-spread in* $\mathrm{PG}(n-1,q)$*, then* t *divides* n*.*

Proof. Suppose there exists a $(t-1)$-spread $\mathcal{S}$ of $\mathrm{PG}(n-1,q)$. Since every point of $\mathrm{PG}(n-1,q)$ is contained in exactly one element of $\mathcal{S}$, the number of points of a $(t-1)$-space has to divide the number of points of $\mathrm{PG}(n-1,q)$. So $\theta_{t-1}(q)|\theta_{n-1}(q)$ or

$$\frac{q^t-1}{q-1} \mid \frac{q^n-1}{q-1}.$$

This implies that t divides n. ■

The converse is also true. If t divides n then there exists a $(t-1)$-spread of $\mathrm{PG}(n-1,q)$. We delay the proof of this statement until we introduced some more theory. From now on we put $n=rt$ for some $r\geq 1$.

Let $\mathcal{S}$ be a $(t-1)$-spread of $\mathrm{PG}(rt-1,q)$. Consider $\mathrm{PG}(rt-1,q)$ as a hyperplane of $\mathrm{PG}(rt,q)$. We define an incidence structure $(\mathcal{P},\mathcal{L},\mathrm{I})$ as follows. The set $\mathcal{P}$ consist of all points of $\mathrm{PG}(rt,q)\setminus\mathrm{PG}(rt-1,q)$ and the set $\mathcal{L}$ consists of all t-spaces of $\mathrm{PG}(rt,q)$ intersecting $\mathrm{PG}(rt-1,q)$ in an element of $\mathcal{S}$. The incidence relation I is symmetric containment. Then the incidence structure $(\mathcal{P},\mathcal{L},\mathrm{I})$ is a $2-(q^{rt},q^t,1)$ design with parallelism, see [11]. If $r=2$ then $(\mathcal{P},\mathcal{L},\mathrm{I})$ is a translation plane of order q^t. This construction is sometimes referred to as the *André-Bruck-Bose construction.*

Remark. Let π be a translation plane with translation group T, let $\mathfrak{P}$ denote the set of parallel classes of π, and let $T(\mathsf{P})$ denote the subgroup of T

which fixes every line of the parallel class $\mathsf{P} \in \mathfrak{P}$. The *kernel* of π is the set of all endomorphisms α of T with $T(\mathsf{P})^\alpha \subseteq T(\mathsf{P})$, for all parallel classes $\mathsf{P} \in \mathfrak{P}$. With this definition of the kernel, we also have the converse of the above relation between spreads and translation planes, namely: every translation plane with dimension at least two over its kernel can be constructed via the André-Bruck-Bose construction from a spread. Hence every translation plane with dimension at least two over its kernel induces a spread. For more on translation planes we refer to [25], [32].

For any $r \geq 2$, we say that the spread is *Desarguesian* if the design is isomorphic to $\mathrm{AG}_1(r, q^t)$. The spread $\mathcal{S}$ is called *normal* or *geometric* if and only if the space generated by two spread elements is partitioned by a subset of $\mathcal{S}$. From this it follows that the space generated by any number of elements from a normal spread is partitioned by elements of $\mathcal{S}$. If $r = 1, 2$ then every $(t-1)$-spread of $\mathrm{PG}(rt-1, q)$ is normal. If $r > 2$ then $\mathcal{S}$ is normal if and only if $\mathcal{S}$ is Desarguesian, see [49].

As promised we will now construct a $(t-1)$-spread of $\mathrm{PG}(rt-1, q)$. Embed $\mathrm{PG}(rt-1, q)$ as a subgeometry of $\mathrm{PG}(rt-1, q^t)$. Since all extensions of the same degree are isomorphic we may assume that this extension is canonical with respect to a fixed basis. Let σ be the automorphic collineation of $\mathrm{PG}(rt-1, q^t)$ induced by the field automorphism $x \mapsto x^q$ of $\mathrm{GF}(q^t)$, i.e.,

$$\sigma : \langle x_0, x_1, \ldots, x_{rt-1} \rangle \mapsto \langle x_0^q, x_1^q, \ldots, x_{rt-1}^q \rangle.$$

Then σ fixes $\mathrm{PG}(rt-1, q)$ pointwise and we have the following lemma.

Lemma 1.5.2 (see [28])
A subspace of $\mathrm{PG}(rt-1, q^t)$ *of dimension* d *is fixed by* σ *if and only if it intersects the subgeometry* $\mathrm{PG}(rt-1, q)$ *in a subspace of dimension* d*.*

Moreover there exists an $(r-1)$-space π skew to the subgeometry $\mathrm{PG}(rt-1, q)$, see [28]. Let P be a point of π and let $L(P)$ denote the $(t-1)$-dimensional subspace generated by the *conjugates* of P, i.e., $L(P) = \langle P, P^\sigma, \ldots, P^{\sigma^{t-1}} \rangle$. Then $L(P)$ is fixed by σ and hence it intersects $\mathrm{PG}(rt-1, q)$ in a $(t-1)$-dimensional subspace over $\mathrm{GF}(q)$ because of Lemma 1.5.2. We can do this for every point of π and in this way we obtain a set $\mathcal{S}$ of $(t-1)$-spaces of the subgeometry $\mathrm{PG}(rt-1, q)$. Because π is skew to the subgeometry $\mathrm{PG}(rt-1, q)$, any two distinct elements of $\mathcal{S}$ are disjoint. It follows that $\mathcal{S}$ forms a $(t-1)$-spread of $\mathrm{PG}(rt-1, q)$. Moreover this spread is Desarguesian (follows from the construction) and every Desarguesian spread can be constructed this way, see [49], [70]. So together with Lemma 1.5.1 this proves the following theorem.

Theorem 1.5.3 (Segre [70])
A $(t-1)$*-spread of* $\mathrm{PG}(n-1, q)$ *exists if and only if* t *divides* n*.*

In this construction we see a correspondence between the points of the $(r-1)$-dimensional Desarguesian projective space over $\mathrm{GF}(q^t)$ and the elements of a Desarguesian $(t-1)$-spread of $\mathrm{PG}(rt-1,q)$. This correspondence will play a key role in the next chapter. We can also see this in the following way. The points of $\mathrm{PG}(r-1,q^t)$ are the subspaces of rank 1 of $\mathrm{V}(r,q^t)$. If we look at $\mathrm{GF}(q^t)$ as a vector space of rank t over $\mathrm{GF}(q)$ then $\mathrm{V}(r,q^t)$ becomes a vector space, $\mathrm{V}(rt,q)$ of rank rt over $\mathrm{GF}(q)$. A subspace of rank 1 in $\mathrm{V}(r,q^t)$ induces a subspace of rank t in $\mathrm{V}(rt,q)$. So the points of $\mathrm{PG}(r-1,q^t)$ induce subspaces of rank t in $\mathrm{V}(rt,q)$. The lines of $\mathrm{PG}(r-1,q^t)$, which are subspaces of rank 2 of $\mathrm{V}(r,q^t)$, induce subspaces of rank $2t$ in $\mathrm{V}(rt,q)$. So it is clear that the points of $\mathrm{PG}(r-1,q^t)$, can be seen as the elements of a Desarguesian $(t-1)$-spread $\mathcal{S}$ of $\mathrm{PG}(rt-1,q)$. This gives us an alternative view on the correspondence between the points of $\mathrm{PG}(r-1,q^t)$ and the elements of a Desarguesian $(t-1)$-spread $\mathcal{S}$.

Let $\mathcal{S}$ be a Desarguesian spread in $\mathrm{PG}(rt-1,q)$ and let U be a subspace of dimension $kt-1$ of $\mathrm{PG}(rt-1,q)$, spanned by spread elements. The quotient geometry of U in $\mathrm{PG}(rt-1,q)$ is isomorphic to $\mathrm{PG}(rt-kt-1,q)$. Equivalently, we may consider U to be a $(k-1)$-dimensional subspace of $\mathrm{PG}(r-1,q^t)$. The quotient geometry of U in $\mathrm{PG}(r-1,q^t)$ is isomorphic to $\mathrm{PG}(r-k-1,q^t)$. This induces an $(rt-kt-1)$-dimensional space over $\mathrm{GF}(q)$, with a Desarguesian spread $\mathcal{S}'$ induced by the points of $\mathrm{PG}(r-k-1,q^t)$. We say $\mathcal{S}'$ is *the spread induced by $\mathcal{S}$ in the quotient geometry of U in* $\mathrm{PG}(rt-1,q)$. The following theorem now easily follows.

Theorem 1.5.4 *If $\mathcal{S}$ is a Desarguesian spread in $\mathrm{PG}(rt-1,q)$ then the spread induced by $\mathcal{S}$ in the quotient geometry of a subspace spanned by spread elements in $\mathrm{PG}(rt-1,q)$ is Desarguesian.*

1.6 Tensor products

In this section we develop a representation of Desarguesian spreads inside the tensor product of two vector spaces. Let V and W be two vector spaces over the field $\mathrm{GF}(q)$, with $\mathrm{rk}(V)=n$, $\mathrm{rk}(W)=m$. The *tensor product* of V and W, denoted by $V \bigotimes W$ is the set of all linear combinations of elements of $\{v\otimes w \parallel v\in V, w\in W\}$ with coefficients in $\mathrm{GF}(q)$, where $\otimes$ is a binary operation satisfying

$$(v_1+v_2)\otimes w = v_1\otimes w + v_2\otimes w,$$

$$v\otimes(w_1+w_2) = v\otimes w_1 + v\otimes w_2,$$

$$(\alpha v)\otimes w = \alpha(v\otimes w),$$

and

$$v \otimes (\alpha w) = \alpha(v \otimes w),$$

for all $v, v_1, v_2 \in V$, $w, w_1, w_2 \in W$, and $\alpha \in \mathrm{GF}(q)$.

From the definition it follows that $V \bigotimes W$ is a vectorspace over $\mathrm{GF}(q)$ of rank mn. If we choose a basis $\{v_1, v_2, \ldots, v_n\}$ for V and $\{w_1, w_2, \ldots, w_m\}$ for W, then the set

$$\{v_i \otimes w_j \parallel 1 \leq i \leq n, 1 \leq j \leq m\}$$

is a basis for $V \bigotimes W$. Let

$$u = \sum_{i=1}^{n} \sum_{j=1}^{m} u_{ij} v_i \otimes w_j \in V \bigotimes W.$$

Then we can use the linearity to expand u in terms of the basis vectors of V and in terms of the basis vectors of W. We will use the following notation:

$$u = u_1^v \otimes w_1 + \cdots + u_m^v \otimes w_m = v_1 \otimes u_1^w + \cdots + v_n \otimes u_n^w,$$

where $u_i^v \in V$ and $u_j^w \in W$, for $i = 1, \ldots, m$ and $j = 1, \ldots, n$. Let $V_u = \langle u_i^v \mid i = 1, \ldots, m\rangle$ and $W_u = \langle u_i^w \mid i = 1, \ldots, n\rangle$.

Lemma 1.6.1 *The vector spaces V_u and W_u are independent of the choice of basis of V and W.*

Proof. Suppose $\{v_1, \ldots, v_n\}$ and $\{v'_1, \ldots, v'_n\}$ are two bases of V. Let $v'_i = a_{i1} v_1 + \cdots + a_{in} v_n$, for $i = 1, \ldots, n$. Hence

$$\begin{aligned} \begin{bmatrix} v'_1 \\ \vdots \\ v'_n \end{bmatrix} &= \begin{bmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \ldots & a_{nn} \end{bmatrix} \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} \\ &= A \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} \end{aligned}$$

with $\det A \neq 0$, $A(i,j) = a_{ij}$. Let $u = v'_1 \otimes {u'}_1^w + \cdots + v'_n \otimes {u'}_n^w$. Then

$$\begin{aligned} u &= (a_{11} v_1 + \cdots + a_{1n} v_n) \otimes {u'}_1^w + \cdots + (a_{n1} v_1 + \cdots + a_{nn} v_n) \otimes {u'}_n^w \\ &= v_1 \otimes (a_{11} {u'}_1^w + \cdots + a_{n1} {u'}_n^w) + \cdots + v_n \otimes (a_{1n} {u'}_1^w + \cdots + a_{nn} {u'}_n^w) \\ &= v_1 \otimes u_1^w + \cdots + v_n \otimes u_n^w. \end{aligned}$$

This implies

$$\begin{bmatrix} u_1^w \\ \vdots \\ u_n^w \end{bmatrix} = \begin{bmatrix} a_{11} & \dots & a_{n1} \\ \vdots & & \vdots \\ a_{1n} & \dots & a_{nn} \end{bmatrix} \begin{bmatrix} {u'}_1^w \\ \vdots \\ {u'}_n^w \end{bmatrix}.$$

Since $\det A \neq 0$, this shows that W_u is independent of the choice of the basis of V. The proof for V_u is completely analogous. ■

If a vector u of $V \bigotimes W$ can be written as $v \otimes w$, with $v \in V$ and $w \in W$, then u is called a *pure tensor* of $V \bigotimes W$.

Lemma 1.6.2 *If $u \in V \bigotimes W$ and k is minimal such that u can be written as the sum of k pure tensors, then* $\mathrm{rk} V_u = \mathrm{rk} W_u = k$.

Proof. Suppose u is the sum of k pure tensors, $u = z_1 + z_2 + \cdots + z_k$, with

$$z_l = \sum_{i=1}^{n} \lambda_i(z_l) v_i \otimes \sum_{j=1}^{m} \mu_j(z_l) w_j.$$

Expanding z_l in terms of the basis vectors of V gives

$$z_l = v_1 \otimes \lambda_1(z_l) \sum_{j=1}^{m} \mu_j(z_l) w_j + \cdots + v_n \otimes \lambda_n(z_l) \sum_{j=1}^{m} \mu_j(z_l) w_j.$$

Expanding u in terms of the basis vectors of V then gives us

$$\begin{aligned} u \quad = \quad & v_1 \otimes \sum_{l=1}^{k} \lambda_1(z_l) \sum_{j=1}^{m} \mu_j(z_l) w_j \\ & + v_2 \otimes \sum_{l=1}^{k} \lambda_2(z_l) \sum_{j=1}^{m} \mu_j(z_l) w_j \\ & + \cdots \\ & + v_n \otimes \sum_{l=1}^{k} \lambda_n(z_l) \sum_{j=1}^{m} \mu_j(z_l) w_j. \end{aligned}$$

From this we can see that W_u is contained in the space spanned by the set

$$\left\{ \sum_{j=1}^{m} \mu_j(z_1) w_j, \sum_{j=1}^{m} \mu_j(z_2) w_j, \dots, \sum_{j=1}^{m} \mu_j(z_k) w_j \right\}.$$

Analogously, we can show that V_u is spanned by the set

$$\left\{ \sum_{i=1}^{n} \lambda_i(z_1) v_i, \sum_{i=1}^{n} \lambda_i(z_2) v_i, \dots, \sum_{i=1}^{n} \lambda_i(z_k) v_i \right\}.$$

So we have proven that the rank of V_u, respectively W_u, is at most k. Now suppose the rank of V_u is less than k, then we can write

$$\sum_{i=1}^{n} \lambda_i(z_k)v_i$$

as a linear combination of the previous $k-1$ elements of the above set, let's say

$$\sum_{i=1}^{n} \lambda_i(z_k)v_i = a_1 \sum_{i=1}^{n} \lambda_i(z_1)v_i + \cdots + a_{k-1} \sum_{i=1}^{n} \lambda_i(z_{k-1})v_i.$$

It follows that

$$\begin{aligned} z_k &= \left[a_1 \sum_{i=1}^{n} \lambda_i(z_1)v_i + \cdots + a_{k-1} \sum_{i=1}^{n} \lambda_i(z_{k-1})v_i \right] \otimes \sum_{j=1}^{m} \mu_j(z_k)w_j, \\ &= \sum_{i=1}^{n} \lambda_i(z_1)v_i \otimes a_1 \sum_{j=1}^{m} \mu_j(z_k)w_j \\ &\quad + \cdots \\ &\quad + \sum_{i=1}^{n} \lambda_i(z_{k-1})v_i \otimes a_{k-1} \sum_{j=1}^{m} \mu_j(z_k)w_j. \end{aligned}$$

So we get that

$$\begin{aligned} u &= \sum_{i=1}^{n} \lambda_i(z_1)v_i \otimes \left[\sum_{j=1}^{m} \mu_j(z_1)w_j + a_1 \sum_{j=1}^{m} \mu_j(z_k)w_j \right] \\ &\quad + \cdots \\ &\quad + \sum_{i=1}^{n} \lambda_i(z_{k-1})v_i \otimes \left[\sum_{j=1}^{m} \mu_j(z_{k-1})w_j + a_{k-1} \sum_{j=1}^{m} \mu_j(z_k)w_j \right], \end{aligned}$$

which shows that u can be written as the sum of $k-1$ pure tensors, a contradiction. We can conclude that

$$\mathrm{rk} V_u = \mathrm{rk} W_u = k,$$

where k is minimal such that u can be written as the sum of k pure tensors.■

Remark. Given a basis for V and W the tensor product $V \bigotimes W$ can be identified with the set of $n \times m$ matrices over $\mathrm{GF}(q)$. The above then essentially says that row and column rank of a matrix are equal, and that every rank k matrix can be written as the sum of k rank 1 matrices.

Lemma 1.6.3 *If H is a subspace of $\mathrm{GF}(q^n) = \mathrm{V}(n,q)$ and $\alpha \in \mathrm{GF}(q^n)$, such that $\alpha H \subseteq H$, then H is a vector space over the extension field $\mathrm{GF}(q)(\alpha)$.*

Proof. If the degree of the minimal polynomial of α over $\mathrm{GF}(q)$ is $k+1$, then every element $\beta \in \mathrm{GF}(q)(\alpha)$, can be written as $\beta = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_k\alpha^k$, with $a_0, \ldots, a_k \in \mathrm{GF}(q)$. Let $h \in H$, then

$$\beta h = a_0 h + a_1 \alpha h + \cdots + a_k \alpha^k h.$$

Since $\alpha^k H = \alpha^{k-1}\alpha H \subseteq \alpha^{k-1} H \subseteq \ldots \subseteq \alpha H \subseteq H$, there exist $h_0, h_1, \ldots, h_k \in H$, such that

$$a_0 h = h_0, \ldots, a_k \alpha^k h = h_k.$$

This implies $\beta h \in H$. Clearly H is closed under addition, so we can conclude that H is a vector space over $\mathrm{GF}(q)(\alpha)$. ■

Consider the vector space $V = \mathrm{V}(rt, q) = \mathrm{GF}(q)^r \bigotimes \mathrm{GF}(q)^t$ of rank rt over $\mathrm{GF}(q)$. We define a multiplication of elements of $\mathrm{GF}(q^r) \cup \mathrm{GF}(q^t)$ with vectors of V. We leave it up to the reader to interpret elements of $\mathrm{GF}(q)^t \cong \mathrm{GF}(q^t)$ as vectors over $\mathrm{GF}(q)$ or as elements of the finite field $\mathrm{GF}(q^t)$. For a pure tensor $v \otimes w$ for example we write $\lambda(v \otimes w) = (\lambda v) \otimes w = v \otimes (\lambda w)$ for $\lambda \in \mathrm{GF}(q)$, $\lambda(v \otimes w) = (\lambda v) \otimes w$ for $\lambda \in \mathrm{GF}(q^r) \setminus \mathrm{GF}(q^t)$, $\lambda(v \otimes w) = v \otimes (\lambda w)$ for $\lambda \in \mathrm{GF}(q^t) \setminus \mathrm{GF}(q^r)$. If $\lambda \in \mathrm{GF}(q^r) \cap \mathrm{GF}(q^t)$ then we write $\lambda(v \otimes w) = (\lambda v) \otimes w$ if we consider λ as an element of $\mathrm{GF}(q^r)$ and we write $(v \otimes w)\lambda = v \otimes (\lambda w)$ if we consider λ as an element of $\mathrm{GF}(q^t)$. So we write multiplication with elements of $\mathrm{GF}(q^r)$ on the left and multiplication with elements of $\mathrm{GF}(q^t)$ on the right. For $v \in V$ we define the following subspaces of V.

$$S_r(v) = \{\alpha v \parallel \alpha \in \mathrm{GF}(q^r)\},$$

$$S_t(v) = \{v\beta \parallel \beta \in \mathrm{GF}(q^t)\}.$$

We have the following theorem.

Theorem 1.6.4 *The set $\mathcal{S}_r = \{S_r(v) \parallel v \in V\}$ is a Desarguesian r-spread of V. The set $\mathcal{S}_t = \{S_t(v) \parallel v \in V\}$ is a Desarguesian t-spread of V.*

Proof. The proof is easy if we consider V as a vector space $\mathrm{V}(r, q^t)$ of rank r over $\mathrm{GF}(q^t)$ (or projectively as $\mathrm{PG}(r-1, q^t)$), respectively as a vector space $\mathrm{V}(t, q^r)$ of rank t over $\mathrm{GF}(q^r)$ (or as $\mathrm{PG}(t-1, q^r)$). The elements of $\mathcal{S}_r$ are then the points of $\mathrm{PG}(t-1, q^r)$, and the elements of $\mathcal{S}_t$ are the points of $\mathrm{PG}(r-1, q^t)$. The theorem now easily follows. ■

Chapter 2

Scattered spaces

2.1 Introduction

Let $\mathcal{S}$ be a spread in $\mathrm{V}(n, q)$. A subspace of $\mathrm{V}(n, q)$ is called *scattered with respect to* $\mathcal{S}$ if it intersects each spread element in a subspace of rank at most one. Projectively, if $\mathcal{S}$ is a spread in $\mathrm{PG}(n-1, q)$, a subspace of $\mathrm{PG}(n-1, q)$ is called *scattered with respect to* $\mathcal{S}$ if it intersects each spread element in at most one point. It is clear that the definitions are consistent with each other and give rise to equivalent problems.

As an example of a scattered space consider a spread $\mathcal{S}$ of lines in $\mathrm{PG}(3, q)$, and a line not contained in the spread. The line intersects $q+1$ spread elements in a point and is skew to all other lines of $\mathcal{S}$. Since a plane of $\mathrm{PG}(3, q)$ contains q^2+q+1 points and a line spread of $\mathrm{PG}(3, q)$ consists of q^2+1 elements, it is clear that a plane of $\mathrm{PG}(3, q)$ necessarily contains exactly one line of the spread. So the dimension of a scattered space with respect to a line spread in $\mathrm{PG}(3, q)$ is at most 1, the dimension of a line.

A scattered space of highest possible dimension is called a *maximum scattered space*. In the previous example it was easy to determine the dimension of a maximum scattered space. As we shall see later on this is not always the case. In this chapter we prove some upper and lower bounds for the dimension of a maximum scattered space with respect to a $(t-1)$-spread of $\mathrm{PG}(rt-1, q)$.

Note that if $t=1$, the space $\mathrm{PG}(rt-1, q)$ containing the spread is scattered with respect to every $(t-1)$-spread in $\mathrm{PG}(rt-1, q)$, since in this case the spread elements are just the points of the projective space. From now on we assume that $t \geq 2$. If $r=1$ then a $(t-1)$-spread of $\mathrm{PG}(rt-1, q)$ consists of one element, the space itself. The dimension of a maximum scattered space is clearly 0, i.e., the dimension of a point. From now on we assume that $r \geq 2$.

2.2 A lower bound on the dimension of a maximum scattered subspace

In this section we give a procedure to enlarge a scattered subspace, whenever this is possible, and obtain a lower bound on the dimension of a maximum scattered space.

Theorem 2.2.1 ([18, Theorem 2.1])
Let $\mathcal{S}$ be a $(t-1)$-spread of $\mathrm{PG}(rt-1, q)$ and let T be an m-dimensional scattered subspace with respect to $\mathcal{S}$. If

$$m < \frac{rt-t}{2}$$

then T is contained in an $(m+1)$-dimensional scattered subspace with respect to $\mathcal{S}$. Moreover, the dimension of a maximum scattered subspace with respect to $\mathcal{S}$ is at least $\lceil \frac{rt-t}{2} \rceil$.

Proof. Let $\mathcal{S}$ be a t-spread in $\mathrm{V}(rt, q)$ and $T = \langle w_0, w_1, \ldots, w_m \rangle$ be scattered with respect to $\mathcal{S}$ of rank $m+1$. For $w_{m+1} \notin T$, the space $\langle T, w_{m+1} \rangle$ will be scattered with respect to $\mathcal{S}$ if and only if

$$w_{m+1} \notin \bigcup_{Q:(Q \in S) \wedge (Q \cap T \neq \{0\})} \langle Q, T \rangle.$$

So T is contained in a larger scattered subspace if

$$q^{rt} > (q^{t+m} - q^{m+1})(q^m + q^{m-1} + \ldots + 1) + q^{m+1}.$$

The term on the left is the number vectors in $\mathrm{V}(rt, q)$. The first factor on the right hand side is the number of non-zero vectors in the subspace spanned by T and a spread element intersecting T, which are not contained in T. The second factor on the right hand side is the number of spread elements intersecting T. The last term is the number of vectors contained in T. Hence this allows us to extend T to a scattered subspace of rank $m+2$ if $m < \frac{rt-t}{2}$. It follows that the maximum dimension of a scattered subspace with respect to $\mathcal{S}$ is at least $\lceil \frac{rt-t}{2} \rceil$. This concludes the proof. ■

2.3 An upper bound on the dimension of a scattered subspace

Let $\mathcal{S}$ be a $(t-1)$-spread in $\mathrm{PG}(rt-1,q)$. The number of spread elements is $(q^{rt}-1)/(q^t-1) = q^{(r-1)t} + q^{(r-2)t} + \ldots + q^t + 1$. Since a scattered subspace can contain at most one point of every spread element, the number of points in a scattered space must be less than or equal to the number of spread elements. So we have the following trivial upper bound.

Theorem 2.3.1 ([18, Theorem 3.1])
If T is an m-dimensional scattered space with respect to a $(t-1)$-spread in $\mathrm{PG}(rt-1,q)$ then

$$m \leq rt - t - 1.$$

Let us illustrate these bounds with an example. First of all we remark that for a line spread in $\mathrm{PG}(3,q)$ the upper and lower bound coincide. But this is quite exceptional. Comparing the lower and the upper bound we see that these bounds can only coincide if $t(r-1) \leq 4$. Since we assumed t and r both at least 2, it follows that we already know the exact dimension of a maximum scattered space for $(r,t) \in \{(2,2),(2,3)\}$, i.e., a line spread in $\mathrm{PG}(3,q)$ and a plane spread in $\mathrm{PG}(5,q)$. The dimension of a maximum scattered space in these cases is respectively 1, the dimension of a line, and 2, the dimension of a plane. There is a large variety of spreads and there is not much that can be said about the possible dimension of a scattered subspace with respect to an arbitrary spread. This is one reason to consider scattered spaces with respect to a Desarguesian spread. Another reason is the correspondence between the elements of a Desarguesian spread and the points of a projective space over an extension field, as explained in Chapter 1. First, however, we show that for any subspace W of dimension $rt-t-1$, we can always find a spread $\mathcal{S}$ such that W is scattered with respect to $\mathcal{S}$. Hence with respect to the spread $\mathcal{S}$ there exists a scattered subspace W attaining the upper bound given in Theorem 2.3.1.

2.4 Scattering spreads with respect to a subspace

A spread is called *a scattering spread with respect to a subspace*, if this subspace is scattered with respect to the spread.

Theorem 2.4.1 ([18, Theorem 3.2])
If W is an $(rt-t-1)$-dimensional subspace of $\mathrm{PG}(rt-1,q)$, $r \geq 2$, then there exists a scattering $(t-1)$-spread $\mathcal{S}$ with respect to W.

Proof. We remark that since all $(rt-t-1)$-dimensional subspaces in $\mathrm{PG}(rt-1,q)$ are isomorphic, it suffices to prove that we can find a spread $\mathcal{S}$ and an $(rt-t-1)$-dimensional subspace W, such that W is scattered with respect to $\mathcal{S}$. We give a proof using induction. In Theorem 2.5.5 we will show that there exists a scattered $(t-1)$-dimensional subspace with respect to a Desarguesian $(t-1)$-spread in $\mathrm{PG}(2t-1,q)$. Assume $r>2$. Let S' be a Desarguesian $(t-1)$-spread in $\mathrm{PG}(rt-1,q)$ and let U be a $(rt-2t-1)$-dimensional subspace of $\mathrm{PG}(rt-1,q)$, spanned by elements of S'. Note that such a subspace can be obtained by taking the span of $r-2$ spread elements corresponding to $r-2$ points of $\mathrm{PG}(r-1,q^t)$ which span an $r-3$ space of $\mathrm{PG}(r-1,q^t)$, i.e., a space of codimension 2. Now we consider the quotient geometry of U in $\mathrm{PG}(rt-1,q)$, which is isomorphic to $\mathrm{PG}(2t-1,q)$. Moreover, the $(t-1)$-spread in $\mathrm{PG}(rt-1,q)$ induces a Desarguesian $(t-1)$-spread in this quotient geometry. The spread elements in the quotient geometry correspond with the $(rt-t-1)$-dimensional subspaces of $\mathrm{PG}(rt-1,q)$ obtained by taking the span of U and a spread element not intersecting U. Since S' is a spread, it is clear that two such subspaces are either equal or only have U in their intersection. By Theorem 2.5.5, we can find a $(t-1)$-dimensional scattered subspace with respect to this spread in the quotient geometry. This induces an $(rt-t-1)$-dimensional space W containing U which intersects spread elements outside U in at most a point. Let W' be an $(rt-t-1)$-dimensional subspace obtained by taking the space spanned by U and a spread element of S' not intersecting W. By induction on r, we can change the spread locally in W' in order to find a spread $\mathcal{S}$ which is scattering with respect to U. The new spread $\mathcal{S}$ is a scattering spread with respect to W. ■

2.5 Scattered spaces with respect to a Desarguesian spread

Suppose we want to know the dimension of a maximum scattered space with respect to a line spread in $\mathrm{PG}(5,q)$. From the lower bound Theorem 2.2.1 and the upper bound Theorem 2.3.1 it follows that this dimension lies between 2 and 3. So we can always find a scattered plane but it is not clear if we can find a scattered 3-space. The dimension of a maximum scattered space with respect to a line spread in $\mathrm{PG}(5,q)$ will follow from Theorem 2.5.4.

Let $\mathcal{S}$ be a Desarguesian $(t-1)$-spread of $\mathrm{PG}(rt-1,q)$. Using the correspondence between the points of $\mathrm{PG}(r-1,q^t)$ and the elements of a Desarguesian $(t-1)$-spread of $\mathrm{PG}(rt-1,q)$, explained in Chapter 1, we now associate a set of points of $\mathrm{PG}(r-1, q^t)$, with every subspace of $\mathrm{PG}(rt-1, q)$. If W is a subspace in $\mathrm{PG}(rt-1, q)$, then we define $B(W)$ as the set of points of $\mathrm{PG}(r-1, q^t)$, which correspond to the elements of $\mathcal{S}$ which have a non-empty intersection with W in $\mathrm{PG}(rt-1, q)$. If W has dimension $m-1$, $m > 0$, then the cardinality of $B(W)$ is at most $\theta_{m-1}(q)$ and at least one. However, dependent on the relationship between m and t we can say more. For instance if $m \leq t$, then $B(W)$ can consist of one point, namely if W is contained in a spread element. Note that if there exists a scattered m-space with respect to $\mathcal{S}$, then the cardinality of $B(W)$ is maximal if and only if W is scattered.

Remark. Let W be a scattered subspace with respect to a Desarguesian $(t-1)$-spread of $\mathrm{PG}(rt-1, q)$. If the dimension of the intersection of W with a $(2t-1)$-dimensional space of $\mathrm{PG}(rt-1, q)$ corresponding with a line L of $\mathrm{PG}(r-1, q^t)$ is bigger than 1, then there are three non-collinear points of $W \cap L$, which are contained in spread elements corresponding with three collinear points of $\mathrm{PG}(r-1, q^t)$. This implies that the set $B(W)$ is not necessarily an embedding of W in $\mathrm{PG}(r-1, q^t)$. For more about embeddings we refer to [47].

Using the structure of $\mathrm{PG}(r-1, q^t)$, we are able to improve the bounds for a maximum scattered space with respect to a Desarguesian $(t-1)$-spread in $\mathrm{PG}(rt-1, q)$ in a number of cases. First we show that certain scattered spaces of $\mathrm{PG}(rt-1, q)$ induce two-intersection sets with respect to hyperplanes of $\mathrm{PG}(r-1, q^t)$. To prove this result we use a standard counting technique in finite geometry.

Theorem 2.5.1 ([18, Theorem 4.2])
If rt is even and $W_{\frac{rt}{2}}$ is a subspace of rank $\frac{rt}{2}$ of $\mathrm{V}(rt, q)$, which is scattered with respect to a Desarguesian t-spread $\mathcal{S}$ of $\mathrm{V}(rt, q)$, then $B(W_{\frac{rt}{2}})$ is a two-intersection set in $\mathrm{PG}(r-1, q^t)$ with respect to hyperplanes with intersection numbers $\theta_{\frac{rt}{2}-t-1}(q)$ and $\theta_{\frac{rt}{2}-t}(q)$.

Proof. Let $rt = 2m$ and h_i $(i = 1, \ldots, m)$ be the number of hyperplanes of $\mathrm{PG}(r-1, q^t)$, seen as subspaces of rank $rt-t$ in $\mathrm{V}(rt, q)$, that intersect W_m in a subspace of rank i. It is clear that a subspace of rank m and $rt-t$ contained in $\mathrm{V}(rt, q)$ necessarily meet in a subspace of rank at least $m-t$ and since W_m is scattered, such a hyperplane can not meet W_m in a subspace of rank bigger than $rt-2t$, because of the number of points contained in that hyperplane. Counting hyperplanes, point-hyperplane pairs $(P, H), P \subset B(W) \cap H$, and point-point-hyperplane triples $(P, Q, H), P, Q \subset B(W) \cap H$, we get the set of equations

$$\begin{cases} \sum_{i=m-t}^{rt-2t} h_i = \theta_{r-1}(q^t); & (1) \\ \sum_{i=m-t}^{rt-2t} \theta_{i-1}(q)h_i = \theta_{m-1}(q)\theta_{r-2}(q^t); & (2) \\ \sum_{i=m-t}^{rt-2t} \theta_{i-1}(q)(\theta_{i-1}(q)-1)h_i = \theta_{m-1}(q)(\theta_{m-1}(q)-1)\theta_{r-3}(q^t). & (3) \end{cases}$$

Consider the expression

$$\sum_{i=m-t}^{rt-2t} \left[(\theta_{i-1}(q)-\theta_{m-t-1}(q))\ (\theta_{i-1}(q)-\theta_{m-t}(q))\right] h_i. \quad (2.1)$$

We can write the coefficient of h_i in (3.3) as

$$\theta_{i-1}(q)(\theta_{i-1}(q)-1) - [\theta_{m-t-1}(q)+\theta_{m-t}(q)-1]\theta_{i-1}(q) + \theta_{m-t-1}(q)\theta_{m-t}(q).$$

Using the equations (1), (2) and (3), expression (3.3) is equal to

$$\begin{aligned} & \theta_{m-1}(q)(\theta_{m-1}(q)-1)\theta_{r-3}(q^t) \\ - \quad & [\theta_{m-t-1}(q)+\theta_{m-t}(q)-1]\theta_{m-1}(q)\theta_{r-2}(q^t) + \theta_{m-t-1}(q)\theta_{m-t}(q)\theta_{r-1}(q^t). \end{aligned}$$

Replacing rt by $2m$ and $\theta_{n-1}(q)$ by it's definition, this expression is equal to

$$\begin{aligned} & (q^t-1)^{-1}(q-1)^{-2}\big[(q^m-1)(q^m-q)(q^{2m-2t}-1) \\ & -[(q^{m-t}-1)+(q^{m-t+1}-1)-(q-1)](q^m-1)(q^{2m-t}-1) \\ & +\ (q^{m-t}-1)(q^{m-t+1}-1)(q^{2m}-1)\big] \\ = \quad & (q^t-1)^{-1}(q-1)^{-2}\,[(q^m-1)(q^{m-t}-1)\ [(q^m-q)(q^{m-t}+1) \\ & -\ (q+1)(q^{2m-t}-1)+(q^{m-t+1}-1)(q^m+1)]\big] \\ = \quad & 0. \end{aligned}$$

Hence

$$\sum_{i=m-t}^{rt-2t} \left[(\theta_{i-1}(q)-\theta_{m-t-1}(q))(\theta_{i-1}(q)-\theta_{m-t}(q))\right] h_i = 0,$$

which implies that $h_i = 0$, for all $i \geq m - t + 2$. Since a scattered subspace of rank i intersects $\theta_{i-1}(q)$ spread elements, this concludes the proof. ■

If the hypotheses of Theorem 2.5.1, rt is even is not satisfied, then we have the following.

Theorem 2.5.2 *If W_m is a scattered subspace of $\mathrm{V}(rt, q)$, rt odd, with respect to a Desarguesian t-spread of rank $m = \frac{rt-1}{2}$, then $B(W_m)$ has at most $\frac{t+3}{2}$ different intersection numbers with respect to hyperplanes in $\mathrm{PG}(r-1, q^t)$.*

Proof. Starting with the equation (3.3) and using the equations (1), (2) and (3) from the proof of Theorem 2.5.1 gives

$$\begin{aligned}
& (q^t-1)(q-1)^2 \sum_{i=m-t}^{rt-2t} [(\theta_{i-1}(q) - \theta_{m-t-1}(q))\ (\theta_{i-1}(q) - \theta_{m-t}(q))]\, h_i \\
= \ & (q^t-1)(q-1)^2\, [\theta_{m-1}(q)(\theta_{m-1}(q)-1)\theta_{r-3}(q^t) \\
& - \ [\theta_{m-t-1}(q) + \theta_{m-t}(q) - 1]\theta_{m-1}(q)\theta_{r-2}(q^t) + \theta_{m-t-1}(q)\theta_{m-t}(q)\theta_{r-1}(q^t)] \\
= \ & (q^{rt-2t+1} + q^{2m-t+1} + q^{2m-t} + q^{rt}) \\
& - (q^{rt-t+1} + q^{2m-2t+1} + q^{2m} + q^{rt-t}).
\end{aligned}$$

With $m = \frac{rt-1}{2}$ this is

$$\begin{aligned}
& (q^t-1)(q-1)^2 \sum_{i=m-t}^{rt-2t} [(\theta_{i-1}(q) - \theta_{m-t-1}(q))\ (\theta_{i-1}(q) - \theta_{m-t}(q))]\, h_i \\
= \ & (q^{2m-2t+2} + q^{2m-t+1} + q^{2m-t} + q^{2m+1}) \\
& - (q^{2m-t+2} + q^{2m-2t+1} + q^{2m} + q^{2m-t+1}).
\end{aligned}$$

The coefficient of $h_{m-t+j-1}$ in this expression is $(q^t-1)\ (q^{m-t+j-1} - q^{m-t})\ (q^{m-t+j-1} - q^{m-t+1})$. The highest order term has degree $2m - t + 2j - 2$. This implies that $h_{m-t+j-1} = 0$ for $j > (t+3)/2$. ■

We can extract some more information from the proof of Theorem 2.5.1 than was mentioned in the theorem. First of all we can solve for $h_{\frac{rt}{2}-t}$ and $h_{\frac{rt}{2}-t+1}$ in (1) and (2) to obtain the unique solution

$$\begin{cases} h_i &= 0,\ i < \frac{rt}{2} - t, \\ h_{\frac{rt}{2}-t} &= \theta_{r-1}(q^t) - \theta_{\frac{rt}{2}-1}(q), \\ h_{\frac{rt}{2}-t+1} &= \theta_{\frac{rt}{2}-1}(q), \\ h_i &= 0,\ i > \frac{rt}{2} - t + 1. \end{cases}$$

Secondly, by considering some of the equations obtained in the proof, we get an upper bound for the dimension of a maximum scattered subspace.

Theorem 2.5.3 ([18, Theorem 4.3])
If W_m is a subspace of rank m of $\mathrm{V}(rt, q)$, which is scattered with respect to a Desarguesian t-spread $\mathcal{S}$ of $\mathrm{V}(rt, q)$ then $m \le \frac{rt}{2}$. Equivalently, the dimension of a maximum scattered subspace with respect to a Desarguesian $(t-1)$-spread in $\mathrm{PG}(rt-1, q)$ is at most $\frac{rt}{2} - 1$.

Proof. Starting with a scattered subspace of rank m with respect to a Desarguesian t-spread in $\mathrm{V}(rt, q)$, we use the same set of equations as in the proof of Theorem 2.5.1 to obtain the equation

$$\begin{aligned} & (q^t-1)(q-1)^2 \sum_{i=m-t}^{rt-2t} \left[(\theta_{i-1}(q) - \theta_{m-t-1}(q))\ (\theta_{i-1}(q) - \theta_{m-t}(q))\right] h_i \\ = \ & (q^m-1)(q^m-q)(q^{rt-2t}-1) \\ & - [(q^{m-t}-1) + (q^{m-t+1}-1) - (q-1)](q^m-1)(q^{rt-t}-1) \\ & + (q^{m-t}-1)(q^{m-t+1}-1)(q^{rt}-1) \\ = \ & (q^{rt-2t+1} + q^{2m-t+1} + q^{2m-t} + q^{rt}) - (q^{rt-t+1} + q^{2m-2t+1} + q^{2m} + q^{rt-t}). \end{aligned}$$

We remark that these equations are also valid for rt odd. Since the coefficient of h_i in this expression is always positive, it follows that $m \le \frac{rt}{2}$. ■

Returning to the previous example of a line spread in $\mathrm{PG}(5, q)$, we see that this new upper bound tells us that the dimension of a maximum scattered space is at most 2. The lower bound already told us that this dimension is at least 2. Hence a maximum scattered subspace with respect to a Desarguesian line spread in $\mathrm{PG}(5, q)$, must be a plane and we see that the bounds are sharp in this case. This is not surprising since the lower bound $\lceil \frac{rt-t}{2} \rceil$ and the upper bound $\frac{rt}{2} - 1$ coincide whenever $t = 2$. So the problem is completely solved for

Desarguesian line spreads of $\mathrm{PG}(2r-1,q)$. As we mentioned before it is hard to deal with arbitrary spreads. However, for line spreads of $\mathrm{PG}(2r-1,q)$ we can prove the following.

Theorem 2.5.4 ([18, Theorem 4.5])
Let $\mathcal{S}$ be a line spread in $\mathrm{PG}(2r-1,q)$ and let T be a maximum scattered subspace of dimension $m-1$. Then

$$\begin{cases} m = r & \text{if } \mathcal{S} \text{ is a Desarguesian spread,} \\ m \geq r+1 & \text{otherwise.} \end{cases}$$

Proof. If $\mathcal{S}$ is a Desarguesian line spread then the result follows from Theorem 2.2.1 and Theorem 2.5.3. Suppose $\mathcal{S}$ is not a Desarguesian spread. There exist spread elements l_i, l_j, l_k such that l_k and $\langle l_i, l_j\rangle$ intersect in a point P. In $\langle l_i, l_j\rangle$ there are q^2+q+1 planes through P, at least $q+1$ of which must be scattered. Let π be such a scattered plane in $\langle l_i, l_j\rangle$. Then it is clear that $\langle \pi, l_i\rangle = \langle \pi, l_j\rangle$. By Theorem 2.2.1 we can construct a scattered $(r-1)$-dimensional subspace T_{r-1} containing π. But then we have that $\langle T_{r-1}, l_i\rangle = \langle T_{r-1}, l_j\rangle$ and since the number of r-dimensional spaces containing T_{r-1} in $\mathrm{PG}(2r-1,q)$ is equal to the number of spread lines intersecting T_{r-1} $(=\theta_{r-1}(q))$, there exists at least one r-dimensional scattered subspace containing T_{r-1}. This concludes the proof. ■

Remark. In [12], Beutelspacher and Ueberberg give some combinatorial characterizations of Desarguesian spreads. The previous theorem also follows from their results. The first part from [12, Section 2, Lemma 1], the second from their main theorem in [12]. The proof given here is a shorter, more direct proof.

We remark that in the case of a Desarguesian line spread in $\mathrm{PG}(2r-1,q)$ a maximum scattered spaces is induced by a canonical Baer subgeometry of $\mathrm{PG}(r-1,q^2)$. More generally, a canonical subgeometry $\mathrm{PG}(r-1,q)$ of $\mathrm{PG}(r-1,q^t)$ induces a scattered $(r-1)$-space (not necessarily maximum) with respect to a Desarguesian spread in $\mathrm{PG}(rt-1,q)$. It follows from the above theorem that in the case of line spreads, spreads which are not Desarguesian admit a scattered subspace of higher dimension than those admitted by a Desarguesian spreads. We do not know if this is true in general. We now return to Desarguesian spreads. In the next theorem we improve the lower bound for a maximum scattered subspace with respect to a Desarguesian $(t-1)$-spread in $\mathrm{PG}(rt-1,q)$. The result gives us the exact answer whenever r is even. If r is odd there is some more work to do.

Theorem 2.5.5 *If W is a maximum scattered subspace of dimension m with respect to a Desarguesian $(t-1)$-spread of $\mathrm{PG}(rt-1,q)$, then*

$$\begin{cases} m = \frac{rt}{2} - 1 & \text{if } r \text{ is even,} \\ m \geq \frac{rt-t}{2} - 1 & \text{otherwise.} \end{cases}$$

Proof. Let $\mathcal{S}$ be a $(t-1)$-spread in $\mathrm{PG}(rt-1,q)$. We can write the vectors of $\mathrm{V}(rt,q)$ as vectors over $\mathrm{GF}(q^t)$ as following. Let α be a primitive root of unity in $\mathrm{GF}(q^t)$, and let v be a vector of $\mathrm{V}(rt,q)$. The first t coordinates $(v_1,v_2,\ldots,v_t)$ of v determine the element $v_1+v_2\alpha+v_3\alpha^q+\ldots+v_t\alpha^{q^{t-2}}$ of $\mathrm{GF}(q^t)$. The same for the second t coordinates and so on. Thus with a vector of $\mathrm{V}(rt,q)$ there corresponds a vector of $\mathrm{V}(r,q^t)$. Conversely, every element of $\mathrm{GF}(q^t)$ can be uniquely written as $v_1+v_2\alpha+v_3\alpha^q+\ldots+v_t\alpha^{q^{t-2}}$, for some $v_i\in\mathrm{GF}(q)$, and hence determines t coordinates $(v_1,v_2,\ldots,v_t)$ over $\mathrm{GF}(q)$. With this one-to-one correspondence we can write the set of vectors of $\mathrm{V}(rt,q)$ as $\{(x_1,x_2,\ldots,x_r)\parallel x_i\in\mathrm{GF}(q^t)\}$. Without loss of generality we may assume that $\mathcal{S}$ is the canonical Desarguesian spread, i.e., the spread element on the vector v is $\{\lambda v\parallel\lambda\in\mathrm{GF}(q^t)\}$.
Suppose r is even and let W be the set of vectors

$$\{(x_1,x_2,\ldots,x_{r/2},x_1^q,x_2^q,\ldots,x_{r/2}^q)\parallel x_i\in\mathrm{GF}(q^t),\ i=1,\ldots,\frac{r}{2}\}.$$

Then we claim that W is a scattered subspace of rank $\frac{rt}{2}$. First of all it is clear that W is a subspace of $\mathrm{V}(rt,q)$ of rank $\frac{rt}{2}$. Suppose W is not scattered with respect to $\mathcal{S}$. Then there exists a vector $v\in\mathrm{V}(rt,q)\setminus\{0\}$, such that $v\in W$ and $\lambda v\in W$ for some $\lambda\in\mathrm{GF}(q^t)\setminus\mathrm{GF}(q)$. Suppose i is the smallest number such that the i-th coordinate x_i of v is not zero. Then $i\le r/2$, and since $v,\lambda v\in W$, the equality $\lambda x_i^q=\lambda^q x_i^q$ holds. But this implies $\lambda^q=\lambda$ and hence $\lambda\in\mathrm{GF}(q)$, a contradiction. Hence W is scattered with respect to $\mathcal{S}$ and has rank $\frac{rt}{2}$.
If r is odd, then we can consider the following subspace

$$W=\{(x_1,x_2,\ldots,x_{\frac{r-1}{2}},x_1^q,x_2^q,\ldots,x_{\frac{r-1}{2}}^q,x_1)\parallel x_i\in\mathrm{GF}(q^t),\ i=1,\ldots,\frac{r-1}{2}\}.$$

Then W is a subspace of $\mathrm{V}(rt,q)$ of rank $\frac{rt-t}{2}$. In the same way as before one shows that W is scattered. ∎

Remark. In the case that r is odd, the bound we obtained in Theorem 2.5.5 on the dimension of scattered spaces with respect to a Desarguesian spread does not improve the bound we obtained in Theorem 2.2.1. However in the proof of Theorem 2.5.5 an explicit construction is given.

So for r even there always exists a scattered subspace of dimension $\frac{rt}{2}-1$ with respect to a Desarguesian $(t-1)$-spread of $\mathrm{PG}(rt-1,q)$, and an example is given explicitly in Theorem 2.5.5 with respect to the canonical Desarguesian spread of $\mathrm{V}(rt,q)$. We now investigate these subspaces in more detail. Put

$$W=\{(x_1,x_2,\ldots,x_{r/2},x_1^q,x_2^q,\ldots,x_{r/2}^q)\parallel x_i\in\mathrm{GF}(q^t),\ i=1,\ldots,\frac{r}{2}\}.$$

Then W is a linear space over $\mathrm{GF}(q)$, but not over an extension field of $\mathrm{GF}(q)$. In fact, the subspace W does not contain a subspace which is linear over some extension field of $\mathrm{GF}(q)$. Hence it is a scattered subspace with respect to the canonical Desarguesian t-spread in $\mathrm{V}(rt, q)$. If U is a subspace over $\mathrm{GF}(q)$, and n is maximal such that a U is linear over $\mathrm{GF}(q^n)$, then we say that $\mathrm{GF}(q^n)$ is the *kernel of* U. The scattered subspaces in the proof of Theorem 2.5.5 all have kernel $\mathrm{GF}(q)$. This is not a necessary condition however. In the next theorem we will consider subspaces over $\mathrm{GF}(q)$ with an extension field of $\mathrm{GF}(q)$ as kernel, and which are scattered with respect to the canonical Desarguesian t-spread. But then of course it is necessary that this extension field only has $\mathrm{GF}(q)$ in common with $\mathrm{GF}(q^t)$. This means that the extension field is $\mathrm{GF}(q^{r'})$ for some r' relative prime with t.

Theorem 2.5.6 ([18, Theorem 4.4])
Let W_m be a maximum scattered subspace of dimension $m-1$ of $\mathrm{PG}(rt-1, q)$ with respect to a Desarguesian $(t-1)$-spread $\mathcal{S}$ of $\mathrm{PG}(rt-1, q)$. Then $m \geq r'k$, where k, r', with $r'|r$ and $(r', t) = 1$, are choosen such that $r'k$ is maximal satisfying

$$r'k < \begin{cases} \frac{rt-t+3}{2} & \text{if } q = 2 \text{ and } r' = 1, \\ \frac{rt-t+r'+3}{2} & \text{otherwise}; \end{cases}$$

Proof. We use the representation of a Desarguesian spread in the tensor product $\mathrm{V}(rt, q) = \mathrm{GF}(q^r) \bigotimes \mathrm{GF}(q^t)$ introduced in section 1.6.
Let C be the class of subspaces of $\mathrm{V}(rt, q)$ of rank $r'k$, obtained from subspaces of $\mathrm{V}(rt/r', q^{r'})$ of rank k, which intersect at least one spread element in a subspace of rank at least two. Let $W \in C$. Since W is a linear space over $\mathrm{GF}(q^{r'})$, $\lambda W = W$, for all $\lambda \in \mathrm{GF}(q^{r'}) \subset \mathrm{GF}(q^r)$. A vector $u \in \mathrm{GF}(q^r) \bigotimes \mathrm{GF}(q^t)$ is contained in the spread element $S_t(u) = \{u\alpha \parallel \alpha \in \mathrm{GF}(q^t)\}$. This implies that spread elements are fixed by multiplication with elements of $\mathrm{GF}(q^t)$. If $\beta \in \mathrm{GF}(q^{r'}) \setminus \mathrm{GF}(q)$ then

$$\{\beta u\alpha \parallel \alpha \in \mathrm{GF}(q^t)\} \cap \{u\alpha \parallel \alpha \in \mathrm{GF}(q^t)\} = \{0 \otimes 0\},$$

since $(r', t) = 1$. Moreover, the spread elements are permuted by elements of $\mathrm{GF}(q^{r'})$. For every spread element P the set $\{\beta P \parallel \beta \in \mathrm{GF}(q^{r'})\}$ contains exactly $\theta_{r'-1}(q)$ different spread elements. If W has an intersection of rank two with a spread element P then W will have an intersection of rank two with at least $\theta_{r'-1}(q)$ spread elements since the spaces $W \cap P$, $\lambda(W \cap P)$ and $(W \cap P)\mu$ have the same rank, for all $\lambda \in \mathrm{GF}(q^r)^* = \mathrm{GF}(q^r) \setminus \{0\}$, $\mu \in \mathrm{GF}(q^t)^*$.
We count 4-tuples (W, P, v_1, v_2), where $W \in C$, $P \in \mathcal{S}$, and v_1 and v_2 are two independent vectors in the intersection of P and W, in two different ways. Starting with the number of spread elements, then counting the possibilities

for v_1 and v_2 and then counting the number of elements of C containing $\langle v_1, v_2\rangle$, we get roughly

$$\theta_{r-1}(q^t)(q^t-1)(q^t-q)\begin{bmatrix} \frac{rt}{r'}-2 \\ k-2 \end{bmatrix}_{q^{r'}} \simeq q^{(r'k-2r')(\frac{rt}{r'}-k)+rt+t}.$$

Starting with the number of elements of C, then choosing the spread element and then choosing v_1 and v_2 in their intersection, we get roughly

$$|C|\theta_{r'-1}(q)(q^2-1)(q^2-q) \simeq |C|q^{r'+3}.$$

The total number of subspaces of $\mathrm{V}(rt/r', q^{r'})$ of rank k has order $q^{r'k(rt/r'-k)}$. If the order of $|C|$ is smaller than this, there must exist a scattered subspace of rank $r'k$. By computation there exists a scattered subspace of rank $r'k$ with respect to $\mathcal{S}$ if

$$r'k < \frac{rt-t+r'+3}{2}.$$

By doing the computation in detail we see that there exists a scattered subspace if

$$\frac{(q^{t-1}-1)(q^{kr'}-1)(q^{kr'-r'}-1)}{(q^{r'}-1)(q^2-1)(q^{rt-r'}-1)} < 1.$$

This is satisfied if $r'k < \frac{rt-t+r'+3}{2}$ unless $r'=1$ and $q=2$, in which case $r'k < \frac{rt-t+r'+2}{2}$ implies the existence of a scattered subspace of rank $r'k$. This concludes the proof. ■

Using the computer package GAP we did some computing for small values of q, r, t. The results are listed in Table 2.1.
The first three columns give the values of q, r and t for which the computer search was performed.
Column 4 contains the upper bound (UB) $\frac{rt}{2}$, obtained in Theorem 2.5.3, on the rank of a maximum scattered space with respect to a Desarguesian t-spread $\mathcal{S}$ in $\mathrm{V}(rt, q)$.
The next column gives the theoretical lower bound (LB) obtained in Theorem 2.5.5, Theorem 2.5.4 or Theorem 2.5.6. The theorem from which the theoretical lower bound follows for the specified values of q, r and t, is given in the last column. In the case that Theorem 2.5.6 implies the lower bound, the theorem is not mentioned, but the values of r' and k, as in Theorem 2.5.6, which determine the best lower bound , can be deduced from the given vector spaces. In the fifth row for example, Theorem 2.5.6 states that the lower bound 6 can be obtained by a rank 2 vector space over $\mathrm{GF}(2^3)$ or by a rank 6 vector space over $\mathrm{GF}(2)$. In the first case $r'=3,\ k=2$, in the second case $r'=1,\ k=6$.
In column 6 we give the rank of the scattered subspace with respect to the t-spread of $\mathrm{V}(rt, q)$, for the specified r, t, and q, which we found using the computer package GAP.

q	r	t	UB = $\lfloor rt/2 \rfloor$	LB	GAP	Theorem
q	even	t	$rt/2$	$rt/2$	-	Theorem 2.5.5
q	r	2	r	r	-	Theorem 2.5.4
q	3	3	4	4	4	$\mathrm{V}(4, q)$
q	3	4	6	6	6	$\mathrm{V}(2, q^3)$
2	3	5	7	6	7	$\mathrm{V}(2, 2^3), \mathrm{V}(6, 2)$
2	3	6	9	7	8	$\mathrm{V}(7, 2)$
2	3	7	10	9	MP	$\mathrm{V}(3, 2^3)$
2	3	8	12	9	11	$\mathrm{V}(2, 2^3), \mathrm{V}(9, 2)$
2	5	3	7	7	7	$\mathrm{V}(7, 2)$
2	5	4	10	10	MP	$\mathrm{V}(2, 2^5)$
3	3	3	4	4	4	$\mathrm{V}(3, 3)$
3	3	4	6	6	6	$\mathrm{V}(2, 3^3)$
3	3	5	7	6	MP	$\mathrm{V}(6, 3), \mathrm{V}(2, 3^3)$

Table 2.1: Computer results on maximum scattered spaces with respect to a Desarguesian t-spread in $\mathrm{V}(rt, q)$ using GAP

In all the cases where the lower bound is smaller that the upper bound, the result improved the lower bound or the computer search ran into memory problems, which we denoted with (MP).
Note that the lower bound was always obtained by a computer search, unless the search ran into memory problems.
Row 5 is the most interesting. With a computer search we find a scattered space meeting the upper bound, and improving the lower bound. It follows from the data in rows 6 and 8 that the computer result improves the lower bound, although the upper bound is not reached.
It must be mentioned that none of the computer searches was complete. As computers become more powerful, it is hoped to attain more data than included in the Table 2.1.

2.6 Two-intersection sets

In this section we want to say something more about the two-intersection sets we obtained in Theorem 2.5.1. First we point out the relation between two-intersection sets with respect to hyperplanes, two-weight linear codes and strongly regular graphs. For a more detailed survey of these objects we refer to [27].

A *q-ary linear code* C is a linear subspace of $\mathrm{GF}(q)^n$. If C has dimension r, then C is called a $[n, r]$-code. A *generator matrix* G for a linear code C is an

$(r \times n)$-matrix for which the rows are a basis of C. If G is a generator matrix for C then $C = \{xG \parallel x \in \mathrm{GF}(q)^r\}$. The *weight* $w(c)$ of a codeword $c \in C$ is the number of non-zero coordinates of c or equivalently the Hamming distance between the all-zero codeword and c. If no two of the vectors defined by the columns of G are linearly dependent, then C is called *projective*.

Consider a two-intersection set T with respect to hyperplanes in $\mathrm{PG}(r-1,q)$ of size n, with intersection numbers h_1 and h_2. In [27], such a set is called a *projective* (n, r, h_1, h_2) *set*. We assume that the points of T span $\mathrm{PG}(r-1,q)$. Put $T = \{\langle g_{1i}, \dots, g_{ri}\rangle \parallel i = 1, \dots n\}$. Let G be the $(r \times n)$-matrix with the points of T as columns. The points of T span $\mathrm{PG}(r-1,q)$, hence the matrix G has rank r. The rows of G span an $[n,r]$-code C. Suppose that the j-th coordinate of a codeword, $c = (c_1, \dots, c_n) = (x_1, \dots, x_r)G$, is zero. That is

$$c_j = \sum_{i=1}^{r} x_i g_{ij} = 0.$$

This is equivalent with saying that the point with coordinates $(g_{1j}, \dots, g_{rj})$ lies on the hyperplane of $\mathrm{PG}(r-1,q)$, with equation

$$\sum_{i=1}^{r} x_i X_i = 0.$$

Since T is a projective (n, r, h_1, h_2) set, the number of zeros in a codeword is either h_1 or h_2. This implies that C is a two-weight code with weights $w_1 = n - h_1$ and $w_2 = n - h_2$. Conversely, we can start with a two-weight linear code and obtain a two-intersection set. We have the following correspondence.

Theorem 2.6.1 ([27, Theorem 3.1])

- *If the code C is a q-ary projective two-weight $[n,r]$ code, then the points defined by the columns of a generator matrix of C form a projective $(n, r, n-w_1, n-w_2)$ set that spans* $\mathrm{PG}(r-1,q)$.

- *Conversely, if the columns of a matrix G are the points of a projective (n, r, h_1, h_2) set that spans* $\mathrm{PG}(r-1,q)$*, then the code C, with G as a generator matrix, is a q-ary projective two-weight $[n,r]$ code with weights $n-h_1$ and $n-h_2$.*

Applying this to the two-intersection set obtained in Theorem 2.5.1, we get a projective

$$\left(\frac{q^{\frac{rt}{2}}-1}{q-1}, r, \frac{q^{\frac{rt}{2}-t}-1}{q-1}, \frac{q^{\frac{rt}{2}-t+1}-1}{q-1}\right)$$

set which gives rise to a two-weight $[\frac{q^{\frac{rt}{2}}-1}{q-1}, r]$-code with weights

$$\begin{cases} w_1 & = q^{\frac{rt}{2}-t}\left(\frac{q^t-1}{q-1}\right), \\ w_2 & = q^{\frac{rt}{2}-t+1}\left(\frac{q^{t-1}-1}{q-1}\right). \end{cases}$$

We remark that the condition that the two-intersection set spans $\mathrm{PG}(r-1,q^t)$ is satisfied because of Theorem 2.5.3. The parameters of the obtained two-weight codes correspond to $SU2$, $CY4$ and $RT1$ in [27], which arise from two-intersection sets obtained as follows. If t is even this set has the same parameters as the disjoint union of $(q^{t/2}-1)/(q-1)$ Baer subgeometries isomorphic to $\mathrm{PG}(r-1,q^{t/2})$. We say that a two-intersection set isomorphic to such a union of subgeometries is of *type I*. If t is odd this set has the same parameters as the union of $(q^t-1)/(q-1)$ elements of an $(r/2-1)$-spread in $\mathrm{PG}(r-1,q^t)$. We call these two-intersection sets of *type II*. In [62], Penttila and Royle give a complete characterization of two-intersection sets in planes of order nine. According to their terminology the parameters of the two-intersection set obtained in Theorem 2.5.1 for $r=3$ are called *standard parameters*. These sets occur in planes of square order and have type $(m, m+\sqrt{q})$ in $\mathrm{PG}(2,q)$. We will prove that the sets arising from a scattered space are neither of type I nor of type II.

Theorem 2.6.2 ([19])
The two-intersection sets arising from scattered spaces of dimension $rt/2$ with respect to a Desarguesian $(t-1)$-spread $\mathcal{S}$ in $\mathrm{PG}(rt-1,q)$ are not isomorphic with the two-intersection sets of type I or type II.

Proof. First suppose that t is odd. An element E of an $(r/2-1)$-spread in $\mathrm{PG}(r-1,q^t)$ induces an $(rt/2-t)$-dimensional space in $\mathrm{PG}(rt-1,q)$, partitioned by a subset of the $(t-1)$-spread $\mathcal{S}$. Theorem 2.5.3 implies that W intersects this subspace in a subspace of dimension at most $rt/4-1$, since the intersection is scattered with respect to the restriction of $\mathcal{S}$ to this subspace. Hence $B(W)$ can not contain this spread element E. Note that using the same argument, it is easy to show that $B(W)$ can not contain a line of $\mathrm{PG}(r-1,q^t)$.
Now suppose that t is even. We will prove that $B(W)$ can not contain a Baer hyperplane $\mathcal{B}$, i.e., a subgeometry of $\mathrm{PG}(r-1,q^t)$ isomorphic with $\mathrm{PG}(r-2,q^{t/2})$. Note that this is again, as in the case where t is odd, a stronger property than needed to prove the theorem.
To avoid confusion in what follows $P(\alpha)$ will denote a point in $\mathrm{PG}(r-1,q^t)$, while $\langle\lambda\rangle$ will denote a point in $\mathrm{PG}(rt-1,q)$.
Suppose $\mathcal{B}$ is contained in $B(W)$ and let H be the hyperplane of $\mathrm{PG}(r-1,q^t)$,

that contains $\mathcal{B}$. Without loss of generality we can assume that $\mathcal{B}$ and H are generated by the same points. So

$$\mathcal{B} = \{P(\alpha_1 u_1 + \ldots + \alpha_{r-1} u_{r-1}) \parallel \alpha_1, \ldots, \alpha_{r-1} \in \mathrm{GF}(q^{t/2})\}$$

and

$$H = \{P(a_1 u_1 + \ldots + a_{r-1} u_{r-1}) \parallel a_1, \ldots, a_{r-1} \in \mathrm{GF}(q^t)\}.$$

Since $\mathcal{B}$ is contained in $B(W)$, the hyperplane H intersects $B(W)$ in n points, where $n = (q^{rt/2-t+1} - 1)/(q-1)$ is the larger of the two intersection numbers. So the subspace in $\mathrm{PG}(rt-1, q)$ induced by H intersects W in a subspace of dimension $k - 1 := rt/2 - t$. We denote the set of points in $\mathrm{PG}(r-1, q^t)$ corresponding with spread elements intersecting this subspace with $\mathcal{W}$. Put

$$\mathcal{W} = \{P(\lambda_1 v_1 + \ldots + \lambda_k v_k) \parallel \lambda_1, \ldots, \lambda_k \in \mathrm{GF}(q)\}.$$

Moreover we can express the vectors v_i, $(i = 1, \ldots, k)$, as a linear combination of $u_1, \ldots, u_{r-1}$ over $\mathrm{GF}(q^t)$. Let C be the matrix over $\mathrm{GF}(q^t)$ such that

$$\begin{bmatrix} v_1 \\ v_2 \\ \ldots \\ v_k \end{bmatrix} = C^t \begin{bmatrix} u_1 \\ u_2 \\ \ldots \\ u_{r-1} \end{bmatrix}.$$

Then $\mathcal{B}$ will be contained in $B(W)$ if

$$\forall \alpha_1, \ldots, \alpha_{r-1} \in \mathrm{GF}(q^{t/2}) : \exists \lambda_1, \ldots, \lambda_k \in \mathrm{GF}(q), \exists a \in \mathrm{GF}(q^t)^*$$

such that

$$a \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \ldots \\ \alpha_{r-1} \end{bmatrix} = C \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \ldots \\ \lambda_k \end{bmatrix}.$$

Putting $\alpha := (\alpha_1, \ldots, \alpha_{r-1})^T$, and $\lambda := (\lambda_1, \ldots, \lambda_k)^T$ this equation becomes

$$a\alpha = C\lambda.$$

Let

$$T = \{(a, \alpha, \lambda) \in \mathrm{GF}(q^t)^* \times \mathrm{GF}(q^{t/2})^{r-1} \times \mathrm{GF}(q)^k \ : \ a\alpha = C\lambda\}.$$

If (a, α, λ), $(b, \alpha, \mu) \in T$, then $C(b\lambda - a\mu) = 0$. This implies that

$$b\lambda^T (v_1, \ldots, v_k)^T = a\mu^T (v_1, \ldots, v_k)^T,$$

or $(v_1, \ldots, v_k)\lambda = a/b\ (v_1, \ldots, v_k)\mu$. Since W is scattered with respect to $\mathcal{S}$ and $\langle\lambda\rangle, \langle\mu\rangle \in W$, we must have that $a/b \in \mathrm{GF}(q)$ and so $\langle\lambda\rangle = \langle\mu\rangle$. Let

$$T_a = \{\langle\lambda\rangle \parallel \exists\alpha : (a, \alpha, \lambda) \in T\}.$$

Note that if $a/b \in \mathrm{GF}(q^{t/2})$ then $T_a = T_b$ and that T_a is a subspace of $\mathrm{PG}(rt-1, q)$. Now if $T_a \neq \emptyset$ and $\langle\mu\rangle \in T_b \setminus T_a$, $\langle\nu\rangle \in T_c \setminus T_a$, $\langle\mu\rangle \neq \langle\nu\rangle$, and $\langle T_a, \langle\mu\rangle\rangle = \langle T_a, \langle\nu\rangle\rangle$, then the line joining $\langle\mu\rangle$ and $\langle\nu\rangle$ intersects T_a, so without loss of generality $\lambda + \mu + \nu = 0$ and

$$(a, \alpha, \lambda), (b, \beta, \mu), (c, \gamma, \nu) \in T,$$

for certain β and γ. It follows that

$$a\alpha + b\beta + c\gamma = 0.$$

Let $\delta \in \mathrm{GF}(q^{t/2})^{r-1}$ be such that $\delta^T\alpha = 0 \neq \delta^T\beta$. This is possible since we saw that if $P(\alpha) = P(\beta)$ then $\langle\lambda\rangle = \langle\mu\rangle$, but $\langle\mu\rangle \notin T_a$. We get $b\delta^t\beta + c\delta^t\gamma = 0$, and $b/c \in \mathrm{GF}(q^{t/2})$. This implies that $T_b = T_c$. Thus

$$(a, \alpha, \lambda), (b, \beta, \mu), (b, \gamma, \nu) \in T,$$

for certain β and γ. Now we have that

$$b(\beta + \gamma) + a\alpha = 0.$$

So $b/a \in \mathrm{GF}(q^{t/2})$ or $T_a = T_b$, which is a contradiction. This shows that if T_a has dimension $d - 1$, then there is at most one point in every subspace of dimension d, containing T_a. So the set

$$\{\langle\mu\rangle\ :\ \exists b, \beta : (b, \beta, \mu) \in T\}$$

contains at most

$$\frac{q^d - 1}{q - 1} + \frac{q^{k-d} - 1}{q - 1}$$

points. Every $P(\alpha)$ determines a different $\langle\mu\rangle$, so we must have

$$\frac{q^{(r-1)t/2} - 1}{q^{t/2} - 1} \leq \frac{q^d - 1}{q - 1} + \frac{q^{k-d} - 1}{q - 1}.$$

Recall that $k = rt/2 - t + 1$. Since we assumed $d \geq 1$ this implies that $d = k$, but this is clearly impossible, since that would imply that $\mathcal{W}$ is completely contained in the smaller set $\mathcal{B}$. ■

For the correspondence between two-intersection sets with respect to hyperplanes and strongly regular graphs, we refer to [27] and simply state the result.

Theorem 2.6.3 ([27])
A projective $(n, r, n - w_1, n - w_2)$ set for which the points span $\mathrm{PG}(r-1, q)$ *is equivalent with a strongly regular graph for which the parameters (N, K, λ, μ) are given by*

$$\begin{cases} N &= q^r, \\ K &= n(q-1), \\ \lambda &= K^2 + 3K - q(w_1 + w_2) - Kq(w_1 + w_2) + q^2 w_1 w_2, \\ \mu &= \frac{q^2 w_1 w_2}{q^r} = K^2 + K - Kq(w_1 + w_2) + q^2 w_1 w_2. \end{cases}$$

We remark that since strongly regular graphs with these parameters exist this theorem does not give us non existence results for scattered spaces.

2.7 Blocking sets

Here we only consider blocking sets in projective spaces. Blocking sets in affine spaces are far from equivalent to the blocking sets in projective spaces. For results concerning blocking sets in affine spaces, we refer to S. Ball [5].
An *s-fold blocking set with respect to k-dimensional subspaces in* $\mathrm{PG}(n, q)$ is a set of points, at least s on every k-dimensional subspace of $\mathrm{PG}(n, q)$. A point of an s-fold blocking set with respect to k-dimensional subspaces which lies on a k-dimensional subspace intersecting the blocking set in exactly s points, is called *essential*. If every point contained in the s-fold blocking set is essential, then we say that the blocking set is *minimal* or *irreducible*. This is equivalent with saying that no proper subset of the s-fold blocking set is itself an s-fold blocking set. If $k = n - 1$, then we omit the words " with respect to $(n-1)$-dimensional subspaces". If $s = 1$, then we simply speak of a *blocking set*, otherwise they are sometimes called *multiple blocking sets*. If a blocking set with respect to k-dimensional subspaces contains an $(n-k)$-dimensional subspace then we call the blocking set *trivial*. Here, we will only consider non-trivial blocking sets, and from now on with a blocking set we mean a non-trivial blocking set. One example of a blocking set in $\mathrm{PG}(n, q)$ is a blocking set in a plane of $\mathrm{PG}(n, q)$. On the other hand if B is a blocking set in $\mathrm{PG}(n, q)$, then we can project B from a point not in B on to a hyperplane. Since this projection will then be a blocking set in that hyperplane, it follows that the size of the smallest blocking set with respect to hyperplanes, will be at least the size of the smallest blocking set in a plane. Moreover, this implies that the smallest blocking sets in $\mathrm{PG}(n, q)$ are the smallest minimal blocking sets in a plane.
A blocking set B in $\mathrm{PG}(2, q)$ is called *small* if $|B| < 3(q+1)/2$. If ℓ is a line and B a blocking set in $\mathrm{PG}(2, q)$ then ℓ intersects B in at most $|B| - q$ points. If B is a blocking set in $\mathrm{PG}(2, q)$ of size $q + m$, and there is a line ℓ intersecting B in exactly m points, then we say that B is *of Rédei type*, and ℓ is called a *Rédei*

line. For a long time all known examples of small minimal blocking sets were of Rédei type, but in 1997 Polito and Polverino [65] constructed small minimal blocking sets which are not of Rédei type. The examples were constructed using the correspondence between the points of $\mathrm{PG}(2, q^t)$ and the spread elements of a Desarguesian $(t-1)$-spread of $\mathrm{PG}(3t-1, q)$, as explained in Chapter 1. Let us give an example. Suppose we want a blocking set in $\mathrm{PG}(2, q^t)$. Then we can look at the points of $\mathrm{PG}(2, q^t)$ as the elements of a $(t-1)$-spread $\mathcal{S}$ in $\mathrm{PG}(3t-1, q)$ and the $(2t-1)$ spaces spanned by two spread elements correspond with the lines of $\mathrm{PG}(2, q^t)$. If W is a subspace of dimension t in $\mathrm{PG}(3t-1, q)$ then W meets every $(2t-1)$-space in at least a point. Hence the set of points $B(W)$ in $\mathrm{PG}(2, q^t)$ induced by W intersects every line of $\mathrm{PG}(2, q^t)$ in at least a point, i.e., $B(W)$ is a blocking set of $\mathrm{PG}(2, q^t)$. Moreover if W is scattered with respect to $\mathcal{S}$ then it follows that the blocking set has size $q^t + q^{t-1} + \ldots + q + 1$. A blocking set that can be constructed in such a way is called a *linear blocking set*. So with a linear blocking set B of $\mathrm{PG}(r-1, q^t)$ there always corresponds a subspace W over a subfield of $\mathrm{GF}(q^t)$, such that $B = B(W)$. The *kernel* of the blocking set $B(W)$ is the kernel of the subspace W, as defined in 2.5. The following theorem states what type of blocking sets we get using scattered spaces.

Theorem 2.7.1 ([18])
A scattered subspace W of rank m, with respect to a Desarguesian t-spread, in $\mathrm{V}(rt, q)$ induces a $(\theta_{k-1}(q))$-fold blocking set, with respect to $(\frac{rt-m+k}{t} - 1)$-dimensional subspaces in $\mathrm{PG}(r-1, q^t)$, of size $\theta_{m-1}(q)$, where $1 \leq k \leq m$ such that $t \mid m-k$.

Proof. Let U be an $(\frac{rt-m+k}{t} - 1)$-dimensional subspace in $\mathrm{PG}(r-1, q^t)$. Then U induces a $(rt-m+k-1)$-dimensional subspace in $\mathrm{PG}(rt-1, q)$, which intersects an $(m-1)$-dimensional subspace in a subspace of dimension at least $k-1$. The rest of the proof follows from the fact that W is scattered. ■

Remark. In [36] Heim introduced a *proper blocking set* as a blocking set in $\mathrm{PG}(n, q)$ not containing a blocking set in a hyperplane of $\mathrm{PG}(n, q)$. In $\mathrm{PG}(r-1, q^t)$, we can always construct a proper blocking set if $t > r-2$, with $r \geq 3$. To do this, we use Theorem 2.2.1, with the extra property that we always choose a vector that lies in a spread element, which corresponds with a point in $\mathrm{PG}(r-1, q^t)$ that is independent from the points corresponding with the previously intersected spread elements, as long as that is possible. In this way we can construct a scattered t-dimensional subspace W of $\mathrm{PG}(rt-1, q)$, with the additional property that $B(W)$ is a minimal blocking set not contained in a hyperplane.

2.7.1 Linear blocking sets of size $q^t + q^{t-1} + \ldots + q^i + 1$ in $\mathrm{PG}(2, q^t)$

Let $\mathcal{S}$ be a Desarguesian $(t-1)$-spread in $\mathrm{PG}(3t-1, q)$ and $S_P \in \mathcal{S}$. The quotient space of S_P in $\mathrm{PG}(3t-1, q)$ is isomorphic with $\mathrm{PG}(2t-1, q)$, and the Desarguesian spread $\mathcal{S}$ induces a Desarguesian $(t-1)$-spread in this quotient space. Let U be a maximum scattered space in this quotient geometry. Such a space exists and has dimension $t-1$, see Theorem 2.5.5. Returning to $\mathrm{PG}(3t-1, q)$, U induces a subspace T of dimension $2t-1$, with the property that T contains S_P and it intersects every other element of $\mathcal{S}$ in at most a point. Using the correspondence between the elements of a Desarguesian $(t-1)$-spread in $\mathrm{PG}(3t-1, q)$ and the points of $\mathrm{PG}(2, q^t)$, T induces a set of points $B(T)$ of size $q^{2t-1} + q^{2t-2} + \ldots + q^t + 1$, containing the point P, which corresponds with the spread element S_P, see [18]. Taking subspaces of T of dimension t intersecting S_P in a subspace of dimension $i-1$ we obtain small minimal blocking sets of $\mathrm{PG}(2, q^t)$, of size $q^t + q^{t-1} + \ldots + q^i + 1$, $i \in \{1, \ldots t-1\}$, containing P.

Theorem 2.7.2 *The intersection numbers of $B(T)$ with lines of $\mathrm{PG}(2, q^t)$ are 1, $q^t + 1$ and $q^{t-1} + q^{t-2} + \ldots + 1$. Moreover there are $q^{t-1} + q^{t-2} + \ldots + 1$ lines contained in $B(T)$, and $q^t - (q^{t-1} + q^{t-2} + \ldots + 1)$ tangents at P.*

Proof. Suppose the line L of $\mathrm{PG}(2, q^t)$ contains P. Such a line induces a spread element in the quotient geometry of S_P in $\mathrm{PG}(3t-1, q)$. Since U is scattered, this spread element does not intersect U or it has exactly one point in common with U. This implies that the $(2t-1)$-space corresponding with L in $\mathrm{PG}(3t-1, q)$ intersects T in a subspace of dimension $t-1$ or t. This gives the intersection numbers 1 and $q^t + 1$, respectively. Counting the points on the lines P, we obtain that there are $q^{t-1} + q^{t-2} + \ldots + 1$ lines intersecting $B(T)$ in $q^t + 1$ points , i.e., are contained in $B(T)$, and $q^t - (q^{t-1} + q^{t-2} + \ldots + 1)$ lines intersect $B(T)$ only in P, i.e., are tangents at P.
If the line L does not contain P, then T intersects the $(2t-1)$-dimensional subspace of $\mathrm{PG}(3t-1, q)$, corresponding with L, in a subspace of dimension at most $t-1$. On the other hand its dimension should be at least $t-1$. This gives the intersection number $q^{t-1} + q^{t-2} + \ldots + 1$. ■

Blocking sets of size $q^t + q^{t-1} + 1$

Let W be a t-dimensional subspace of T, intersecting S_P in a subspace of dimension $t-2$.

Theorem 2.7.3 *The set $B(W)$ is a small minimal blocking set of size $q^t + q^{t-1} + 1$, of Rédei type.*

Proof. It is clear that $B(W)$ is a small minimal blocking set. It is easy to see that every non-tangent line through P is a Rédei line. ■

Remark. Since every non-tangent line containing P is a Rédei line, it is easy to check that the blocking set must have $q+1$ Rédei lines, and so it follows from [50] that the blocking set is equivalent to the blocking set defined by the trace function.

Blocking sets of size $q^t + q^{t-1} + \ldots + q^i + 1$, $i \in \{2, \ldots, t-2\}$

Let W be a t-dimensional subspace of T, intersecting S_P in a subspace of dimension $i-1$, $i \in \{2, \ldots, t-2\}$.

Theorem 2.7.4 *The set $B(W)$ is a small minimal blocking set of size $q^t + q^{t-1} + \ldots + q^i + 1$, not of Rédei type.*

Proof. It is clear that $B(W)$ is a small minimal blocking set. A line of $\mathrm{PG}(2, q^t)$, not on P, corresponds to $(2t-1)$-dimensional subspaces L of $\mathrm{PG}(3t-1, q)$ intersecting W in a scattered subspace M with respect to the Desarguesian $(t-1)$-spread $\mathcal{S}$, induced by the points of $\mathrm{PG}(2, q^t)$. Since M is scattered with respect to the induced Desarguesian spread in L, it follows from Theorem 2.5.3 that a line not on P cannot intersect $B(W)$ in $q^{t-1} + \ldots + q^i + 1$ points, since $i \geq 2$. Lines on P are tangents, or they intersect $B(T)$ in $q^t + 1$ points. From this it follows that such lines intersect W in $i-1$ or in i dimensions. Since $i \leq t-2$, such a line will never be a Rédei line. ■

Blocking sets of size $q^t + q^{t-1} + \ldots + 1$

Let W be a t-dimensional subspace of T, intersecting S_P in a point.

Theorem 2.7.5 *The set $B(W)$ is a small minimal blocking set of size $q^t + q^{t-1} + \ldots + 1$, and depending on the choice of W it is of Rédei type or not.*

Proof. It is clear that $B(W)$ is a small minimal blocking set. Lines of $\mathrm{PG}(2, q^t)$, not on P, correspond to $(2t-1)$-dimensional subspaces of $\mathrm{PG}(3t-1, q)$ intersecting T in a subspace of dimension $t-1$. Two such $(t-1)$-subspaces of T intersect each other in at most a point. If Q is a point of S_P and π is a subspace of dimension $t-1$ of $T \setminus S_P$, then $\langle Q, \pi \rangle$ is a t-dimensional subspace of T, intersecting S_P in the point Q. If we choose π as an intersection of a $(2t-1)$-dimensional subspaces of $\mathrm{PG}(3t-1, q)$, corresponding with a line of $\mathrm{PG}(2, q^t)$

not containing P, with T then $B(\langle Q, \pi \rangle)$ is of Rédei type. If we choose π not contained in one of the $(t-1)$-dimensional subspaces of T corresponding with lines of $\mathrm{PG}(2, q^t)$, then $B(\langle Q, \pi \rangle)$ is not of Rédei type. ■

Remark. In the case of Theorem 2.7.5 the subspace W is scattered with respect to the Desarguesian spread $\mathcal{S}$. If the blocking set is of Rédei type then the W can not be extended to a maximum scattered space, because a maximum scattered space induces a two-intersection set in $\mathrm{PG}(2, q^t)$ and $q^{t-1} + \ldots + 1$ is bigger than both intersection numbers.

2.7.2 Linear blocking sets of size $q^t + q^{t-1} + 1$

Theorem 2.7.6 *If λ is a primitive element in $\mathrm{GF}(q^t)$, and $a + b + c = t - 2$, then*

$$B = \{\langle x_0 + x_1\lambda + \ldots + x_a\lambda^a, y_0 + y_1\lambda + \ldots + y_b\lambda^b, z_0 + z_1\lambda + \ldots + z_c\lambda^c\rangle$$

$$\| \; x_0, \ldots, x_a, y_0, \ldots, y_b, z_0, \ldots, z_c \in \mathrm{GF}(q)\},$$

is a small minimal linear blocking set in $\mathrm{PG}(2, q^t)$ of size $q^t + q^{t-1} + 1$.

Proof. It is clear that the set of all vectors of the form

$$(x_0 + x_1\lambda + \ldots + x_a\lambda^a, y_0 + y_1\lambda + \ldots + y_b\lambda^b, z_0 + z_1\lambda + \ldots + z_c\lambda^c),$$

with $x_0, \ldots, x_a, y_0, \ldots, y_b, z_0, \ldots, z_c \in \mathrm{GF}(q)$, is a vectorspace over $\mathrm{GF}(q)$ of rank $t + 1$. This induces a small minimal linear blocking set in $\mathrm{PG}(2, q^t)$. If the points $P = \langle x, y, z \rangle$ and $Q = \langle u, v, w \rangle$ belong to the blocking set then

$$\begin{aligned} x &= x_0 + x_1\lambda + \ldots + x_a\lambda^a, \\ y &= y_0 + y_1\lambda + \ldots + y_b\lambda^b, \\ z &= z_0 + z_1\lambda + \ldots + z_c\lambda^c, \end{aligned}$$

and

$$\begin{aligned} u &= x'_0 + x'_1\lambda + \ldots + x'_a\lambda^a, \\ v &= y'_0 + y'_1\lambda + \ldots + y'_b\lambda^b, \\ w &= z'_0 + z'_1\lambda + \ldots + z'_c\lambda^c, \end{aligned}$$

for some $x_0, x'_0, \ldots, x_a, x'_a, y_0, y'_0, \ldots, y_b, y'_b, z_0, z'_0, \ldots, z_c, z'_c \in \mathrm{GF}(q)$. If $P = Q$, then there is an $\alpha \in \mathrm{GF}(q^t)$ such that $(x, y, z) = \alpha(u, v, w)$. This implies that, if we look at the elements of $\mathrm{GF}(q^t)$ as polynomials in λ, there will be a "representative" for every point P with $\gcd(x, y, z) = 1$. So if we count the number of triples (x, y, z), where x, y, and z are polynomials in λ of degree at most a, b, and c, respectively, with $\gcd(x, y, z) = 1$, then we will have counted the number of points of B. We denote this number with $I(a, b, c)$. If u is a polynomial in λ over $\mathrm{GF}(q)$, then with $I_u(a,b,c)$, we denote the number of triples (x,y,z), where x, y, and z are polynomials in λ of degree at most a, b, and c, respectively, with $\gcd(x,y,z)=u$. If we sum over all monic polynomials $u \in \mathrm{GF}(q)[\lambda] \setminus \{0\}$, we get

$$T(a,b,c) := \sum_{u \in M} I_u(a,b,c) = \frac{q^{a+b+c+3}-1}{q-1},$$

where M denotes the set of all monic polynomials in $\mathrm{GF}(q)[\lambda] \setminus \{0\}$.
On the other hand, we have a triple (x,y,z) with $\gcd(x,y,z)=u$, if and only if $\gcd(x/u, y/u, z/u) = 1$. So $I_u(a,b,c) = I(a-u^\circ, b-u^\circ, c-u^\circ)$, where u° denotes the degree of u. This implies that $I_u(a,b,c)$ only depends on the degree of u. Since there are q^k monic polynomials of degree k we have

$$T(a,b,c) = \sum_{k=0}^{\infty} q^k I(a-k, b-k, c-k).$$

From this it follows that

$$\begin{aligned} I(a,b,c) &= T(a,b,c) - qT(a-1,b-1,c-1) \\ &= \tfrac{q^{a+b+c+3}-1}{q-1} - q\tfrac{q^{a+b+c}-1}{q-1} \\ &= q^t + q^{t-1} + 1. \end{aligned}$$

■

2.7.3 A $(q+1)$-fold blocking set in $\mathrm{PG}(2,q^4)$

In this section we are interested in a maximum scattered subspace of dimension 5 with respect to a Desarguesian 3-spread in $\mathrm{PG}(11,q)$. This is how the concept of scattered spaces found its origin. Let us first give some background information on multiple blocking sets in a projective plane. For a survey on blocking sets (1-blocking sets) we refer to [15], [16]. There is less known about s-fold blocking sets, where $s>1$. If the s- fold blocking set B in $\mathrm{PG}(2,q)$ contains a line ℓ, then $B \setminus \ell$ is an $(s-1)$-fold blocking set in $AG(2,q) = \mathrm{PG}(2,q) \setminus \ell$. The result from [6] gives the following.

Theorem 2.7.7 (Ball [6])
Let B be an s-fold blocking set in $\mathrm{PG}(2,q)$ that contains a line and e maximal such that $p^e|(s-1)$, then $|B| \geq (s+1)q - p^e + 1$.

This covers previous results by Bruen [22, 23], who proved the general bound $(s+1)(q-1)+1$ and Blokhuis [14], who proved $(s+1)q$ in the case $(p, s-1) = 1$.

If the s-fold-blocking set does not contain a line then Hirschfeld [37, Theorem 13.31] states that it has at least $sq + \sqrt{sq} + 1$ points. A *Baer subplane* of a projective plane of order q is a subplane of order $\sqrt{q}$. A strong result concerning s-fold blocking sets in $\mathrm{PG}(2, q)$ not containing a line is the following.

Theorem 2.7.8 (Blokhuis, Storme, Szőnyi [17])
Let B be an s-fold blocking set in $\mathrm{PG}(2, q)$ of size $s(q + 1) + c$. Let $c_2 = c_3 = 2^{-1/3}$ and $c_p = 1$ for $p > 3$.

1. *If $q = p^{2d+1}$ and $s < q/2 - c_p q^{2/3}/2$ then $c \geq c_p q^{2/3}$.*
2. *If $4 < q$ is a square, $s \leq q^{1/4}/2$ and $c < c_p q^{2/3}$, then $c \geq s\sqrt{q}$ and B contains the union of s disjoint Baer subplanes.*
3. *If $q = p^2$ and $s < q^{1/4}/2$ and $c < p\lceil \frac{1}{4} + \sqrt{\frac{p+1}{2}}\rceil$, then $c \geq s\sqrt{q}$ and B contains the union of s disjoint Baer subplanes.*

This result is proved using lacunary polynomials. It is clear that the union of s disjoint Baer subplanes in $\mathrm{PG}(2, q)$, where q is a square, is an s-fold blocking set. A line intersects this set in either s or $\sqrt{q} + s$ points. The result stated above means that an s-fold blocking set of size $s(q+1)+c$, where c is a constant, necessarily contains the union of s disjoint Baer subplanes if s and c are small enough ($s \leq q^{1/6}$).
In this section we show that this bound is indeed quite good. We construct s-fold blocking sets of size $s(q^4 + q^2 + 1)$ in $\mathrm{PG}(2, q^4)$, with $s = q + 1$, which are not the union of s disjoint Baer subplanes by constructing a scattered space of dimension 5 with respect to a Desarguesian 3-spread in $\mathrm{PG}(11, q)$. Because the constructed blocking set arises from a scattered space it follows from Theorem 2.6.2 that it is not the union of disjoint Baer subplanes. However, in the next paragraph we prove this again in this special case. We give two construction methods for a maximum scattered space of dimension 5 with respect to a Desarguesian 3-spread in $\mathrm{PG}(11, q)$. The first one shows the use of polynomials in finite geometry, the second one is using the representation of a Desarguesian spread in the tensor product, developped in section 1.6.

A construction using polynomials

Let $\mathcal{S}$ be a t-spread in $\mathrm{V}(3t, q)$. If W is a subspace of $\mathrm{V}(3t, q)$, then we define

$$\tilde{W} = \bigcup_{P:(P\in S)\wedge(P\cap W\neq\{0\})} \{v \mid v \in P\}.$$

So in fact, $\tilde{W}$ is the union of the vectors of the spread elements corresponding to the points of $B(W)$. In the following we will use representations of projective spaces used in [4] and [9].

The points of $\mathrm{PG}(2, q)$ are the 1-dimensional subspaces of $\mathrm{GF}(q^3)$, considered as a 3-dimensional vector space over $\mathrm{GF}(q)$. Such a subspace has an equation that is $\mathrm{GF}(q)$-linear of the form $P' = 0$, with

$$P' := x^q - \gamma x,$$

where $\gamma \in \mathrm{GF}(q^3)$. So a point of $\mathrm{PG}(2, q)$ is in fact a set $\{x \in \mathrm{GF}(q^3) \mid x^q - \gamma x = 0\}$. Since elements of this set are also zeros of

$$-P'^{q^2} + (x^{q^3} - x) - \gamma^{q^2} P'^q - \gamma^{q^2+q} P' = (\gamma^{q^2+q+1} - 1)x$$

and this is an equation of degree ≤ 1, we necessarily have that $\gamma^{q^2+q+1} = 1$. So points of $\mathrm{PG}(2, q)$ can be represented by polynomials of the form $x^q - \gamma x$ over $\mathrm{GF}(q^3)$, where $\gamma \in \mathrm{GF}(q^3)$ and $\gamma^{q^2+q+1} = 1$. Actually this is just a special case of the representation of $\mathrm{PG}(n, q)$ in $\mathrm{GF}(q^{n+1})$, where, by analogous arguments, points can be represented by polynomials of the form $x^q - \gamma x$ over $\mathrm{GF}(q^{n+1})$, with $\gamma \in \mathrm{GF}(q^{n+1})$ and $\gamma^{q^n + q^{n-1} + \ldots + 1} = 1$.

Now consider $\mathrm{PG}(3, q)$. Points are represented by a polynomial of the form $x^q - \gamma x$ over $\mathrm{GF}(q^4)$, with $\gamma \in \mathrm{GF}(q^4)$ and $\gamma^{q^3+q^2+q+1} = 1$. A line in $\mathrm{PG}(3, q)$ is a 2-dimensional linear subspace of $\mathrm{GF}(q^4)$ (or $\mathrm{GF}(q)^4$), which has a polynomial equation of degree q^2. Since this equation has to be $\mathrm{GF}(q)$-linear, it is of the form $W' = 0$, with

$$W' := x^{q^2} + \alpha x^q + \beta x,$$

where $\alpha, \beta \in \mathrm{GF}(q^4)$. So a line of $\mathrm{PG}(3, q)$ is in fact a set $\{x \in \mathrm{GF}(q^4) \mid x^{q^2} + \alpha x^q + \beta x = 0\}$. Since elements of this set are also zeros of

$$\begin{aligned} &W'^{q^2} - (x^{q^4} - x) - \alpha^{q^2} W'^q - (\beta^{q^2} - \alpha^{q^2+q}) W' \\ &= (-\alpha^{q^2} \beta^q - \alpha \beta^{q^2} + \alpha^{q^2+q+1}) x^q + (\alpha^{q^2+q} \beta - \beta^{q^2+1} + 1) x \end{aligned}$$

and this is an equation of degree $\leq q$, both coefficients on the right-hand side must be identically zero. Manipulating these coefficients we get the conditions $\beta^{q^3+q^2+q+1} = 1$ and $\alpha^{q+1} = \beta^q - \beta^{q^2+q+1}$. Again this is just a special case of the representation of $\mathrm{PG}(n, q)$ in $\mathrm{GF}(q^{n+1})$, where a k-dimensional subspace can be represented by a polynomial of the form

$$x^{q^{k+1}} + \alpha_1 x^{q^k} + \alpha_2 x^{q^{k-1}} + \ldots + \alpha_k x,$$

for some $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathrm{GF}(q^{n+1})$. For a survey on the use of polynomials of this type in finite geometries, see [4].

Let

$$W' := x^{q^6} + \alpha x^{q^3} + \beta x$$

and

$$P' := x^{q^4} - \gamma x,$$

with $\alpha, \beta, \gamma \in \mathrm{GF}(q^{12})$, $\gamma^{q^8+q^4+1} = 1$, $\beta^{q^9+q^6+q^3+1} = 1$ and $\alpha^{q^3+1} = \beta^{q^3} - \beta^{q^6+q^3+1}$. It is clear that $W = \{x \in \mathrm{GF}(q^{12}) \| W' = 0\}$ is a 6-dimensional subspace of $\mathrm{V}(12, q)$ and the set $P = \{x \in \mathrm{GF}(q^{12}) \| P' = 0\}$ is a 4-dimensional subspace of $\mathrm{V}(12, q)$.

Theorem 2.7.9 ([7])
The set $B(W)$ is a $(q+1)$-fold blocking set of size $(q+1)(q^4+q^2+1)$ in $\mathrm{PG}(2, q^4)$ and is not the union of $q+1$ disjoint Baer subplanes.

Proof. First we show that the dimension of the intersection of the subspaces W and P in $\mathrm{V}(12, q)$ is less than or equal to one. Solutions of both $W' = 0$ and $P' = 0$ are also solutions of

$$\alpha^q \beta^{q^2}(\gamma^{q^3}(W' - P'^{q^2}) - \alpha((W' - P'^{q^2})^q - \alpha^q P'))$$

$$-\gamma^{q^3+q^2}(((W'-P'^{q^2})^q)-\alpha^q P')\gamma^{q^4}-(\gamma^{q^3}(W'-P'^{q^2})-\alpha((W'-P'^{q^2})^q-\alpha^q P'))^q) = 0.$$

This is

$$(-\beta^{(q^2+q)}\alpha^{(q+1)} - \gamma^{(q^3+q^2+q)}\alpha^{(q^2+q)})x^q$$
$$+(-\gamma\beta^{q^2}\alpha^{(2q+1)} + \gamma^{q^3}\beta^{(q^2+1)}\alpha^q - \gamma^{(q^4+q^3+q^2+1)}\alpha^q)x = 0,$$

which is a equation of degree q in x. If the coefficients are not identically zero, then this equation will have at most q solutions. This means that the 6- dimensional subspace W intersects every spread element P in at most one dimension. So we have to prove that there exist $\alpha, \beta \in \mathrm{GF}(q^{12})$, for which these coefficients are not identically zero.
Suppose

$$-\beta^{(q^2+q)}\alpha^{(q+1)} - \gamma^{(q^3+q^2+q)}\alpha^{(q^2+q)} = 0 \tag{2.2}$$

and

$$-\gamma\beta^{q^2}\alpha^{(2q+1)} + \gamma^{q^3}\beta^{(q^2+1)}\alpha^q - \gamma^{(q^4+q^3+q^2+1)}\alpha^q = 0. \tag{2.3}$$

Equation (2.2) implies that $\gamma^{q^3+q^2+q} = -\beta^{q^2+q}\alpha^{1-q^2}$, assuming $\alpha \neq 0$. Substitution in (2.3) gives us

$$-\alpha^{q+1} + \alpha^{q(q^{10}-1)(q-1)}\beta^{q^2} + \alpha^{q-q^3}\beta^{q^3} = 0$$

or

$$-\alpha^{q^3+1} + \beta^{q^3} + \alpha^{q^{12}-q^{11}+q^3-q^2}\beta^{q^2} = 0.$$

Since $\alpha^{q^3+1} = \beta^{q^3} - \beta^{q^6+q^3+1}$, this is equivalent with

$$\beta^{q^7+q^4-q^3+q} = -\alpha^{q^4-q^3+q-1}$$

or again using $\alpha^{q^3+1} = \beta^{q^3} - \beta^{q^6+q^3+1}$ that

$$\beta^{q^7+q^4-q^3+q} = -(\beta^{q^3+1} - \beta^{q^6+q^3+1})^{q-1}. \tag{2.4}$$

This results in an equation of degree less than $q^7 + q^4$. So there are less than $q^7 + q^4$ possibilities for $\beta \in \mathrm{GF}(q^{12})$ such that both coefficients are zero. We can conclude that there exist $\alpha, \beta \in \mathrm{GF}(q^{12})$, for which these coefficients are not identically zero; namely where $\alpha \neq 0$ and β does not satisfy (2.4).
Let m_i denote the number of lines of $\mathrm{PG}(2, q^4)$, which intersect $B(W)$ in i points. Since a line induces a $2t$-dimensional subspace in $\mathrm{V}(12, q)$, it is obvious that $m_i = 0$, for all $i \notin \{q+1, q^2+q+1, q^3+q^2+q+1, q^4+q^3+q^2+q+1, q^5+q^4+q^3+q^2+q+1\}$. If one of the last two intersection numbers occurs, this means that there is a line, seen in $\mathrm{V}(12, q)$ as a 8-dimensional subspace, having a 5 or 6-dimensional intersection with W. In both cases this implies that there is an element of the Desarguesian spread S intersecting W in more than one dimension, which is impossible. So we have that $m_i = 0$, for all $i \notin \{q+1, q^2+q+1, q^3+q^2+q+1\}$. Let us put $l_2 = m_{q+1}$, $l_3 = m_{q^2+q+1}$ and $l_4 = m_{q^3+q^2+q+1}$. Then by counting lines, point-line pairs and point-point-line triples we obtain a set of equations from which we can solve l_2, l_3 and l_4 and these imply $l_2 = p^8 - p^5 - p^3 - p^2 - p$, $l_3 = p^5 + p^4 + p^3 + p^2 + p + 1$ and $l_4 = 0$. This implies that the 8-dimensional subspace corresponding to a line of $\mathrm{PG}(2, q^4)$, intersects W in a 2 or 3-dimensional subspace of $\mathrm{V}(12, q)$.
Suppose now that the $(q+1)$-fold blocking set $B(W)$ is the union of $q+1$ disjoint Baer subplanes of $\mathrm{PG}(2, q^4)$. Let $B(\mathcal{B})$ be one of the Baer sublines of these Baer subplanes and let L be the line of $\mathrm{PG}(2, q^4)$ containing $B(\mathcal{B})$. Then the 8-dimensional subspace induced by L will intersect W in a 3-dimensional subspace D and $B(\mathcal{B})$ induces a 4-dimensional subspace $\mathcal{B}$ of $\mathrm{V}(12, q)$ contained in the 8-dimensional subspace corresponding to L, which intersect every element of the spread S in a zero or two-dimensional subspace of $\mathrm{V}(12, q)$. (See Bose, Freeman and Glynn [21, Section 3] for a representation of a Baer subplane in $\mathrm{PG}(5, q)$, which is analogous to this.) We will prove that $\tilde{\mathcal{B}}$ cannot be contained in $\tilde{D}$. First we observe that $\mathcal{B}$ is in fact a 2-dimensional subspace over $\mathrm{GF}(q^2)$, so $\mathcal{B} = \{\alpha u + \beta v \parallel \alpha, \beta \in \mathrm{GF}(q^2)\}$; while D is a 3-dimensional subspace over $\mathrm{GF}(q)$, so $D = \{\lambda w + \mu x + \nu y \parallel \lambda, \mu, \nu \in \mathrm{GF}(q)\}$. From this it follows that $\tilde{\mathcal{B}} = \{a(\alpha u + \beta v) \parallel \alpha, \beta \in \mathrm{GF}(q^2), a \in \mathrm{GF}(q^4)\}$ and $\tilde{D} = \{\ b(\lambda w + \mu x + \nu y) \parallel \lambda, \mu, \nu \in \mathrm{GF}(q), b \in \mathrm{GF}(q^4)\}$. Now observe that $\langle B(u), B(v)\rangle$ over $\mathrm{GF}(q^4)$ is in fact the line L. So we can write w, x and y as a linear combination of u and v over $\mathrm{GF}(q^4)$. Without loss of generality, we can write

$$\begin{aligned} w &= c_1 u \\ x &= c_2 v \\ y &= c_3 u + c_4 v, \end{aligned}$$

with $c_1, c_2, c_3, c_4 \in \mathrm{GF}(q^4)$. But if $\tilde{\mathcal{B}}$ is contained in $\tilde{D}$, then for all $a \in \mathrm{GF}(q^4)$

and $\alpha, \beta \in \mathrm{GF}(q^2)$ there exist $b \in \mathrm{GF}(q^4)$ and $\lambda, \mu, \nu \in \mathrm{GF}(q)$ such that

$$\begin{cases} a\alpha &= b(\lambda c_1 + \nu c_3) \\ a\beta &= b(\mu c_2 + \nu c_4), \end{cases}$$

which results in the equation

$$\frac{\lambda c_1 + \nu c_3}{\mu c_2 + \nu c_4} = \frac{\alpha}{\beta} \in \mathrm{GF}(q^2) \cup \{\infty\}.$$

Let f be the map

$$f: \ \mathrm{GF}(q) \times \mathrm{GF}(q) \times \mathrm{GF}(q) \to \mathrm{GF}(q^4) \cup \{\infty\}$$

$$f(\lambda, \mu, \nu) = \frac{\lambda c_1 + \nu c_3}{\mu c_2 + \nu c_4}.$$

Then the image of f, $\Im(f)$, must contain $\mathrm{GF}(q^2)$. We remark that if $\Im(f) = \mathrm{GF}(q^2) \cup \{\infty\}$, then $\tilde{D}$ must be contained in $\tilde{\mathcal{B}}$, which is of course impossible. But if $f(\lambda, \mu, \nu) \in \mathrm{GF}(q^2)$, then

$$\left(\frac{\lambda c_1 + \nu c_3}{\mu c_2 + \nu c_4}\right)^{q^2} = \frac{\lambda c_1 + \nu c_3}{\mu c_2 + \nu c_4},$$

which gives us the equation

$$(\lambda c_1 + \nu c_3)^{q^2}(\mu c_2 + \nu c_4) - (\mu c_2 + \nu c_4)^{q^2}(\lambda c_1 + \nu c_3) = 0.$$

Since $\lambda, \mu, \nu \in \mathrm{GF}(q)$, this equation results in an quadratic equation in λ, μ and ν. Triples $(\lambda, \mu, \nu) \in \mathrm{GF}(q)^3$ can only give different values for f if they do not belong to the same 1-dimensional subspace of $\mathrm{GF}(q)^3$, i.e., if they represent different points in $\mathrm{PG}(2, q)$. So the above equation will have at most $2q + 1$ different solutions, namely the points of a degenerate quadric in $\mathrm{PG}(2, q)$. If $q > 2$ then $2q + 1 < q^2 + 1$ and if $q = 2$ it can be verified that if $\mathrm{GF}(4) \subset \Im(f)$, then $\Im(f) = \mathrm{GF}(4) \cup \{\infty\}$, a contradiction. ■

A construction using tensor products

In this section we use the terminology introduced in Section 1.6. Let $\{e_1, \ldots, e_r\}$ be a basis of $\mathrm{GF}(q^r)$ and $\{f_1, \ldots, f_t\}$ a basis of $\mathrm{GF}(q^t)$. If $v \in \mathrm{GF}(q^r) \bigotimes \mathrm{GF}(q^t)$, then we can define two subspaces related with v, namely $S_r(v) = \{\beta v \parallel \beta \in \mathrm{GF}(q^r)\}$ and $S_t(v) = \{v\alpha \parallel \alpha \in \mathrm{GF}(q^t)\}$.

Theorem 2.7.10 *The subspace*

$$W = \langle S_3(e_1 \otimes f_1 + e_2 \otimes f_2), S_3(e_3 \otimes f_3)\rangle$$

of $\mathrm{GF}(q^3) \bigotimes \mathrm{GF}(q^4)$, *is scattered with respect to the spread*

$$S = \{S_4(v) \mid v \in \mathrm{GF}(q^3) \bigotimes \mathrm{GF}(q^4)\}.$$

Proof. If w is vector of W, then w can be written as

$$e_1 \otimes u_1 + e_2 \otimes u_2 + e_3 \otimes u_3,$$

with $\langle u_1, u_2, u_3 \rangle \subseteq \langle f_1, f_2, f_3 \rangle$. We will prove that for each vector w in W, it is impossible to find an $\alpha \in \mathrm{GF}(q^4) \setminus \mathrm{GF}(q)$, such that $w\alpha \in W$. Suppose the rank of $\langle u_1, u_2, u_3 \rangle$ is 3. Then $\langle u_1, u_2, u_3 \rangle = \langle f_1, f_2, f_3 \rangle$ and the existence of an $\alpha \in \mathrm{GF}(q^4)$, such that $w\alpha \in W$ implies that $\langle \alpha u_1, \alpha u_2, \alpha u_3 \rangle \subseteq \langle u_1, u_2, u_3 \rangle$. Using Lemma 1.6.3 we get that $\alpha \in \mathrm{GF}(q)$. If the rank of $\langle u_1, u_2, u_3 \rangle$ is 1 then w is a pure tensor. Since $w \in W$, there exist $\beta, \gamma \in \mathrm{GF}(q^3)$, such that

$$w = \beta e_1 \otimes f_1 + \beta e_2 \otimes f_2 + \gamma e_3 \otimes f_3.$$

If $\beta \neq 0$, then $\beta^{-1} w$ is a pure tensor, since w is a pure tensor, and using Lemma 1.6.2 we get a contradiction since the rank of $\langle e_1, e_2, \beta^{-1}\gamma e_3 \rangle$ is at least 2. Thus $\beta = 0$ and $w \in S_3(e_3 \otimes f_3)$. If w is a pure tensor, then clearly $w\alpha$ is also a pure tensor. So $w\alpha \in S_3(e_3 \otimes f_3)$. But $w\alpha = \gamma e_3 \otimes \alpha f_3 \in S_3(e_3 \otimes f_3)$ implies that $\alpha \in \mathrm{GF}(q)$. Suppose that the rank of $\langle u_1, u_2, u_3 \rangle$ is 2. Then w is the sum of two pure tensors. Since $w \in W$, there exist $\beta, \gamma \in \mathrm{GF}(q^3)$, such that

$$w = \beta e_1 \otimes f_1 + \beta e_2 \otimes f_2 + \gamma e_3 \otimes f_3.$$

If $\beta = 0$, then w is a pure tensor and the rank of $\langle u_1, u_2, u_3 \rangle$ is one. So $\beta \neq 0$, and we can write

$$\beta^{-1} w = e_1 \otimes f_1 + e_2 \otimes f_2 + \beta^{-1}\gamma e_3 \otimes f_3.$$

Using Lemma 1.6.2 we have that $\mathrm{rk}\langle e_1, e_2, \beta^{-1}\gamma e_3 \rangle = 2$. So there exist $\lambda, \mu \in \mathrm{GF}(q)$ such that $\beta^{-1}\gamma e_3 = \lambda e_1 + \mu e_2$. Then we can write $\beta^{-1} w$ as

$$\beta^{-1} w = e_1 \otimes (f_1 + \lambda f_3) + e_2 \otimes (f_2 + \mu f_3). \tag{2.5}$$

Suppose there exist an $\alpha \in \mathrm{GF}(q^4)$ and $\delta, \varepsilon \in \mathrm{GF}(q^3)$, such that

$$w\alpha = \delta e_1 \otimes f_1 + \delta e_2 \otimes f_2 + \varepsilon e_3 \otimes f_3.$$

If $\delta = 0$, then $w\alpha$ is a pure tensor and this implies that w is a pure tensor. So $\delta \neq 0$ and we can write

$$\delta^{-1} w\alpha = e_1 \otimes f_1 + e_2 \otimes f_2 + \delta^{-1}\varepsilon e_3 \otimes f_3.$$

Since w is the sum of two pure tensors, $w\alpha$ can also be written as the sum of two tensors and Lemma 1.6.2 implies that $\mathrm{rk}(\langle e_1, e_2, \delta^{-1}\varepsilon e_3 \rangle) \leq 2$. So there exist $\nu, \omega \in \mathrm{GF}(q)$, such that $\delta^{-1}\varepsilon e_3 = \nu e_1 + \omega e_2$. So we can write $\delta^{-1} w\alpha$ as

$$\delta^{-1} w\alpha = e_1 \otimes (f_1 + \nu f_3) + e_2 \otimes (f_2 + \omega f_3). \tag{2.6}$$

Combining (2.5) and (2.6) we get

$$\begin{aligned}\delta\beta^{-1}\delta^{-1}w\alpha &= \delta\beta^{-1}e_1 \otimes (f_1+\nu f_3) + \delta\beta^{-1}e_2 \otimes (f_2+\omega f_3)\\ &= e_1 \otimes \alpha(f_1+\lambda f_3) + e_2 \otimes \alpha(f_2+\mu f_3)\end{aligned}$$

from which follows that $\langle \delta\beta^{-1}e_1, \delta\beta^{-1}e_2\rangle \subseteq \langle e_1, e_2\rangle$. Using Lemma 1.6.3 this implies that $\delta\beta^{-1} \in \mathrm{GF}(q)$. So we get

$$\begin{aligned}& e_1 \otimes (f_1+\nu f_3) + e_2 \otimes (f_2+\omega f_3)\\ = \;& e_1 \otimes \tfrac{\alpha}{\delta\beta^{-1}}(f_1+\lambda f_3) + e_2 \otimes \tfrac{\alpha}{\delta\beta^{-1}}(f_2+\mu f_3).\end{aligned}$$

This implies that $\frac{\alpha}{\delta\beta^{-1}}(f_1+\lambda f_3) = (f_1+\nu f_3)$ and $\frac{\alpha}{\delta\beta^{-1}}(f_2+\mu f_3) = (f_2+\omega f_3)$. Elimination of $\frac{\alpha}{\delta\beta^{-1}}$, gives

$$\frac{f_1+\nu f_3}{f_1+\lambda f_3} = \frac{f_2+\omega f_3}{f_2+\mu f_3}.$$

Without loss of generality we can put $f_3 = 1$. Eventually we get that

$$\omega f_1 + \lambda f_2 + \lambda\omega = \mu f_1 + \nu f_2 + \mu\nu.$$

Since $\{f_1, f_2, f_3, f_4\}$ forms a basis for $\mathrm{GF}(q^4)$, this implies that $\lambda = \nu$ and $\omega = \mu$. We have proved that $\alpha \in \mathrm{GF}(q)$. This concludes the proof. ∎

2.8 Hyperovals of translation planes

In this section we treat the equivalence of translation hyperovals of a translation plane and scattered $(t-1)$-dimensional spaces with respect to a $(t-1)$-spread in $\mathrm{PG}(2t-1,2)$. First we show that with every $(t-1)$-dimensional of $\mathrm{PG}(2t-1,2)$ which is scattered with respect to a $(t-1)$-spread there corresponds a translation hyperoval of a translation plane. For the converse we refer to [40], and only give an outline of the construction.

Let W be a scattered $(t-1)$-space with respect to a $(t-1)$-spread $\mathcal{S}$ of $\mathrm{PG}(2t-1,2)$. Note that there are 2^t+1 spread elements, 2^t-1 of which intersect W. Now we apply the André-Bruck-Bose construction by embedding $\mathrm{PG}(2t-1,2)$ in $\mathrm{PG}(2t,2)$ as a hyperplane (see Chapter 1). In this way we obtain a translation plane π of order 2^t. Now consider a t-dimensional space T which intersects $\mathrm{PG}(2t-1,2)$ in W. The claim is that the set $\mathcal{H}$ consisting of the affine points contained in T together with the points corresponding with the two spread elements not intersected by T form a translation hyperoval of π. To prove this, we consider all types of lines of the translation plane π. First of all it is clear that the line of π corresponding with the hyperplane $\mathrm{PG}(2t-1,2)$

intersects $\mathcal{H}$ in two points, the points corresponding with the two spread elements which are skew from W. Next consider a line L corresponding with a t-dimensional subspace T intersecting the hyperplane in a spread element U. If U does not intersect W then this t-dimensional space intersects T in a point of $\mathrm{PG}(2t,2)\backslash\mathrm{PG}(2t-1,2)$. This point together with the point corresponding with U gives us two points of $\mathcal{H}$ on the line L. If U intersects W in a point P then a t-space on U either intersects T in a line M on P or just in P. In the first case the line L is a secant containing the two affine points of $\mathcal{H}$ on the line M different from P, in the second case L is an external line. Hence $\mathcal{H}$ is a hyperoval of the translation plane π. It immediatly follows that $\mathcal{H}$ is a translation hyperoval with the translations of the affine space induced on $\mathrm{PG}(2t,2)\backslash\mathrm{PG}(2t-1,2)$.

Conversely, consider a translation hyperoval $\mathcal{H}$ in a translation plane π of order 2^t with translation group G. Let $\mathcal{S}$ be the $(t-1)$-spread associated with π, see [32]. The elements of the spread correspond with the subgroups of G fixing every line of a parallel class. G acts regularly on two parallel classes of lines and has precisely two orbits on the other parallel classes of lines. This implies that G corresponds with a $(t-1)$-dimensional space of $\mathrm{PG}(2t-1,2)$ skew from 2 elements of $\mathcal{S}$ and intersecting every other element of $\mathcal{S}$ in a point, i.e., a scattered subspace of dimension $t-1$ with respect to $\mathcal{S}$.

It follows from Theorem 2.5.5 that if the spread is Desarguesian then such a scattered space of dimension $t-1$ always exists. This implies the existence of a translation hyperoval in $\mathrm{PG}(2,2^t)$. From Theorem 2.2.1 it follows that for a line spread in $\mathrm{PG}(3,2)$, respectively a plane spread in $\mathrm{PG}(5,2)$, there exists a scattered line, respectively a scattered plane. This implies the existence of a translation hyperoval in every translation plane of order 2^2, respectively 2^3. The existence of a non-Desarguesian plane of order 2^t $(t>3)$ that admits a translation hyperoval is still an open problem.

Chapter 3

Translation generalized quadrangles and eggs

3.1 Generalized quadrangles

The theory of generalized quadrangles can be considered as part of the theory of generalized polygons. Generalized quadrangles were introduced in 1959 by Tits in his celebrated work on triality [84].

A *generalized quadrangle of order* (s,t), $(GQ(s,t))$, $s \geq 1, t \geq 1$, is an incidence structure $(\mathcal{P}, \mathcal{L}, \mathrm{I})$ of points and lines with the property that any two points are incident with at most one common line, any two lines are incident with at most one common point, any line is incident with $s+1$ points, every point is incident with $t+1$ lines, and given an antiflag (P,l), there is a unique flag (Q,m), such that m is incident with P, and Q is incident with l. We say that s and t are the parameters of the GQ. If $s=t$ then we call this incidence structure a GQ of order s $(GQ(s))$. From a GQ of order (s,t) we get a GQ of order (t,s) by interchanging points and lines, called the (*point-line*) *dual* of the GQ of order (s,t). The standard reference for GQ's is *Finite Generalized Quadrangles* by Payne and Thas [60], published in 1984.

A *grid* is an incidence structure $(\mathcal{P}, \mathcal{L}, \mathrm{I})$ with $\mathcal{P} = \{P_{ij} \parallel i = 0, \ldots, s_1,\ j = 0, \ldots, s_2\}$, $s_1 > 0$, and $s_2 > 0$, $\mathcal{L} = \{l_0, l_1, \ldots, l_{s_1}, m_0, m_1, \ldots, m_{s_2}\}$, $P_{ij} \,\mathrm{I}\, l_k$ if and only if $i = k$, and $P_{ij} \,\mathrm{I}\, m_k$ if and only $j = k$. A grid for which all lines are incident with the same number of points $(s_1 = s_2)$, respectively a dual grid for which all points are incident with the same number of lines, is an example of a generalized quadrangle of order (s,t) with $t = 1$, respectively $s = 1$. Conversely, if a $GQ(s,t)$ has $t = 1$, respectively $s = 1$, then it is a grid, respectively a dual grid. These examples are called *trivial*.

Remark. If we consider a generalized quadrangle of order (s, t) with $s, t > 1$, then from the definition it follows that (i) there are no ordinary k-gons for $2 \leq k < 4$; (ii) any two vertices are contained in an ordinary quadrangle (4-gon); and (iii) there exists an ordinary pentagon (5-gon). Generalising these three properties, by replacing 4 by n, and 5 by $n + 1$, gives the definition for a generalized n-gon. For more on generalized polygons we refer to the book *Generalized Polygons* by Van Maldeghem [86].

The first known non-trivial examples of GQ's are all associated with classical groups and were first recognised as generalized quadrangles by Tits [84]. They are called *classical*. We give a brief description of these GQ's.

(i) Consider a non-degenerate quadric $Q(d, q)$ of Witt index 2, with $d \in \{3, 4, 5\}$, in the projective space $\mathrm{PG}(d, q)$, i.e., a hyperbolic quadric in $\mathrm{PG}(3, q)$, a parabolic quadric in $\mathrm{PG}(4, q)$ and an elliptic quadric in $\mathrm{PG}(5, q)$. Then the points on the quadric together with the lines on the quadric form a generalized quadrangle, which we denote by $Q(d, q)$.

(ii) Let $H(d, q^2)$ be a nonsingular Hermitian variety of the projective space $\mathrm{PG}(d, q^2)$, $d = 3$ or 4. Then the points of the variety together with the lines on the variety, form a generalized quadrangle, which we denote by $H(d, q^2)$.

(iii) The points of $\mathrm{PG}(3, q)$ together with the totally isotropic lines with respect to a symplectic polarity form a generalized quadrangle denoted by $W(q)$.

The earliest known non-trivial non-classical examples of GQ's were constructed by Tits and first appeared in Dembowski [32] in 1968. The construction of the incidence structure $(\mathcal{P}, \mathcal{L}, \mathrm{I})$ goes as follows. Let $d = 2$, respectively $d = 3$, and let $\mathcal{O}$ be an oval, respectively an ovoid, of $\mathrm{PG}(d, q)$. Consider $\mathrm{PG}(d, q)$ as a hyperplane of $\mathrm{PG}(d + 1, q)$. We define 3 types of points:

(i) the points of $\mathrm{PG}(d + 1, q) \setminus \mathrm{PG}(d, q)$;

(ii) the hyperplanes of $\mathrm{PG}(d + 1, q)$ intersecting $\mathrm{PG}(d, q)$ in a tangent space of $\mathcal{O}$;

(iii) a new symbol (∞).

We define two types of lines:

(a) the lines of $\mathrm{PG}(d+1,q)$ intersecting $\mathrm{PG}(d,q)$ in a point of $\mathcal{O}$;

(b) the points of $\mathcal{O}$.

This defines the set $\mathcal{P}$ of points and the set $\mathcal{L}$ of lines. The incidence relation I is defined as follows: a line of type (a) is incident with the point of type (ii) that contains it, and with the points of type (i) contained in it; a line of type (b) is incident with the points of type (ii) containing it, and with the point (∞). It is straightforward to prove that the incidence structure $(\mathcal{P},\mathcal{L},\mathrm{I})$ is a generalized quadrangle of order q if $d=2$ and of order (q,q^2) if $d=3$. We will give a proof of this in a more general setting in Section 3.3. These examples are denoted by $T_d(\mathcal{O})$, $d=2,3$, or just $T(\mathcal{O})$ if no confusion is possible.

Further non-trivial non-classical examples of GQ's were found by Ahrens and Szekeres [1] in 1969, by Hall [35], Jr., in 1971, and by Payne [56] in 1971. These examples have order $(q-1,q+1)$ and they yield the only known examples of generalized quadrangles where the parameters s and t, with $s>1$ and $t>1$, are not powers of the same prime. In 1981, Kantor [42] introduced a construction method for GQ's starting from a so-called *4-gonal family* consisting of a finite group with a set of subgroups satisfying certain conditions. Let G be a finite group of order s^2t, $s>1$, $t>1$. Let $J=\{A_i \parallel 0\le i\le t\}$ be a family of subgroups of G, each of order s. Assume that for each A_i there exists a subgroup A_i^* of G of order st, containing A_i. Put $J^*=\{A_i^* \parallel 0\le i\le t\}$. Define an incidence structure $(\mathcal{P},\mathcal{L},\mathrm{I})=S(G,J)$ as follows. We define three types of points:

(i) the elements of G;

(ii) the right cosets A_i^*g, $A_i^*\in J^*$, $g\in G$;

(iii) a new symbol (∞).

We define two types of lines:

(a) the right cosets A_ig, $A_i\in J$, $g\in G$;

(b) the symbols $[A_i]$, $A_i\in J$.

This defines the set of points $\mathcal{P}$ and the set of lines $\mathcal{L}$. The incidence relation I is defined as follows: a point g of type (i) is incident with each line A_ig, $A_i\in J$; a point A_i^*g of type (ii) is incident with $[A_i]$ and with each line A_ih contained in A_i^*g; the point (∞) is incident with each line $[A_i]$ of type (b).

Then Kantor [42] proved that $S(G, J)$ is a GQ of order (s, t) if

(K1): $A_iA_j \cap A_k = \{1\}$, for distinct i, j, k, and

(K2): $A_i^* \cap A_j = \{1\}$, for $i \neq j$.

If (K1) and (K2) are satisfied then J is called a *4-gonal family for G*.

A combination of results by Payne [57], [58] and Kantor [43], translates the conditions for a 4-gonal family for a specific group yielding a GQ of order (q^2, q), to conditions for a set of 2×2 matrices. A *q^n-clan* is a set $\{A_t \| t \in \mathrm{GF}(q^n)\}$ of q^n 2×2 matrices over $\mathrm{GF}(q^n)$, such that the difference of each two distinct matrices is anisotropic, i.e., $\alpha(A_t - A_s)\alpha^T = 0$ for $s \neq t$ implies $\alpha = (0, 0)$. A q^n-clan is *additive* if $A_t + A_s = A_{t+s}$. If

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

then A is anisotropic if and only if the polynomial $ax^2 + (b + c)x + d$ is an irreducible polynomial in x over $\mathrm{GF}(q^n)$. If q is odd, then A is anisotropic if and only if $(b + c)^2 - 4ad$ is a non-square in $\mathrm{GF}(q^n)$. If q is even, then A is anisotropic if and only if the polynomial $x^2 + x + ad(b + c)^{-1}$ is irreducible over $\mathrm{GF}(q)$, i.e. the element $ad(b + c)^{-1}$ has trace 1, see [37].

Let $\mathcal{C} = \{A_t \| t \in \mathrm{GF}(q^n)\}$ be a q^n-clan, put $K_t = A_t + A_t^T$, and define $g_t(\gamma) = \gamma A_t \gamma^T$ and $\gamma^{\delta_t} = \gamma K_t$ for $\gamma \in \mathrm{GF}(q^n)^2$. Let $G = \{(\alpha, c, \beta) \| \alpha, \beta \in \mathrm{GF}(q^n)^2, c \in \mathrm{GF}(q^n)\}$, and define a binary operation $*$ on G by:

$$(\alpha, c, \beta) * (\alpha', c', \beta') = (\alpha + \alpha', c + c' + \beta\alpha'^T, \beta + \beta').$$

This makes G into a group. Let J be the family of subgroups

$$A(t) = \{(\alpha, g_t(\alpha), \alpha^{\delta_t}) \| \alpha \in \mathrm{GF}(q^n)\},\ t \in \mathrm{GF}(q^n),$$

and

$$A(\infty) = \{(0, 0, \beta) \| \beta \in \mathrm{GF}(q^n)^2\}.$$

Let J^* be the family of subgroups

$$A^*(t) = \{(\alpha, c, \alpha^{\delta_t}) \| \alpha \in \mathrm{GF}(q^n)^2, c \in \mathrm{GF}(q^n)\},\ t \in \mathrm{GF}(q^n),$$

and

$$A^*(\infty) = \{(0, c, \beta) \| c \in \mathrm{GF}(q^n), \beta \in \mathrm{GF}(q^n)^2\}.$$

Then the following theorem is a combination of results by Payne and Kantor.

Theorem 3.1.1 (Payne [57], [58] and Kantor [43])
The set J is a 4-gonal family for G if and only if $\mathcal{C}$ is a q^n-clan.

A *flock of a quadratic cone in* PG$(3, q)$ is a partition of the points of the cone different from the vertex into q conics. The planes containing the conics of the flock are called the *planes of the flock*. The classical example of a flock is constructed by taking the set of planes on a fixed line disjoint from the cone. In this case the flock is called *linear*. In 1987 Thas [75], showed that the conditions for a q-clan are exactly the conditions for a set of q planes to define a flock of a quadratic cone in PG$(3, q)$; and hence that a flock of a quadratic cone gives rise to a GQ of order (q^2, q). The corresponding GQ is called a *flock quadrangle*. If the flock is linear then the corresponding flock quadrangle is isomorphic to $H(3, q^2)$, which is isomorphic to the point-line dual of $Q(5, q)$. Furthermore we have the following theorem.

Theorem 3.1.2 (Thas, [75])
If two flocks of a quadratic cone have more than $\frac{q-1}{2}$ conics in common then they are equal.

As early as 1976 Thas and Walker had discovered, independently, that with each flock of a quadratic cone there corresponds a translation plane of order q^2 and dimension at most two over its kernel, see [87]. Currently there are many examples of flock quadrangles known, and a classification seems unlikely in the foreseeable future. In this context it is worth mentioning the work of Thas, Herssens and De Clerck [81], of Penttila and Royle [63], and the recent work of Law and Penttila, [46], where many examples of flocks for q odd are found by extensive computer searches.

3.2 Translation generalized quadrangles

A collineation σ of a generalized quadrangle S is called an *elation about the point P* provided that either σ is the identity or it fixes each line incident with P and no point not collinear with P. If σ fixes every point collinear with P, we say that σ is a *symmetry with center P*. If the GQ S has a collineation group E which acts regular on the points not collinear with P while fixing every line incident with P, then S is called an *elation generalized quadrangle* (*EGQ*) *with base point P*. The group E is called the *elation group* of the EGQ. The classical GQ's and the GQ's arising from a 4-gonal family are EGQ's, and in particular all flock quadrangles are EGQ's. Suppose S is an EGQ of order (s, t) with elation group E and base point P. Let Q be a point of S, and suppose $\{l_i \parallel i = 0, \ldots, t\}$ is the set of lines incident with P. If Q is not collinear with P, then there exist points $R_0, \ldots, R_t$ and lines $m_0, \ldots, m_t$, such that R_i is the unique point on l_i collinear with Q and m_i is the unique line incident with Q and R_i. Define

$$E_i = \{g \in E \parallel m_i^g = m_i\},$$
$$E_i^* = \{g \in E \parallel R_i^g = R_i\},$$

for all $i \in \{0, \dots, t\}$. Then E_i has order s and E_i^* has order st.

Theorem 3.2.1 (Payne and Thas [60])
The set $J = \{E_i \parallel i = 0, \dots, t\}$ is a 4-gonal family.

In [33] Frohardt proved that a finite group of order s^2t, which yields a 4-gonal family, is a p-group if $s \leq t$. This implies that the examples of generalized quadrangles of order $(q-1, q+1)$ of Ahrens and Szekeres [1] , Hall, Jr. [35], and Payne [56], together with their point-line duals are not EGQ's.

A *translation generalized quadrangle* (*TGQ*) *with base point* P is an EGQ with base point P with an abelian elation group T. The group T is called the *translation group* of the TGQ. Let S be a TGQ of order (s, t) with translation group T. In the same way as we defined the subgroups E_i and E_i^* for an the elation group E of an EGQ we can define subgroups T_i and T_i^* for $i = 0, \dots, t$ of T. The *kernel* K of S is the set of endomorphisms g of T for which $T_i^g \subset T_i$, $i = 0, \dots, t$. In [60] it is proved that K is a field, T is elementary abelian, s and t must be powers of the same prime, and if $s < t$, then there is a prime power q and an odd integer a for which $s = q^a$ and $t = q^{a+1}$. In contrast with the number of examples of EGQ's, there are (up to isomorphism) only 4 known classes of examples of TGQ's. At the end of this chapter we will consider all these examples and give a uniform presentation of them.

3.3 Eggs

A *weak egg* $\mathcal{E}_{n,m}$ *of* $\mathrm{PG}(2n+m-1, q)$, is a set of $q^m + 1$ $(n-1)$-spaces of $\mathrm{PG}(2n+m-1, q)$ such that any three different elements of $\mathcal{E}_{n,m}$ span a $(3n-1)$-space. If each element E of $\mathcal{E}_{n,m}$ is contained in an $(n+m-1)$-dimensional subspace of $\mathrm{PG}(2n+m-1, q)$, T_E, which is skew from any element of $\mathcal{E}_{n,m}$ different from E, then $\mathcal{E}_{n,m}$ is called an *egg of* $\mathrm{PG}(2n+m-1, q)$. The space T_E is called the *tangent space* of $\mathcal{E}_{n,m}$ at E. The set of tangent spaces of an egg $\mathcal{E}_{n,m}$ is denoted by $T_{\mathcal{E}_{n,m}}$. If we project the egg elements from an egg element onto a $\mathrm{PG}(n+m-1, q)$ skew from that egg element, then we obtain q^m mutually skew $(n-1)$-spaces, i.e., a partial $(n-1)$-spread of $\mathrm{PG}(n+m-1, q)$. Consequently there are $\theta_{m-1}(q)$ points of $\mathrm{PG}(n+m-1, q)$ not contained in one of these partial spread elements. The tangent space of the egg element we projected from, intersects $\mathrm{PG}(n+m-1, q)$ in an $(m-1)$-space skew to the partial spread elements, and hence contains these remaining $\theta_{m-1}(q)$ points.

This shows that the tangent spaces of an egg are uniquely determined by the egg elements. On the other hand it is not clear whether every weak egg is contained in an egg. As will be clear from Theorem 3.3.4 later on, the cases $n = m$ and $2n = m$ will be important cases.

Remark. From now on an egg $\mathcal{E}_{n,m}$ of $\mathrm{PG}(2n + m - 1, q)$ will simply be denoted by $\mathcal{E}$, if no confusion is possible concerning the values of the integers n and m.

If n=m then a (weak) egg $\mathcal{E}$ of $\mathrm{PG}(3n-1, q)$ is called a (weak) *pseudo-oval* or a (weak) *generalized oval*. Every weak pseudo-oval can be extended to a pseudo-oval, i.e., the tangent spaces always exist. One can easily see this by projecting the pseudo-oval from an element onto a $\mathrm{PG}(2n - 1, q)$ skew to that element, similar to what we did before to show that the tangent spaces of an egg are uniquely determined by the egg elements. Now, the partial $(n - 1)$-spread can be extended to a spread, because it has deficiency 1 and such a partial $(n-1)$-spread of $\mathrm{PG}(2n-1, q)$ can be uniquely extended to a spread of $\mathrm{PG}(2n-1, q)$, see e.g. [25]. If $n = 1$ then a pseudo-oval is an oval of $\mathrm{PG}(2, q)$. Other examples are induced by ovals of $\mathrm{PG}(2, q^n)$, by seeing them over $\mathrm{GF}(q)$. In fact the only known examples of pseudo-ovals are ovals of $\mathrm{PG}(2, q^n)$, seen over $\mathrm{GF}(q)$. All pseudo-ovals of $\mathrm{PG}(3n-1, q)$, $q^n \leq 16$ have been classified, see Penttila [61].

If $2n = m$ then a (weak) egg $\mathcal{E}$ of $\mathrm{PG}(4n - 1, q)$ is called a (weak) *pseudo-ovoid* or a (weak) *generalized ovoid*. If $n = 1$ then a pseudo-ovoid is an ovoid of $\mathrm{PG}(3, q)$. An ovoid of $\mathrm{PG}(3, q^n)$ seen over $\mathrm{GF}(q)$ is an example of a pseudo-ovoid. In the case of pseudo-ovoids more examples are known, which will be described later. The existence of weak pseudo-ovoids, which can not be extended to a pseudo-ovoid, i.e., for which the tangent spaces do not exist, is an open problem.

All known examples of eggs are generalized ovals or generalized ovoids, see Section 3.8

Following Thas [76] we say that a (weak) egg $\mathcal{E}$ of $\mathrm{PG}(4n - 1, q)$ is *good at an element* $E \in \mathcal{E}$ if every $(3n - 1)$-space containing E and at least two other (weak) egg elements, contains exactly $q^n + 1$ (weak) egg elements. So an egg of $\mathrm{PG}(4n - 1, q)$ which is good at an element induces an egg of $\mathrm{PG}(3n - 1, q)$ in every $(3n - 1)$-space containing the good element and at least two other elements of the egg. We say that an egg $\mathcal{E}$ of $PG(4n - 1, q)$ is a *good egg* if there exists an element $E \in \mathcal{E}$ such that $\mathcal{E}$ is good at the element E, and E is called a *good element of* $\mathcal{E}$.

Remark. In 1974, Thas [74] defined the following geometrical objects in finite projective spaces. A $[k, n-1]$-arc ($k > 2$) in $\mathrm{PG}(3n-1, q)$ is a set of k $(n-1)$-dimensional subspaces such that every three of them span $\mathrm{PG}(3n-1, q)$. A $[k, n-1]$-cap ($k > 2$) in $\mathrm{PG}(4n-1, q)$ is a set of k $(n-1)$-dimensional subspaces satisfying the following conditions: (i) every three of these subspaces span a $(3n-1)$-dimensional subspace, and (ii) every four of these subspaces are either contained in a $(3n-1)$-dimensional subspace or they span $\mathrm{PG}(4n-1, q)$. With a $[k, n-1]$-arc there corresponds a k-arc of the projective plane over the total matrix algebra of the $(n \times n)$-matrices with elements in the finite field $\mathrm{GF}(q)$, and with a $[k, n-1]$-cap there corresponds a k-cap of the three-dimensional projective space over the total matrix algebra of the $(n \times n)$-matrices with elements in the finite field $\mathrm{GF}(q)$. In 1971, Thas [73] proved that for such a k-arc $k \leq q^n + 1$ if q is odd, and $k \leq q^n + 2$ if q is even, and that for such a k-cap $k \leq q^{2n} + 1$, except in the case where $q = 2$, $n = 1$, where there exists a 8-cap. A $[k, n-1]$-arc in $\mathrm{PG}(3n-1, q)$ with k maximal is called an $[n-1]$-*oval* of $\mathrm{PG}(3n-1, q)$. A $[k, n-1]$-cap in $\mathrm{PG}(4n-1, q)$ with k maximal is called an $[n-1]$-*ovaloid* of $\mathrm{PG}(4n-1, q)$. If we compare the definition of an $[n-1]$-ovaloid in $\mathrm{PG}(4n-1, q)$ with the definition of a weak egg of $\mathrm{PG}(4n-1, q)$ given above, we see that there is one extra condition in the definition of an $[n-1]$-ovaloid, namely that every four elements either span a $\mathrm{PG}(4n-1, q)$ or are contained in a $(3n-1)$-dimensional space; we call this condition $(*)$. It follows that an $[n-1]$-ovaloid is a weak egg of $\mathrm{PG}(4n-1, q)$ satisfying condition $(*)$. This makes a significant difference as shown by Thas in 1974, [74], where he proves the following two results. Firstly, every weak egg of $\mathrm{PG}(4n-1, q)$ satisfying condition $(*)$ is an egg of $\mathrm{PG}(4n-1, q)$ (excluding the exceptional case $q = 2, n = 1$), and secondly, every weak egg of $\mathrm{PG}(4n-1, q)$ satisfying condition $(*)$ is an ovoid of $\mathrm{PG}(3, q^n)$ seen over $\mathrm{GF}(q)$ (excluding the exceptional case $q = 2, n = 1$). In [60] the term $[n-1]$-ovaloid is no longer used and neither is the term eggs, although we find the same definition of an egg as given above, and such a structure is denoted by $O(n, m, q)$. To my knowledge, it was Payne [59] who introduced the term “Kantor’s bad eggs” in 1989, referring to the new generalized quadrangles constructed by Kantor [43] in 1986, although it is said that Kantor already used the term “badd eggs” on an international conference. However, no definition of an egg was given at this point. In 1995 Thas and Van Maldeghem [83] give the definition of $O(n, m, q)$ and they call such a structure a *generalized oval* or an $[n-1]$-*oval* if $n = m$, and a *generalized ovoid*, an $[n-1]$-*ovoid*, or an *egg* if $n \neq m$. In 1998 Lunardon and Thas [51] define an egg by the definition given above. Later the term pseudo-oval was introduced by Wild [88]. Here we use the term egg for the previous $O(n, m, q)$. We will also introduce pseudo-oval, generalized oval, pseudo-ovoid and generalized ovoid. Motivated by the examples we are of the opinion that these are good terms for these objects. We hope that these definition are clear and that they do not confuse the reader.

Following Thas [79] we call the examples of eggs which are ovals of $\mathrm{PG}(2, q^n)$ or ovoids of $\mathrm{PG}(3, q^n)$ seen over $\mathrm{GF}(q)$, *classical.*

Remark. In Thas [74] eggs which are ovals of $\mathrm{PG}(2, q^n)$ or ovoids of $\mathrm{PG}(3, q^n)$ seen over $\mathrm{GF}(q)$, are called *elementary* instead of classical.

Let $\mathcal{E}$ be an egg of $\mathrm{PG}(2n+m-1, q)$. We embed $\mathrm{PG}(2n+m-1, q)$ as a hyperplane π in a $\mathrm{PG}(2n+m, q)$ and construct the incidence structure $T(\mathcal{E}) = (\mathcal{P}, \mathcal{L}, \mathrm{I})$ as follows. Points, the elements of $\mathcal{P}$, are of three types:

(i) the points of $\mathrm{PG}(2n+m, q) \setminus \pi$;

(ii) the $(n+m)$-dimensional subspaces of $\mathrm{PG}(2n+m, q)$ which intersect π in a tangent space of the egg;

(iii) the symbol (∞).

Lines, the elements of $\mathcal{L}$, are of two types:

(a) the n-dimensional subspaces of $\mathrm{PG}(2n+m, q)$ which intersect π in an egg element;

(b) the egg elements.

The incidence relation I is defined as follows: a line of type (b) is incident with points of type (ii) which contain it and with the point (∞); a line of type (a) is incident with points of type (i) contained in it and with the point of type (ii) that contains it. Note that when $\mathcal{E}$ is an oval of $\mathrm{PG}(2, q)$ or an ovoid of $\mathrm{PG}(3, q)$,respectively, this construction coincides with the construction of Tits of $T_2(\mathcal{E})$ or $T_3(\mathcal{E})$, respectively.

Theorem 3.3.1 (8.7.1 of Payne and Thas [60])
The incidence structure $T(\mathcal{E})$ is a TGQ of order (q^n, q^m) with base point (∞). Conversely, every TGQ is isomorphic to $T(\mathcal{E})$ for some egg $\mathcal{E}$ of $\mathrm{PG}(2n+m-1, q)$.

Proof. We consider this as an exercise, to become familiar with the notation and terminology concerning eggs and TGQs. The proof that the incidence structure is a GQ of order (q^n, q^m) is left as an exercise to the reader in [60]. Let $\mathcal{E}$ be an egg of $\mathrm{PG}(2n+m-1, q)$, and consider the construction of the incidence structure $T(\mathcal{E})$. Straightforward counting arguments show that every

line is incident with q^n+1 points and every point is incident with q^m+1 lines. Two points of type (i) determine a line in $\mathrm{PG}(2n+m,q)$ which intersects the hyperplane $\mathrm{PG}(2n+m-1,q)$ in a point. If this point belongs to an egg element E then they are collinear; the unique line incident with them is the line of type (a) determined by the egg element E and the line determined by the two points. If this point does not belong to an egg element then these two points of type (i) are not collinear. A point of type (i) and a point of type (ii) are collinear if and only if the point of type (i) is contained in the point of type (ii). The unique line of $T(\mathcal{E})$ on these two points is the line determined by the point of type (i) and the egg element contained in the point of type (ii). Two points of type (ii) are collinear if they contain the same egg element; the unique line of $T(\mathcal{E})$ incident with these two points of type (ii) is the line of type (b) corresponding with the egg element. A point of type (i) is never collinear with the point (∞). Every point of type (ii) is collinear with the point (∞); the unique line of $T(\mathcal{E})$ incident with these two points is the line of type (b) corresponding with the egg element contained in the point of type (ii). We have shown that any two points lie on at most one line.
Two lines of type (b) intersect in the point (∞). Two lines of type (a) containing distinct egg elements intersect in at most one point of type (i). Two lines of type (a) containing the same egg element intersect in at most one point of type (ii). A line of type (a) and a line of type (b) intersect in a point of type (ii) if and only if the line of type (a) contains the egg element corresponding with the line of type (b); the point of type (ii) is completely determined by the line of type (a). We have shown that any two lines have at most one point in common.
Consider an antiflag consisting of a point P of type (i) and a line of type (a), which are denoted by $\langle E,Q\rangle$, $E\in\mathcal{E}$, $Q\in\mathrm{PG}(2n+m,q)\setminus\pi$. If $P\subset\langle T_E,Q\rangle$, then the line $\langle E,P\rangle$ of type (a) is the unique line incident with the point P of type (i) and the unique point $\langle T_E,Q\rangle$ of type (ii), incident with the line $\langle E,Q\rangle$ of type (a). Suppose P is not contained in $\langle T_E,Q\rangle$. Project $\langle E,Q\rangle$ onto $\mathrm{PG}(2n+m-1,q)$ from P. This gives an n-space containing the egg element E. From the definition of an egg it follows that two distinct $(2n-1)$-spaces spanned by E and distinct egg elements must intersect each other in exactly E. Counting the number of points contained in a $(2n-1)$-space spanned by E and another egg element we get

$$q^m\left(\frac{q^{2n}-q^n}{q-1}\right)$$

points. Together with the $\theta_{m+n-1}(q)$ points contained in T_E, these are all the points of $\mathrm{PG}(2n+m-1,q)$. Hence the projection of $\langle E,Q\rangle$ from P must intersect one of these $(2n-1)$-spaces spanned by E and a second egg element F. Then the line $\langle F,P\rangle$ of type (a) is the unique line incident with P which intersects the line $\langle E,Q\rangle$ in a point of type (i).

Consider an antiflag consisting of a point P of type (i) and a line E of type (b). Then the line $\langle E, P \rangle$ of type (a) is the unique line incident with P which intersects E in the unique point $\langle T_E, P \rangle$.
Consider an antiflag consisting of a point $\langle T_E, P \rangle$ of type (ii) and and a line $\langle F, Q \rangle$ of type (a) with $E \neq F$. These two spaces intersect in a point R. The line $\langle E, R \rangle$ of type (a) is the unique line incident with the point $\langle T_E, P \rangle$ of type (ii) . The point R of type (i) is the unique point incident with the line $\langle E, R \rangle$ and the line $\langle F, Q \rangle$.
Consider an antiflag consisting of a point $\langle T_E, P \rangle$ of type (ii) and a line F of type (b). The point (∞) is the unique point incident with the line F and with the line E of type (b).
Consider an antiflag consisting of the point (∞) and a line $\langle E, P \rangle$ of type (a). Then E is the unique line incident with (∞) intersecting the line $\langle E, P \rangle$ in the point $\langle T_E, P \rangle$ of type (ii).
We have shown that the incidence structure $T(\mathcal{E})$ is a GQ of order (q^n, q^m). The group of translations of the affine space $\mathrm{PG}(2n+m, q) \setminus \mathrm{PG}(2n+m-1, q)$ acts transitively on the points not collinear with (∞) and fixes each line on (∞). We may conclude that the GQ $T(\mathcal{E})$ is a TGQ with base point (∞).
Conversely suppose that S is a TGQ of order (s, t) with base point P and translation group T with kernel $\mathrm{GF}(q)$. Then by section 8.5 of [60] there exist integers n and m such that $s = q^n$ and $t = q^m$. Fix a point Q not collinear with P, and let $l_0, l_1, \ldots, l_t$ be the lines of S incident with P. For $i = 0, 1, \ldots, t$ let R_i be the point of l_i collinear with Q, and let m_i be the line incident with R_i and Q. Define $T_i = \{\tau \in T \parallel m_i^\tau = m_i\}$, i.e. the subgroup of T fixing the line m_i, and define $T_i^* = \{\tau \in T \parallel R_i^\tau = R_i\}$, i.e. the subgroup of T fixing the point R_i. Then T_i has order q^n and T_i^* has order q^m and T_i is a subgroup of T_i^*. Since T is elementary abelian, T can be seen as a vector space of rank $2n+m$ over $\mathrm{GF}(q)$, T_i as a subspace of rank n over $\mathrm{GF}(q)$, and T_i^* as a subspace of rank m over $\mathrm{GF}(q)$. It follows from section 8.2 of [60] that the corresponding projective spaces satisfy the conditions for an egg. ■

Corollary 3.3.2 (Payne and Thas [60])
The theory of TGQs is equivalent with the theory of eggs.

By the following theorem we know that isomorphic eggs give isomorphic TGQs and conversely.

Theorem 3.3.3 (L. Bader, G. Lunardon, I. Pinneri [2])
Let $\mathcal{E}_1$, $\mathcal{E}_2$ be two eggs of $\mathrm{PG}(2n+m-1, q)$. *Then there is an isomorphism from $T(\mathcal{E}_1)$ to $T(\mathcal{E}_2)$, which maps the point (∞) to the point (∞) if and only if there is a collineation of* $\mathrm{PG}(2n+m-1, q)$ *which maps $\mathcal{E}_1$ to $\mathcal{E}_2$.*

The next theorem gives strong restrictions on the parameters m and n of an egg and states a nice property about the tangent spaces. It is proved using the theory of TGQs.

Theorem 3.3.4 (8.7.2 of Payne and Thas [60])
If $\mathcal{E}$ is an egg of $\mathrm{PG}(2n+m-1,q)$*, then*

1. *$n = m$ or $n(a+1) = ma$ with a odd.*
2. *If q is even, then $n = m$ or $m = 2n$.*
3. *If $n \neq m$ (resp., $2n = m$), then each point of* $\mathrm{PG}(2n+m-1,q)$ *which is not contained in an egg element belongs to* 0 *or* $q^{m-n}+1$ *(resp., to exactly q^n+1) tangent spaces of $\mathcal{E}$.*
4. *If $n \neq m$ the q^m+1 tangent spaces of $\mathcal{E}$ form an egg $\mathcal{E}^D$ in the dual space of* $\mathrm{PG}(2n+m-1,q)$*, called the dual egg. So in addition to $T(\mathcal{E})$ there arises a TGQ $T(\mathcal{E}^D)$.*
5. *If $n \neq m$ (resp., $2n = m$), then each hyperplane of* $\mathrm{PG}(2n+m-1,q)$ *which does not contain a tangent space of $\mathcal{E}$ contains* 0 *or* $q^{m-n}+1$ *(resp., contains exactly q^n+1) egg elements.*

The TGQ $T(\mathcal{E}^D)$ corresponding with the dual egg $\mathcal{E}^D$ of $\mathcal{E}$ is called the *translation dual* of $T(\mathcal{E})$. We will sometimes refer to the dual of a GQ as the point-line dual, introduced in Section 3.1, to make clear it is not the translation dual. Note that for q is even the restrictions on the parameters are stronger than for q odd. The only known examples of eggs for q even are classical, see Section 3.8.

We have already seen that a 4-gonal family gives rise to a GQ. Moreover the corresponding GQ is an EGQ, and from every EGQ one can construct a 4-gonal family, Theorem 3.2.1. In [59] Payne studies the 4-gonal family associated with an EGQ whose point-line dual is a TGQ. Starting with a 4-gonal family corresponding with such an EGQ, S, he deduces the 4-gonal family for the TGQ, S^D. The following theorem states the connection in terms of additive q^n-clans and eggs and it is a corollary of the work done by Payne in [59] and Theorem 3.1.1. We remark that we could have stated a similar result in terms of 4-gonal families and eggs. For notational convenience we put $F = \mathrm{GF}(q^n)$. We represent the points of $\mathrm{PG}(4n-1,q)$ as 4-tuples over F, or sometimes by two elements of F and one element of F^2.

Theorem 3.3.5 ([44])
The set $\mathcal{C} = \{A_t \parallel t \in F\}$ of two by two matrices over F is an additive q^n-clan if and only if the set $\mathcal{E} = \{E(\gamma) \parallel \gamma \in F^2 \cup \{\infty\}\}$, with

$$E(\gamma) = \{\langle t, -g_t(\gamma), -\gamma^{\delta_t}\rangle \parallel t \in F\},\ \forall \gamma \in F^2,$$

$$E(\infty) = \{\langle 0, t, 0, 0\rangle \parallel t \in F\},$$

together with the set $T_{\mathcal{E}} = \{T_E(\gamma) \parallel \gamma \in F^2 \cup \{\infty\}\}$, *with*

$$T_E(\gamma) = \{\langle t, \beta\gamma^T + \gamma^{\delta_t}\gamma^T - g_t(\gamma), \beta\rangle \parallel t \in F,\ \beta \in F^2\},\ \forall\gamma \in F^2,$$

$$T_E(\infty) =\ \langle(0, t, \beta\rangle \parallel t \in F,\ \beta \in F^2\},$$

is an egg of $\mathrm{PG}(4n-1, q)$, *where* $g_t(\gamma) = \gamma A_t \gamma^T$ *and* $\gamma^{\delta_t} = \gamma(A_t + A_t^T)$.

If we are in the situation of the above theorem then, since $\mathcal{C}$ is additive, we can write A_t as

$$A_t = \sum_{i=0}^{n-1} \begin{bmatrix} a_i & b_i \\ 0 & c_i \end{bmatrix} t^{q^i},$$

for some $a_i, b_i, c_i \in F$. If an egg $\mathcal{E}$ can be written in this form then we denote the egg as $\mathcal{E}(\overline{a}, \overline{b}, \overline{c})$, where $\overline{a} = (a_0, \ldots, a_{n-1})$, $\overline{b} = (b_0, \ldots, b_{n-1})$, and $\overline{c} = (c_0, \ldots, c_{n-1})$. In this case we can deduce the explicit form of the dual egg in terms of $\overline{a}, \overline{b}, \overline{c}$. To do this we need the following lemma.

Lemma 3.3.6 *Let* tr *be the trace map from* F *to* $\mathrm{GF}(q)$, *and* $\alpha_i \in F$, $i = 0, \ldots, n-1$. *Then*

$$\mathrm{tr}(\sum_{i=0}^{n-1} \alpha_i t^{q^i}) = 0,$$

for all $t \in F$ *if and only if*

$$\sum_{i=0}^{n-1} \alpha_i^{q^{n-1-i}} = 0.$$

Proof. Since the trace function is additive and $\mathrm{tr}(x) = \mathrm{tr}(x^q)$, we get

$$\mathrm{tr}\left[\sum_{i=0}^{n-1} \alpha_i t^{q^i}\right] = \mathrm{tr}\left[\left(\sum_{i=0}^{n-1} \alpha_i^{q^{n-i-1}}\right) t^{q^{n-1}}\right].$$

Since $\mathrm{tr}(ax) = 0,\ \forall x \in F$ implies $a = 0$ the proof is complete. ■

Theorem 3.3.7 ([44])
The elements of the dual egg $\mathcal{E}^D(\overline{a}, \overline{b}, \overline{c})$ *of an egg* $\mathcal{E}(\overline{a}, \overline{b}, \overline{c})$ *are given by*

$$\tilde{E}(\gamma) = \{\langle -\tilde{g}_t(\gamma), t, -\gamma t\rangle \parallel t \in F\},\ \forall\gamma \in F^2,$$

$$\tilde{E}(\infty) = \{\langle t, 0, 0, 0\rangle \parallel t \in F\},$$

$$T_{\tilde{E}}(\gamma) = \{\langle \tilde{f}(\beta, \gamma) + \tilde{g}_t(\gamma), t, \beta\rangle \parallel t \in F,\ \beta \in F^2\},\ \forall\gamma \in F^2,$$

$$T_{\tilde{E}}(\infty) = \{\langle t, 0, \beta\ \rangle\parallel t \in F,\ \beta \in F^2\},$$

with

$$\tilde{g}_t(a,b) = \sum_{i=0}^{n-1}(a_i a^2 + b_i ab + c_i b^2)^{1/q^i} t^{1/q^i},$$

and

$$\tilde{f}((a,b),(c,d)) = \sum_{i=0}^{n-1}(2a_i ac + b_i(ad+bc) + 2c_i bd)^{1/q^i}.$$

Proof. To find $\tilde{E}(\gamma)$, respectively $T_{\tilde{E}}(\gamma)$, we calculate the vector space dual of $T_E(\gamma)$, respectively of $E(\gamma)$, in $\mathrm{V}(4n,q)$ with respect to the inner product

$$((x,y,z,w),(x',y',z',w')) \mapsto \mathrm{tr}(xx' + yy' + zz' + ww'),$$

where tr is the trace map from $F \to \mathrm{GF}(q)$. If (x,y,z,w) is in the vector space dual of $E^*(\gamma)$ then $\mathrm{tr}\left[xt + y(\beta\gamma^T + \gamma^{\delta_t}\gamma^T - g_t(\gamma)) + (z,w)\beta^T\right] = 0$, for all $t \in F$, for all $\beta \in F^2$. With $\gamma = (a,b)$ and $\beta = (c,d)$, this is

$$\mathrm{tr}\left[xt + y(ac + bd + \gamma^{\delta_t}\gamma^T - g_t(\gamma)) + zc + wd\right] = 0,$$

for all $c, d, t \in F$. For $t = 0$, this equation is satisfied if $w = -by$ and $z = -ay$. Substituting this back into the equation we get that $\mathrm{tr}\left[xt + y(\gamma^{\delta_t}\gamma^T - g_t(\gamma))\right] = 0$, for all $t \in F$. Using the formula for g_t and δ_t this is equivalent with

$$\mathrm{tr}\left[(x + y(a_0a^2 + b_0ab + c_0b^2))t + \sum_{i=1}^{n-1}(a_ia^2 + b_iab + c_ib^2)t^{q^i}\right] = 0,$$

for all $t \in F$, and using the above lemma, it follows that (x,y,z,w) is of the form

$$(-\sum_{i=0}^{n-1}(a_ia^2 + b_iab + c_ib^2)^{1/q^i}t^{1/q^i}, t, -at, -bt),$$

for some $t \in F$. This proves the form of the elements $\tilde{E}(\gamma)$ of the dual egg. The tangent spaces are obtained in the same way. ∎

For reasons that will become clear later, we will now check if the egg $\mathcal{E}^D$ satisfies the conditions in the definition of an egg.

(i) **Every three elements span a $(3n-1)$-space.**

Suppose E_1, E_2, E_3 are three distinct egg elements such that E_3 has a non-empty intersecion with $\langle E_1, E_2\rangle$. If one of these egg elements is the element $\tilde{E}(\infty)$, then this implies, supposing $E_1 = \tilde{E}(\infty)$, $E_2 = \tilde{E}(\beta)$, and $E_3 = \tilde{E}(\gamma)$, that there exist $r, s, t \in F^* = F\setminus\{0\}$ such that $(r, 0, (0,0)) + (-\tilde{g}_s(\beta), s, -\beta s) =$

$(-\tilde{g}_t(\gamma), t, -\gamma t)$. However it then easily follows that $s = t$, and hence $\gamma = \beta$, a contradiction. Now suppose that none of the egg elements E_1, E_2, E_3 is $\tilde{E}(\infty)$, then, supposing $E_1 = \tilde{E}(\gamma_1), E_2 = \tilde{E}(\gamma_2)$, and $E_3 = \tilde{E}(\gamma_3)$, there exist $t_1, t_2, t_3 \in F^*$ such that

$$(-\tilde{g}_{t_1}(\gamma_1), t_1, -\gamma_1 t_1) + (-\tilde{g}_{t_2}(\gamma_2), t_2, -\gamma_2 t_2) = (-\tilde{g}_{t_3}(\gamma_3), t_3, -\gamma_3 t_3).$$

It then follows from the second coordinate it follows that $t_1 + t_2 = t_3$. Put $\gamma_1 = (\alpha_1, \beta_1), \gamma_2 = (\alpha_2, \beta_2)$, with $\alpha_1, \alpha_2, \beta_1, \beta_2 \in F$. Then from the third coordinate it follows that

$$\gamma_3 = \left(\frac{t_1\alpha_1 + t_2\alpha_2}{t_1 + t_2}, \frac{t_1\beta_1 + t_2\beta_2}{t_1 + t_2} \right).$$

Note that $t_1 + t_2 \neq 0$ by assumption. It then follows from the first coordinate that

$$\tilde{g}_{t_1}(\alpha_1, \beta_1) + \tilde{g}_{t_2}(\alpha_2, \beta_2) = \tilde{g}_{t_1+t_2} \left(\frac{t_1\alpha_1 + t_2\alpha_2}{t_1 + t_2}, \frac{t_1\beta_1 + t_2\beta_2}{t_1 + t_2} \right). \quad (3.1)$$

We want to use the formula for $\tilde{g}$ but for convenience of notation we may re-index the coefficients a_i, b_i, c_i such that $\tilde{g}_t(a, b)$ becomes

$$\sum_{i=0}^{n-1} (a_i a^2 + b_i ab + c_i b^2)^{q^i} t^{q^i}.$$

Then the condition (3.1) becomes

$$\sum_{i=0}^{n-1} \left(a_i\alpha_1^2 t_1 + b_i\alpha_1\beta_1 t_1 + c_i\beta_1^2 t_1\right)^{q^i} + \sum_{i=0}^{n-1} \left(a_i\alpha_2^2 t_2 + b_i\alpha_2\beta_2 t_2 + c_i\beta_2^2 t_2\right)^{q^i}$$

$$= \sum_{i=0}^{n-1} \left[a_i \left(\frac{t_1\alpha_1 + t_2\alpha_2}{t_1 + t_2} \right)^2 (t_1 + t_2) \right.$$

$$+ b_i \left(\frac{t_1\beta_1 + t_2\beta_2}{t_1 + t_2} \right) \left(\frac{t_1\alpha_1 + t_2\alpha_2}{t_1 + t_2} \right) (t_1 + t_2)$$

$$\left. + \ c_i \left(\frac{t_1\beta_1 + t_2\beta_2}{t_1 + t_2} \right)^2 (t_1 + t_2) \right]^{q^i}.$$

Working out the right hand side of this equation we have

$$
\begin{aligned}
& \sum_{i=0}^{n-1} \left[a_i \left(\frac{\alpha_1^2 t_1^2 + \alpha_2^2 t_2^2 + 2\alpha_1\alpha_2 t_1 t_2}{t_1 + t_2} \right) \right. \\
& + b_i \left(\frac{\alpha_1\beta_1 t_1^2 + (\alpha_1\beta_2 + \alpha_2\beta_1) t_1 t_2 + \beta_1\beta_2 t_2^2}{t_1 + t_2} \right) \\
& \left. + c_i \left(\frac{\beta_1^2 t_1^2 + \beta_2^2 t_2^2 + 2\beta_1\beta_2 t_1 t_2}{t_1 + t_2} \right) \right]^{q^i} \\
= & \sum_{i=0}^{n-1} (t_1 + t_2)^{-q^i} \left[a_i(\alpha_1^2 t_1^2 + \alpha_2^2 t_2^2 + 2\alpha_1\alpha_2 t_1 t_2) \right. \\
& + b_i(\alpha_1\beta_1 t_1^2 + (\alpha_1\beta_2 + \alpha_2\beta_1) t_1 t_2 + \beta_1\beta_2 t_2^2) \\
& \left. + c_i(\beta_1^2 t_1^2 + \beta_2^2 t_2^2 + 2\beta_1\beta_2 t_1 t_2) \right]^{q^i} .
\end{aligned}
$$

Now we multiply both sides with $\prod_{j=0}^{n-1} (t_1 + t_2)^{q^j}$. We get

$$
\begin{aligned}
& \sum_{i=0}^{n-1} \prod_{j=0, i\neq j}^{n-1} (t_1 + t_2)^{q^j} \left[a_i(\alpha_1^2 t_1^2 + (\alpha_1^2 + \alpha_2^2) t_1 t_2 + \alpha_2^2 t_2^2) \right. \\
& + b_i(\alpha_1\beta_1 t_1^2 + (\alpha_1\beta_1 + \alpha_2\beta_2) t_1 t_2 + \alpha_2\beta_2 t_2^2) \\
& \left. + c_i(\beta_1^2 t_1^2 + (\beta_1^2 + \beta_2^2) t_1 t_2 + \beta_2^2 t_2^2) \right]^{q^i} \\
= & \sum_{i=0}^{n-1} \prod_{j=0, i\neq j}^{n-1} (t_1 + t_2)^{q^j} \left[a_i(\alpha_1^2 t_1^2 + \alpha_2^2 t_2^2 + 2\alpha_1\alpha_2 t_1 t_2) \right. \\
& + b_i(\alpha_1\beta_1 t_1^2 + (\alpha_1\beta_2 + \alpha_2\beta_1) t_1 t_2 + \beta_1\beta_2 t_2^2) \\
& \left. + c_i(\beta_1^2 t_1^2 + \beta_2^2 t_2^2 + 2\beta_1\beta_2 t_1 t_2) \right]^{q^i} .
\end{aligned}
$$

This equation is equivalent to

$$\begin{aligned}&\sum_{i=0}^{n-1}\prod_{j=0,i\neq j}^{n-1}(t_1+t_2)^{q^j}\left[(a_i(\alpha_1-\alpha_2)^2\right.\\&\left.+\,b_i(\alpha_1-\alpha_2)(\beta_1-\beta_2)+c_i(\beta_1-\beta_2)^2)t_1t_2\right]^{q^i}\\=\quad&0.\end{aligned}$$

Since $t_1+t_2\neq 0$ this is equivalent to

$$\tilde{g}_{\frac{t_1t_2}{t_1+t_2}}(\alpha_1-\alpha_2,\beta_1-\beta_2)=0.$$

So if we assume that there exist egg elements which do not satisfy the first condition then we get that there exist a $t\in F^*$ and a $\gamma\in F^2\setminus\{(0,0)\}$ such that $\tilde{g}_t(\gamma)=0$.

(ii) **The tangent space at an element $E\in\mathcal{E}^D$ is skew to the elements of $\mathcal{E}^D\setminus\{E\}$.**

Suppose the tangent space at an egg element E_1 intersects an egg element $E_2\neq E_1$. If one of these egg elements is $E(\infty)$, we immediately get a contradiction. If not then put $E_1=\tilde{E}(\gamma_1)$ and $E_2=\tilde{E}(\gamma_2)$ with $\gamma_1\neq\gamma_2\in F^2$. Then there exist elements $t_1,t_2\in F,\beta\in F^2$, such that

$$(\tilde{f}(\gamma_1,\beta)+\tilde{g}_{t_1}(\gamma_1),t_1,\beta)=(-\tilde{g}_{t_2}(\gamma_2),t_2,-\gamma_2t_2).$$

From the second and third coordinate it follows that $t_1=t_2$ and $\beta=-\gamma_2t_2$. With $t=t_1=t_2$, $\gamma_1=(\alpha_1,\beta_1)$, and $\gamma_2=(\alpha_2,\beta_2)$, $\alpha_1,\alpha_2,\beta_1,\beta_2\in F$, the first coordinate implies

$$\tilde{f}((\alpha_1,\beta_1),(-\alpha_2t,-\beta_2t))+\tilde{g}_t(\alpha_1,\beta_1)=-\tilde{g}_t(\alpha_2,\beta_2). \tag{3.2}$$

Again, for convenience of notation, we permute the indices of the coefficients a_i,b_i,c_i in the formulae for $\tilde{g}$ and $\tilde{f}$ such that we can write

$$\tilde{g}_t(a,b)=\sum_{i=0}^{n-1}(a_ia^2+b_iab+c_ib^2)^{q^i}t^{q^i},$$

and

$$\tilde{f}((a,b),(c,d))=\sum_{i=0}^{n-1}(2a_iac+b_i(ad+bc)+2c_ibd)^{q^i}.$$

Equation (3.2) becomes

$$\sum_{i=0}^{n-1}\left[-2a_i\alpha_1\alpha_2 t - b_i(\alpha_1\beta_2 t + \alpha_2\beta_1 t) - 2c_i\beta_1\beta_2 t + (a_i\alpha_1^2 + b_i\alpha_1\beta_1 + c_i\beta_1^2)t\right]^{q^i}$$

$$= -\sum_{i=0}^{n-1}\left[(a_i\alpha_2^2 + b_i\alpha_2\beta_2 + c_i\beta_2^2)t\right]^{q^i}.$$

This implies

$$\sum_{i=0}^{n-1}\left[a_i(\alpha_2-\alpha_1)^2 + b_i(\alpha_2-\alpha_1)(\beta_2-\beta_1) + c_i(\beta_2-\beta_1)^2\right]^{q^i} t^{q^i} = 0,$$

and hence $\tilde{g}_t(\alpha_2-\alpha_1,\beta_2-\beta_1) = 0$. So if we assume that there exists a tangent space and an egg element that do not satisfy the condition concerning the tangent spaces in the definition of an egg, then there exist $t \in F^*$ and $\gamma \in F^2\backslash\{(0,0)\}$ such that $\tilde{g}_t(\gamma) = 0$, which is the same condition as we obtained in the above from verifying that every three egg elements span a $(3n-1)$-space.

It follows that the only condition required for $\mathcal{E}^D$ to be an egg is that $\tilde{g}_t(a,b)$ implies $t = 0$ or $a = b = 0$. From the form of $\tilde{g}$ it follows that this is equivalent to the condition for the matrices

$$\tilde{A}_t = \sum_{i=0}^{n-1}\begin{bmatrix} a_i^{1/q^i} & b_i^{1/q^i} \\ 0 & c_i^{1/q^i}\end{bmatrix} t^{1/q^i},\ t \in F,$$

to form a q^n-clan. Hence we have the following theorem.

Theorem 3.3.8 *The set* $\tilde{C}_{q^n} = \{\tilde{A}_t \parallel t \in F\}$ *is a* q^n*-clan if and only if* $\mathcal{E}^D$*, as defined in Theorem 3.3.7, is an egg of* $\mathrm{PG}(4n-1,q)$*.*

The next theorem is a consequence of Theorem 3.3.5 and the above theorem. However, here we will give a direct proof of this result. Together with the above theorem we have then provided a proof for Theorem 3.3.5.

Theorem 3.3.9 *The following two conditions are equivalent.*

(1) $$\sum_{i=0}^{n-1}(a_i a^2 + b_i ab + c_i b^2)t^{q^i} = 0 \text{ implies } t = 0 \text{ or } a = b = 0.$$

(2) $$\sum_{i=0}^{n-1}(a_i a^2 + b_i ab + c_i b^2)^{1/q^i} t^{1/q^i} = 0 \text{ implies } t = 0 \text{ or } a = b = 0.$$

Proof. Suppose the equation

$$\sum_{i=0}^{n-1} \alpha_i t^{q^i} = 0,\ \alpha_i \in F \tag{3.3}$$

has q^{n-k} different solutions for t in F. The solutions form an $(n-k)$-dimensional subspace in $\mathrm{V}(n,q)$. Hence there are k independent hyperplanes of $\mathrm{V}(n,q)$, represented by the equations $\mathrm{tr}(a_i t) = 0$, $a_i \in F$, $i = 0, \ldots, n-1$, independent over $\mathrm{GF}(q)$, such that the solutions of the equation (3.3) are the same as the solutions of the equation

$$\sum_{i=0}^{k-1} \gamma_i \,\mathrm{tr}(a_i t) = 0,$$

where $\gamma_0, \ldots, \gamma_{k-1}$ are k elements of $\mathrm{GF}(q^n)$ independent over $\mathrm{GF}(q)$. (Here we use the representation explained in Section 2.7.3.) We show that there exist such γ_i and a_i, $(i = 0, \ldots, k-1)$, such that

$$\alpha_j = \sum_{i=0}^{k-1} \gamma_i a_i^{q^j},$$

for $j = 0, \ldots, k-1$. First we remark that $\langle \alpha_0, \ldots, \alpha_{n-1} \rangle$ has dimension k, since they satisfy $n-k$ independent relations. Assume $\alpha_0, \ldots, \alpha_{k-1}$ are independent. Then it suffices to solve the set of equations:

$$\begin{array}{lcl} \alpha_0 & = & \gamma_0 a_0 + \gamma_1 a_1 + \ldots + \gamma_{k-1} a_{k-1} \\ \alpha_1 & = & \gamma_0 a_0^q + \gamma_1 a_1^q + \ldots + \gamma_{k-1} a_{k-1}^q \\ \ldots & = & \ldots \\ \alpha_{k-1} & = & \gamma_0 a_0^{q^{k-1}} + \gamma_1 a_1^{q^{k-1}} + \ldots + \gamma_{k-1} a_{k-1}^{q^{k-1}}. \end{array}$$

The corresponding matrix has rank k since the hyperplanes are independent. It follows that there is a unique solution. Now suppose that $k = n$, then $\alpha_i^{1/q^i} = \gamma_0^{1/q^i} a_0 + \gamma_1^{1/q^i} a_1 + \ldots + \gamma_{n-1}^{1/q^i} a_{n-1}$, for all α_i, $i = 0, \ldots, n-1$. So $\sum_{i=0}^{n-1} \alpha_i^{1/q^i} t^{1/q^i} = a_0 \,\mathrm{tr}(\gamma_0 t) + \ldots + a_{n-1} \,\mathrm{tr}(\gamma_{n-1} t)$. Since both the γ_i's and the a_i's are independent it follows that

$$\sum_{i=0}^{n-1} \alpha_i^{1/q^i} t^{1/q^i} = 0 \tag{3.4}$$

implies $t = 0$. This proves that the equation (3.3) has only the trivial solution or is the zero-polynomial in t if and only if the equation (3.4) has only the trivial solution or is the zero-polynomial in t. ■

3.4 A model for eggs of $\mathrm{PG}(4n-1,q)$

Motivated by the previous section and in the spirit of the model for skew translation generalized quadrangles (STGQ) presented in [60], we present a model for a weak egg $\mathcal{E}$ of $\mathrm{PG}(4n-1,q)$. Put $F = \mathrm{GF}(q^n)$.
Let $E(\gamma) = \{\langle(t, -g_t(\gamma), -\gamma^{\delta_t})\rangle \parallel t \in F\}$, and $E(\infty) = \{\langle(0,t,0,0)\rangle \parallel t \in F\}$, with $g_t : F^2 \to F$, $\delta_t : F^2 \to F^2$. If $\mathcal{E}(g,\delta)$ is the set $\{E(\gamma) \parallel \gamma \in F^2 \cup \{\infty\}\}$, with $g : t \to g_t$, $\delta : t \to \delta_t$ then we have the following theorem.

Theorem 3.4.1 ([44])
The set $\mathcal{E}(g,\delta)$ is a weak egg of $\mathrm{PG}(4n-1,q)$ if and only if

- *the functions g and δ are linear in t over $\mathrm{GF}(q)$,*
- *δ_t is a bijection for $t \neq 0$,*
- *$g_{t_1}(\gamma_1) + g_{t_2}(\gamma_2) \neq g_{t_1+t_2}((\gamma_1^{\delta_{t_1}} + \gamma_2^{\delta_{t_2}})^{\delta^{-1}_{t_1+t_2}})$, for all $t_1 \neq 0$, $t_2 \neq 0$, $t_1+t_2 \neq 0$, $\gamma_1 \neq \gamma_2$ and $\gamma_1 \neq (\gamma_1^{\delta_{t_1}} + \gamma_2^{\delta_{t_2}})^{\delta^{-1}_{t_1+t_2}} \neq \gamma_2$.*

Proof. These conditions easily follow from working out the conditions for a weak egg from the definition. ■

Theorem 3.4.2 ([44])
A weak egg $\mathcal{E}$ is good at an element if and only if $\mathcal{E}$ is isomorphic to a weak egg $\mathcal{E}(g,\delta)$ with $\delta_t : \gamma \mapsto \gamma t$, and the egg $\mathcal{E}$ is good at $E(\infty)$.

Proof. Suppose $\mathcal{E}(g,\delta)$ is a weak egg with $\delta_t : \gamma \mapsto \gamma t$. Projecting $\mathcal{E}(g,\delta)$ from $E(\infty)$ shows that $\mathcal{E}(g,\delta)$ is good at $E(\infty)$. Conversely suppose that $\mathcal{E}$ is a weak egg which is good at an element. Without loss of generality we may assume that $\mathcal{E}$ is of the form $\mathcal{E}(g,\delta)$ and is good at $E(\infty)$. Projecting from $E(\infty)$ onto $W = \{\langle(r,0,s,t)\rangle \parallel r,s,t \in F\}$, gives a partial $(n-1)$-spread $\mathcal{P}$ of W. Since $\mathcal{E}(g,\delta)$ is good at $E(\infty)$, every $(2n-1)$-space of W spanned by two elements of $\mathcal{P}$, contains exactly q^n elements of $\mathcal{P}$. If $\mathcal{B}$ is the set of $(2n-1)$-spaces spanned by two elements of $\mathcal{P}$, then with respect to inclusion, the elements of $\mathcal{P}$ and $\mathcal{B}$ form the points and lines of an affine plane $\mathcal{A}$ of order q^n. Let T be the set of points of W, not contained in an element of $\mathcal{P}$. Every two elements of $\mathcal{B}$ necessarily meet in an $(n-1)$-space of W. Two elements of $\mathcal{B}$ which correspond with two parallel lines of $\mathcal{A}$, meet in an $(n-1)$-space contained in T. It follows that all lines belonging to the same parallel class of $\mathcal{A}$, intersect T in a common $(n-1)$-space. Let $\mathcal{L}$ be the set of all these $(n-1)$-spaces of T. Any two elements of $\mathcal{L}$ are disjoint since two non-parallel lines of $\mathcal{A}$ meet in a point of $\mathcal{A}$, i.e., an element of $\mathcal{P}$. This shows that $\mathcal{L}$ partitions the set T. We completed the partial spread $\mathcal{P}$ to a normal spread of W. By a theorem of Segre [70] it follows that the affine plane $\mathcal{A}$ is Desarguesian. This implies that the set $\mathcal{P}$ is isomorphic to the set $\{\{\langle t,0,-at,-bt\rangle \parallel t\in F\} \parallel a,b\in F\}$, under a collineation of W. Extending this collineation to a collineation of $\mathrm{PG}(4n-1,q)$, the result follows. ■

In [76], Thas proves that, for q odd, every subquadrangle that arises from a $(3n-1)$-space on the good element is isomorphic to $Q(4,q^n)$. Together with Theorem 3.3.3, this implies the following lemma.

Lemma 3.4.3 *If $\mathcal{E}$ is an egg of $\mathrm{PG}(4n-1,q)$, q odd, which is good at an element E, then every pseudo-oval on E contained in $\mathcal{E}$ is classical.*

The next theorem proves a conjecture of Thas [76]. The conjecture was first proved by Thas in [78], as a corollary of a more general result. Here a shorter direct proof of the conjecture is given.

Theorem 3.4.4 (Thas [78]; [44])
An egg $\mathcal{E}$ of $\mathrm{PG}(4n-1,q)$, q odd, is good at an element if and only if $T(\mathcal{E})$ is the translation dual of the point-line dual of a flock GQ.

Proof. Starting from a flock GQ, it follows from Theorem 3.3.7 and Theorem 3.4.2 that the egg is good at an element. Conversely, let $\mathcal{E}$ be an egg of $\mathrm{PG}(4n-1,q)$ which is good at an element. Without loss of generality we may assume that $\mathcal{E}$ is of the form $\mathcal{E}(g,\delta)$ and good at $E(\infty)$. From Theorem 3.2 it follows that we may assume that $\delta_t:\gamma\mapsto\gamma t$. Define the following $(3n-1)$-spaces:

$$V_a=\{\langle r,s,-ar,t)\rangle \parallel r,s,t\in F\},\forall a\in F,$$

$$W_b=\{\langle r,s,t,-br\rangle \parallel r,s,t\in F\},\forall b\in F,$$

$$U=\{\langle r,s,t,t\rangle \parallel r,s,t\in F\}.$$

Then every one of these $(3n-1)$-spaces contains exactly q^n+1 egg elements. Hence they intersect $\mathcal{E}(g,\delta)$ in a pseudo-oval on $E(\infty)$. Now fix $b\in F$ and consider the pseudo-oval $\mathcal{C}_b$ lying in W_b. By the above lemma $\mathcal{C}_b$ is isomorphic to an oval of $\mathrm{PG}(2,q^n)$, seen over $\mathrm{GF}(q)$. Since q is odd, this oval is a conic C (see Segre [68], [69]). So we can write the points of C as $\langle 1,f_1x^2+f_2x+f_3,x\rangle$, for some $f_1,f_2,f_3\in F$. If we look at the points of C as $(n-1)$-spaces over $\mathrm{GF}(q)$, then we may write them as $\{\langle t,(f_1x^2+f_2x+f_3)t,xt\rangle \parallel t\in F\}$. The set of these $(n-1)$-spaces is a pseudo-oval of $\mathrm{PG}(3n-1,q)$. We denote this pseudo-oval with $\mathcal{C}$. So there exists a collineation of W_b mapping $\mathcal{C}$ to $\mathcal{C}_b$. The elements of $\mathcal{C}_b$ are of the form $\{\langle t,-g_t(a,b),-at\rangle \parallel t\in F\}$, where we omit the last coordinate, which is fixed in W_b. Without loss of generality we may assume that there exists a collineation $(A,\sigma)\in \mathrm{P\Gamma L}(3n,q)$, which maps the $(n-1)$-space $\{\langle t,(f_1a^2+f_2a+f_3)t,-at\rangle \parallel t\in F\}$ to $\{\langle t,-g_t(a,b),-at\rangle \parallel t\in F\}$, such that

$$A \begin{bmatrix} t \\ (f_1a^2 + f_2a + f_3)t \\ -at \end{bmatrix} = \begin{bmatrix} t \\ -g_t(a,b) \\ -at \end{bmatrix}$$

This implies that $\sigma = 1$ and A is of the form

$$\begin{bmatrix} I_n & 0 & 0 \\ A_1 & A_2 & A_3 \\ 0 & 0 & I_n \end{bmatrix},$$

where I_n is the $(n \times n)$ identity matrix, and A_1, A_2, A_3 are $(n \times n)$ matrices over $\mathrm{GF}(q)$. Since every linear operator on F over $\mathrm{GF}(q)$ can be represented by a unique q-polynomial over F (see Theorem 9.4.4 in [67]), there exist $\alpha_i, \beta_i, \gamma_i \in F$ such that

$$-g_t(a,b) = \sum_{i=0}^{n-1} \alpha_i t^{q^i} + \sum_{i=0}^{n-1} \beta_i((f_1a^2 + f_2a + f_3)t)^{q^i} + \sum_{i=0}^{n-1} \gamma_i(-at)^{q^i}.$$

Simplifying this expression we get that there exist $a_i, b_i, c_i \in F$ such that

$$g_t(a,b) = \sum_{i=0}^{n-1} (a_ia^2 + b_ia + c_i)^{q^i} t^{q^i}.$$

This was for a fixed $b \in F$, so the coefficients may depend on b. Repeating the same argument for all $b \in F$, we get that there exist maps a_i, b_i, c_i from F to F such that

$$g_t(a,b) = \sum_{i=0}^{n-1} (a_i(b)a^2 + b_i(b)a + c_i(b))^{q^i} t^{q^i}.$$

We can apply the same reasoning to the pseudo-ovals contained in the $(3n-1)$-spaces V_a, for all $a \in F$, and for U. So there exist maps d_i, e_i, f_i from F to F, and constants, $u_i, v_i, w_i \in F$, such that

$$g_t(a,b) = \sum_{i=0}^{n-1} (d_i(a) + e_i(a)b + f_i(a)b^2)^{q^i} t^{q^i},$$

and

$$g_t(a,a) = \sum_{i=0}^{n-1} (u_ia^2 + v_ia + w_i)^{q^i} t^{q^i}.$$

Consider the pseudo-ovals in W_0 and V_0. Their elements are of the form $\{\langle (t, -g_t(a,0), -at, 0)\rangle \parallel t \in F\}$ and $\{\langle (t, -g_t(0,b), 0, -bt)\rangle \parallel t \in F\}$, respectively. Using a coordinate transformation involving only the first $3n$ coordinates we can get rid of the linear terms (terms with a in) and the constant terms (terms without a) in $g_t(a,0)$. This only adds constant terms or linear terms to $g_t(a,b)$. Using a coordinate transformation involving the second n and the last n coordinates, we can get rid of the linear terms in $g_t(0,b)$. Again this only adds linear terms to $g_t(a,b)$. We use the same notation for the possible new $g_t(a,b)$. It follows that $g_t(0,0)=0$, which implies that

$$\sum_{i=0}^{n-1}(w_i t)^{q^i}=\sum_{i=0}^{n-1}(c_i(0)t)^{q^i}=\sum_{i=0}^{n-1}(d_i(0)t)^{q^i}=0.$$

The form of $g_t(a,0)$ and $g_t(0,b)$ implies that

$$\sum_{i=0}^{n-1}(b_i(0)at)^{q^i}=\sum_{i=0}^{n-1}(e_i(0)bt)^{q^i}=0,$$

and therefore

$$\sum_{i=0}^{n-1}(c_i(b)t)^{q^i}=\sum_{i=0}^{n-1}(f_i(0)b^2t)^{q^i},$$

and

$$\sum_{i=0}^{n-1}(a_i(0)a^2t)^{q^i}=\sum_{i=0}^{n-1}(d_i(a)t)^{q^i}.$$

It also follows that the total degree in a and b must be 2 (up to the exponents q_i). This implies that we obtained the following formula for $g_t(a,b)$:

$$g_t(a,b)=\sum_{i=0}^{n-1}(a_i(0)a^2+b_i(b)a+f_i(0)b^2)^{q^i}t^{q^i},$$

and

$$g_t(a,b)=\sum_{i=0}^{n-1}(a_i(0)a^2+e_i(a)b+f_i(0)b^2)^{q^i}t^{q^i}.$$

From $g_t(a,a)$ it then follows that we can also replace $b_i(b)a$ and $e_i(a)b$ by a constant times ab. We have shown that there exist constants $a_i,b_i,c_i\in F$ such that $g_t(a,b)$ can be written as

$$g_t(a,b)=\sum_{i=1}^{n-1}(a_ia^2+b_iab+c_ib^2)^{q^i}t^{q^i}.$$

Theorem 3.3.7 implies that $\mathcal{E}(g,\delta)$ is the dual of an egg $\mathcal{E}^D$, such that $T(\mathcal{E}^D)$ is the point-line dual of a flock GQ. ■

3.5 The classical generalized quadrangle $Q(4,q)$

In the first section of this chapter we gave a brief description of the classical GQs. One of these examples is the GQ corresponding to a non-degenerate quadric in $\mathrm{PG}(4,q)$, which we have denoted by $Q(4,q)$. Another example of a GQ of order q is the generalized quadrangle constructed by Tits from an oval of $\mathrm{PG}(2,q)$, which we have denoted by $T(\mathcal{O})$.

Theorem 3.5.1 (Payne and Thas [60, 3.2.2])
If $\mathcal{O}$ is an oval in $\mathrm{PG}(2,q)$, then the GQ $T(\mathcal{O})$ is isomorphic to the classical GQ $Q(4,q)$ if and only if $\mathcal{O}$ is an irreducible conic.

If follows from the construction that $T(\mathcal{O})$ is a translation generalized quadrangle with base point (∞). Since the collineation group of the classical GQ $Q(4,q)$ acts transitively on the points of $Q(4,q)$, we have the following corollary.

Corollary 3.5.2 (Payne and Thas [60])
The GQ $Q(4,q)$ is a TGQ with base point P, for any point P of $Q(4,q)$.

If q is odd then every oval in $\mathrm{PG}(2,q)$ is a conic $\mathcal{C}$, and hence $Q(4,q)$ is isomorphic to $T(\mathcal{C})$. Let us take a closer look at the isomorphism between these two generalized quadrangles. To find the isomorphism we have to let the point (∞) of $T(\mathcal{C})$ correspond with a point of $Q(4,q)$. Since the collineation group of $Q(4,q)$ acts transitively on the points of $Q(4,q)$, we may choose any point P. The lines incident with P should correspond with the lines incident with (∞), i.e., the points of a conic. Intersecting the polar space of P with $Q(4,q)$ we get a quadratic cone $\mathcal{K}$ with vertex P. The base of the cone $\mathcal{K}$ is a conic $\mathcal{C}$ and hence there arises a natural way of making the necessary correspondence between the lines incident with P and the points of a conic by projecting the cone $\mathcal{K}$ onto its base $\mathcal{C}$. Let π be the plane containing the conic $\mathcal{C}$. Take a hyperplane H of $\mathrm{PG}(4,q)$, containing π but not incident with P. Now we have the setting to construct the TGQ $T(\mathcal{C})$ in the hyperplane H. Again a natural correspondence arises between the q^3 points of H not in π, i.e., the points of type (i) of $T(\mathcal{C})$, and the q^3 points not collinear with P by projecting $Q(4,q)$ from P onto H. The lines incident with a point y not collinear with P meet the cone $\mathcal{K}$ in a point, and hence they are projected from P onto a line of H meeting the plane π in a point of $\mathcal{C}$, this is a line of type (a) of $T(\mathcal{C})$. The points collinear with P now have to correspond with planes of H intersecting π in a tangent line to the conic $\mathcal{C}$. We can deduce this by considering the lines not on P and incident with a point Q collinear with P. All these lines are projected onto lines of H intersecting π in the same point of $\mathcal{C}$, and contained in a plane, namely the intersection of the polar space of Q with H. This plane is a point of type (ii) of $T(\mathcal{C})$, and hence by the above we obtained a bijection between the points collinear with P and the points of type (ii) of $T(\mathcal{C})$. It is straightforward to prove that the deduced correspondence defines an isomorphism ϕ between $Q(4,q)$ and $T(\mathcal{C})$.

Now we will be a bit more precise and introduce coordinates, so that we can give this isomorphism explicitly. For $Q(4,q)$ we take the non-degenerate quadric with equation $X_2^2 = X_0X_1 + X_3X_4$, for P we take the point $\langle 0,0,0,0,1\rangle$, and for the hyperplane H we choose the hyperplane defined by the equation $X_4 = 0$. Then the plane π has equation $X_3 = X_4 = 0$ and the conic $\mathcal{C}$ has equation $X_2^2 = X_0X_1$. We denote the tangent line at the point $\langle x_0, x_1, x_2, x_3, x_4\rangle$ of the conic $\mathcal{C}$ by $T_{\mathcal{C}}(x_0, x_1, x_2, x_3, x_4)$. Then the isomorphism $\phi : Q(4,q) \rightarrow T(\mathcal{C})$ can be defined by its action on the points of $Q(4,q)$

$$\begin{array}{lcl}
\langle 0,0,0,0,1\rangle & \mapsto & (\infty), \\
\langle a,b,c,1,c^2-ab\rangle & \mapsto & \langle a,b,c,1,0\rangle, \\
\langle a^2,1,a,0,b\rangle & \mapsto & \langle T_{\mathcal{C}}(a^2,1,a,0,0),(-b,0,0,1,0)\rangle, \\
\langle 1,0,0,0,a\rangle & \mapsto & \langle T_{\mathcal{C}}(1,0,0,0,0),(0,-a,0,1,0)\rangle.
\end{array}$$

Theorem 3.5.1 can be extended to TGQs corresponding with classical pseudo-ovals, in the case where q is odd. The pseudo-oval then arises from a conic of $\mathrm{PG}(2,q^n)$, and the corresponding TGQ is isomorphic to $Q(4,q^n)$. It is clear that the isomorphism can easily be deduced from the isomorphism ϕ between $Q(4,q)$ and $T(\mathcal{C})$.

In the following section we need this isomorphism in detail. Put $F = \mathrm{GF}(q^n)$. Consider the good egg $\mathcal{E}$ corresponding with an additive q^n-clan as before. The elements of $\mathcal{E}$ can be written as

$$E(\gamma) = \{\langle -g_t(\gamma), t, -\gamma t\rangle \| \ t \in F\}, \ \forall \gamma \in F^2,$$

$$E(\infty) = \{\langle t, 0, (0,0)\rangle \| \ t \in F\},$$

$$T_E(\gamma) = \{\langle f(\gamma,\delta) + g_t(\gamma), t, \delta\rangle \| \ t \in F, \delta \in F^2\}, \ \forall \gamma \in F^2,$$

$$T_E(\infty) = \{\langle t, 0, c\rangle \| \ t \in F, c \in F^2\},$$

with

$$g_t(a,b) = a^2 t + \sum_{i=0}^{n-1} (b_i ab + c_i b^2)^{1/q^i} t^{1/q^i},$$

and

$$f((a,b),(c,d)) = 2ac + \sum_{i=0}^{n-1} (b_i(ad+bc) + 2c_i bd)^{1/q^i}.$$

With these notations the pseudo-ovoid $\mathcal{E}$ is good at its element $E(\infty)$.

Consider the pseudo-oval $\mathcal{O}$ determined by the the good triple $(E(\infty), E(0,0), E(1,0))$. So $\mathcal{O}$ consists of the elements $E(\gamma)$, with $\gamma \in \{(a,0) \| \ a \in F\} \cup \{\infty\}$. From the coordinates we see that this pseudo-oval is classical. It is the conic with equation $X_0X_1 + X_2^2 = 0$ seen over GF(q).

Consider the projective space $\mathrm{PG}(4n,q) = \{\langle r,s,t,u,x_{4n}\rangle \| \ r,s,t,u \in F, \ x_{4n} \in \mathrm{GF}(q)\}$, and suppose that the good egg is contained in the hyperplane with equation $X_{4n} = 0$. The pseudo-oval $\mathcal{O}$ is then contained in the $(3n-1)$-dimensional subspace $\rho = \{\langle r,s,t,0,0\rangle \| \ r,s,t \in F\}$. We construct $T(\mathcal{O})$ in the $3n$-dimensional subspace $\mathcal{G} = \{\langle r,s,t,0,x_{4n}\rangle \| \ r,s,t \in F, \ x_{4n} \in \mathrm{GF}(q)\}$. Now we can define, in a similar way as we defined the isomorphism $\phi : Q(4,q^n) \rightarrow T(\mathcal{C})$, an isomorphism $\psi \ : \ Q(4,q^n) \rightarrow T(\mathcal{O})$:

$$
\begin{array}{lcl}
\langle 0,0,0,0,1\rangle & \mapsto & (\infty), \\
\langle a,b,c,1,c^2-ab\rangle & \mapsto & \langle -a,b,-c,0,1\rangle, \\
\langle a^2,1,a,0,b\rangle & \mapsto & \langle T_E(a,0) \cap \rho, (b,0,0,0,1)\rangle, \\
\langle 1,0,0,0,a\rangle & \mapsto & \langle T_E(\infty) \cap \rho, (0,-a,0,0,1)\rangle.
\end{array}
$$

So points collinear with x are mapped onto points of type (ii) of $T(\mathcal{O})$, i.e., the span of a tangent space of $\mathcal{O}$ with a point of $\mathcal{G} \setminus \rho$, and points not collinear with x are mapped onto points of type (i) of $T(\mathcal{O})$, i.e., points of $\mathcal{G} \setminus \rho$.

3.6 Semifield flocks and translation ovoids

An *ovoid* of a generalized quadrangle is a set of points such that every line of the GQ contains exactly one of these points. An ovoid is called a *translation ovoid* or *semifield ovoid* if there is a group of collineations of the GQ fixing a point of the ovoid and acting regularly on the other points of the ovoid. If a GQ of order (s,t) contains a subGQ of order (s',t') then the set of points in the subGQ collinear with a point not in the subGQ has the property that no two of these points are collinear. If $s = s'$ then every line of the subGQ will contain one of these points, i.e., these points form an ovoid of the subGQ. The ovoid is called a *subtended ovoid*.

In this section we will give the connection between certain type of flocks (semifield flocks) of a quadratic cone in $\mathrm{PG}(3,q^n)$ and translation ovoids of $Q(4,q^n)$, first explained by Thas in [77] in 1997, and later on by Lunardon [48] with more details. By my knowledge the explicit calculations given here have not appeared anywhere before.

Put $F = \mathrm{GF}(q^n)$, q odd, and consider the quadratic cone $\mathcal{K}$ in $\mathrm{PG}(3,q)$ with vertex $v = \langle 0,0,0,1\rangle$ and base the conic $\mathcal{C}$ with equation $X_0X_1 = X_2^2$. The planes of a flock of $\mathcal{K}$ can be written as $\pi_t \ : \ tX_0 + f(t)X_1 + g(t)X_2 + X_3 = 0$,

$t \in F$, for some $f, g \; : \; F \to F$. We denote this flock by $\mathcal{F}(f,g)$.

Remark. The notations f and g are usually used for the functions defining the flock. Although sometimes $-f$ is used instead of f. This probably has its origin from spreads of $\mathrm{PG}(3,q)$. But it would take us too far to explain this in detail. In this section we choose to use f and not $-f$ because using $-f$ would imply that we have to drag the minus sign along in all the calculations, of which we don't see the point. However when we present the known examples we will use $-f$ again. The reason for this is to make it easier for the reader to compare with the examples in the literature.

If f and g are linear over a subfield then the flock is called a *semifield flock*. The maximal subfield with this property is called the *kernel of the flock*. If we assume that the kernel of $\mathcal{F}$ is $\mathrm{GF}(q)$, then we can write f and g as

$$f(t) = \sum_{i=0}^{n-1} c_i t^{q^i} \text{ and } g(t) = \sum_{i=0}^{n-1} b_i t^{q^i}, \tag{3.5}$$

for some $b_i, c_i \in F$, $i = 1, \ldots, n-1$. Now we look at the dual space of $\mathrm{PG}(3,q^n)$ with respect to the standard inner product, i.e., a point $\langle a,b,c,d \rangle$ gets mapped to the plane with equation $aX_0 + bX_1 + cX_2 + dX_3 = 0$. The lines of the cone $\mathcal{K}$ become lines of $\mathrm{PG}(3,q^n)$ all contained in the plane $\pi : X_3 = 0$ corresponding with the vertex of $\mathcal{K}$. They had the property that no three of them were contained in a plane, so now they form a dual oval of π. Since q is odd, this dual oval is a dual conic, i.e., the set of lines of the cone corresponds with the set of tangents of a conic $\mathcal{C}'$. We want to know the equation of the conic $\mathcal{C}'$. A point $\langle 1, a^2, a \rangle$ of the conic $\mathcal{C}$ becomes the plane ρ with equation $X_0 + a^2 X_1 + aX_2 = 0$. So the line of the cone $\mathcal{K}$ on that point becomes the intersection of the planes π and ρ, i.e. the line with equation $X_0 + a^2 X_1 + aX_2 = 0$ in the plane π. Dualising with respect to the inner product corresponding with the polarity defined by the dual conic, i.e.,

$$((x,y,z),(u,v,w)) \mapsto (xv + yu - 2zw),$$

we obtain the point $\langle 1, a, -2a \rangle$ corresponding with the line of the cone we started from. We can do this for all the lines of the cone and we see that the equation of the corresponding conic $\mathcal{C}'$ in π is $4X_0X_1 - X_2^2 = 0$. Two planes π_t and π_s of the flock $\mathcal{F}$ correspond with the points $\langle t, f(t), g(t), 1 \rangle$ and $\langle s, f(s), g(s), 1 \rangle$. Since π_t and π_s do not intersect on the cone $\mathcal{K}$, the line $\langle \langle t, f(t), g(t), 1 \rangle, \langle s, f(s), g(s), 1 \rangle \rangle$ intersects π in an internal point $\langle t - s, f(t) - f(s), g(t) - g(s), 0 \rangle$ of $\mathcal{C}'$. Since f and g are additive, we obtain a set $\{\langle t, f(t), g(t), 0 \rangle \parallel t \in F\}$ of internal points of $\mathcal{C}'$. Over $\mathrm{GF}(q)$ the plane π becomes a $(3n-1)$-dimensional space, the conic $\mathcal{C}'$ becomes a pseudo-oval

$\mathcal{O}$ and the set of internal points, becomes an $(n-1)$- space skew to all the tangent spaces of $\mathcal{O}$. Dualising in the $(3n-1)$-space corresponding with π with respect to $\mathcal{O}$ yields a $(2n-1)$-dimensional space U skew to the elements of the pseudo-oval. To find U we use the inner product corresponding with the polarity defined by the conic $\mathcal{C}'$:

$$((x,y,z),(u,v,w)) \mapsto \mathrm{tr}(4xu + 4yv - 2zw),$$

where tr is the trace map from $\mathrm{GF}(q^n)$ to $\mathrm{GF}(q)$. So the point $\langle u,v,w\rangle \in U$ if $\mathrm{tr}(2uf(t) + 2vt + wg(t)) = 0$, for all $t \in F$. Using the expressions from (3.5) for f and g we obtain the condition

$$\mathrm{tr}\left[(2v + 2uc_0 + wb_0)t + \sum_{i=1}^{n-1}(2c_iu + b_iw)t^{q^i}\right] = 0, \text{ for all } t \in F.$$

Using Lemma 3.3.6, it follows that we can write U as $\{\langle u, -\tilde{F}(u,w), w\rangle \| \ u,w \in F\}$, with

$$\tilde{F}(u,w) = \sum_{i=0}^{n-1}(c_iu + \frac{1}{2}b_iw)^{1/q^i}.$$

Let ρ be the $(3n-1)$-space containing $\mathcal{O}$ and consider the construction of $T(\mathcal{O})$. If we extend U with a point not contained in ρ and we apply the isomorphism ψ^{-1}, then we get a $2n$-dimensional space containing q^{2n} points of type (i) of $T(\mathcal{O})$. Because U is skew to the pseudo-oval $\mathcal{O}$, no two of these points are collinear. Adding the point (∞) we get an ovoid of $T(\mathcal{O})$. Since $\mathcal{O}$ is a classical pseudo-oval this gives us an ovoid of $Q(4,q^n)$. In order to give the coordinates of the points of the ovoid of $Q(4,q^n)$ we have to apply a coordinate transformation such that the conic $\mathcal{C}'$ with equation $4X_0X_1 - X_2^2$ is mapped onto the conic with equation $X_0X_1 + X_2^2 = 0$, and then apply the isomorphism ψ^{-1}. After this transformation U becomes the subspace $\{\langle u, F(u,w), w\rangle \| \ u,w \in F\}$, with

$$F(u,w) = \sum_{i=0}^{n-1}(c_iu + b_iw)^{1/q^i}.$$

If we extend U with the point $\langle 0,\ldots,0,1\rangle$, we can write the ovoid as the set of points of $\mathrm{PG}(4,q^n)$

$$\{\langle -u, F(u,v), -v, 1, v^2 - uF(u,v)\rangle \| \ u,v \in F\} \cup \{\langle 0,0,0,0,1\rangle\}.$$

After a coordinate transformation fixing $Q(4,q^n)$, we get the ovoid $\mathcal{O}(\mathcal{F})$

$$\{\langle u, -F(u,v), v, 1, v^2 - uF(u,v)\rangle \| \ u,v \in F\} \cup \{\langle 0,0,0,0,1\rangle\}.$$

This construction also works starting with a translation ovoid of $Q(4,q^n)$ to obtain a semifield flock of a quadratic cone in $\mathrm{PG}(3,q^n)$. We define the *kernel* *of the translation ovoid* as the kernel of the corresponding semifield flock.

We conclude this section with a result on isomorphisms between flocks and ovoids.

Theorem 3.6.1 (Lunardon [48, Theorem 4])
If $\mathcal{F}_1$ and $\mathcal{F}_2$ are isomorphic semifield flocks of a quadratic cone in $\mathrm{PG}(3, q^n)$, *then the corresponding translation ovoids of $Q(4, q)$ are also isomorphic and conversely.*

3.7 Subtended ovoids of $Q(4, q)$

We already mentioned that in a good egg of $\mathrm{PG}(4n-1, q)$ there arise a lot of pseudo-ovals and hence in the corresponding GQ a lot of subGQs. Subtending gives ovoids of $Q(4, q)$. In 1994 Payne and Thas [82] used this method to construct a new ovoid of $Q(4, q^n)$, using the Roman GQ, arising from the Cohen-Ganley semifield flock, [59], by using only one subGQ. The question remained if using different subGQs, new ovoids could be obtained.

In [64] Penttila and Williams constructed a new translation ovoid of $Q(4, 3^5)$. This implies, as we mentioned in Section 3.6, a semifield flock and hence a good pseudo-ovoid. It was an open question if new ovoids could be obtained by subtending from points in the corresponding TGQ.

In this section we show that all the ovoids subtended from points of type (ii) are equivalent starting from an arbitrary good egg of $\mathrm{PG}(4n-1, q)$, q odd. This solves both questions concerning the ovoids subtended from points of type (ii). We also show that in at least one of the subquadrangles the ovoids subtended from points of type (i) are all equivalent. Moreover they are equivalent to the ovoids subtended by points of type (ii).

Consider the good egg $\mathcal{E}$ from the previous sections (here we denote it with $\mathcal{E}$ instead of $\mathcal{E}^D$) and suppose $\mathcal{E}$ is contained in the hyperplane with equation $X_{4n} = 0$ as before. We construct the TGQ $T(\mathcal{E})$ in $\mathrm{PG}(4n, q)$. Let $\mathcal{O}$ be the pseudo-oval $\{E(a, 0) \| \; a \in F\} \cup \{E(\infty)\}$, let ρ denote the $(3n-1)$-space $\{\langle r, s, t, 0, 0\rangle \| \; r, s, t \in F\}$ and $\mathcal{G}$ the $3n$-space $\{\langle r, s, t, 0, x_{4n}\rangle \| \; r, s, t \in F, \; x_{4n} \in \mathrm{GF}(q)\}$. We construct $T(\mathcal{O})$ in $\mathcal{G}$. We see $T(\mathcal{O})$ as a subGQ of $T(\mathcal{E})$, i.e., we identify the points $\langle T_E(a, 0) \cap \rho, x\rangle$ of type (ii) of $T(\mathcal{O})$ with the points $\langle T_E(a, 0), x\rangle$ of type (ii) of $T(\mathcal{E})$. Since $T(\mathcal{E})$ has order (q^n, q^{2n}), and $T(\mathcal{O})$ has order (q^n, q^n), the above method yields subtended ovoids in $T(\mathcal{O})$.

First we consider the ovoids subtended from a point of type (ii) of $T(\mathcal{E})$. The obtained ovoids are translation ovoids determined by a $(2n-1)$-space which is skew to the elements of the pseudo-oval $\mathcal{O}$. Since $\mathcal{O}$ is classical, and q is odd, this is equivalent with a semifield flock. Let $Q = \langle T_E(a,b), \langle x_0, \ldots, x_{4n-1}, 1\rangle\rangle$ be a point of type (ii) of $T(\mathcal{E})$ not contained in $T(\mathcal{O})$. It follows that $b \neq 0$. We may assume that $a = 0$, since there is a collineation of $T(\mathcal{E})$ mapping $E(a,b)$ to $E((a,b) + d(1,0))$ for all $d \in F$, and fixing $T(\mathcal{O})$, see [82]. Then

$$T_E(0,b) \cap \rho = \{\langle \sum_{i=0}^{n-1} (b_i bc + c_i b^2 t)^{1/q^i}, t, c, 0\rangle \| \ t, c \in F\},$$

is a $(2n-1)$-space skew to the classical pseudo-oval arising from the conic of $\mathrm{PG}(2, q^n)$ with equation $X_0X_1 + X_2^2 = 0$. From the previous section it follows that the semifield flock corresponding with this ovoid is $\mathcal{F}(\tilde{f}, \tilde{g})$, with

$$\tilde{f}(t) = b^2 \sum_{i=0}^{n-1} c_i t^{q^i}, \text{ and } \tilde{g}(t) = b \sum_{i=0}^{n-1} b_i t^{q^i}.$$

In $\mathrm{PG}(3, q^n)$ we can apply a coordinate transformation fixing the cone $\mathcal{K}$ such that the planes of the flock $\mathcal{F}(\tilde{f}, \tilde{g})$ are mapped onto the planes of the flock $\mathcal{F}(f, g)$. The matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & d^2 & 0 & 0 \\ 0 & 0 & d & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

induces such a coordinate transformation. It follows that the subtended ovoids obtained by subtending from points of type (ii) are isomorphic to the translation ovoid $\mathcal{O}(\mathcal{F})$.

Next we consider the ovoids subtended from a point Q of type (i) of $T(\mathcal{E})$. We may assume that $Q = \langle 0, 0, 0, d, 1\rangle$, with $d \in F^*$, since we can apply a translation fixing $T(\mathcal{O})$ if necessary, see [82]. Points of type (i) of $T(\mathcal{O})$ collinear with Q are $\langle E(a,b), Q\rangle \cap \mathcal{G}$, with $b \neq 0$. We get the $q^{2n} - q^n$ points

$$\langle -g_t(a,b), t, -at, 0, 1\rangle, \ a \in F, \ b \in F^*, \ t = \frac{d}{b}$$

of type (i). Points of type (ii) collinear with Q are $\langle T_E(a,0) \cap \rho, Q\rangle$, $a \in F$ and $\langle T_E(\infty) \cap \rho, Q\rangle$. We want to use the isomorphism ψ given earlier between $Q(4, q^n)$ and $T(\mathcal{O})$. First we remark that $\langle T_E(a,0) \cap \rho, Q\rangle = \langle T_E(a,0) \cap \rho, \langle f((a,0),(0,-d)), 0, 0, 0, 1\rangle\rangle$, and $\langle T_E(\infty) \cap \rho, Q\rangle = \langle T_E(\infty) \cap \rho, \langle 0,0,0,0,1\rangle\rangle$. So applying ψ^{-1} we obtain the q^n points

$$\langle a^2, 1, a, 0, -\sum_{i=0}^{n-1} (b_i ad)^{1/q^i}\rangle, \ a \in F,$$

and the point $\langle 1,0,0,0,0\rangle$ of $Q(4,q^n)$. Applying ψ^{-1} to the $q^{2n}-q^n$ points of type (i) we obtain the points

$$\begin{aligned}&\langle g_{\frac{d}{b}}(a,b),\frac{a}{b},\frac{ad}{b},1,(\frac{ad}{b})^2-\frac{d}{b}g_{\frac{d}{b}}(a,b)\rangle\\ =\ &\langle a^2+\frac{b}{d}\sum_{i=0}^{n-1}(b_iad+c_ibd)^{1/q^i},1,a,\frac{b}{d},-\sum_{i=0}^{n-1}(b_iad+c_ibd)^{1/q^i}\rangle\end{aligned}$$

for $a\in F$, and $b\in F^*$ of $Q(4,q^n)$. So the ovoid can be written as the set of points of $\mathrm{PG}(4,q^n)$

$$\left\{\langle a^2+b\sum_{i=0}^{n-1}(b_ida+c_id^2b)^{1/q^i},1,a,b,-\sum_{i=0}^{n-1}(b_ida+c_id^2b)^{1/q^i}\rangle \parallel a,b\in F\right\}$$
$$\cup\{\langle 1,0,0,0,0\rangle\}.$$

It follows that the subtended ovoid of $Q(4,q^n)$ is the translation ovoid corresponding with the semifield flock determined by the functions

$$\tilde{f}(t)=d^2\sum_{i=0}^{n-1}c_it^{q^i},\ \text{and}\ \tilde{g}(t)=d\sum_{i=0}^{n-1}b_it^{q^i}.$$

From the previous section together with the above it follows that the ovoid is a translation ovoid and the corresponding semifield flock is isomorphic to the semifield flock $\mathcal{F}(f,g)$ we started with.
So for every $d\in F^*$ we obtain an ovoid of $Q(4,q^n)$, by subtending from a point $\langle 0,0,0,d,1\rangle$ of type (i). Also for every $b\in F^*$ we obtained an ovoid by subtending from a point $\langle T_E(0,b),\langle 0,0,0,0,1\rangle$ of type (ii), and in the above we have shown that all these ovoids are isomorphic translation ovoids of $Q(4,q^n)$.

Theorem 3.7.1 *Let $\mathcal{E}$ be a good egg of $\mathrm{PG}(4n-1,q)$, q odd, represented as in Section 3.5. Then all the ovoids of the subquadrangle S determined by the elements $E(\infty)$, $E(0,0)$, and $E(1,0)$ of the good egg $\mathcal{E}$, obtained by subtending from points of $T(\mathcal{E})\backslash S$ are isomorphic translation ovoids of $Q(4,q^n)$. Moreover, these ovoids are isomorphic to the ovoid of $Q(4,q^n)$ arising from the semifield flock which corresponds with the good egg $\mathcal{E}$.*

Next we will show that the ovoids subtended from points of type (ii) in all the subGQs induced by the good element are equivalent. They all arise from the same semifield flock $\mathcal{F}(f,g)$.

Consider a quadratic cone $\mathcal{K}$ in $\mathrm{PG}(3,q^n)$ with vertex $\langle 0,0,0,1\rangle$ and with base the conic with equation $X_0X_1 - X_2^2 = 0$ in the plane with equation $X_3 = 0$. Let $\mathcal{F}(f,g)$ be a semifield flock of $\mathcal{K}$ with kernel $\mathrm{GF}(q)$, where the planes of the flock have the equation $tX_0 + f(t)X_1 + g(t)X_2 + X_3 = 0,\ t \in F$. Then there exist $b_i, c_i \in F$ such that $f(t) = \sum_{i=0}^{n-1} c_i t^{q^i}$, and $g(t) = \sum_{i=0}^{n-1} b_i t^{q^i}$. Consider the egg $\mathcal{E}$ of $\mathrm{PG}(4n-1,q)$ from above and let $\rho_{a,b}$ be the $(3n-1)$-space spanned by the elements $E(\infty), E(0,0)$ and $E(a,b)$ and put $\rho = \rho_{1,0}$. We will construct the $(2n-1)$-space $T_E(c,d) \cap \rho_{a,b}$, where $E(c,d)$ is not contained in $\rho_{a,b}$, i.e., (c,d) is not a multiple of (a,b), or $ad - bc \neq 0$. This condition implies that the matrix

$$\begin{bmatrix} a^2 & c^2 & 2ac & 0 \\ b^2 & d^2 & 2bd & 0 \\ ab & cd & ad+bc & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

induces a collineation of $\mathrm{PG}(3,q^n)$ fixing the cone $\mathcal{K}$. Applying to the planes of the flock we get the planes with equations

$$(a^2t + b^2f(t) + abg(t))\ X_0 +\ (c^2t + d^2f(t) + cdg(t))\ X_1$$

$$+\ (2act + 2bdf(t) + (ad+bc)g(t))\ X_2 +\ X_3 = 0,\ t \in F.$$

In the dual flock model we get the $(n-1)$-space (over $\mathrm{GF}(q)$)

$$\{\langle a^2t + b^2f(t) + abg(t), c^2t + d^2f(t) + cdg(t),$$

$$2act + 2bdf(t) + (ad+bc)g(t), 0\rangle \parallel t \in F\}$$

which is skew to the tangent spaces of the pseudo-oval corresponding with the conic $\mathcal{C}$ with equation $4X_0X_1 - X_2^2 = 0$ in the plane with equation $X_3 = 0$. Let A be the bijection mapping $t \mapsto a^2t + b^2f(t) + abg(t)$ (this is a bijection since the functions f and g induce a flock), and let ρ be the $(3n-1)$-space corresponding with the plane with equation $X_3 = 0$. Applying the collineation induced by the matrix

$$\begin{bmatrix} A^{-1} & 0 & 0 \\ 0 & I_n & 0 \\ 0 & 0 & I_n \end{bmatrix},$$

to ρ the pseudo-oval corresponding with the conic $\mathcal{C}$ is mapped onto the pseudo-oval with elements $\{\{\langle A^{-1}t, r^2t, 2rt, 0\ \rangle \parallel t \in F\} \parallel r \in F\} \cup \{\langle 0,t,0,0\rangle \parallel t \in F\}$ or rewriting the coordinates we obtain the pseudo-oval with elements

$$\{\{\langle t, r^2At, 2rAt, 0\ \rangle \parallel t \in F\} \parallel r \in F\} \cup \{\langle 0,t,0,0\rangle \parallel t \in F\}.$$

The $(n-1)$-space skew to the tangent spaces of this pseudo-oval becomes the $(2n-1)$-space

$$\{\langle t, c^2t + d^2f(t) + cdg(t), 2act + 2bdf(t) + (ad+cb)g(t), 0\rangle \parallel t \in F\}.$$

Now we dualise with respect to the inproduct

$$((x,y,z),(u,v,w)) = \mathrm{tr}(xu + yv + zw),$$

where tr is the trace map from $F \to \mathrm{GF}(q)$. The dual space of the pseudo-oval element $\{\langle t, r^2At, 2rAt, 0\ \rangle \parallel t \in F\}$ becomes

$$\{\langle -\sum_{i=0}^{n-1} \left[(a_i a^2 + b_i ab + c_i b^2)(r^2 v + 2rw)\right]^{1/q^i}, v, w, 0\rangle \parallel v, w \in F\},$$

where we introduced $(a_0, \ldots, a_{n-1}) = (1, 0, \ldots, 0)$ for convenience of notation. The dual of the $(n-1)$-space skew to the tangent spaces of the pseudo-oval becomes

$$\{\langle -\sum_{i=0}^{n-1} [(2a_i ac + b_i(ad + cb) + 2c_i bd)w$$

$$+(a_i c^2 + b_i cd + c_i d^2)v\big]^{1/q^i}, v, w, 0\rangle \parallel v, w \in F\}$$

skew to the elements of the new pseudo-oval in ρ. Now we apply the coordinate transformation mapping ρ to the $(3n-1)$-space $\rho_{a,b} = \{\langle r, s, at, bt\rangle \parallel r, s, t \in F\}$. This transformation maps the tangent space

$$\{\langle -\sum_{i=0}^{n-1} \left[(a_i a^2 + b_i ab + c_i b^2)(r^2 v + 2rw)\right]^{1/q^i}, v, w, 0\rangle \parallel v, w \in F\}.$$

of the pseudo-oval to the space

$$\{\langle \sum_{i=0}^{n-1} \left[(a_i a^2 + b_i ab + c_i b^2)(r^2 v + 2rw)\right]^{1/q^i}, v, wa, wb\rangle \parallel v, w \in F\},$$

which is the tangent space $T_E(ra, rb) \cap \rho_{a,b}$ of the pseudo-oval in $\rho_{a,b}$ at the element $E(ra, rb)$. (Note that we applied an extra coordinate transformation $X_0 \mapsto -X_0$ to get rid of the minus sign in the first coordinate). The $(2n-1)$-space skew to the pseudo-oval in ρ is mapped to the $(2n-1)$-space $T_E(c,d) \cap \rho_{a,b}$, i.e., the $(2n-1)$-space which induces the translation ovoid subtended from a point of type (ii) on the tangent space $T_E(c,d)$ of the egg $\mathcal{E}$. Since the elements of a pseudo-oval are determined by the tangent spaces it follows that the obtained pseudo-oval is the one determined by the elements $E(\infty)$, $E(0,0)$ and $E(a,b)$ of the good egg corresponding with the semifield flock. Moreover we have shown that all the ovoids of $Q(4,q^n)$ obtained by subtending from points of type (ii) are isomorphic to the ovoid arising from the semifield flock corresponding with the good egg.

Theorem 3.7.2 *Let $\mathcal{E}$ be a good egg of* $\mathrm{PG}(4n-1,q)$*, q odd, represented as in Section 3.5. Then all the ovoids of a subquadrangle S, determined by a pseudo-oval on $E(\infty)$ contained in $\mathcal{E}$, obtained by subtending from points of type (ii) of $T(\mathcal{E}) \setminus S$ are isomorphic translation ovoids of $Q(4,q^n)$. Moreover, these ovoids are isomorphic to the ovoid of $Q(4,q^n)$ arising from the semifield flock which corresponds with the good egg $\mathcal{E}$.*

3.8 Examples of eggs

In this section we list all know examples of eggs. From Theorem 3.3.4 we know that either $n = m$ or $ma = n(a+1)$ with a odd. The only known examples satisfy $n = m$, i.e., pseudo-ovals, or $m = 2n$, i.e., pseudo-ovoids.

3.8.1 Pseudo ovals

All known examples of pseudo-ovals are classical, i.e., they arise from ovals of $\mathrm{PG}(2,q^n)$. Pseudo ovals are classified for $q^n \leq 16$, see Theorem 3.9.3. If q is odd then the tangent spaces of a pseudo-oval form a pseudo-oval in the dual space. If q is even then the tangent spaces of a pseudo-oval all pass through an $(n-1)$-space of $\mathrm{PG}(3n-1,q)$, called the *nucleus* of the pseudo-oval, see [74].

3.8.2 Pseudo ovoids

The only known examples of eggs with $n \neq m$ are pseudo-ovoids, of which there are four classes of examples. Pseudo-ovals are classified for $q^n \leq 4$, see Section 3.10. In this section we will treat all of the examples and give the elements of the egg explicitly.

Let us start with an additive q^n-clan $C = \{A_t \parallel t \in \mathrm{GF}(q^n)\}$, with

$$A_t = \begin{bmatrix} t & g(t) \\ 0 & -f(t) \end{bmatrix},$$

where f and g are linear in t over $\mathrm{GF}(q)$. The corresponding semifield flock of a quadratic cone $\mathcal{K}$ with vertex $v = \langle 0,0,0,1 \rangle$, and base the conic $\mathcal{C} : X_0X_1 - X_2^2 = 0$ in $\mathrm{PG}(3,q^n)$ is denoted by $\mathcal{F}(f,g)$. The planes of the corresponding semifield flock are $tX_0 - f(t)X_1 + g(t)X_2 + X_3 = 0$. The condition for C to be a q^n-clan is

$$a^2t + g(t)ab - f(t)b^2 = 0 \;\Rightarrow\; a = b = 0 \text{ or } t = 0 \tag{3.6}$$

or the polynomial $tx^2 + g(t)x - f(t)$ is an irreducible polynomial over $\mathrm{GF}(q^n)$, for all $t \in GF(q^n)^* = \mathrm{GF}(q^n) \setminus \{0\}$. Since q is odd this is equivalent to

$g(t)^2 + 4tf(t)$ is a non-square in $\mathrm{GF}(q^n)$ for all $t \in \mathrm{GF}(q^n)^*$. Let $\mathcal{E}$ be the corresponding egg. Since f and g are linear over $\mathrm{GF}(q)$ we can write

$$f(t) = -\sum_{i=0}^{n-1} c_i t^{q^i},\ g(t) = \sum_{i=0}^{n-1} = b_i t^{q^i}.$$

From Theorem 3.3.8 it follows that the condition for the corresponding good egg $\mathcal{E}^D$ to be an egg is

$$\sum_{i=0}^{n-1}(a_i a^2 + b_i ab + c_i b^2)^{1/q^i} t^{1/q^i} = 0 \ \Rightarrow\ a = b = 0 \text{ or } t = 0.$$

Theorem 3.3.9 implies that the condition

$$\sum_{i=0}^{n-1}(a_i a^2 + b_i ab + c_i b^2) t^{q^i} = 0 \ \Rightarrow\ a = b = 0 \text{ or } t = 0.$$

is equivalent, indeed this is the condition (3.6). Maybe we should remark that in this chapter we have shown that all these conditions are equivalent, independent of the results by Payne [58], [59] or Kantor [42].

Classical pseudo-ovoid

If m is a non-square in $\mathrm{GF}(q^n)$, then the equation $a^2t - mb^2t = 0$ implies $a = b = 0$ or $t = 0$. Hence

$$f(t) = mt \text{ and } g(t) = 0$$

are functions satisfying the conditions to define an egg $\mathcal{E}_C$. The planes of the corresponding semifield flock $\mathcal{F}_C$ are

$$\pi_t : tX_0 - mtX_1 + X_3 = 0,\ t \in \mathrm{GF}(q^n).$$

All these planes contain the line with equation $X_3 = X_0 - mX_1 = 0$, and hence the flock $\mathcal{F}_C$ is linear. The elements of the corresponding egg $\mathcal{E}_C$ are

$$E(a,b) = \{\langle t, -a^2t + mb^2t, -at, mbt\rangle \parallel t \in \mathrm{GF}(q^n)\},\ \forall (a,b) \in F^2,$$

$$E(\infty) = \{\langle 0, t, 0, 0\rangle \parallel t \in \mathrm{GF}(q^n)\},$$

together with the set $T_{\mathcal{E}_C}$ of tangent spaces. All the coordinates of an egg element are linear in t over $\mathrm{GF}(q^n)$. Hence such an egg element $E(a,b)$ can be seen as a point $\langle 1, -a^2 + mb^2, -a, mb\rangle$ of $\mathrm{PG}(3, q^n)$. The coordinates of these points all satisfy $X_0X_1 + X_2^2 - m^{-1}X_3^2 = 0$, i.e., they are the points of an elliptic quadric in $\mathrm{PG}(3, q^n)$. In Section 3.5 we treated the isomorphism between $Q(4, q^n)$ and $T_2(\mathcal{O})$ when $\mathcal{O}$ is a conic of $\mathrm{PG}(2, q^n)$. In the same way there is a isomorphism between $Q(5, q^n)$ and $T_3(\mathcal{O})$ when $\mathcal{O}$ is an elliptic quadric, see [60]. One can start with the elliptic quadric with equation $X_0X_1 + X_2^2 - m^{-1}X_3^2 + X_4X_5 = 0$ in $\mathrm{PG}(5, q^n)$ to obtain an isomorphism between the GQ corresponding with this elliptic quadric and $T_3(\mathcal{O})$, where $\mathcal{O}$ is the elliptic quadric with equation $X_0X_1+X_2^2-m^{-1}X_3^2 = 0$ in the 3-dimensional subspace $X_4 = X_5 = 0$.

More generally every ovoid $\mathcal{O}$ of $\mathrm{PG}(3, q^n)$ yields a pseudo-ovoid in $\mathrm{PG}(4n - 1, q)$. The coordinates of the egg elements are linear in t over $\mathrm{GF}(q^n)$, and hence the kernel is $\mathrm{GF}(q^n)$, i.e., this is a classical pseudo-ovoid. The corresponding TGQ is isomorphic to $Q(5, q^n)$ if and only if the ovoid of $\mathrm{PG}(3, q^n)$ is an elliptic quadric. If q is odd then every ovoid of $\mathrm{PG}(3, q^n)$ is an elliptic quadric, and hence for q odd the TGQ corresponding to a classical ovoid is always isomorphic with $Q(5, q^n)$. Since every plane different from a tangent plane at a point of the ovoid intersects the ovoid in an oval, it follows that a classical pseudo-ovoid is good at every element. The converse also holds, i.e., if an egg is good at every element then it is classical, see Theorem 3.9.1.

Kantor pseudo-ovoid (q odd)

If q is odd and m is a non-square in $\mathrm{GF}(q^n)$ then the equation $a^2t - mb^2t^\sigma = 0$ with σ a $\mathrm{GF}(q)$-automorphism of $\mathrm{GF}(q^n)$, implies $t = 0$ or $a = b = 0$ (since $t^{\sigma-1}$ is a square). Hence the functions

$$f(t) = mt^\sigma \text{ and } g(t) = 0$$

are functions satisfying the conditions to define a semifield flock $\mathcal{F}_K$, sometimes called the *Kantor-Knuth semifield flock*. The planes of the flock are

$$\pi_t \; : \; tX_0 - mt^\sigma X_1 + X_3 = 0, \; t \in \mathrm{GF}(q^n).$$

All these planes contain the point $\langle 0, 0, 1, 0\rangle$, and the Kantor-Knuth semifield flock is characterized by the property that all the planes of the flock contain a common point but not a common line, see Theorem 3.9.4. The elements of the corresponding egg $\mathcal{E}_K$ are

$$E(a, b) = \{\langle t, -a^2t + mb^2t^\sigma, -at, mbt^\sigma\rangle \parallel t \in \mathrm{GF}(q^n)\}, \; \forall (a, b) \in \mathrm{GF}(q^n)^2,$$

$$E(\infty) = \{\langle 0, t, 0, 0\rangle \parallel t \in \mathrm{GF}(q^n)\},$$

together with the set $T_{\mathcal{E}_K}$ of tangent spaces. If we project the egg elements onto the $(3n-1)$-space $W = \{\langle r, 0, s, t\rangle \parallel r, s, t \in \mathrm{GF}(q^n)\}$ from the element $E(\infty)$, we obtain the set $\mathcal{S}$ of disjoint $(n-1)$- spaces

$$\{\langle t, 0, -at, mbt^\sigma\rangle \parallel t \in \mathrm{GF}(q^n)\},\ \forall (a,b) \in \mathrm{GF}(q^n)^2.$$

The matrix

$$\begin{bmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & \sigma^{-1} \end{bmatrix}$$

defines a collineation of $\mathrm{PG}(4n-1, q)$ fixing W. (With the entry σ^{-1} we mean the corresponding non-singular $(n \times n)$-matrix over $\mathrm{GF}(q)$.) Applying this collineation to the elements of $\mathcal{S}$ gives q^{2n} $(n-1)$-spaces which can be extended to a canonical Desarguesian spread of W. It follows that the Kantor pseudo-ovoid is good at the element $E(\infty)$. Now we apply this collineation to the elements of $\mathcal{E}_K$. We obtain the set of $(n-1)$-spaces

$$\{\langle t, -a^2t + mb^2t^\sigma, -at, (mb)^{\sigma^{-1}}t\rangle \parallel t \in \mathrm{GF}(q^n)\},\ \forall (a,b) \in \mathrm{GF}(q^n)^2,$$
$$\{\langle 0, t, 0, 0\rangle \parallel t \in \mathrm{GF}(q^n)\}.$$

Applying the coordinate transformation $X_4 \mapsto -m^\sigma X_4$, and rewriting the second coordinate gives

$$\{\langle t, -a^2t + (m^{\sigma^{-1}}(b^{\sigma^{-1}})^2t)^\sigma, -at, -b^{\sigma^{-1}}t\rangle \parallel t \in \mathrm{GF}(q^n)\},\ \forall (a,b) \in \mathrm{GF}(q^n)^2,$$
$$\{\langle 0, t, 0, 0\rangle \parallel t \in \mathrm{GF}(q^n)\}.$$

The elements of the dual egg $\mathcal{E}_K^D$ are

$$\{\langle -a^2t + (mb^2t)^{\sigma^{-1}}, t, -at, -bt\rangle \parallel t \in \mathrm{GF}(q^n)\},\ \forall (a,b) \in \mathrm{GF}(q^n)^2,$$
$$\{\langle t, 0, 0, 0\rangle \parallel t \in \mathrm{GF}(q^n)\}.$$

Now it is easy to see that by applying another coordinate transformation to the element $E(a,b)$ of $\mathcal{E}_K$ we obtain the element $\tilde{E}(a, b^{\sigma^{-1}})$ of the dual egg $\mathcal{E}_K^D$, but then for the automorphism σ^{-1} and the non-square $m^{\sigma^{-1}}$. It follows that the dual of a Kantor pseudo-ovoid with the automorphism σ^{-1} and the non-square $m^{\sigma^{-1}}$ is isomorphic to a Kantor pseudo-ovoid with the automorphism σ and the non-square m. But Kantor [43] has shown that the associated GQ obtained by replacing m with $m^{\sigma^{-1}}$ and σ with σ^{-1} is isomorphic to the original. This implies the following theorem.

Theorem 3.8.1 (Payne [59])
The TGQ $T(\mathcal{E}_K)$ corresponding with the Kantor pseudo-ovoid is isomorphic to its translation dual.

Cohen-Ganley pseudo-ovoid ($q = 3$)

If m is a non-square in $\mathrm{GF}(3^n)$ then

$$\begin{aligned} & t^6 + m^{-1}t^2 + mt^{10} \\ = \; & mt^2(m^{-1}t^4 + m^{-2} + t^8) \\ = \; & mt^2(t^4 - m^{-1})^2 \end{aligned}$$

is a non-square for all $t \in \mathrm{GF}(3^n)^*$. Hence the functions

$$f(t) = m^{-1}t + mt^9 \text{ and } g(t) = t^3$$

satisfy the conditions to define a semifield flock $\mathcal{F}_{CG}$. The planes of the flock are

$$\pi_t \; : \; tX_0 - (m^{-1}t + mt^9)X_1 + t^3X_2 + X_3 = 0, \; t \in \mathrm{GF}(3^n).$$

The elements of the corresponding egg $\mathcal{E}_{CG}$ are

$$E(a, b) = \{\langle t, -a^2t - abt^3 + m^{-1}b^2t + mb^2t^9, -at - bt^3, -at^3 + m^{-1}bt + mbt^9\rangle$$

$$\| \; t \in \mathrm{GF}(3^n)\}, \; \forall (a, b) \in \mathrm{GF}(3^n)^2, \; E(\infty) = \{\langle 0, t, 0, 0\rangle \; \| \; t \in \mathrm{GF}(3^n)\},$$

together with the set $T_{\mathcal{E}_{CG}}$ of tangent spaces. The dual egg was first calculated by Payne in [59] in 1989, where it was shown that the Cohen-Ganley pseudo-ovoid is not self dual. Hence the corresponding TGQ $T(\mathcal{E}^D_{CG})$ is not isomorphic to its translation dual $T(\mathcal{E}_{CG})$, and was called the *Roman GQ* by Payne [59]. It was the first example of a TGQ which is not the translation dual of the point-line dual of flock GQ. The elements of the dual egg $\mathcal{E}^D_{CG}$ are

$$\tilde{E}(a, b) = \{\langle -a^2t - (abt)^{1/3} + m^{-1}b^2t + (mb^2t)^{1/9}, t, -at, -bt\rangle \; \| \; t \in \mathrm{GF}(3^n)\},$$

$$\forall (a, b) \in \mathrm{GF}(3^n)^2, \; \tilde{E}(\infty) = \{\langle t, 0, 0, 0\rangle \; \| \; t \in \mathrm{GF}(3^n)\},$$

together with the set $T_{\mathcal{E}^D_{CG}}$ of tangent spaces. The egg $\mathcal{E}^D_{CG}$ is good at its element $\tilde{E}(\infty)$

The corresponding semifield flock is sometimes refered to as the *Ganley semifield flock*. We choose to use Cohen-Ganley, because we believe that the origin of this example is in a very nice paper by Cohen and Ganley [31].

Penttila-Williams pseudo-ovoid ($q = 3, n = 5$)

Put

$$f(t) = t^9 \text{ and } g(t) = t^{27}.$$

Penttila and Williams [64] proved with the help of a computer that these functions f and g yield a translation ovoid of $Q(4, 3^5)$. Using the connection first given by Thas [77], Bader, Lunardon and Pinneri [2] calculated the corresponding semifield flock, sometimes called a *sporadic semifield flock*. The planes of the flock are

$$\pi_t \ : \ tX_0 - t^9 X_1 + t^{27} X_2 + X_3 = 0, \ t \in \mathrm{GF}(3^5).$$

To prove that the functions f and g define a pseudo-ovoid we must show that $g(t)^2 + 4tf(t) = t^{54} + t^{10}$ is a non-square for all $t \in \mathrm{GF}(3^5)^*$, or equivalently $t^{44} + 1$ is a non-square for all $t \in \mathrm{GF}(3^5)^*$. If $u = t^{44}$ then u is an 11-th root of unity. Note that

$$(u+1)^{121} = (u+1)^{1+3+3^2+3^3+3^4},$$

which is 1 or -1 depending if $(u+1)$ is a square or a non-square. Now,

$$\begin{aligned} & (u+1)^{1+3+3^2+3^3+3^4} \\ = \ & (u+1)(u^3+1)(u^{3^2}+1)(u^{3^3}+1)(u^{3^4}+1) \\ = \ & 2 + \sum_{i=1}^{120} a_i u^i \qquad \text{modulo } u^{11} - 1, \end{aligned}$$

where a_i is the number of ways that i can be written as the sum of a subset of $\{1, 3, 3^2, 3^3, 3^4\}$ modulo 11. The exponents $1, 3, 3^2, 3^3, 3^4$ are the squares modulo 11, and every non-zero integer modulo 11 can be written in exactly three ways as the sum of the elements of a subset of $\{1, 3, 3^2, 3^3, 3^4\}$ modulo 11. Hence in $\mathrm{GF}(3^5)$, the product

$$(u+1)(u^3+1)(u^{3^2}+1)(u^{3^3}+1)(u^{3^4}+1) = 2 = -1 \text{ modulo } (u^{11} - 1).$$

It follows that $(u+1)^{121} = -1$ modulo $(u^{11} - 1)$, and hence $(t^{44} + 1)^{121} = -1$ modulo $t^{242} - 1$ implying $(t^{44} + 1)^{121} = -1$ for all $t \in \mathrm{GF}(3^5)^*$. This implies that $t^{44} + 1$ is a non-square for all $t \in \mathrm{GF}(3^5)^*$. This proof is taken from [3].

The elements of the corresponding egg $\mathcal{E}_{PW}$ are given by

$$E(a,b) = \{\langle t, -a^2 t - abt^{27} + b^2 t^9, -at - bt^{27}, -at^{27} + bt^9 \rangle \parallel t \in \mathrm{GF}(3^5)\},$$

$$\forall (a,b) \in \mathrm{GF}(3^5)^2, E(\infty) = \{\langle 0, t, 0, 0 \rangle \parallel t \in \mathrm{GF}(3^5)\},$$

together with the set $T_{\mathcal{E}_{PW}}$ of tangent spaces. The elements of the dual egg $\mathcal{E}_{PW}^D$ are

$$\tilde{E}(a,b) = \{\langle -a^2 t - (abt)^{1/27} + (b^2 t)^{1/9}, t, -at, -bt \rangle \parallel t \in \mathrm{GF}(3^5)\},$$

$$\forall (a,b) \in \mathrm{GF}(3^5)^2,\ \tilde{E}(\infty) = \{\langle t,0,0,0\rangle \parallel t \in \mathrm{GF}(3^5)\},$$

together with the set $T_{\mathcal{E}^D_{PW}}$ of tangent spaces. The egg $\mathcal{E}^D_{PW}$ is good at its element $\tilde{E}(\infty)$.

3.9 Some characterizations of eggs

In the previous section we proved that for q odd, good pseudo-ovoids correspond with semifield flocks. In this section we list a number of characterizations of eggs. Almost all results were obtained by Thas.

It is quite surprising that, although it is known since 1981 that eggs and TGQs are equivalent objects, still, apart from Thas his results, eggs were not studied in more detail until recently. The first characterization was given by Thas in 1974, [74]. At that time eggs of $\mathrm{PG}(4n-1,q)$ where called $[n-1]$-ovaloids and their definition included the extra property that every four elements either span $\mathrm{PG}(4n-1,q)$, or they are contained in a $\mathrm{PG}(3n-1,q)$. In the paper [74] Thas then shows that every $[n-1]$-ovaloid of $\mathrm{PG}(4n-1,q)$ is classical. This implies the following theorem.

Theorem 3.9.1 (Thas [74])
If every four elements of a pseudo-ovoid in $\mathrm{PG}(4n-1,q)$ *either are contained in a* $(3n-1)$*-dimensional space or span* $\mathrm{PG}(4n-1,q)$*, then the pseudo-ovoid is classical.*

Note that from this theorem it follows that if an egg of $\mathrm{PG}(4n-1,q)$ is good at every element then it is classical.

A strong result about pseudo-ovals was obtained by Casse, Thas and Wild [29] in 1985. The result is also contained in [60]. Consider a pseudo-oval with elements $E_0,\ldots,E_{q^n}$. By projecting the elements $E_j, j=1,\ldots,q^n$ from an element E_0 of a pseudo-oval onto a $(2n-1)$-space W skew to E_0 we obtain q^n mutually skew $(n-1)$-spaces of W. Together with $T_{E_0}\cap W$, we get an $(n-1)$-spread S_0 of W, and hence a translation plane of order q^n. In this way we obtain q^n+1 $(n-1)$-spreads $S_0,\ldots,S_{q^n}$ of $\mathrm{PG}(2n-1,q)$. Next consider the $(n-1)$-spaces defined by $T(E_i)\cap T(E_0), i=1\ldots q^n$. Together with E_0 we get an $(n-1)$-spread S_0^* of the $(2n-1)$-space $T(E_0)$, and hence again a translation plane of order q^n. We can do this for every tangent space of the pseudo-oval and in this way we obtain q^n+1 $(n-1)$-spreads $S_0^*,\ldots,S_{q^n}^*$ of $\mathrm{PG}(2n-1,q)$.

Theorem 3.9.2 (Casse, Thas, Wild [29])
Consider a pseudo-oval in $\mathrm{PG}(3n-1,q)$ *with q odd. Then at least one of*

the $(n-1)$*-spreads* $S_0^*, \ldots, S_{q^n}^*$ *is regular if and only if at least one of the* $(n-1)$*-spreads* $S_0, \ldots, S_{q^n}$ *is regular. In such a case all the* $(n-1)$*-spreads* $S_0, \ldots, S_{q^n}, S_0^*, \ldots, S_{q^n}^*$ *are regular and the TGQ corresponding with the pseudo-oval is isomorphic to the classical GQ* $Q(4, q^n)$*.*

Pseudo-ovals are classified for $q^n \leq 16$.

Theorem 3.9.3 (Penttila [61])
If $\mathcal{O}$ *is a pseudo-oval of* $\mathrm{PG}(3n-1, q)$*, with* $q^n \leq 16$*, then* $\mathcal{O}$ *is classical.*

If all the planes of a flock of a quadratic cone in $\mathrm{PG}(3, q^n)$ contain a fixed line, then the flock is linear. We have a similar characterisation for the semifield flock of Kantor type.

Theorem 3.9.4 (Thas [75])
If all the planes of a flock contain a common point, but not containing a common line, then the flock is a semifield flock of Kantor type.

If q is odd, then the semifield flock $\mathcal{F}$ induces a good pseudo-ovoid $\mathcal{E}$. In Section 3.7 we gave a geometric construction of the egg elements starting from the flock $\mathcal{F}$, using the explicit coordinates of the egg elements. In particular we constructed every intersection $T_F \cap \langle E, E_1, E_2 \rangle$, where E_1, E_2, F are three different egg elements such that F is not contained in the $(3n-1)$-space $\langle E, E_1, E_2 \rangle$. Note that the pseudo-conic induced by the elements E, E_1, E_2 is contained in a Desarguesian spread of $\langle E, E_1, E_2 \rangle$, which we denote by $\mathcal{S}$. If all the planes of the flock contain a common line, then from the construction it follows that $T_F \cap \langle E, E_1, E_2 \rangle$ is a line over $GF(q^n)$, i.e., a $(2n-1)$-space spanned by two elements of $\mathcal{S}$. If this is the case then we say that (F, E_1, E_2) is a *supernormal triple*. Conversely if there exists such a supernormal triple, then all the planes contain a common line. This gives a characterization of the classical pseudo-ovoids.

Theorem 3.9.5 *Let* $\mathcal{E}$ *be an egg of* $\mathrm{PG}(4n-1, q)$*,* q *odd, which is good at an element* E*. Then the following properties are equivalent.*

- $\mathcal{E}$ *is a classical pseudo-ovoid.*
- *There exists a triple* (F, E_1, E_2)*, where* F *is not contained in the pseudo-conic* $\mathcal{C}$ *induced by the elements* E_1 *and* E_2 *in the* $(3n-1)$*-space* $\langle E, E_1, E_2 \rangle$*, which is supernormal.*
- *All triples* (F, E_1, E_2)*, where* F *is not contained in the pseudo-conic* $\mathcal{C}$ *induced by the elements* E_1 *and* E_2 *in the* $(3n-1)$*-space* $\langle E, E_1, E_2 \rangle$ *are supernormal.*

If all the planes of $\mathcal{F}$ contain a common point but not a common line, then by following the construction given in Section 3.7 step by step, it is clear that the $(2n-1)$-space $T_F \cap \langle E, E_1, E_2 \rangle$ contains exactly one element of $\mathcal{S}$. If this is the case then we say that (F, E_1, E_2) is a *normal triple.* Note that we can do this for every such egg elements F, E_1, E_2. Conversely if there exists one normal triple (F, E_1, E_2), then again from the construction it follows that the planes of $\mathcal{F}$, must all meet in a point, and by the above every such triple of egg elements F, E_1, E_2 is normal. So we translated the property that all planes of the flock contain a common point into a property of the corresponding good pseudo-ovoid, resulting in the following characterization of the Kantor pseudo-ovoid.

Theorem 3.9.6 *Let $\mathcal{E}$ be a non-classical egg of* $\mathrm{PG}(4n-1, q)$*, q odd, which is good at an element E. Then the following properties are equivalent.*

- *$\mathcal{E}$ is a Kantor pseudo-ovoid.*
- *There exists a triple (F, E_1, E_2), where F is not contained in the pseudo-conic $\mathcal{C}$ induced by the elements E_1 and E_2 in the $(3n-1)$-space $\langle E, E_1, E_2 \rangle$, which is normal.*
- *All triples (F, E_1, E_2), where F is not contained in the pseudo-conic $\mathcal{C}$ induced by the elements E_1 and E_2 in the $(3n-1)$-space $\langle E, E_1, E_2 \rangle$ are normal.*

Proof. The theorem follows from the above and Theorem 3.9.4. ■

Remark. The equivalence of the first two properties of the last theorem is a result of Thas [80]. The proof of the result given here is an alternative proof.

In 1997 Thas published a long paper [77] on eggs of $\mathrm{PG}(4n-1, q)$, q odd, making the connection with Veronese varieties. It would take us too far to go in detail. Let us mention the main theorem of the paper.

Theorem 3.9.7 (Thas [77, Theorem 6.9])
Suppose the egg $\mathcal{E}$ of $\mathrm{PG}(4n-1, q)$ *is good at an element E, then we have one of the following.*

(a) There exists a $\mathrm{PG}(3, q^n)$ *in the extension* $\mathrm{PG}(4n-1, q^n)$ *of* $\mathrm{PG}(4n-1, q)$ *which has exactly one point in common with each of the extensions of the egg elements. The set of these $q^{2n}+1$ points is an elliptic quadric of* $\mathrm{PG}(3, q^n)$ *and $T(\mathcal{E})$ is isomorphic to the classical GQ $Q(5, q^n)$.*

(b) We are not in case (a) and there exists a $\mathrm{PG}(4, q^n)$ *in* $\mathrm{PG}(4n-1, q^n)$

which intersects the extension of E in a line M and which has exactly one point r_i in common with the extension of the other egg elements. Let $\mathcal{W}$ be the set of these intersection points r_i, $i = 0 \dots q^{2n}$ and let $\mathcal{M}$ be the set of all common points of M and the conics which contain exactly q^n points of $\mathcal{W}$. Then the set $\mathcal{W} \cup \mathcal{M}$ is the projection of a quadric Veronesian $\mathcal{V}_2^4$ from a point P in a conic plane of $\mathcal{V}_2^4$ onto $\mathrm{PG}(4, q^n)$; the point P is an exterior point of the conic of $\mathcal{V}_2^4$ in the conic plane. Also if the point-line dual of the translation dual of $T(\mathcal{E})$ is a flock GQ, then $\mathcal{E}$ is of Kantor type.

(c) We are not in cases (a) and (b) and there exists a $\mathrm{PG}(5, q^n)$ in $\mathrm{PG}(4n - 1, q^n)$ which intersects the extension of E in a plane π, and which has exactly one point r_i in common with the extension of the other egg elements. Let $\mathcal{W}$ be the set of these intersection points r_i, $i = 0 \dots q^{2n}$ and let $\mathcal{P}$ be the set of all common points of π and the conics which contain exactly q^n points of $\mathcal{W}$. Then the set $\mathcal{W} \cup \mathcal{P}$ is a quadric Veronesean in $\mathrm{PG}(5, q^n)$

If we are in case (a), then the egg is classical, and hence can be extended to a Desarguesian $(n-1)$-spread of $\mathrm{PG}(4n-1, q)$. Since now we know that the TGQ corresponding with a good egg of $\mathrm{PG}(4n-1, q)$, q odd, is the translation dual of the point-line dual of a flock GQ, it follows that in case (b) the egg is always of Kantor type. The following conjectures were given by Thas in the same paper.

Conjectures (Thas [77])
1. *In case (c) of the above theorem and if the point-line dual of the translation dual of $T(\mathcal{E})$ is a flock GQ, then $\mathcal{E}$ is of Cohen-Ganley type*
2. *Any TGQ $T(\mathcal{E})$ of order (s, s^2) and $s \neq 1$, with $\mathcal{E}$ good at some element, is the point-line dual of the translation dual of a semifield flock GQ.*

The first conjecture was disproved in 1999 by the discovery of the Penttila-Williams translation ovoid of $Q(4, 3^5)$ [64]. The connection between translation ovoids of $Q(4, q^n)$, semifield flocks, and eggs of $\mathrm{PG}(4n-1, q)$, q odd, was treated earlier on in this chapter. The second conjecture was proved by Thas in 1999, [78], in a more general setting. A direct and shorter proof of this conjecture was given in Section 3.4.

Another characterization of the Kantor pseudo-ovoid was given in 1999, depending on a result by Thas and Van Maldeghem [83].

Theorem 3.9.8 (Bader, Lunardon, Pinneri [2])
If both an egg $\mathcal{E}$ of $\mathrm{PG}(4n - 1, q)$, q odd, and its dual are good at an element, then the egg is classical or of Kantor type.

The next theorem for q even follows from the fact that all semifield flocks for q even are linear.

Theorem 3.9.9 (Johnson [41])
If a TGQ $T(\mathcal{E})$ of order (q, q^2), q even, is the point-line dual of a flock GQ then $T(\mathcal{E})$ is classical.

The next two theorems are from a recent paper of Thas [79], treating eggs of $\mathrm{PG}(4n-1, q)$, q even.

Theorem 3.9.10 (Thas [79, Theorem 6.1])
An egg $\mathcal{E}$ of $\mathrm{PG}(4n-1, q)$, q even, is classical if and only if $\mathcal{E}$ is good at some element and contains at least one pseudo-conic.

Theorem 3.9.11 (Thas [79, Theorem 6.2])
An egg $\mathcal{E}$ of $\mathrm{PG}(4n-1, q)$, q even, is classical if and only if $\mathcal{E}$ contains at least two intersecting pseudo-conics.

3.10 On the classification of semifield flocks

In this section we give an important result towards the classification of semifield flocks, obtained in 2000. We already mentioned that if q is even, all semifield flocks of a quadratic cone of $\mathrm{PG}(3, q^n)$ are linear. Now we consider the case when q is odd. In 1998 Bloemen, Thas and Van Maldeghem obtained the following results.

Theorem 3.10.1 (Bloemen, Thas and Van Maldeghem [13])
Let $\mathcal{F}$ be a semifield flock of a quadratic cone in $\mathrm{PG}(3, q^n)$, q odd, with kernel $\mathrm{GF}(q)$. If $n = 1$ then the $\mathcal{F}$ is linear. If $n = 2$ then $\mathcal{F}$ is of Kantor type.

Theorem 3.10.2 (Bloemen, Thas and Van Maldeghem [13])
Let $\mathcal{F}$ be a semifield flock of a quadratic cone in $\mathrm{PG}(3, q^3)$, q odd, with kernel containing $\mathrm{GF}(q)$. If $3 \leq q \leq 31$ then $\mathcal{F}$ is linear or of Kantor type.

In Section 3.6 we saw that with a semifield flock of $\mathrm{PG}(3, q^n)$, q odd, there corresponds an $(n-1)$-dimensional projective space over $\mathrm{GF}(q)$, contained in the set of internal points of a non-degenerate conic $\mathcal{C}$ of $\mathrm{PG}(2, q^n)$. If Q is the quadratic form whose zeros are the conic $\mathcal{C}$, then the value of Q on the internal points is either a non-zero square or a non-square in $\mathrm{GF}(q^n)$, see [37], and after multiplying by a suitable scalar we may assume it is a non-zero square. We will show that this implies an upper bound on the value of q, determined by the value of n. First we need the following lemmas.

The first lemma is due to Weil and can be found in Schmidt [72].

Lemma 3.10.3 (see [72])
The number of solutions N in GF(q) *of the hyperelliptic equation*

$$y^2 = g(x)$$

where $g \in \mathrm{GF}(q)[X]$ is not a square and has degree $2m > 2$ satisfies

$$|N - q + 1| < (2m-2)\sqrt{q}.$$

Lemma 3.10.4 ([8])
Let $f(X) = X^2 + uX + v \in \mathrm{GF}(q^n)[X]$ be a non-zero square in GF(q^n) *for all $X = x \in \mathrm{GF}(q)$, q odd and $q \geq 4n^2 - 8n + 2$. At least one of the following holds.*

1. *f is the square of a linear polynomial in X over $GF(q^n)$.*
2. *n is even and f has two distinct roots in* GF$(q^{n/2})$.
3. *The roots of f are α and α^σ for some* GF(q)*-automorphism of* GF(q^n)*, σ, and $\alpha \in \mathrm{GF}(q^n)$.*

Proof. Let n_1 be the order of the smallest subfield such that $f(X) \in \mathrm{GF}(q^{n_1})[X]$ and $f(x)$ is a non-zero square in GF(q^{n_1}) for all $x \in \mathrm{GF}(q)$. If $n_1 \neq n$ simply replace n by n_1 and assume that no such subfield exists. Let f_i be the polynomial obtained from f by raising all coefficients to the power q^i. The roots of f_i are the roots of f raised to the power q^i. For all $x \in \mathrm{GF}(q)$ we have that $f(x)$ is a square in GF(q^n) implies that

$$g(x) = \prod_{i=0}^{n-1} f_i(x)$$

is a square in GF(q). The degree of g is $2n$, $g(X) \in \mathrm{GF}(q)[X]$ and by assumption

$$|2q - q + 1| > (2n-2)\sqrt{q},$$

The number of solutions (x, y) of $y^2 = g(x)$, where $g(x)$ is always a square, is $2q$, and hence the previous lemma implies that g is a square. Assume that f is not a square and let $\alpha, \beta \neq \alpha$ be the roots of f. The roots of g are

$$\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}, \beta, \beta^q, \ldots, \beta^{q^{n-1}}$$

and every value occurs in this list an even number of times since g is a square. Therefore there exists a GF(q)-automorphism of GF(q^n), σ, such that $\beta = \alpha^\sigma$ or there exists GF(q)-automorphisms of GF(q^n),σ and τ, such that $\alpha = \alpha^\sigma$ and $\beta = \beta^\tau$.

Suppose there is a σ such that $\alpha = \alpha^\sigma$, and there is no σ such that $\beta = \alpha^\sigma$. Let d be minimal such that $x^\sigma = x^{q^d}$. Then each element of $\{\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}\}$ occurs in the list $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ an even number of times. It follows that $n = md$ with m, the order of σ, an even integer. In particular n is even and $\alpha = \alpha^\sigma = \alpha^{\sigma^{m/2}} = \alpha^{q^{n/2}}$ and $\alpha \in \mathrm{GF}(q^{n/2})$. Likewise $\beta \in \mathrm{GF}(q^{n/2})$. This implies that f has two distinct roots in $\mathrm{GF}(q^{n/2})$.

Suppose there is a σ such that $\beta = \alpha^\sigma = \alpha^{q^d}$ where d is chosen to be minimal. Then the list $\{\beta, \beta^q, \ldots, \beta^{q^{n-d-1}}\}$ is equal to the list $\{\alpha^{q^d}, \alpha^{q^{d+1}}, \ldots, \alpha^{q^{n-1}}\}$. Therefore each value which occurs in the list

$$\{\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}, \alpha^{q^n}, \alpha^{q^{n+1}}, \ldots, \alpha^{q^{n+d-1}}\},$$

occurs an even number of times. Let e be minimal such that $\alpha = \alpha^{q^e}$. Note that $e < 2n$ since α is a root of f and $e > d$ by the minimality of d, and so the elements in the list $\{\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}\}$ are all distinct. Hence

$$\{\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}\} = \{\alpha^{q^n}, \alpha^{q^{n+1}}, \ldots, \alpha^{q^{n+d-1}}\}$$

and

$$\{\alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^d}\} = \{\alpha^{q^{n+1}}, \alpha^{q^{n+2}}, \ldots, \alpha^{q^{n+d}}\}$$

which by taking the symmetric difference implies $\{\alpha, \alpha^{q^d}\} = \{\alpha^{q^n}, \alpha^{q^{n+d}}\}$. If $\alpha = \alpha^{q^n}$, then f has two roots α and α^σ, where $\alpha \in \mathrm{GF}(q^n)$. If $\alpha \neq \alpha^{q^n}$ then $\alpha = \alpha^{q^{n+d}}$ and $\alpha^{q^d} = \alpha^{q^n}$ which combine to give $\alpha = \alpha^{q^{2d}}$ and therefore e divides $2d$. Moreover since $e > d$ we have that $e = 2d$ and since e divides $2n$ that d divides n. The coefficients of f are $-\alpha - \alpha^{q^d}$ and α^{q^d+1} respectively which are in the subfield $\mathrm{GF}(q^d)$. Hence $f \in \mathrm{GF}(q^d)[X]$. If n/d is even then $2d$ divides n and f has two roots α and α^σ where $\alpha \in \mathrm{GF}(q^n)$. If n/d is odd then for all $x \in \mathrm{GF}(q)$

$$1 = f(x)^{(q^n-1)/2} = f(x)^{(1+q^d+\ldots+q^{n-d})(q^d-1)/2} = f(x)^{(n/d)(q^d-1)/2}.$$

Since $f(x)^{(q^d-1)/2} \in \mathrm{GF}(q^d)$, with q odd, and since n/d is odd and

$$f(x)^{(n/d)(q^d-1)/2} = 1,$$

it follows that $f(x)^{(q^d-1)/2} = 1$. This implies that $f(x)$ is a square in $\mathrm{GF}(q^d)$, for all $x \in \mathrm{GF}(q)$. However we assumed at the start of the proof that this was not the case. ■

Theorem 3.10.5 ([8])
If there is a subplane of order q contained in the set of internal points of a non-degenerate conic $\mathcal{C}$ in $PG(2, q^n)$, $n \geq 3$, then $q < 4n^2 - 8n + 2$.

Proof. Let Q be the quadratic form

$$Q(X, Y, Z) = X^2 + aXY + bXZ + cY^2 + dYZ + eZ^2$$

whose set of zeros is the conic $\mathcal{C}$. Suppose that Q is a non-zero square on the set $\{(x, y, z) \,|\, x, y, z \in \mathrm{GF}(q)\}$, i.e., we suppose that the set of internal points of the conic $\mathcal{C}$ contains a subplane of order q. Let n_1 be the order of the smallest subfield such that all the coefficients of Q are elements of $\mathrm{GF}(q^{n_1})$. If $n_1 \neq n$ simply replace n by n_1 in the theorem and assume that all coefficients of Q do not lie in a subfield.

Assume that $q \geq 4n^2 - 8n + 2$. For a fixed y and z in $\mathrm{GF}(q)$ not both zero let

$$f_{yz}(X) = Q(X, y, z).$$

The polynomial $f_{yz} \in \mathrm{GF}(q^n)[X]$ is a square for all x in $\mathrm{GF}(q)$. If f_{yz} is a square of another polynomial then Q is a square for all points on the line $zY - yZ = 0$. However, the lines that contain internal points also contain external points on which Q is a non-square.

If f_{yz} has two distinct roots α and β in $\mathrm{GF}(q^{n/2})$ then (α, y, z) and (β, y, z) are points of the conic $\mathcal{C}$. Moreover, since $y, z \in \mathrm{GF}(q)$, they are points of the conic $\mathcal{C}''$ defined by the quadratic form whose coefficients are the coefficients of Q raised to the power $q^{n/2}$. The coefficients of Q do not all lie in a subfield so $\mathcal{C} \neq \mathcal{C}''$. Since a conic in is determined by five points, the conics $\mathcal{C}$ and $\mathcal{C}''$ meet in at most four points. Hence f_{yz} can have two distinct roots in $\mathrm{GF}(q^{n/2})$ for at most two projective pairs (y, z). We assume henceforth that (y, z) is not one of these two.

By the previous lemma the roots of f_{yz} are therefore α and α^σ for some $\alpha \in \mathrm{GF}(q^n)$ and some $\mathrm{GF}(q)$-automorphism σ of $\mathrm{GF}(q^n)$. Let $g(Y, Z) = aY + bZ$ and $h(Y, Z) = cY^2 + dYZ + eZ^2$ so we have that

$$f_{yz}(X) = (X - \alpha)(X - \alpha^\sigma) = X^2 + g(y, z)X + h(y, z).$$

There are two cases to consider, namely when the order of σ is odd and when it is even.

Consider first the case that the order m of σ is odd. Since

$$(\alpha^{1+\sigma})^{1-\sigma+\sigma^2-\cdots+\sigma^{m-1}} = \alpha^{1+\sigma^m} = \alpha^2$$

and

$$(\alpha^{1+\sigma})^{\sigma(1-\sigma+\sigma^2-\cdots+\sigma^{m-1})} = \alpha^{\sigma+\sigma^{m+1}} = \alpha^{2\sigma},$$

we have the identity

$$(\alpha+\alpha^\sigma)^2 = (\alpha^{1+\sigma})^{1-\sigma+\sigma^2-\ldots+\sigma^{m-1}} + 2\alpha^{1+\sigma} + (\alpha^{1+\sigma})^{\sigma(1-\sigma+\sigma^2-\ldots+\sigma^{m-1})}$$

which implies

$$g(y,z)^2 = h(y,z)^{1-\sigma+\sigma^2-\ldots+\sigma^{m-1}} + 2h(y,z) + h(y,z)^{\sigma(1-\sigma+\sigma^2-\ldots+\sigma^{m-1})}.$$

There is such an automorphism σ for $q-1$ projective pairs (y,z) and hence, since there are $n-1$ possibilities for σ, there exists an automorphism $\tilde{\sigma}$ which occurs for at least

$$(q-1)/(n-1) > 2n \geq 2m$$

projective pairs. Note that for the last inequality we used the hypotheses $n \geq 3$ and $q \geq 4n^2 - 8n + 2$. We modify our notation and let f_i be the polynomial obtained from f by raising all coefficients to the power $\tilde{\sigma}^i$. The above relation implies

$$h_1h_2\ldots h_{m-1}g^2 = h_0(h_2h_4\ldots h_{m-1} + h_1h_3\ldots h_{m-2})^2$$

which has total degree $2m$ and holds for at least $2m+1$ pairs, holds for every projective pair (y,z), $y,z \in \mathrm{GF}(q)$, and is therefore an identity. For all $x \in \mathrm{GF}(q)$

$$f_{yz}(X+x) = X^2 + (g+2x)X + h + xg + x^2 = (X-(\alpha-x))(X-(\alpha^\sigma - x))$$

and we get the more general relation

$$w_1w_2\ldots w_{m-1}(g+2x)^2 = w_0(w_2w_4\ldots w_{m-1} + w_1w_3\ldots w_{m-2})^2$$

where $w(x,y,z) = h(y,z)+g(y,z)x+x^2$. This equation is valid for all $(x,y,z) \in \mathrm{GF}(q)^3$ and since it is of total degree $2m$ the equation is again an identity. We may replace $w_0 = w$ by Q and it follows that

$$Q_1 \mid Q_0Q_2\ldots Q_{m-1}.$$

Therefore either $Q_1 = Q_i$ for some $i \in \{0,2,4,\ldots,m-1\}$ and the coefficients of Q lie in some subfield or Q_1, and hence Q, splits into linear factors, and Q is degenerate. In both cases, we get a contradiction.

In the second case when the order m of σ is even

$$h(y,z)^{1+\sigma^2+\ldots+\sigma^{m-2}} = h(y,z)^{\sigma+\sigma^3+\ldots+\sigma^{m-1}}$$

and, by the same reasoning, there exists an automorphism $\tilde{\sigma}$ for which this is an identity. We define $w(x,y,z)$ as before and obtain the more general relation

$$w_0w_2\ldots w_{m-2} = w_1w_3\ldots w_{m-1}$$

which is also an identity. We may replace $w_0 = w$ by Q and since

$$Q \mid Q_1 Q_3 \dots Q_{m-1}$$

either $Q = Q_i$ for some i and the coefficients of Q lie in some subfield or Q splits into linear factors and Q is degenerate. In both of these cases, we get a contradiction. ■

Theorem 3.10.6 ([8])
If $\mathcal{F}$ is a semifield flock of a quadratic cone in $\mathrm{PG}(3, q^n)$, and $q \geq 4n^2 - 8n + 2$, then $\mathcal{F}$ is linear or of Kantor type.

Proof. Let $\mathcal{F}$ be a semifield flock of a quadratic cone in $PG(3, q^n)$, with kernel $GF(q)$. If q is even then all semifield flocks are linear, see e.g. [41]. If $n = 1, 2$, then by Theorem 3.10.1, $\mathcal{F}$ is linear or of Kantor type. If $n \geq 3$ and q is odd, the result follows from the last theorem. ■

For q odd, this yields the following corollary.

Corollary 3.10.7 *If $\mathcal{E}$ is a good egg of $\mathrm{PG}(4n-1, q)$, q odd, and $q \geq 4n^2 - 8n + 2$ then $\mathcal{E}$ is classical or a Kantor pseudo-ovoid.*

If we restrict ourselves to the case $n = 3$, the above results imply the following theorem.

Theorem 3.10.8 *If $\mathcal{E}$ is a good egg of $\mathrm{PG}(11, q)$, q odd, then $\mathcal{E}$ is classical or a Kantor pseudo-ovoid.*

Proof. If $q < 14$ the result follows from Theorem 3.10.2. If $q \geq 14$ the result follows from the above corollary. ■

3.11 Classification of eggs in PG(7, 2)

The TGQ $Q(5, 2)$ is the unique GQ of order $(2, 4)$, and the TGQ $Q(5, 3)$ is the unique GQ of order $(3, 9)$, [60]. In this section, we show by computer that classical GQ $Q(5, 4)$ is the unique TGQ of order $(4, 16)$. This is based on the classification of eggs in PG(7, 2). The fundamental, underlying, computer-based result is the following lemma.

Lemma 3.11.1 ([44])
Let $\mathcal{E}$ be an egg of $\mathrm{PG}(7, 2)$, and H be a hyperplane containing no tangent space to $\mathcal{E}$. Then H contains 5 elements of $\mathcal{E}$ which span a 5-space.

Proof. By Theorem 3.3.4, H contains 5 elements of $\mathcal{E}$. We must show that these span a 5-space. The stabiliser of H in $\mathrm{PGL}(8, 2)$ is transitive on unordered triples of lines of H spanning a 5-space. It has two orbits on unordered quadruples of lines of H, any triple of which span a 5-space, namely, those which span a 5-space and those which span H. It has at most three orbits on ordered quintuples of lines of H, any triple of which span a 5-space, and such that the quintuple spans H. We must show that such quintuples cannot be the set of lines of $\mathcal{E}$ in H. We use the tangent spaces to $\mathcal{E}$ to do this. Since H contains no tangent space to $\mathcal{E}$, each tangent space to $\mathcal{E}$ must meet H in a 4-space. Considering each of the three possible quintuples of lines in turn, we find that each has one line lying on four 4-spaces disjoint from the remaining 4 lines, and the other 4 lines lie on two 4-spaces disjoint from the other lines. Thus there are 64 possible tangent structures on intersection with H. Using the fact that the remaining 12 lines of $\mathcal{E}$ meet H in a point on no tangent space to $\mathcal{E}$,and on no transversal line to a pair of elements of the quintuple, we can rule out all but one of the quintuples, and only 6 possible tangent structures survive for that quintuple, each of which leaves 14 possible candidates for the 12 points. Finally, these 6 possibilities can be eliminated by noting that there must be no lines joining 2 of the 12 points and meeting an element of the quintuple. ■

Theorem 3.11.2 ([44])
If $\mathcal{E}$ is a pseudo-ovoid of $PG(7, 2)$, then $\mathcal{E}$ is classical.

Proof. By the Lemma above, each $\mathrm{PG}(5, 2)$ containing 3 elements of $\mathcal{E}$ contains exactly 5 elements of $\mathcal{E}$. This implies that $\mathcal{E}$ is good at every element. The result follows from Theorem 3.9.1. ■

Equivalently we have the following.

Theorem 3.11.3 ([44])
There is a unique translation generalized quadrangle of order $(4, 16)$, namely, the classical generalized quadrangle $Q(5, 4)$.

Bibliography

[1] R. W. Ahrens, G. Szekeres; On a combinatorial generalization of 27 lines associated with a cubic surface. *J. Austral. Math. Soc.* **10** (1969), 485–492.

[2] Laura Bader, Guglielmo Lunardon, Ivano Pinneri; A new semifield flock. *J. Combin. Theory Ser. A* **86** (1999), no. 1, 49–62.

[3] Laura Bader, Dina Ghinelli, Tim Penttila On Monomial Flocks. Preprint.

[4] S. Ball; Polynomials in finite geometries. Surveys in combinatorics, 1999 (Canterbury), 17–35, *London Math. Soc. Lecture Note Ser.*, **267**, Cambridge Univ. Press, Cambridge, 1999.

[5] S. Ball; On intersection sets in Desarguesian affine spaces. *European J. Combin.* **21** (2000), no. 4, 441–446.

[6] S. Ball; On nuclei and blocking sets in Desarguesian spaces. *J. Combin. Theory Ser. A* **85** (1999), no. 2, 232–236.

[7] Simeon Ball, Aart Blokhuis, Michel Lavrauw; Linear $(q+1)$-fold blocking sets in $PG(2, q^4)$. *Finite Fields Appl.*, **6** (2000), no. 4, 294–301.

[8] Simeon Ball, Aart Blokhuis, Michel Lavrauw; On the classification of semifield flocks. Preprint.

[9] Simeon Ball, Aart Blokhuis, Christine M. O'Keefe; On unitals with many Baer sublines. *Des. Codes Cryptogr.* **17** (1999) no. 1-3, 237–252.

[10] A. Barlotti; *Some topics in finite geometrical structures.* Institute of Statistics Mimeo Series, no. 439, University of North Carolina, 1965.

[11] A. Barlotti, J. Cofman; Finite Sperner spaces constructed from projective and affine spaces. *Abh. Math. Sem. Univ. Hamburg* **40** (1974), 230–241.

[12] A. Beutelspacher, J. Ueberberg; A characteristic property of geometry t-spreads in finite projective spaces. *European J. Combin.* **12** (1991), 277-281.

[13] I. Bloemen, J. A. Thas, H. Van Maldeghem; Translation ovoids of generalized quadrangles and hexagons. *Geom. Dedicata* **72** (1998), no. 1, 19–62.

[14] A. Blokhuis; On multiple nuclei and a conjecture of Lunelli and Sce. *Bull. Belg. Math. Soc. Simon Stevin* **3** (1994), 349–353.

[15] A. Blokhuis; Blocking sets in Desarguesian planes. *Combinatorics, Paul Erdős is Eighty, Vol. 2 (Keszthely, 1993)*, 133–155, Bolyai Soc. Math. Stud., **2**, *János Bolyai Math. Soc., Budapest*, 1996.

[16] A. Blokhuis; Blocking sets in finite projective and affine planes. *Intensive course on Galois Geometry and Generalized Polygons*, University of Ghent, 14-25 April 1998.
http://cage.rug.ac.be/ fdc/intensivecourse/intensivecourse_final.html.

[17] A. Blokhuis, L. Storme T. Szőnyi; Lacunary polynomials, multiple blocking sets and Baer subplanes. *J. London Math. Soc.* (2) **60** (1999), no. 2, 321–332.

[18] Aart Blokhuis, Michel Lavrauw; Scattered spaces with respect to a spread in $\mathrm{PG}(n, q)$. *Geom. Dedicata* **81** (2000), no. 1-3, 231–243.

[19] Aart Blokhuis, Michel Lavrauw; On two-intersecion sets. Preprint.

[20] R. C. Bose; Mathematical theory of the symmetrical factorial design. *Sankhya* **8** (1947), 107–166.

[21] R. C. Bose, J. W. Freeman and D. G. Glynn; On the intersection of two Baer subplanes in a finite projective plane. *Utilitas Math.* **17** (1980), pp. 65–77.

[22] Aiden A. Bruen; Arcs and multiple blocking sets. *Symposia Mathematica, Vol. XXVIII (Rome, 1983)*, 15–29, Sympos. Math., XXVIII, *Academic Press, London*, 1986.

[23] A. A. Bruen; Polynomial multiplicities over finite fields and intersection sets. *J. Combin. Theory Ser. A* **60** (1992), no. 1, 19–33.

[24] Matthew Brown; (Hyper)ovals and ovoids in projective spaces. *Socrates Intensive Course Finite Geometry and its Applications Ghent*, 3-14 April 2000, lecture notes. Available from
http://cage.rug.ac.be/ fdc/intensivecourse2/brown_2.pdf

[25] F. BUEKENHOUT; *Handbook of incidence geometry. Buildings and foundations.* Edited by F. Buekenhout. North-Holland, Amsterdam, 1995. xii+1420 pp. ISBN: 0-444-88355-X

[26] P. J. CAMERON; Projective and Polar spaces. Queen Mary & Westfield College math notes 13.

[27] R. CALDERBANK, W. M. KANTOR; The geometry of two-weight codes. *Bull. London Math. Soc.* **18** (1986), 97–122.

[28] L. R. CASSE, C. M. O'KEEFE; Indicator sets for t-spreads of $PG((s+1)(t+1)-1,q)$. *Boll. Un. Mat. Ital. B (7)* **4** (1990), 13–33.

[29] L. R. A. CASSE, J. A. THAS, P. R. WILD; (q^n+1)-sets of $\mathrm{PG}(3n-1,q)$, generalized quadrangles and Laguerre planes. *Simon Stevin* **59** (1985), no. 1, 21–42.

[30] BILL CHEROWITZO; Hyperoval page. http://www-math.cudenver.edu/ wcherowi/research/hyperoval/hyindex.htm

[31] STEPHEN D. COHEN, MICHAEL J. GANLEY; Commutative semifields, two-dimensional over their middle nuclei. *J. Algebra* **75** (1982), no. 2, 373–385.

[32] P. DEMBOWSKI; *Finite geometries.* Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44 Springer-Verlag, Berlin-New York 1968 xi+375 pp.

[33] DANIEL FROHARDT; Groups which produce generalized quadrangles. *J. Combin. Theory Ser. A* **48** (1988), no. 1, 139–145.

[34] MICHAEL J. GANLEY; Central weak nucleus semifields. *European J. Combin.* **2** (1981), no. 4, 339–347.

[35] MARSHALL HALL, JR.; Affine generalized quadrilaterals. 1971 *Studies in Pure Mathematics (Presented to Richard Rado)* pp. 113–116 *Academic Press, London*

[36] U. HEIM; Proper blocking sets in projective spaces. *Discrete Math.* **174** (1997), 167–176.

[37] J. W. P. HIRSCHFELD; *Projective geometries over finite fields.* Second edition. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1998. xiv+555 pp. ISBN: 0-19-850295-8.

[38] J. W. P. HIRSCHFELD, J. A. THAS; *General Galois geometries.* Oxford Mathematical Monographs. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1991. xiv+407 pp. ISBN: 0-19-853537-6

[39] J. W. P. Hirschfeld; *Finite projective spaces of three dimensions.* Oxford Mathematical Monographs. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1985. x+316 pp. ISBN: 0-19-853536-8

[40] V. Jha, N. L. Johnson; On the ubiquity of translation ovals in generalised André planes. *Annals Discrete Math.* **52** (1992), 279–296.

[41] N. L. Johnson; Semifield flocks of quadratic cones. *Simon Stevin* **61** (1987), no. 3-4, 313–326.

[42] William M. Kantor; Generalized quadrangles associated with $G_2(q)$. *J. Combin. Theory Ser. A* **29** (1980), no. 2, 212–219.

[43] William M. Kantor; Some generalized quadrangles with parameters q^2, q. *Math. Z.* **192** (1986), no. 1, 45–50.

[44] Michel Lavrauw, Tim Penttila; On eggs and translation generalised quadrangles. *J. Combin. Theory Ser. A*. To appear.

[45] Michel Lavrauw; On semifield flocks, eggs and ovoids of $Q(4, q)$. Preprint.

[46] Maska Law, Tim Penttila; some flocks in characteristic 3. *J. Combin. Th. (A)*, to appear.

[47] Monique Limbos; A characterisation of the embeddings of PG(m, q) into PG(n, q^r). *J. Geom.* **16** (1981), no. 1, 50–55.

[48] Guglielmo Lunardon; Flocks, ovoids of Q$(4, q)$ and designs. *Geom. Dedicata* **66** (1997), no. 2, 163–173.

[49] Guglielmo Lunardon; Normal spreads. *Geom. Dedicata* **75** (1999), no. 3, 245–261.

[50] G. Lunardon,; O. Polverino; Blocking sets of size $q^t + q^{t-1} + 1$. *J. Combin. Theory Ser. A* **90** (2000), no. 1, 148–158.

[51] G. Lunardon, J. A. Thas; Finite Generalized Quadrangles. Lecture notes, *Intensive Course on Galois Geometry and Generalized Polygons*, (1998),
http://cage.rug.ac.be/ fdc/intensivecourse/intensivecourse_final.html.

[52] C. M. O'Keefe; Ovoids in $PG(3, q)$: a survey. *Discrete Math.* **151** (1996), no. 1-3, 175–188.

[53] Christine M. O'Keefe, Tim Penttila; Ovoids of PG$(3, 16)$ are elliptic quadrics. *J. Geom.* **38** (1990), no. 1-2, 95–106.

[54] Christine M. O'Keefe, Tim Penttila; Ovoids of PG(3, 16) are elliptic quadrics. II. *J. Geom.* **44** (1992), no. 1-2, 140–159.

[55] Christine M. O'Keefe, Tim Penttila, Gordon F. Royle; Classification of ovoids in PG(3, 32). *J. Geom.* **50** (1994), no. 1-2, 143–150.

[56] Stanley E. Payne; Nonisomorphic generalized quadrangles. *J. Algebra* **18** (1971), 201–212.

[57] Stanley E. Payne; Generalized quadrangles as group coset geometries. *Proceedings of the Eleventh Southeastern Conference on Combinatorics, Graph Theory and Computing (Florida Atlantic Univ., Boca Raton, Fla., 1980)*, Vol. II. Congr. Numer. **29** (1980), 717–734.

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

[59] Stanley E. Payne; An essay on skew translation generalized quadrangles. Geom. Dedicata **32** (1989), no. 1, 93–118.

[60] S. E. Payne, J. A. Thas; *Finite generalized quadrangles.* Research Notes in Mathematics, 110. Pitman (Advanced Publishing Program), Boston, MA, 1984. vi+312 pp. ISBN 0-273-08655-3

[61] Tim Penttila; Translation generalised quadrangles and elation Laguerre planes of order 16. European J. Combin., to appear.

[62] T. Penttila, G. F. Royle; Sets of type (m, n) in the affine and projective planes of order nine. *Des. Codes Cryptogr.* **6** (1995), no. 3, 229–245.

[63] Tim Penttila, Gordon F. Royle; BLT-sets over small fields. *Australas. J. Combin.* **17** (1998), 295–307.

[64] Tim Penttila, Blair Williams; Ovoids of parabolic spaces. *Geom. Dedicata* **82** (2000), no. 1-3, 1–19.

[65] Pompeo Polito, Olga Polverino; On small blocking sets. *Combinatorica* **18** (1998), no. 1, 133–137.

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

[67] S. Roman; *Field theory.* Graduate Texts in Mathematics, 158. Springer-Verlag, New York, 1995. xii+272 pp. ISBN: 0-387-94407-9; 0-387-94408-7.

[68] Beniamino Segre; Sulle ovali nei piani lineari finiti. (Italian) *Atti Accad. Naz. Lincei. Rend. Cl. Sci. Fis. Mat. Nat.* (8) **17**, (1954). 141–142.

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

[70] B. Segre; Teoria di Galois, fibrazioni proiettive e geometrie non Desarguesiane. *Ann. Mat. Pura Appl.* **64** (1964), 1–76.

[71] E. Seiden; A theorem in finite projective geometry and an application to statistics. *Proc. Amer. Math. Soc.* **1** (1950), 282–286.

[72] W. M. Schmidt; *Equations over Finite Fields*, Lecture Notes in Mathematics 536, Springer, 1976.

[73] 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** (1971), 459–532.

[74] J. A. Thas; Geometric characterization of the $[n-1]$-ovaloids of the projective space $\mathrm{PG}(4n-1, q)$. *Simon Stevin* **47** (1973/74), 97–106.

[75] J. A. Thas; Generalized quadrangles and flocks of cones. *European J. Combin.* **8** (1987), no. 4, 441–452.

[76] J. A. Thas; Generalized quadrangles of order (s, s^2). I. *J. Combin. Theory Ser. A* **67** (1994), 140–160.

[77] J. A. Thas; Generalized quadrangles of order (s, s^2). II. *J. Combin. Theory Ser. A* **79** (1997), 223–254.

[78] J. A. Thas; Generalized quadrangles of order (s, s^2). III. *J. Combin. Theory Ser. A* **87** (1999), 247–272.

[79] J. A. Thas; Translation generalized quadrangles of order (s, s^2), s even, and eggs. Preprint.

[80] J. A. Thas; TGQs and eggs. *Seminar on Incidence Geometry*, Department of Pure Mathematics and Computer Algebra, Ghent University. March 30, 2001.

[81] J. A. Thas, C. Herssens, F. De Clerck; Flocks and partial flocks of the quadratic cone in $\mathrm{P}G(3, q)$. Finite geometry and combinatorics (Deinze, 1992), 379–393, *London Math. Soc. Lecture Note Ser.*, **191**, Cambridge Univ. Press, Cambridge, 1993.

[82] J. A. Thas, S. E. Payne; Spreads and ovoids in finite generalized quadrangles. *Geom. Dedicata* **52** (1994), no. 3, 227–253.

[83] Thas, J. A., Van Maldeghem, H.; The classification of finite generalized quadrangles admitting a group acting transitively on ordered pentagons. *J. London Math. Soc.* (2) **51** (1995), no. 2, 209–218.

[84] Tits, J.; Sur la trialité et certains groupes qui s'en déduisent. *Inst. Hautes Etudes Sci. Publ. Math.* **2** (1959), 14–60.

[85] Tits, J.; Les goupes simples de Suzuki et de Ree, *Seminaire Bourbaki*, 3e année, no. 210 (1960).

[86] H. Van Maldeghem; *Generalized Polygons.* Monographs in Mathematics, 93. Birkhuser Verlag, Basel, 1998. xvi+502 pp. ISBN: 3-7643-5864-5.

[87] M. Walker; A class of translation planes. *Geom. Dedicata*, **5** (1976), 135–146.

[88] P. Wild; Higher-dimensional ovals and dual translation planes. *Ars Combin.* **17** (1984), 105–112.

Index

Acknowledgement

Amongst the many people who I had the pleasure of working with during my years of research as a PhD student I want to thank some of them by name. First of all I want to thank my supervisor Aart Blokhuis, Professor at Eindhoven University of Technology, who was always willing to listen to my problems and was able to give me a lot of good ideas. The second chapter is more or less summarizing the research I did during the first two years of my PhD and most of this work was done jointly with Aart. I am also indebted to my visiting supervisor during my stay in Perth, Tim Penttila, Professor at the University of Western Australia, who was able to guide me, in the short period of six months, towards some very interesting problems in the theory of translation generalized quadrangles. Many of the ideas that lie at the base of the third chapter are of his hand. I am very grateful to my friend and colleague Simeon Ball of the University of London, who was a research fellow at Eindhoven University of Technology during the first two years of my PhD, for his ideas and co-operation, for stimulating me at all times, and for his reading of (part of) the original manuscript. Thanks are also due to my colleagues and friends Matthew Brown for his time spent on reading several parts of my thesis, and his very helpful comments, and Maska Law for the many pleasant hours discussing mathematics. Finally, it is a great pleasure to acknowledge the friendly and efficient help I received from Frank De Clerck, Professor at Ghent University, during the creation of my thesis.

I thank NWO for their financial support. I thank the departments of mathematics and its members at Eindhoven University of Technology, at the University of Western Australia, and at Ghent University for a very enjoyable stay.

Nederlandse samenvatting

Dit proefschrift kan beschouwd worden als bestaande uit twee delen, die beide afzonderlijk kunnen gelezen worden. Het eerste deel behandeldt verstrooide deelruimte ("scattered spaces") ten opzicht van een spreiding ("spread") in een eindige projectieve ruimte. Het tweede deel is gesitueerd in de theorie van de veralgemeende vierhoeken en de equivalente zogenaamde eieren ("eggs") in eindige projectieve ruimten. Daartegenover staat echter dat de onderwerpen die in beide delen behandeld worden, deelstructuren zijn van Galois ruimten, en dus vanuit dit oogpunt dicht bij elkaar liggen.

In hoofdstuk 1 worden enkele definities en fundamentele resultaten uit de incidentie meetkunde en de eindige projectieve meetkunde bijeen gebracht als basis voor de volgende hoofdstukken.

Hoofstuk 2 behandeld verstrooide deelruimten ten opzichte van een spreiding in een eindige projectieve ruimte. Een *spreiding* is een verdeling van de punten van een projectieve ruimte in deelruimten van gelijke dimensie en een deelruimte wordt *verstrooid* genoemd ten opzichte van een spreiding indien ze elk element van de spreiding in ten hoogste 1 punt snijdt. Eerst beschouwen we willekeurige spreidingen en leiden een bovengrens af voor de dimensie van een verstrooide deelruimte. Als de dimensie van een verstrooide deelruimte deze bovengrens bereikt, dan wordt de verstrooide deelruimte *maximaal* genoemd. Een constructie van verstrooide deelruimten leidt tot een ondergrens voor de dimensie van een maximale verstrooide deelruimte. Daarna beperken we ons tot Desarguaanse spreidingen en we verbeteren de bovengenoemde grenzen. Indien de elementen van de spreiding even dimensie hebben en de projectieve ruimte, waarvan ze een spreiding vormen, oneven dimensie heeft, dan zijn deze grenzen scherp. Het blijkt bovendien dat maximale verstrooide deelruimten ten opzicht van Desarguaanse spreidingen twee-intersectie verzamelingen ten opzichte van hypervlakken induceren in een projectieve ruimte van lagere dimensie over een lichaamsuitbreiding en we bewijzen dat de verkregen twee-intersectie verzamelingen nieuw zijn. Daarna wordt de theorie van verstrooide deelruimten toegepast op de theorie der blokkeer-verzamelingen ("blocking sets") en we geven de constructie van zulke blokkeer-verzamelingen gebruik makende van verstrooide ruimten. Op het einde van het hoofdstuk geven we nog twee expliciete constructies van verstrooide deelruimten, één met behulp van de techniek "veeltermen in eindige meetkunde" en één gebruik makende van de representatie van spreidingen in het tensor produkt van twee vector ruimten, zoals uitgelegd in het eerste hoofdstuk. De geconstrueerde blokkeer-verzamelingen zijn van belang in verband met een resultaat van Blokhuis, Storme en Szőnyi.

In het derde hoofdstuk gaan we wat dieper in op de theorie der eieren, welke equivalent is met de theorie der translatie veralgemeende vierhoeken ("translation generalized quadrangles"). We geven een nieuw model voor eieren in projectieve ruimten over eindige lichamen van oneven karakteristiek en gebruik makende van dat model zijn we in staat een kort bewijs te leveren voor een belangrijk resultaat van Thas (bewezen in een algemenere context). In het tweede deel van het hoofdstuk bestuderen we ovoiden van de veralgemeende vierhoek korresponderend met een niet-singuliere parabolische kwadriek in een eindige vier-dimensionale projectieve ruimte over een eindig lichaam van oneven karakteristiek. Het hoofdresultaat in deze paragraaf leidt tot een nieuwe methode om een goed ei te construeren en een onmiddellijk gevolg daarvan is een karakterisatie van de eieren van Kantor type. We geven ook een overzicht van alle gekende voorbeelden gebruik makende van het nieuw model voor eieren, samen met hun duale. Daarna geven we een recent resultaat in verband met de classificatie van goede eieren in projectieve ruimten over een eindig lichaam van oneven karakteristiek en we eindigen het hoofdstuk met de classificatie van eieren in de zeven-dimensionale projective ruimte over het lichaam met twee elementen.

Curriculum Vitae

Michel Lavrauw was born in Izegem on December 2, 1974. He did his undergraduate and graduate studies in mathematics at Ghent University, with Finite Geometry as main subject, and was awarded his degree in Pure Mathematics with Great Distinction in 1996 with a thesis on Knot Theory under the supervision of Prof. Dr. W. Mielants. In 1997 he got a position as a PhD student at Eindhoven University of Technology under the supervision of Prof. Dr. A. Blokhuis, employed by NWO. During the first years of his PhD he got acquainted with polynomial techniques applied to Finite Geometry, and in collaboration with Aart Blokhuis and Simeon Ball this led to several publications with results on blocking sets and scattered subspaces with respect to a spread in finite projective spaces. In 2000 he spent the first 6 months at the University of Western Australia, where he worked on problems related to translation generalized quadrangles and the equivalent theory of the so-called eggs of projective spaces, under the supervision of Prof. Dr. T. Penttila who is a leading expert in generalized quadrangles. A joint paper with Tim Penttila led to further research in the theory of eggs, obtaining significant results on the classification of semifield flocks, with Aart Blokhuis and Simeon Ball, and on the relation between semifield flocks, eggs and ovoids of the classical generalized quadrangle arising from a non-degenerate quadric in a four-dimensional projective space over a finite field with odd characteristic.