Faculteit Wetenschappen
Vakgroep Zuivere Wiskunde en Computeralgebra

Blocking sets

in finite projective spaces and coding theory

Geertrui Van de Voorde

Promotoren:
Dr. M. Lavrauw
Prof. Dr. L. Storme

Proefschrift voorgelegd aan
de Faculteit Wetenschappen
tot het behalen van de graad van
Doctor in de Wetenschappen
richting Wiskunde

Preface

The book in front of you represents my work as a PhD student. Using the word 'work' in this context is not really appropriate. During the past three years, I never had the feeling to 'work', but rather to play around with various structures, to have fun trying to prove theorems and to enjoy discovering just a tiny bit of the enormous mathematical world.

This thesis is a structured way of telling you about some new and old results, discovered -or created- in this ever expanding mathematical universe. As the title suggests, most of the subjects treated in this thesis are closely related to blocking sets in a finite projective space.

Obviously, these results were not found in a nice structured way, so instead of summarising the contents chapter by chapter, I provide an overview of the journey that led to each of these chapters.

In the very beginning, there was my master thesis, entitled 'Codewords of small weight in linear codes'. I used the book of Assmus and Key to learn about the code of points and lines of a projective plane. Soon Leo Storme, who was the advisor of my master thesis too, recognised that the theory of blocking sets could be useful for the study of codewords of small weight in these codes. The link with blocking sets was not new, but it had never been shown that these particular blocking sets were minimal. This observation led us to an easier view on the codewords of small weight. As a highlight, we used the classification of small minimal blocking sets in $\mathrm{PG}(2,p)$, $\mathrm{PG}(2,p^2)$ and $\mathrm{PG}(2,p^3)$ to show that there was a gap in the weight enumerator of the code of points and lines in these particular planes.

In my first year as a PhD student, Leo and I started to develop similar techniques for higher dimensions. One of the first lemmas we needed was a unique reducibility result for blocking sets, which we proved using Rédei polynomials. Rédei polynomials provide a very useful tool to study blocking sets, for example, they were used by Szőnyi to prove a $1 \bmod p$ result. The $1 \bmod p$ result and some bounds on the size of a small minimal blocking set arising from it can be found in CHAPTER 2, together with the unique reducibility result for k-blocking sets.

At a certain point, linear blocking sets attracted our attention and we asked Michel

Lavrauw, who would become my second advisor, for help with this kind of blocking sets. I remember sitting together with Leo in Michels office, when Michel summarised possible ways to attack our coding theoretical problem on the blackboard. One of the items stated: 'prove the linearity conjecture', immediately followed by '(ambitious)'. This was the first time I heard about this conjecture, and it intrigued me ever since.

We extended the code of points and lines in a projective plane to the code of points and k-spaces of a projective space and proved that there is a gap in the weight enumerator of these codes, provided that the linearity conjecture holds. For the dual code, we extended results of Sachar in the planar case to general dimension. Moreover, also here, we were able to exploit our knowledge on blocking sets to derive a new upper bound on the minimum weight of the dual code.

After more than a year, Leo got back from a visit to Peter Sziklai, and told us that Peter and he could avoid the linearity conjecture to prove that there is a gap in the weight enumerator of the code of points and lines of a projective plane of arbitrary order. We extended this proof to higher dimensions. The results on the code of points and k-spaces can be found in CHAPTER 6.

But before that, Valentina Pepe, from the University of Naples, was visiting Ghent for three months. Valentina, Leo and I studied the LDPC codes arising from linear representations. The results of this research can be found in CHAPTER 7.

After that, Leo told me he had a nice problem: the linearity conjecture in projective spaces with order the square of a prime. Using the equivalent definition of linear sets via spreads, Michel and I started working on this problem. But it turned out to be much more complicated than we -at least I- thought. I learned a lot while trying to prove lemmas and theorems in this spread representation. We were close to giving a proof when we discovered that the result we were trying to prove was already found and published by Zsuzsa Weiner. The next open case was the linearity conjecture for k-blocking sets in spaces of order the cube of a prime. It made sense to work on this particular case, since Leo and Zsuzsa proved it already for 1-blocking sets, which opened the door for a proof by induction on k. Proving the linearity conjecture in this particular case became my new research goal, but it turned out to be even harder than the previous case, so Leo gave me some other problems to work on.

In the beginning of 2008, Leo started working on partial covers of a projective space while Stefan Dodunekov was visiting our department. I got involved in the study of these sets because they have a lot in common with blocking sets; in fact partial

covers are dual 'almost' blocking sets. Moreover, it was nice to be working on a problem that gave results; they can be found in CHAPTER 5. Somewhat later, Valentina was visiting our department for the second time, and Valentina, Leo and I decided to continue our research on LDPC codes. This time, we investigated the dual codes from polar spaces; all results can be found in CHAPTER 7.

In the meantime, the linearity conjecture kept puzzling me. I had a lot of bad ideas and performed numerous worthless calculations. But by the beginning of July 2008, Michel and I came up with a proof for our particular case. It took Leo, Michel and I a few more months to write everything down in a nice and readable way and to extend this proof to a characterisation of small point sets in $\mathrm{PG}(n, q^3)$ meeting every $(n-k)$-space in $1 \bmod q$ points. In CHAPTER 4, we give an overview of what is presently known about the linearity conjecture, including this proof. It's worth noticing that the ideas of the proof in Chapter 4 also prove the result for the case $\mathrm{PG}(n, p^2)$ found by Zsuzsa.

For the proof of the linearity conjecture in $\mathrm{PG}(n, p^3)$, we needed more information on the intersection of a linear set and a subline. This question gave rise to a lot of other open problems concerning linear sets and I spent almost all of 2009 working on these topics. It took me some time to get a grip on the different views of linear sets and at first there was very little progress; most of the arguments were lengthy calculations that did not show much insight. But after Michel gave a very easy geometric proof for the intersection problem of a subline and a linear set of rank 3, some of the pieces of the puzzle fell into place: I managed to extend this proof to general rank and proved some results on irregular sublines.

After three years of refusing to learn to work with the computer program GAP [61], I finally got persuaded. It turned out that a few days of swearing and cursing at my MacBook and bothering Michel and Jan De Beule with stupid questions were sufficient to learn the basics. Using FinInG, I calculated some intersections of linear sets and discovered that unexpected things happen with the representation of $\mathbb{F}_q$-linear sets in a space over a field of order q^3. When writing up what we knew about these linear sets, Michel noticed that we did not yet give a proof for the correspondence between the different views of isomorphic linear sets, which we had used throughout most of our arguments on the equivalence problem. From the hours it took us to prove this correspondence, I have learned never to say 'Isn't that trivial?' again. CHAPTER 3 deals with the equivalence problem, the intersection problem and the representation problem for linear sets. Most of the general cases of these kinds of questions for linear sets are still wide open, and it would be nice to solve some of them in the future.

This research was supported by grants from

'Bijzonder Onderzoeksfonds UGent' (BOF),
01/10/2006-31/12/2006

'Agentschap voor Innovatie door Wetenschap en Technologie-Vlaanderen' (IWT),
01/01/2007-30/09/2008

'Fonds Wetenschappelijk Onderzoek-Vlaanderen' (FWO),
01/10/2008-30/09/2010

Contents

1

Preliminaries

It is the glory of geometry
that from so few principles
it is able to accomplish so much.

– –Isaac Newton

In this chapter, the (few) principles needed to understand this thesis will be explained. Most of what follows is standard and can be found in [74] by Hughes and Piper, [47] by Dembowski, [71, 72] by Hirschfeld, in [73] by Hirschfeld and Thas, in [114] by Payne and Thas, or in the *Handbook of Incidence Geometry* [35]. More information and background on coding theory can be found in the book of MacWilliams and Sloane [100]. All of these references provide background on a lot more material than treated here.

The book [44] will provide up-to-date surveys on particular research topics in finite projective spaces. Of relevance for this thesis are the chapters *Blocking sets* by Blokhuis, Sziklai and Szőnyi, *Substructures of finite classical polar spaces* by De Beule and Klein, *LDPC codes and Galois geometries*, by Greferath, Roessing and Storme, and *Finite Semifields* by Lavrauw and Polverino.

1.1 Incidence structures and projective spaces

1.1.1 Incidence structures

In this chapter, projective spaces, generalised quadrangles, linear representations and polar spaces will be introduced. These all are examples of *incidence structures*. Although in this thesis, we never work with a general incidence structure, it is worthwhile to give the general definition for incidence structures in order to introduce certain notions all at once.

An *incidence structure* $\mathcal{I}$ is a triple $(\mathcal{P}, \mathcal{B}, \mathrm{I})$, where $\mathcal{P}$ is a set of elements called *points* and $\mathcal{B}$ is a set of elements called *blocks* or *lines*, and $I \subseteq (\mathcal{P}\times\mathcal{B})\cup(\mathcal{B}\times\mathcal{P})$ is a symmetric relation, called *incidence relation*. For our purposes, a block will always be a set of points. If $(P, B) \in \mathrm{I}$, we say that P is *incident* with B, that P *is on* B, that B *contains* P or that B *goes through* P. If we call the elements of the set $\mathcal{B}$ lines, then we say that points that lie on the same line are *collinear* points, and lines that go through the same point are *concurrent* lines.

The *dual* of an incidence structure $\mathcal{I} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ is $\mathcal{I}^D = (\mathcal{B}, \mathcal{P}, \mathrm{I})$.

1.1.2 Projective spaces over finite fields

Let $\mathbb{F}_q$ denote the finite field with q elements where $q = p^h$, p prime, $h \geq 1$. Throughout this thesis, the symbols q, p and h will always be used in this sense. Let $\mathrm{V}(n+1, q)$ denote the vector space of *rank* $n+1$ over $\mathbb{F}_q$, i.e., $\mathrm{V}(n+1, q) = \mathbb{F}_q^{n+1}$. The *projective space* corresponding to $\mathrm{V}(n+1, q)$ (i.e. the space $\mathrm{V}(n+1, q) \setminus \{0\}/\sim$, where $(x_0, \ldots, x_n) \sim (\lambda x_0, \ldots, \lambda x_n)$, $\forall \lambda \in \mathbb{F}_q \setminus \{0\}$) is denoted by $\mathrm{PG}(n, q)$.

Using the definition, we see that the number of points in $\mathrm{PG}(n, q)$ equals the number of vector lines in $\mathrm{V}(n+1, q)$. This number is equal to $(q^{n+1}-1)/(q-1)$ and will be denoted by θ_n. The *Gaussian coefficient* $\begin{bmatrix} n \\ k \end{bmatrix}_q$ denotes the number of vector spaces of rank k in $\mathrm{V}(n, q)$, or equivalently, the number of $(k-1)$-dimensional subspaces in $\mathrm{PG}(n-1, q)$, i.e.,

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

The subspaces of $\mathrm{PG}(n,q)$ of dimension $0,1,2,3$ and $n-1$ are called *points, lines, planes, solids*, and *hyperplanes*, respectively. A k-dimensional subspace is often called a *k-space*.

The *intersection* of two subspaces U and W of $\mathrm{PG}(n,q)$, denoted by $U \cap W$, is the subspace of $\mathrm{PG}(n,q)$ containing the points that are in both U and W. The *span* of two subspaces U and W of $\mathrm{PG}(n,q)$, denoted by $\langle U, W\rangle$, is the smallest subspace of $\mathrm{PG}(n,q)$ containing the points of U and W.

1.1.3 Axiomatic projective spaces

We can see $\mathrm{PG}(n,q)$ as the incidence structure with as point set $\mathcal{P}$ the vector spaces of rank 1 of $\mathrm{V}(n+1,q)$, as blocks $\mathcal{B}$ the vector spaces of rank 2 of $\mathrm{V}(n+1,q)$ and the natural incidence. It is easy to check that $\mathrm{PG}(n,q) = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ satisfies the following properties.

(A1) Through every two points, there is exactly one line.

(A2) If P, Q, R and S are distinct points and the lines PQ and RS intersect, then so do the lines PR and QS.

(A3) There are at least 3 points on each line.

A projective space can be defined axiomatically as a set $\mathcal{P}$ of points and a set $\mathcal{B}$ of subsets of $\mathcal{P}$, where we call the elements of $\mathcal{B}$ lines, that satisfy (A1)-(A2)-(A3). A *subspace* of the (axiomatic) projective space is a subset X, such that every line containing two points of X is a subset of X. The full space and the empty space are subspaces. The *dimension* of the space is said to be n if n is the largest number for which there is a strictly ascending chain of subspaces for which: $\varnothing = X_{-1} \subset X_0 \subset \cdots \subset X_n = \mathcal{P}$.

We will introduce a particular class of projective spaces: *Desarguesian* projective spaces. Two triangles $P_1P_2P_3$ and $R_1R_2R_3$, contained in a 2-dimensional space, are said to be *in perspective* if the lines P_1R_1, P_2R_2 and P_3R_3 are concurrent, say in the point S. A space is *Desarguesian* if for any two triangles $P_1P_2P_3$ and $R_1R_2R_3$ that are in perspective, the points $P_1P_2 \cap R_1R_2$, $P_1P_3 \cap R_1R_3$ and $P_2P_3 \cap R_2R_3$ are collinear. One can easily check that a projective space $\mathrm{PG}(n,q)$ is Desarguesian. It is shown by Veblen and Young [145] that a finite projective space of dimension $n \geq 3$ satisfying (A1)-(A2)-(A3) is

a projective space $\mathrm{PG}(n,q)$.[1] The Desarguesian spaces are precisely the spaces arising from a vector space over a division ring, a result that dates back to Hilbert [70]. In the finite case, using the famous theorem[2] of Wedderburn [102] which states that a finite division ring is a field, this yields that a finite Desarguesian projective space is necessarily a projective space $\mathrm{PG}(n,q)$.

The theorem of Veblen and Young does not include the case $n = 2$, i.e. the case of *projective planes*: there exist *non-Desarguesian* projective planes. In this thesis, *translation planes* and *Figueroa planes* will be introduced; they provide examples of non-Desarguesian planes. Many other examples of non-Desarguesian projective planes can be found in [74].

1.1.4 Affine spaces

Consider an n-dimensional projective space $\Pi = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ and a hyperplane H_∞ of Π. Let $\mathcal{P}'$ (resp. $\mathcal{B}'$) be the set of points (resp. lines) of $\mathcal{P}$ that are not contained in H_∞ and let I' be the restriction of I to $(\mathcal{P}' \times \mathcal{B}') \cup (\mathcal{B}' \times \mathcal{P}')$. The incidence structure $(\mathcal{P}', \mathcal{B}', \mathrm{I}')$ is an *n-dimensional affine space*. If the n-dimensional affine space is obtained from $\mathrm{PG}(n,q)$ in this way, we denote the affine space by $\mathrm{AG}(n,q)$. Every affine space can be extended to a projective space by adding a hyperplane H_∞ at infinity. If $\mathrm{AG}(n,q)$ is an affine space, extended by the hyperplane H_∞ to the projective space $\mathrm{PG}(n,q)$, then we say that the *point at infinity* of an affine line ℓ is the intersection of the projective line, containing all the points of ℓ, with H_∞. Similarly, one can define the *line, plane, k-space,...* at infinity of an affine plane, solid, $(k+1)$-space,..., respectively.

1.2 Collineations of $\mathrm{PG}(n,q)$

A *collineation* of $U \cong \mathrm{PG}(n,q)$ onto $V \cong \mathrm{PG}(n,q)$, $n \geq 2$, is a bijection between the points of U and the points of V preserving incidence. If $U = V$, a

[1] To be more precise, Veblen and Young showed that if (A1)-(A2)-(A3) hold and an extra axiom requiring the existence of two skew lines is satisfied, the incidence structure is a projective space $\mathrm{PG}(n,q)$, $n \geq 3$.

[2] Wedderburn's first 'proof' had a gap which went unnoticed at the time. Dickson provided the first valid proof of what's now universally known as Wedderburn's theorem. In [102], Wedderburn gives two other proofs for the theorem, using the method used by Dickson, and as Dickson claims: 'only after Wedderburn saw Dickson's proof' (see [112]).

collineation of U onto V is a *collineation of* U. The collineations of PG(n, q) with the operation of composition, form a group, denoted by PΓL$(n+1, q)$ and called the *collineation group* of PG(n, q).

Let A be a non-singular $(n+1) \times (n+1)$-matrix over $\mathbb{F}_q$, $n \geq 2$. The bijection between the points of $U \cong$ PG(n, q) and the points of $V \cong$ PG(n, q) induced by the map $x \mapsto Ax$ induces a collineation of U onto V, called a *projectivity* of U onto V. The group of all projectivities of PG(n, q) is the *projective (general) linear group* PGL$(n+1, q)$. If σ is an automorphism[3] of $\mathbb{F}_q$, then $x \mapsto x^\sigma$ is a collineation of U. The fundamental theorem of projective geometry states that every collineation is the composition of a projectivity with a collineation arising from an automorphism of $\mathbb{F}_q$. More formally, if τ is an element of PΓL$(n+1, q)$, then $\tau : x \mapsto Ax^\sigma$ for some non-singular matrix A and some automorphism σ of $\mathbb{F}_q$, and we write $\tau = (\sigma, A)$. When $n = 1$, we define PΓL$(2, q)$ to be the set of all invertible semi-linear maps $\tau : x \mapsto Ax^\sigma$ for some non-singular 2×2-matrix A, and we call every element of PΓL$(2, q)$ a collineation, analogously, the set of invertible linear maps $\tau : x \mapsto Ax$, with A some non-singular 2×2-matrix, is denoted by PGL$(2, q)$ and every element of PGL$(2, q)$ is called a projectivity.

The subsets $\mathcal{S}$ and $\mathcal{S}'$ of PG(n, q) are called *projectively equivalent* if and only if there is an element φ of PGL$(n+1, q)$ such that $\varphi(\mathcal{S}) = \mathcal{S}'$. Two subsets $\mathcal{S}$ and $\mathcal{S}'$ are called *isomorphic* if and only if there is an element φ of PΓL$(n+1, q)$ such that $\varphi(\mathcal{S}) = \mathcal{S}'$.

If we restrict the coordinates of the points of PG(n, q) with respect to a fixed basis to a subfield of $\mathbb{F}_q$, then we obtain a *subgeometry* of PG(n, q) and with respect to this fixed basis the subgeometry is called *canonical*. If $q = q_0^2$, then a subgeometry isomorphic[4] to PG(n, q_0) is called a *Baer subgeometry*.

Let π be a k-dimensional subspace of PG(n, q), $k \leq n-2$. We define the following incidence structure:

$\mathcal{P}$: set of $(k+1)$-dimensional subspaces of PG(n, q) through π,

$\mathcal{B}$: set of $(k+2)$-dimensional subspaces of PG(n, q) through π,

I : containment.

[3] The automorphism group of $\mathbb{F}_q$, where $q = p^h$, p prime, is the cyclic group of order h, generated by the automorphism $x \mapsto x^p$.

[4] In this definition, one may replace *isomorphic* with *projectively equivalent*, since a set isomorphic to a canonical subgeometry C is always projectively equivalent to C.

The geometry $(\mathcal{P}, \mathcal{B}, \mathrm{I})$ is called the *quotient geometry* of π, and we denote it by $\mathrm{PG}(n,q)/\pi$. Let μ be an $(n-k-1)$-dimensional space, skew to π. If we identify an element ρ of $\mathcal{P}$ or $\mathcal{B}$ with $\rho \cap \mu$, it follows that $\mathrm{PG}(n,q)/\pi \cong \mu = \mathrm{PG}(n-k-1,q)$.

The *dual* of a projective space $\mathcal{S}$, denoted by $\mathcal{S}^D$, is the incidence structure whose points and hyperplanes are the hyperplanes and points of $\mathcal{S}$, respectively.

A collineation of $U \cong \mathrm{PG}(n,q)$ onto its dual space U^D is called a *duality* and if this collineation has order 2, a *polarity*. The image of a subspace V under a polarity is denoted by $V^\perp$ and is called the *polar space of* V. If a subspace π is contained in $\pi^\perp$ or vice versa, then π is called *absolute*. If a subspace V is equal to its polar space $V^\perp$, the subspace is called *totally isotropic*.

There are four types of polarities (σ, A) of $\mathrm{PG}(n,q)$, listed below:

(i) $\sigma = 1$, q odd, $A = A^T$. In this case, the polarity (σ, A) is called an *orthogonal* polarity.

(ii) $\sigma = 1$, $A = -A^T$, and $a_{ii} = 0$ for all i. In this case, every point is an absolute point, n should be odd, and the polarity (σ, A) is called a *symplectic* polarity.

(iii) $\sigma = 1$, q even, $A = A^T$ and $a_{ii} \neq 0$ for some i. In this case, the polarity (σ, A) is called a *pseudo-polarity*.

(iv) $\sigma \neq 1$. In this case, $\sigma : x \mapsto x^{\sqrt{q}}$, q is a square, $A = A^{T\sigma}$ and (σ, A) is called a *Hermitian* or *unitary* polarity.

1.3 Polar spaces

Polar spaces were first described axiomatically by Veldkamp [146]. Other important contributors to the theory of (axiomatic) polar spaces, are Tits [143] and Buekenhout and Shult [36].

Let

$$Q(X_0, \ldots, X_n) = \sum_{i,j=0, i \leq j}^{n} a_{ij} X_i X_j$$

be a quadratic form over $\mathbb{F}_q$. A *quadric* $\mathcal{Q}$ in $\mathrm{PG}(n,q)$ is a set of points $P(X_0,\ldots,X_n)$ whose coordinates, with respect to a fixed basis, satisfy

$$Q(X_0,\ldots,X_n)=0.$$

Let q be a square and let

$$H(X_0,\ldots,X_n)=\sum_{i,j=0}^{n} a_{ij}X_iX_j^{\sqrt{q}}$$

with $a_{ij}=a_{ji}^{\sqrt{q}}$, be a Hermitian form over $\mathbb{F}_q$, q square. A *Hermitian variety* in $\mathrm{PG}(n,q)$, denoted by $\mathcal{H}(n,q)$, is a set of points $P(X_0,\ldots,X_n)$ whose coordinates, with respect to a fixed basis, satisfy $H(X_0,\ldots,X_n)=0$. A quadric or Hermitian variety of $\mathrm{PG}(n,q)$ is called *singular* if there exists a coordinate transformation which reduces the form to one in fewer variables, otherwise, the quadric or Hermitian variety is called *non-singular*.

If n is even, all non-singular quadrics in $\mathrm{PG}(n,q)$ are projectively equivalent to the quadric with equation $X_0^2+X_1X_2+\ldots+X_{n-1}X_n=0$. These quadrics are called *parabolic* and are denoted by $\mathcal{Q}(n,q)$. A non-singular quadric of $\mathrm{PG}(2,q)$ is called a *conic* of $\mathrm{PG}(2,q)$.

If n is odd, a non-singular quadric in $\mathrm{PG}(n,q)$ is either projectively equivalent to the quadric with equation $X_0X_1+\ldots+X_{n-1}X_n=0$ or to the quadric with equation $f(X_0,X_1)+X_2X_3+\ldots+X_{n-1}X_n=0$, where f is an irreducible homogeneous quadratic form over $\mathbb{F}_q$. Quadrics of the first type are called *hyperbolic* and are denoted by $\mathcal{Q}^+(n,q)$, quadrics of the second type are called *elliptic* and are denoted by $\mathcal{Q}^-(n,q)$.

If q is odd, then the absolute points of an orthogonal polarity form a quadric in $\mathrm{PG}(n,q)$. If q is a square, then the absolute points of a Hermitian polarity form a Hermitian variety in $\mathrm{PG}(n,q)$.

Quadrics and Hermitian varieties, together with the subspaces contained in it, are examples of so-called *polar spaces*. A polar space of rank n, $n\geq 3$, is a point set $\mathcal{P}$ together with a family of subsets of $\mathcal{P}$ called subspaces, satisfying the following axioms.

(A1) A subspace, together with the subspaces it contains, is a d-dimensional projective space with $-1\leq d\leq n-1$.

(A2) The intersection of two subspaces is a subspace.

(A3) Given a subspace V of dimension $n-1$ and a point $P \in \mathcal{P} \setminus V$, there is a unique subspace W of dimension $n-1$ such that $P \in W$ and $V \cap W$ has dimension $n-2$. The subspace W contains all points of V that are collinear with P.

(A4) There exist two disjoint subspaces of dimension $n-1$.

The points of $\mathrm{PG}(n,q)$, n odd, $n \geq 3$, together with the totally isotropic subspaces of a non-singular symplectic polarity of $\mathrm{PG}(n,q)$ form a *symplectic* polar space, denoted by $\mathcal{W}(n,q)$.

The *classical polar spaces* are the quadrics, the Hermitian varieties and the symplectic polar spaces. These are the only examples of finite polar spaces with rank at least three because of a result of Tits [143].

A *generator* of a polar space $\mathcal{P}$ is a subspace, contained in $\mathcal{P}$, of the largest possible dimension. Hence, if $\mathcal{P}$ is classical, a generator is a maximal totally isotropic subspace. By a classical result by Witt from 1937 (for a proof, see e.g. [3]) in the study of sesquilinear forms over arbitrary fields, the dimension of the generators of a fixed polar space is a constant. The dimension of the generators is $n-1$ for $\mathcal{Q}(2n,q)$ and $\mathcal{Q}^-(2n+1,q)$ and n for $\mathcal{Q}^+(2n+1,q)$. For a Hermitian variety $\mathcal{H}(2n,q)$, q square, respectively $\mathcal{H}(2n+1,q)$, q square, the dimension of the generators is $n-1$, respectively, n.

1.3.1 The Klein correspondence

There is a classical connection between the lines of a 3-dimensional projective space and the points of a hyperbolic quadric in a projective 5-dimensional space: the Klein correspondence, after F. Klein, who introduced the correspondence for projective spaces over the complex numbers [83]. If L is a line of $\mathrm{PG}(3,q)$ and (y_0,y_1,y_2,y_3) and (z_0,z_1,z_2,z_3) are different points of L, then $p_{ij} = y_i z_j - y_j z_i$ is determined by L up to a scalar multiple[5]. The map $\mathrm{PG}(3,q) \to \mathrm{PG}(5,q)$ defined by $L \mapsto (p_{01},p_{02},p_{03},p_{23},p_{31},p_{12})$ has $\mathcal{Q}^+(5,q)$ as image. There are two types of generators on $\mathcal{Q}^+(5,q)$, called *Latin planes* and *Greek planes*. Two different Latin planes (resp. Greek planes) have exactly one point in common, a Latin and a Greek plane have no point or the points of a line in common. The (lines in) planes of $\mathrm{PG}(3,q)$ correspond to the Greek

[5] The coordinates p_{ij} are called the *Plücker coordinates*, after J. Plücker who introduced them in 1828.

planes of $\mathcal{Q}^+(5,q)$, and the (lines through) points of $\mathrm{PG}(3,q)$ correspond to the Latin planes of $\mathcal{Q}^+(5,q)$.

1.4 Generalised quadrangles

A *generalised quadrangle* is an incidence structure $(\mathcal{P},\mathcal{B},\mathcal{I})$, where we denote the blocks by *lines*, satisfying the following axioms.

(A1) Each point lies on $t+1$ lines ($t \geq 1$) and two distinct points lie on at most one line.

(A2) Each line contains $s+1$ points ($s \geq 1$) and two distinct lines intersect in at most one point.

(A3) If P is a point and L is a line not through P, then there is a unique point-line pair (Q,M), where Q lies on L, such that M contains P and Q.

We say that the generalised quadrangle satisfying (A1)-(A2)-(A3) has *order* (s,t), and sometimes we denote it by $\mathrm{GQ}(s,t)$. A generalised quadrangle of order (s,t) contains $(s+1)(st+1)$ points and $(t+1)(st+1)$ lines. If $s=t$, then $\mathcal{S}$ is said to be of *order* s. If P is a point of a generalised quadrangle, then $P^\perp$ denotes the set of points collinear with P; by definition, $P \in P^\perp$. The *trace* of a pair of distinct points P,Q is defined to be $P^\perp \cap Q^\perp$, and denoted by $\{P,Q\}^\perp$. The set $\{P,Q\}^{\perp\perp}$ is the set of points that are collinear with all points of $\{P,Q\}^\perp$ for distinct points P and Q, and is also called a *hyperbolic line*. A point P is *regular* if $|\{x,y\}^{\perp\perp}| = t+1$, for all points $Q \neq P$, Q not collinear with P.

The classical generalised quadrangles are $\mathcal{Q}^+(3,q)$, $\mathcal{Q}(4,q)$, $\mathcal{Q}^-(5,q)$, $\mathcal{H}(3,q)$, $\mathcal{H}(4,q)$ and $\mathcal{W}(q)$ and have orders $(q,1)$, q, (q,q^2), $(q,\sqrt{q})$, $(q,q\sqrt{q})$ and q respectively.

We have the following isomorphisms between the two classical generalised quadrangles of order q.

Theorem 1.4.1. [71, Theorem 3.2.1]

(i) The generalised quadrangle $\mathcal{Q}(4,q)$ is isomorphic to the dual of $\mathcal{W}(q)$.

(ii) The generalised quadrangles $\mathcal{Q}(4,q)$ and $\mathcal{W}(q)$ are self-dual if and only if q is even.[6]

1.5 Ovals, ovoids, arcs and sets of even type in $\mathrm{PG}(n,q)$

An *oval* $\mathcal{O}$ in $\mathrm{PG}(2,q)$ is a set of $q+1$ points, no three of which are collinear. A *tangent line* to an oval $\mathcal{O}$ is a line containing exactly one point of $\mathcal{O}$, a *secant line* is a line meeting $\mathcal{O}$ in two points and an *external line* is a line not containing a point of $\mathcal{O}$. We have the following lemmas.

Lemma 1.5.1. [25] *The tangent lines to an oval $\mathcal{O}$ in $\mathrm{PG}(2,q)$ are concurrent if and only if q is even.*

Lemma 1.5.2. [10] *If two ovals in $\mathrm{PG}(2,q)$, q even, have more than half of their points in common, they coincide.*

Using Lemma 1.5.1, we see that every oval $\mathcal{O}$ in $\mathrm{PG}(2,q)$, q even, can be extended by the common point n (called the *nucleus* of $\mathcal{O}$) of all tangent lines to $\mathcal{O}$ to a set of $q+2$ points, no three of which are collinear. Such a set is called[7] a *hyperoval*. It is easy to see that hyperovals only exist for q even.

Non-singular conics are examples of ovals. In [129], Segre proves that if q is odd, the converse is true, thus linking the intersection properties of an oval with its algebraic description.

Theorem 1.5.3. [129] *If q is odd, every oval of $\mathrm{PG}(2,q)$ is a conic.*

From Lemma 1.5.1, it follows that a conic in $\mathrm{PG}(2,q)$, q even, and its nucleus, form a hyperoval. The hyperovals arising in this way are called *regular* hyperovals. A regular hyperoval can be written as the set of points $\{(1,t,t^2)|t \in \mathbb{F}_q\} \cup \{(0,0,1)\} \cup \{(0,1,0)\}$. Replacing t^2 by t^{2^v}, where $\gcd(v,h)=1$, yields a broader class of hyperovals, called *translation hyperovals*. Other infinite families of hyperovals are known. Classifying them is a hard problem and the classification of hyperovals remains open, at least for $q \geq 64$ [115]. For more on hyperovals, we refer to *Bill Cherowitzo's hyperoval page* [39].

[6] The fact that $\mathcal{W}(q)$ is self-dual if and only if q is even, was proved in [141].

[7] In many papers dealing with coding theory, hyperovals are called ovals, and ovals are defined to be sets of the largest possible size such that no three of its points are collinear.

Arcs generalise the concept of ovals in PG$(2, q)$. An *arc* $\mathcal{A}$ of degree m is a set of points such that no m points of $\mathcal{A}$ are collinear. If an arc of degree m contains k points, we also denote it by a *k-arc* of degree m. If the degree of the arc is 3, we do not mention the degree. From the definitions, it follows that an oval is a $(q+1)$-arc and a hyperoval is a $(q+2)$-arc. It is clear that an arc of degree m can have at most $mq - q + m$ points. An arc with size exactly $mq - q + m$ is called a *maximal arc* of degree m. The non-existence of hyperovals in planes of odd order is extended to the non-existence of maximal arcs of degree m in PG$(2, q)$, q odd, by Ball, Blokhuis and Mazzocca in the following theorem.

Theorem 1.5.4. [8] *For q an odd prime power, and $1 < m < q$,* PG$(2, q)$ *does not contain a maximal arc of degree m.*

A *k-arc of type* $(0, 2, t)$ generalises the concept of arcs further by admitting 3 possible intersection sizes of a line and the arc: a k-arc $\mathcal{A}$ of type $(0, 2, t)$ is a set of k points such that a line intersects $\mathcal{A}$ in $0, 2$ or t points.

Gács and Weiner proved the following result.

Theorem 1.5.5. [59, Theorem 2.5] *The t-secants of a $(q + t)$-arc of type $(0, 2, t)$ in* PG$(2, q)$*, q even, have a nucleus (i.e. they are concurrent).*

A *set of even type* in PG$(2, q)$ is a set S of points such that every line contains an even number of points of S. Hyperovals and arcs of type $(0, 2, t)$, with t even, provide examples of such sets of even type. More general, a set of even type in a projective space or polar space is a set which has an even intersection number with objects of a fixed dimension in this projective or polar space, e.g. lines, planes or k-spaces.

In the same way as ovals in PG$(2, q)$ are the objects having the same size and intersection properties with respect to lines as conics in PG$(2, q)$, ovoids in PG$(3, q)$ are the objects having the same size and intersection properties with respect to lines of elliptic quadrics in PG$(3, q)$. Hence, an *ovoid* in PG$(3, q)$, $q > 2$, is a set of q^2+1 points, no three of which are collinear. It is clear that an elliptic quadric in PG$(3, q)$ is an ovoid. The following theorem independently proven by Barlotti and Panella shows that if q is odd, the converse also holds.

Theorem 1.5.6. [9, 111] *An ovoid in* PG$(3, q)$*, q odd, is an elliptic quadric.*

For q even, there is, besides the elliptic quadrics, only one other class of ovoids known: the *Suzuki-Tits ovoids*, discovered by Tits in 1962 [142], which only exist in $\mathrm{PG}(3, 2^{2e+1})$, $e \geq 1$. For ovoids in $\mathrm{PG}(3, q)$, q even, the classification remains open for $q \geq 64$ [108].

1.6 The linear representation $T_2^*(\mathcal{K})$

Let $\mathcal{K}$ be a set of points in $H_\infty = \mathrm{PG}(2, q)$ and embed H_∞ in $\mathrm{PG}(3, q)$. The *linear representation* $T_2^*(\mathcal{K})$ is an incidence structure $(\mathcal{P}, \mathcal{L}, \mathrm{I})$ with

$\mathcal{P}$: the set of points of $\mathrm{PG}(3, q) \setminus H_\infty$,

$\mathcal{L}$: the set of lines of $\mathrm{PG}(3, q) \setminus H_\infty$, intersecting H_∞ in a point of $\mathcal{K}$,

I: natural incidence.

Each point of $T_2^*(\mathcal{K})$ lies on $|\mathcal{K}|$ lines and each line contains q points. If $\mathcal{K}$ is a hyperoval, $T_2^*(\mathcal{K})$ is a generalised quadrangle of order $(q-1, q+1)$. The construction of the generalised quadrangle $T_2^*(\mathcal{O})$, where $\mathcal{O}$ is a hyperoval, is due to Ahrens and Szekeres [1], and Hall, Jr. [66].

1.7 Spreads in $\mathrm{PG}(n, q)$

A $(t-1)$-*spread* in $\mathrm{PG}(n-1, q)$ is a set of $(t-1)$-spaces, partitioning $\mathrm{PG}(n-1, q)$. The following theorem gives a necessary and sufficient condition for the existence of a $(t-1)$-spread in $\mathrm{PG}(n-1, q)$.

Theorem 1.7.1. [131] *There exists a $(t-1)$-spread in $\mathrm{PG}(n-1, q)$ if and only if t divides n.*

If there exists a $(t-1)$-spread in $\mathrm{PG}(n-1, q)$, it is clear that the number of points in a $(t-1)$-space has to divide the number of points in $\mathrm{PG}(n-1, q)$. From this, it follows that t has to divide n.

To show that whenever t divides n, there exists a $(t-1)$-spread in $\mathrm{PG}(n-1, q)$, we give the construction of a particular spread, which we will call a *Desarguesian spread*.

Suppose t is a proper divisor of n. By *field reduction*, the points of PG$(\frac{n}{t}-1, q^t)$ correspond to $(t-1)$-dimensional subspaces of PG$(n-1, q)$, since a point of PG$(\frac{n}{t}-1, q^t)$ is a 1-dimensional vector space over $\mathbb{F}_{q^t}$, and so a t-dimensional vector space over $\mathbb{F}_q$. In this way, we obtain a partition $\mathcal{D}$ of the point set of PG$(n-1, q)$ by $(t-1)$-dimensional subspaces.

To explain why the spread obtained here is called 'Desarguesian', we introduce the so-called *André/Bruck-Bose construction* [2, 30] and *translation planes*.

Let $\mathcal{S}$ be a $(t-1)$-spread in PG$(2t-1, q)$. Embed PG$(2t-1, q)$ as a hyperplane H in PG$(2t, q)$. Let $\mathcal{P}$ be the set of points of PG$(2t, q) \setminus H$, together with the q^t+1 elements of $\mathcal{S}$. Let $\mathcal{L}$ be the set of t-spaces of PG$(2t, q)$ intersecting H exactly in an element of $\mathcal{S}$, together with the space H itself. The incidence structure $(\mathcal{P}, \mathcal{L}, \mathrm{I})$, where I is containment, is a *translation plane* of order q^t. We say that this plane is obtained from the *André/Bruck-Bose construction*, starting from the spread $\mathcal{S}$.

The spread $\mathcal{D}$ obtained via field reduction is called Desarguesian because, starting from the spread $\mathcal{D}$, we obtain a Desarguesian projective plane by the André/Bruck-Bose construction.

Remark. An *elation* with *axis* L and *center* P of PG$(2, Q)$ is a collineation that fixes all points on the line L and all lines through a point P, where P lies on L. The group of all elations with axis L and center P is denoted by $El(P, L)$. If for all lines $M \neq L$ through P, $El(P, L)$ acts transitively on the points of $M \setminus \{P\}$, $El(P, L)$ is (P, L)-*transitive*. A projective plane Π is a *translation plane* if there exists a line L such that $El(P, L)$ is (P, L)-transitive for all points P on L.

A *regulus* in PG$(rt-1, q)$, or $(t-1)$-*regulus* if we want to specify the dimension of the elements, is a set $\mathcal{R}$ of $q+1$ mutually skew $(t-1)$-spaces with the property that a line that meets three elements of $\mathcal{R}$ meets all elements of $\mathcal{R}$. If S_1, S_2, S_3 are mutually disjoint $(t-1)$-subspaces of PG$(2t-1, q)$, then there is a unique regulus $\mathcal{R}(S_1, S_2, S_2)$ containing S_1, S_2, S_3. A spread $\mathcal{S}$ is *regular* if the regulus $\mathcal{R}(S_1, S_2, S_3)$ is contained in $\mathcal{S}$ whenever S_1, S_2, S_3 are three distinct elements of $\mathcal{S}$. Now, if $q > 2$, a $(t-1)$-spread of PG$(2t-1, q)$ is Desarguesian if and only if it is regular [30]. This means that the Desarguesian projective planes are precisely those obtained from the André/Bruck-Bose construction starting with a regular spread.

Note that the Desarguesian spread satisfies the property that each subspace spanned by spread elements is partitioned by spread elements. Spreads satisfying this property are called *normal*. Clearly, a $(t-1)$-spread in $\mathrm{PG}(2t-1,q)$ is always normal. A $(t-1)$-spread $\mathcal{S}$ in $\mathrm{PG}(rt-1,q)$, with $r>2$, is normal if and only if $\mathcal{S}$ is Desarguesian [11].

Remark. There is a technique, called *derivation*[8] that enables us, starting from a Desarguesian plane of order q^2, to construct a non-Desarguesian (Hall) plane of order q^2. This method is due to Ostrom [109] and works as follows: let $\mathcal{S}$ be a Desarguesian spread, contained in $\mathrm{PG}(3,q)$. Let $\mathcal{R}$ be a regulus contained in $\mathcal{S}$. It is easy to see that the *transversal lines*, which are the lines meeting the lines of $\mathcal{R}$ in $q+1$ different points, form a regulus $\mathcal{R}^{opp}$, called the *opposite regulus* of $\mathcal{R}$. Let $\mathcal{S}'$ be the spread obtained from $\mathcal{S}$ by replacing the lines of a regulus $\mathcal{R}$ by $\mathcal{R}^{opp}$ [9]. The plane obtained via the André/Bruck-Bose construction of the spread $\mathcal{S}'$ is a non-Desarguesian translation plane if $q>2$.

1.8 k-Blocking sets and covers in $\mathrm{PG}(n,q)$

A *k-blocking set* B in $\mathrm{PG}(n,q)$ is a set of points such that any $(n-k)$-dimensional subspace intersects B. A k-blocking set B is called *trivial* when a k-dimensional subspace is contained in B. A 1-blocking set in $\mathrm{PG}(2,q)$ is simply called a *blocking set* in $\mathrm{PG}(2,q)$.

If an $(n-k)$-dimensional subspace contains exactly one point of a k-blocking set B in $\mathrm{PG}(n,q)$, it is called a *tangent $(n-k)$-space* to B, and a point P of B is called *essential* when it belongs to a tangent $(n-k)$-space of B. A k-blocking set B is called *minimal* when no proper subset of B is also a k-blocking set, i.e., when each point of B is essential. A k-blocking set B is called *small* if $|B|<3(q^k+1)/2$.

Remark. The terminology concerning blocking sets is not standard. In early papers, blocking sets were often referred to as *blocking configurations*, and the definition excluded trivial blocking sets. For a long time, the only blocking sets that were considered in higher dimensions were 1-blocking sets, hence, in many papers, a 1-blocking set in $\mathrm{PG}(n,q)$ was simply called a blocking

[8] Derivation of projective planes can be defined for arbitrary projective planes of order q^2, not only for translation planes (see [74]).

[9] The spread obtained in this way is called a *subregular spread* of index 1 according to [72, p. 54].

set in $\mathrm{PG}(n,q)$. A k-blocking set is often called a *blocking set with respect to $(n-k)$-spaces*. Minimal blocking sets are sometimes called *irreducible* or *reduced* blocking sets.

A *Rédei-type* k-blocking set in $\mathrm{PG}(n,q)$ is a blocking set B such that there exists a hyperplane with $|B|-q^k$ points of B.

A *cone* with *vertex* $\pi=\mathrm{PG}(k,q)$ and *base* $B\subseteq\mu=\mathrm{PG}(n-k-1,q)$, where π and μ are disjoint subspaces of $\mathrm{PG}(n,q)$, is the set of points lying on the lines p_1p_2 where $p_1\in\pi, p_2\in B$. Cones over *planar blocking sets*, which are blocking sets contained in a plane, will give examples of higher dimensional blocking sets (see Theorem 2.1.3).

A *t-fold k-blocking set* is a set B of points such that every $(n-k)$-space contains at least t points of $\mathrm{PG}(n,q)$.

A *cover* of $\mathrm{PG}(n,q)$ is a set $\mathcal{C}$ of hyperplanes such that every point lies on at least one hyperplane of $\mathcal{C}$. A cover of $\mathrm{PG}(n,q)$ is *minimal* if there is no proper subset of $\mathcal{C}$ that forms a cover of $\mathrm{PG}(n,q)$, or equivalently, if every hyperplane $\pi\in\mathcal{C}$ contains a point P such that π is the only element of $\mathcal{C}$ containing P. A cover of $\mathrm{PG}(n,q)$ is a dual 1-blocking set in $\mathrm{PG}(n,q)$.

1.9 Ovoids, blocking sets, spreads and covers of polar spaces

A *blocking set* of a polar space $\mathcal{P}$ is a set B of points such that every generator of $\mathcal{P}$ contains at least one point of B. If every generator contains exactly one element of the set B, then B is called an *ovoid* of $\mathcal{P}$. An *ovoid* of a generalised quadrangle of order (s,t) is a set of $st+1$ pairwise non-collinear points. Showing the (non-)existence of ovoids in generalised quadrangles and polar spaces and classifying them are hard problems, e.g. the existence problem for ovoids in $\mathcal{Q}^+(2n+1,q)$ is not solved in general. For an up-to-date overview of the known cases, we refer to the chapter *Substructures of finite classical polar spaces* in [44]. Every ovoid of $\mathrm{PG}(3,q)$, q even, corresponds to an ovoid of $\mathcal{W}(q)$, q even, and vice versa (see [130, 141]). Since for q even, $\mathcal{W}(q)$ is isomorphic to $\mathcal{Q}(4,q)$, the classification of ovoids in $\mathrm{PG}(3,q)$, q even, is the same as for $\mathcal{Q}(4,q)$, q even.

Analogously with the definition of covers of $\mathrm{PG}(n,q)$, one can define a cover

of a generalised quadrangle Γ as a set of lines such that every point of Γ lies on at least one line of $\mathcal{C}$.

If every point of Γ lies on exactly one line of a cover $\mathcal{C}$, then $\mathcal{C}$ is a *spread* of Γ, i.e. $\mathcal{C}$ is a partition of the point set of $\Gamma = \mathrm{GQ}(s,t)$ into $st+1$ pairwise skew lines.

1.10 Linear (blocking) sets

Linear sets will play an important role throughout this thesis. The terminology was first introduced by Lunardon [96] to describe a particular kind of blocking sets. Linear (blocking) sets can be defined in several equivalent ways. Here we present two points of view, as described in [93], in Chapter 3 we will present a third one.

Let V be an $(n+1)$-dimensional vector space over a finite field $\mathbb{F}$. A set S of points of $\mathrm{PG}(V)$ is called a *linear set (of rank r)* if there exists a subset U of V that forms a $\mathbb{F}_q$-vector space (of rank r) for some $\mathbb{F}_q \subset \mathbb{F}$, such that $S = \mathcal{B}(U)$, where

$$\mathcal{B}(U) := \{\langle u\rangle_{\mathbb{F}} \ : \ u \in U \setminus \{0\}\},$$

where $\langle u\rangle_{\mathbb{F}}$ denotes the projective point of $\mathrm{PG}(V)$, corresponding to the vector u of $U \subset V$.

If we want to specify the subfield, we call S an *$\mathbb{F}_q$-linear set*. In other words, if $\mathbb{F} = \mathbb{F}_{q^t}$, we have the following diagram

$$\begin{array}{ccccc}
\mathbb{F}_{q^t}^{n+1} & \longleftrightarrow & \mathbb{F}_q^{t(n+1)} & \supseteq & U \\
\updownarrow & & \updownarrow & & \updownarrow \\
\mathcal{B}(U) \subseteq \mathrm{PG}(n,q^t) & \longleftrightarrow & \mathrm{PG}((n+1)t-1,q) & \supseteq & \mathrm{PG}(U)
\end{array}$$

It is clear that a subspace π of $\mathbb{F}_q^{t(n+1)}$ or $\mathrm{PG}((n+1)t-1,q)$ induces a subset in $\mathrm{PG}(n,q^t)$ in this way. In what follows we will also use the notation $\mathcal{B}(\pi)$ for the set of points of $\mathrm{PG}(n,q^t)$ induced by π.

As seen in Section 1.7, the points of $\mathrm{PG}(n,q^t)$ correspond to a Desarguesian $(t-1)$-spread $\mathcal{D}$. This gives us a more geometric perspective on the notion of a linear set; namely, an $\mathbb{F}_q$-linear set is a set S of points of $\mathrm{PG}(n,q^t)$ for

which there exists a subspace π in $\mathrm{PG}(t(n+1)-1,q)$ such that the points of S correspond to the elements of $\mathcal{D}$ that have a non-trivial intersection with π. Also in what follows, we will often identify the elements of $\mathcal{D}$ with the points of $\mathrm{PG}(n,q^t)$, which allows us to view $\mathcal{B}(\pi)$ as a subset of $\mathcal{D}$. This is illustrated by the following diagram, where $\mathcal{P}$ denotes the set of points of $\mathrm{PG}(n,q^t)$.

$$\begin{array}{ccccccc} & & \mathrm{PG}(n,q^t) & \longleftrightarrow & \mathrm{PG}(t(n+1)-1,q) & \supseteq & \pi \\ & & \downarrow & & \downarrow & & \Downarrow \\ \mathcal{B}(\pi) & \subseteq & \mathcal{P} & \longleftrightarrow & \mathcal{D} & \supseteq & \mathcal{B}(\pi) \end{array}$$

It follows from this point of view that a linear set $\mathcal{B}(L)$ of rank 2, where L is a line of $\mathrm{PG}(t(n+1)-1,q)$, is a *regulus* of $\mathcal{D}$. If P is a point of $\mathcal{B}(\pi)$ in $\mathrm{PG}(n,q^t)$, where π is a subspace of $\mathrm{PG}(t(n+1)-1,q)$, then we define the *weight of* P as $wt(P) := \dim(P \cap \pi) + 1$, where P is identified with an element of $\mathcal{D}$. This makes a point to have weight 1 if its corresponding spread element intersects π in a point. Note that if $\pi = \mathrm{PG}(U)$, then $wt(P) = \dim\langle\{v \in U \mid \mathrm{PG}(v) = P\}\rangle$.

If we want to make a distinction between points of $\mathrm{PG}(n,q^t)$ and the corresponding elements of the $(t-1)$-spread $\mathcal{D}$, then we denote the element of $\mathcal{D}$ corresponding to a point P of $\mathrm{PG}(n,q^t)$ by $\mathcal{S}(P)$.

Linear blocking sets are blocking sets which form a linear set. We will repeat the previous construction of a Desarguesian spread and a linear set to show that linear blocking sets arise in a very natural way.[10] Using the same arguments as for the correspondence between the points of $\mathrm{PG}(n,q^t)$ and the elements of a Desarguesian $(t-1)$-spread $\mathcal{D}$, we obtain the correspondence between the $(n-k)$-spaces of $\mathrm{PG}(n,q^t)$ and the $((n-k+1)t-1)$-dimensional subspaces of $\mathrm{PG}((n+1)t-1,q)$ spanned by $n-k+1$ elements of $\mathcal{D}$. With this in mind, it is clear that any tk-dimensional subspace U of $\mathrm{PG}(t(n+1)-1,q)$ defines a k-blocking set $\mathcal{B}(U)$ in $\mathrm{PG}(n,q^t)$, and from the construction, it follows that $\mathcal{B}(U)$ is a linear set.

If U intersects the elements of $\mathcal{D}$ in at most a point, i.e. $|\mathcal{B}(U)|$ is maximal, then we say that U is *scattered* with respect to $\mathcal{D}$; in this case $\mathcal{B}(U)$ is called a *scattered linear set*. A *maximum scattered subspace* is a scattered subspace of the largest possible dimension. The following theorem gives a bound on the

[10] This approach follows Lavrauw [87].

dimension of a maximum scattered subspace. For more on scattered spaces, see [20, 87].

Theorem 1.10.1. [20, Theorem 4.3 and 4.4] *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 $m=\frac{rt}{2}-1$ if r is even, and $m\geq\frac{rt-t}{2}-1$ if r is odd.*

The following well-known lemma will be very useful throughout this thesis.

Lemma 1.10.2. *Let $\mathcal{D}$ be the Desarguesian $(t-1)$-spread of $\mathrm{PG}(t(n+1)-1,q)$. Let $\mathcal{B}(\pi)$ be a linear set, where π is a k-dimensional space. For every point R in $\mathrm{PG}(t(n+1)-1,q)$, contained in an element of $\mathcal{B}(\pi)$, there is a k-dimensional space π', through R, such that $\mathcal{B}(\pi)=\mathcal{B}(\pi')$.*

Proof. Let φ be the collineation of $\mathrm{P\Gamma L}(t(n+1),q)$ induced by multiplying with a primitive element α of $\mathbb{F}_{q^t}$. The map φ maps the point x of $\mathrm{PG}(t(n+1)-1,q)$ to a point in $\mathcal{B}(x)$ since $\langle x\rangle_{\mathbb{F}_{q^t}}=\langle x^{\varphi}\rangle_{\mathbb{F}_{q^t}}$. Moreover, the set

$$\{\langle x\rangle_{\mathbb{F}_q},\langle x^{\varphi}\rangle_{\mathbb{F}_q},\ldots,\langle x^{\varphi^{q^t-2}}\rangle_{\mathbb{F}_q}\}$$

consists of the $(q^t-1)/(q-1)$ different points of $\mathcal{B}(x)$.

Let R be a point contained in an element $\mathcal{B}(P)$ of $\mathcal{B}(\pi)$, and let x be a point in $\pi\cap\mathcal{B}(P)$. It follows from the previous part that $R=x^{\varphi^m}$ for some $0\leq m\leq q^t-2$. Hence, the element $\psi:=\varphi^m$ is such that $\psi(x)=R$. Let $\pi':=\psi(\pi)$, then $\mathcal{B}(\pi)=\mathcal{B}(\pi')$ since $\langle y^{\psi}\rangle_{\mathbb{F}_{q^t}}=\langle y\rangle_{\mathbb{F}_{q^t}}$ for all $y\in\mathrm{PG}(t(n+1)-1,q)$. □

1.11 Linear codes

In this thesis, all considered codes will be *linear over a finite field*. More general definitions exist for non-linear codes over arbitrary alphabets.

A q-ary *linear code* C of *length* m is a linear subspace of $V(m,q)$. If C has dimension g, then C is called an $[m,g]$-code. A *generator matrix* G for a linear code C is a matrix whose rows form a basis of C.

The *support* of a codeword c, denoted by $supp(c)$, is the set of all non-zero positions of c. The *weight* of c is the number of non-zero positions of c and is denoted by $wt(c)$. The *minimum weight* of a code C is equal to $\min\{wt(c)|c\neq$

$0 \in \mathrm{C}\}$. The *(Hamming) distance* between c and c', denoted by $d(c, c')$, is equal to the number of positions in which the corresponding coordinates differ. The *minimum distance* $d(\mathrm{C})$ of C is equal to $\min\{d(c, c')|c \neq c' \in \mathrm{C}\}$.

The minimum distance determines the number of errors that can be detected and corrected using this code, when using *nearest-neighbour-decoding*. This method decodes a received vector to the codeword that is nearest to it, in terms of Hamming distance. The following theorem is an immediate corollary of this decoding method.

Theorem 1.11.1. *If* C *is a linear code with minimum distance* d*, then* C *can detect up to* $d-1$ *errors and correct up to* $\lfloor (d-1)/2 \rfloor$ *errors.*

It is easy to see that in a linear code, the minimum weight and the minimum distance are equal. Hence, the minimum weight of a code C is denoted by $d(C)$ too.

We let (c_1, c_2) denote the scalar product in $\mathbb{F}_q$ of two codewords c_1, c_2 of a q-ary code C. The *dual code* $\mathrm{C}^\perp$ of a q-ary code C of length m is the set of all vectors orthogonal to all the codewords of C, hence

$$\mathrm{C}^\perp = \{v \in V(m, q)|(v, c) = 0, \ \forall c \in \mathrm{C}\}.$$

If C is a linear $[m, g]$-code, then $\mathrm{C}^\perp$ is an $[m, m-g]$-code. If G is a generator matrix for a q-ary code C of length m, then $\mathrm{C}^\perp$ consists of all vectors v in $V(m, q)$ such that $xG^T = 0$. The matrix G is called a *parity check matrix* for $\mathrm{C}^\perp$. If H is a generator matrix for $\mathrm{C}^\perp$, then H is a parity check matrix for C and $HG^T = 0$.

The *weight enumerator* of a (linear) code C is the polynomial $\sum_i A_i X^i$, where A_i is the number of codewords with weight i in C.

1.11.1 Linear codes arising from incidence structures

Let $\mathcal{I} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ be an incidence structure. The *incidence matrix* A of $\mathcal{I}$ is a matrix with rows labelled by the blocks of $\mathcal{I}$ and columns labelled by the points of $\mathcal{I}$, with entry

$$a_{ij} = \begin{cases} 1 & \text{if point } j \text{ is incident with block } i, \\ 0 & \text{otherwise.} \end{cases}$$

If the incidence structure $\mathcal{I}$ is embedded in the projective space $\mathrm{PG}(n,q)$, $q=p^h$, we define the p-ary code of points and blocks of $\mathcal{I}$ to be the code generated by the matrix A over $\mathbb{F}_p$ and we denote this code by $\mathrm{C}(\mathcal{I})$. If $\mathcal{I}$ is a linear representation $T_2^*(\mathcal{K})$, where $\mathcal{K}\subset\mathrm{PG}(2,q)$, $q=p^h$, we will always consider the p-ary code, denoted by $\mathrm{C}(T_2^*(\mathcal{K}))$.

If $\mathcal{I}$ is the incidence geometry of points and k-spaces of the projective space $\mathrm{PG}(n,q)$, the p-ary code is denoted by $\mathrm{C}_k(n,q)$ and if $\mathcal{I}$ is the incidence geometry of points and k-spaces of a polar space $\mathcal{P}$, embedded in a projective space of order q, we denote the p-ary code by $\mathrm{C}_k(\mathcal{P})$. In the case that the dimension of the blocks is clear, we omit the subscript k. For example, the code of points and lines in $\mathrm{PG}(2,q)$ is simply denoted by $\mathrm{C}(2,q)$.

If $\mathcal{I}$ is the incidence geometry of s-spaces and t-spaces, $s<t$, of the projective space $\mathrm{PG}(n,q)$, the p-ary code is denoted by $\mathrm{C}_{s,t}(n,q)$, and it is clear that $\mathrm{C}_k(n,q)=\mathrm{C}_{0,k}(n,q)$.

Remark. For our purposes, the incidence between s-spaces and t-spaces is containment. One might as well define an s-space and a t-space to be incident if and only if they intersect non-trivially. The code C' generated by the incidence matrix of s-spaces and t-spaces with this incidence relation has known dimension (see [135, Theorem 1]), but to our knowledge no other results are known. For the code $\mathrm{C}_{s,t}(n,q)$ the situation is opposite: there is no formula for its dimension (if $s\neq 0$) but the minimum weight codewords are known (see Chapter 6).

2

Bounds on the size of k-blocking sets and a unique reducibility theorem

From the 1950's on, blocking sets in the projective plane gained a lot of attention. Originally, they arose from game theory (see e.g. [147]), where a set of individuals that can force a decision forms a coalition and a blocking set is a set of individuals which is able to block every decision[1]. In the projective plane $\mathrm{PG}(2,q)$, individuals are represented by points, coalitions by lines and a blocking set is a set of points, blocking all lines of $\mathrm{PG}(2,q)$. Initial results and constructions appear in the 1954 paper *On finite projective games* by Richardson, where he ends this paper by the following observation.

The problem of determining the number of points in a minimum blocking coalition remains open. In non-gametheoretic terms, the problem is to find the smallest number of points in a set which intersects every line but contains no entire line. Similar questions can be asked, of course, in the higher dimensional cases, in the non-Desarguesian geometries, and in those block designs in which every pair of distinguished sets intersect.

[1] There was one extra condition: the group of individuals that were able to *block* all decisions was not permitted to be able to *force* a decision. In our terminology, the blocking set was requested to be non-trivial.

Now, more than 50 years later, these questions remain unsolved in general; the first question was partially answered in a paper by Bruen from 1970 [31], where the smallest examples of non-trivial minimal blocking sets in Desarguesian planes of square order are characterised as Baer subplanes. For arbitrary planes, as well as for the higher dimensional cases, except for a few cases, only bounds on the smallest size of a non-trivial blocking set are known.

Later, the theory of lacunary polynomials[2], developed by Rédei in 1970 [125], proved very efficient in the study of point sets determining few directions. In 1977, Bruen and Thas noticed that the polynomials studied by Rédei could help with the study of blocking sets (see [33]). In 1994, Blokhuis [16] showed, using these polynomials, that a blocking set in a Desarguesian plane of prime order p contains at least $3(p+1)/2$ points. In Chapter 4, we will relate this result to the linearity conjecture.

After that, Szőnyi used Rédei-polynomials to derive a 1 mod p result and new bounds on the size of a small minimal blocking set; he showed that, if the order of the plane is large enough, the size of a small minimal blocking set is contained in one of several distinct intervals [139]. This result was improved by Polverino [121]. Together with Weiner, Szőnyi extended the 1 mod p result to higher dimensions and derived bounds on the size of a small minimal k-blocking set [140].

In this chapter, we deduce a different bound, valid when $p > 2$ and $p^e > 3$, on this size[3], and we prove a unique reducibility theorem for k-blocking sets in $\mathrm{PG}(n,q)$. This new bound and the unique reducibility theorem will be used in the study of small weight codewords in the code of points and k-spaces in $\mathrm{PG}(n,q)$ (see Chapter 6); these results are joint work with Michel Lavrauw and Leo Storme, see [90].

[2] We say that a polynomial f over $\mathbb{F}_q$ is a lacunary polynomial if it is fully reducible over $\mathbb{F}_q$ and if $f^{00} < f^0 - 1$, where f^0 denotes the degree of f and f^{00} denotes the second degree of f.

[3] Here, e is the *exponent* of the small minimal blocking set contained in $\mathrm{PG}(n,p^h)$. This concept will be introduced later in this chapter.

2.1 Introductory results

2.1.1 Examples of minimal blocking sets of small size

Easy examples of non-trivial blocking sets of small size can be constructed using projective triangles and projective triads. A *projective triangle of side* n in $\mathrm{PG}(2,q)$ is a set T of $3(n-1)$ points such that

(i) on each side of a triangle $P_0P_1P_2$, there are n points of T,

(ii) the vertices P_0, P_1, P_2 are in T,

(iii) if $Q_0 \neq P_0, P_2$ on P_0P_2 and $Q_1 \neq P_0, P_2$ on P_0P_2 are in T, then so is $Q_2 = Q_0Q_1 \cap P_0P_1$.

A *projective triad of side* n in $\mathrm{PG}(2,q)$ is a set T of $3n-2$ points such that

(i) on each line of the three concurrent lines ℓ_0, ℓ_1, ℓ_2, there are n points of T,

(ii) the vertex $P = \ell_0 \cap \ell_1 \cap \ell_2$ is contained in T,

(iii) if $Q_0 \neq P$ on ℓ_0 and $Q_1 \neq P$ on ℓ_1 are contained in T, then also $Q_2 = Q_0Q_1 \cap \ell_2$ is contained in T.

The concept of projective triangles is essentially due to Di Paola [48]. The existence of projective triangles in $\mathrm{PG}(2,q)$, q odd, was shown by Bruen [32].

Theorem 2.1.1. *(i)* [32] *In* $\mathrm{PG}(2,q)$*, q odd, there exists*[4] *a projective triangle of side* $(q+3)/2$ *that is a minimal blocking set of size* $3(q+1)/2$*.*

(ii) [71, Lemma 13.6] *In* $\mathrm{PG}(2,q)$*, q even, there exists a projective triad of side* $(q+2)/2$ *that is a minimal blocking set of size* $(3q+2)/2$*.*

Remark. Note that a small minimal blocking set in $\mathrm{PG}(2,q)$ has size strictly smaller than the size of a projective triangle of side $(q+3)/2$ for q odd and a projective triad of side $(q+2)/2$ for q even. Projective triangles will provide a counterexample to some of the properties that are important for the study of small minimal blocking sets, for example, the 1 mod p result, which will be discussed in the next section.

[4] It is not easy to construct projective triangles in non-Desarguesian planes. The existence of projective triangles in the three non-Desarguesian planes of order 9 is shown in [12].

Richardson constructed other examples of blocking sets of small size, using subgeometries, in the following theorem.

Theorem 2.1.2. [126, Theorem 6] *If d is a divisor of h, $1 < d < h$, then there exists a blocking set B with $2p^h - p^d + 1$ points in $\mathrm{PG}(2, p^h)$.*

The construction goes as follows: let ℓ_1, ℓ_2, ℓ_3 be lines of $\mathrm{PG}(2, p^d)$ through a point P, where $\mathrm{PG}(2, p^d)$ is embedded in $\mathrm{PG}(2, p^h)$. Let L_i be the line of $\mathrm{PG}(2, p^h)$ containing the points of ℓ_i, where $i = 1, 2$. The point set of $\ell_3 \cup (L_1 \setminus \ell_1) \cup (L_2 \setminus \ell_2)$ is a blocking set of size $p^d + 1 + 2(p^h - p^d) = 2p^h - p^d + 1$.

One of the easiest constructions for minimal k-blocking sets uses cones over a 1-blocking set, as described in the following theorem.

Theorem 2.1.3. [140, Construction 2.4] *Let B be a 1-blocking set of $\mathrm{PG}(n, q)$. Embed $\mathrm{PG}(n, q)$ in $\mathrm{PG}(n+k-1, q)$, $k > 1$, as a subspace. Choose an arbitrary $(k-2)$-dimensional subspace P, not intersecting $\mathrm{PG}(n, q)$, and let C be the cone with base B and vertex P. Then $C \cap \mathrm{PG}(n, q) = B$ and C is a k-blocking set in $\mathrm{PG}(n + k - 1, q)$. Furthermore, if B is minimal, then C is minimal.*

Remark. Note that a k-blocking set B in $\pi = \mathrm{PG}(m, q)$ is a k-blocking set in $\mathrm{PG}(n, q)$, where $n > m$ and $\mathrm{PG}(m, q)$ is embedded in $\mathrm{PG}(n, q)$: every $(n-k)$-space in $\mathrm{PG}(n, q)$ meets π in a space of dimension at least $m - k$, and hence, contains a point of B.

Remark. Many other papers on blocking sets contain constructions of blocking sets of a particular size, see e.g. [23, 77, 103].

2.1.2 Lower bounds

Suppose we want to block all lines of $\mathrm{PG}(2, q)$ by a set B of points. A point, not in B, lies on $q+1$ lines, each containing at least one point of B, so B contains at least $q+1$ points. Now assume that $|B| = q+1$ and suppose that the points of B are not collinear. All lines through a point $P \notin B$ on a line L containing at least two points of B have to be blocked, hence, $|B| \geq q + 2$, a contradiction. This shows that the smallest possible blocking sets in $\mathrm{PG}(2, q)$ are trivial.[5] The following theorem of Bose and Burton shows that this property holds in general dimension too.

[5] This is the proof of Theorem 2 in [126].

Theorem 2.1.4. [26] *If B is a k-blocking set in* $\mathrm{PG}(n,q)$*, then* $|B| \geq |\mathrm{PG}(k,q)|$ *and equality holds if and only if B is a k-dimensional subspace.*

A Baer subplane π of $\mathrm{PG}(2,q)$, q a square, consists of $q+\sqrt{q}+1$ points. If P is a point of $\mathrm{PG}(2,q) \setminus \pi$, then P lies on $q+1$ lines of $\mathrm{PG}(2,q)$. Since P cannot lie on two lines of π and a line containing two points of π is contained in π, counting shows that P lies on q lines meeting π in exactly one point and on one line meeting π in exactly $\sqrt{q}+1$ points. Hence, the points of a Baer subplane form a blocking set in $\mathrm{PG}(2,q)$.[6] Bruen characterised the smallest possible non-trivial blocking sets in planes of square order as Baer subplanes.

Theorem 2.1.5. [31, Theorem 2], [32] *Let B be a non-trivial minimal blocking set in* $\mathrm{PG}(2,q)$*. Then* $|B| \geq q+\sqrt{q}+1$ *with equality if and only if q is a square and B is a Baer subplane.*

Remark. Bruen proved this theorem for arbitrary projective planes; not only for $\mathrm{PG}(2,q)$. For the planes of order 4 and 9, the same result was already proved by Di Paola in [48]. In the same paper, Di Paola characterised the smallest non-trivial blocking sets in $\mathrm{PG}(2,3)$ and $\mathrm{PG}(2,5)$ as projective triangles, and conjectured that if p is prime, the smallest possible minimal non-trivial blocking sets in $\mathrm{PG}(2,p)$ have size $3(p+1)/2$. We will come back to this conjecture in Chapter 4.

For planes of square order, containing a Baer subplane, the bound in the previous theorem is sharp. For planes of non-square order, the following result improves on the lower bound.

Theorem 2.1.6. [21, Corollary 3.3], [33] *If B is a minimal blocking set in* $\mathrm{PG}(2,q)$*, then* $|B| \geq q+q^{2/3}+1$ *if q is a nonsquare and $p>3$ and* $|B| \geq q+q^{2/3}/2^{1/3}+1$ *if q is a non-square and $p=2$ or 3.*

The lower bound of Theorem 2.1.5 on the size of a minimal blocking set in $\mathrm{PG}(2,q)$ was extended to a lower bound on the size of a minimal 1-blocking set in $\mathrm{PG}(n,q)$ by Beutelspacher in [13].

Theorem 2.1.7. [13] *The size of a non-trivial 1-blocking set B in a finite projective space* $\mathrm{PG}(n,q)$ *is at least* $q+\sqrt{q}+1$ *and the bound is attained if and only if q is a square and B is a Baer subplane.*

[6] This is the proof of Theorem 7 in [126].

Heim characterised the smallest possible non-trivial k-blocking sets as cones over the smallest possible non-trivial planar blocking sets. Let $r_2(q)$ be the number such that $q + r_2(q) + 1$ is the cardinality of the smallest non-trivial blocking set in $\mathrm{PG}(2, q)$.

Theorem 2.1.8. [69] *Let B be a non-trivial k-blocking set in $\mathrm{PG}(n, q)$, $q > 2$. Then*

$$|B| \geq \theta_k + r_2(q)q^{k-1},$$

with equality if there exists a $(k-2)$-dimensional subspace π, a plane μ with $\mu \cap \pi = \varnothing$ and a non-trivial line blocking set B' of minimal size in μ in which case B is the cone with vertex π and base B'.

The previous theorem and many others concerning blocking sets, exclude the case $q = 2$. For $q = 2$, the smallest minimal blocking sets were determined by Govaerts and Storme.

Theorem 2.1.9. [64, Theorem 1.4]

(i) In $\mathrm{PG}(n, 2)$, $n \geq 3$, the smallest non-trivial 1-blocking sets are skeletons of solids in $\mathrm{PG}(n, 2)$; these are sets of five points in a 3-space, no four of which are coplanar. If $n = 3$, then these are the only minimal non-trivial 1-blocking sets. So, up to isomorphism, there is only one non-trivial minimal blocking set with respect to planes in $\mathrm{PG}(3, 2)$.

(ii) Up to isomorphism, there is only one non-trivial minimal 2-blocking set in $\mathrm{PG}(3, 2)$. It consists of ten points and is the set of points on the edges of a tetrahedron.

(iii) In $\mathrm{PG}(n, 2)$, $n \geq 3$, the smallest non-trivial k-blocking sets, $1 < k \leq n-1$, have size $2^{k+1} + 2^{k-1} + 2^{k-2} - 1$ and are cones with vertex a $(k-3)$-space π_{k-3} and base the set of points on the edges of a tetrahedron in a solid skew to π_{k-3}.

Remark. It is clear that in $\mathrm{PG}(2, 2)$, there are no non-trivial minimal blocking sets. The previous theorem shows that the non-trivial minimal 1- and 2-blocking sets in $\mathrm{PG}(3, 2)$ are unique. In $\mathrm{PG}(4, 2)$, the smallest possible non-trivial minimal 2-blocking set has size 10 and corresponds to the unique minimal 2-blocking set in $\mathrm{PG}(3, 2)$. But there are two other different minimal 2-blocking sets, one of size 12 and one of size 13, both spanning the space

PG(4, 2). The first example consists of 2 planes π_1 and π_2, meeting in a point P. In both π_1 and π_2, we remove one point, say P_1 and P_2, different from P, and we add the third point on the line P_1P_2. The second example consists of two planes π_1, π_2 intersecting in a line L, where we again remove points P_1, P_2 of π_1 and π_2, not on the line L. We add four points R_1, R_2, R_3, R_4 each on one of the planes through P_1P_2, not in $\langle \pi_1, \pi_2 \rangle$. We checked by computer that these are the only possibilities for a non-trivial minimal 2-blocking set in PG(4, 2), however, in these cases, minimal blocking sets of the same size are not necessarily projectively equivalent.

2.1.3 Upper bounds

Most of the results on blocking sets concern small minimal blocking sets; less is known about large minimal blocking sets. A *unital* of PG$(2, q)$, q square, is a set S of $q\sqrt{q}+1$ points such that every line contains one or $\sqrt{q}+1$ points of S. It is clear from the definition that a unital is a blocking set in PG$(2, q)$. A Hermitian curve $\mathcal{H}(2, q)$ in PG$(2, q)$, q square, is an example of a unital.

Bruen and Thas derived the following upper bounds on the size of a minimal 1-blocking set in PG(n, q).

Theorem 2.1.10. [33, Corollary 6] [34] *Let B be a minimal 1-blocking set in* PG(n, q). *Then we have the following:*

(i) If $n = 2$, then $|B| \leq q\sqrt{q}+1$ and equality holds if and only if q is a square and B is a unital.[7]

(ii) If $n = 3$, then $|B| \leq q^2+1$ and equality holds if and only if B is an ovoid.

(iii) If $n \geq 4$, then $|B| < \sqrt{q^{n+1}}+1$.

The following theorem gives an upper bound on the size of a minimal blocking set. If q is not a prime, this improves on Theorem 2.1.10 (i).

Theorem 2.1.11. [42, Theorem 5.1] *Let B be a minimal blocking set in* PG$(2, q)$, *$q \neq 5$, and let s be equal to $\sqrt{q} - \lfloor \sqrt{q} \rfloor$. Then $|B| \leq q\sqrt{q}+1-s(1-s)q/4$.*

[7] In [33, Corollary 6], the upper bound is derived but the authors do not characterise the sets attaining this bound as unitals. This was done in [34].

In Section 2.3, we will give disjoint intervals on the size of a small minimal blocking set. For large minimal blocking sets on the contrary, there are the following results, showing that there is a minimal blocking set for every size in a particular interval.

Theorem 2.1.12. [76] *There exists a minimal blocking set in* $\mathrm{PG}(2,q)$, $q>4$, *for every size in* $[2q-1, 3q-3]$.

Theorem 2.1.13. [42, Theorem 4.2] *For an arbitrary square prime power* q, *there is a minimal blocking set in* $\mathrm{PG}(2,q)$ *for any size in the interval* [8]

$$[4q\log q, q\sqrt{q}-q+2\sqrt{q}].$$

2.2 A 1 mod p result

Szőnyi shows the following in [139].

Theorem 2.2.1. [139, Corollary 4.8] *If* B *is a small minimal blocking set of* $\mathrm{PG}(2,q)$, *then every line intersects* B *in* 1 mod p *points.*

Remark. It is clear that the assumption that B is small, hence, $|B|<3(q+1)/2$, in the previous theorem is necessary since there are lines that intersect the projective triangle of side $(q+3)/2$, which is a minimal blocking set in $\mathrm{PG}(2,q)$, q odd, in three points.

Szőnyi and Weiner extended this result to k-blocking sets in $\mathrm{PG}(n,q)$. This theorem plays an important role in the study of k-blocking sets.[9] We will use it to bound the size of a small minimal k-blocking set.

Theorem 2.2.2. [140, Theorem 2.7] *Let* B *be a small minimal* k*-blocking set of* $\mathrm{PG}(n,q)$, $q=p^h$, $p>2$. *Then any subspace that intersects* B, *intersects it in* 1 mod p *points.*

Remark. The definition of *small* for k-blocking sets arises from the proof of this theorem: Szőnyi and Weiner show that embedding a k-blocking set in $\mathrm{PG}(n,q)$ in $\mathrm{PG}(n,q^k)$, defines a 1-blocking set in $\mathrm{PG}(n,q^k)$ (the same idea will be used later in this chapter to prove Theorem 2.4.8). Since the 1 mod p result

[8] Note that if this interval is not empty, then $q>100$.

[9] For example, it proves the linearity conjecture in the prime case (see Chapter 4).

holds for 1-blocking sets in $\mathrm{PG}(n, q^k)$ of size smaller than $3(q^k+1)/2$, the obtained result is only valid for k-blocking sets in $\mathrm{PG}(n, q)$ of size smaller than $3(q^k+1)/2$. As already mentioned, the bound $|B| < 3(q^k+1)/2$ in Theorem 2.2.2 is sharp for $k = 1$. If $k > 1$, there are no examples of small minimal blocking sets B of size $|B| = 3(q^k+1)/2$. By Theorem 2.1.3, a cone C with vertex a $(k-2)$-space and base a projective triangle provides an example of a minimal k-blocking set in $\mathrm{PG}(n, q)$, contradicting the 1 mod p theorem, but C has size $3(q^k+q^{k-1})/2+\theta_{k-2}$, which is larger than $3(q^k+1)/2$.

We define the *exponent* of a small minimal k-blocking set B to be the largest integer e for which every $(n-k)$-space intersects B in 1 mod p^e points. The previous results assure that the exponent is well-defined.

Szőnyi and Weiner prove a kind of converse statement to their 1 mod p result.

Theorem 2.2.3. [140, Lemma 3.1] *Let B be a k-blocking set of $\mathrm{PG}(n, q)$, and suppose that $|B| \leq 2q^k$. If each $(n-k)$-dimensional subspace of $\mathrm{PG}(n, q)$ intersects B in 1 mod p points, then B is minimal.*

2.3 Bounds on the size of a minimal blocking set using the 1 mod p result

Using Theorem 2.2.2, one can use a counting argument (see the proof of Theorem 2.3.4) to deduce the following upper and lower bounds on the size of a small minimal blocking set.

Theorem 2.3.1. [139, Theorem 5.6] *Let B be a minimal blocking set in $\mathrm{PG}(2, q)$, $q = p^h$, and let e be its exponent, where $e \leq h/2$. Then*

$$|B| \geq q+1+\frac{q}{p^e+2}$$

and

$$|B| \leq qp^e+1-\frac{\sqrt{(qp^e+1)^2-4q^2p^e}}{2} \text{ if } p^e > 7.$$

Moreover,

$$|B| \leq q+\frac{9q}{4p^e} \text{ for all } p \text{ and } e.$$

This theorem shows that the possible sizes of a blocking set in $\mathrm{PG}(2,q)$ are contained in intervals, depending on the value of e. Szőnyi also proved that these intervals are disjoint if $p^e > 8$.

Polverino improved the lower bound of Szőnyi in the following theorem.

Theorem 2.3.2. [121] *If B is a small minimal blocking set in $\mathrm{PG}(2,q)$, $p \geq 7$, then*

$$|B| \geq q + \frac{q+p^e}{p^e+1} + 1.$$

The bounds on the size of planar blocking sets can be used to find bounds for the size of k-blocking sets as is shown in the following results. Szőnyi and Weiner derived disjoint intervals in which the size of a small minimal k-blocking set in $\mathrm{PG}(n,q)$ lies. Let $S(q)$ denote the set of possible sizes of a small minimal blocking set in $\mathrm{PG}(2,q)$.

Theorem 2.3.3. [140, Corollary 3.7] *Let B be a minimal k-blocking set of $\mathrm{PG}(n,q)$. If $p=2$ let $|B| < \sqrt{2}q^k$, otherwise let $|B| < 3(q^k+1)/2$. Then*

(i) $|B| \in S(q^k)$.

(ii) If $p>2$, then $(|B|-1)(q^{k(n-2)}+1) \in S(q^{k(n-1)})$.

In the next theorem, we improve on the upper bound on the size of a small minimal k-blocking set. Note that this new upper bound is only valid for $p^e > 3$.

Theorem 2.3.4. *Let B be a minimal k-blocking set in $\mathrm{PG}(n,q)$, $|B| \leq 2q^k$, with exponent e. If $p>2$ and $p^e>3$, then B is small and*

$$|B| \leq q^k + \frac{2q^k}{p^e}.$$

Proof. Put $E = p^e$ and let τ_{1+iE} be the number of $(n-k)$-dimensional spaces intersecting B in $1+iE$ points. By Theorem 2.2.2, we know that i is a natural number. We count the number of $(n-k)$-dimensional spaces, the number of incident pairs (R,μ), with $R \in B$ and with μ an $(n-k)$-dimensional space through R, and the number of triples (R,R',μ), with R and R' distinct points of B and μ an $(n-k)$-dimensional space passing through R and R'. This gives us the following formulas:

$$\sum_{i\geq 0}\tau_{1+iE} = \begin{bmatrix} n+1 \\ n-k+1 \end{bmatrix}_q, \tag{2.1}$$

$$\sum_{i\geq 0}(1+iE)\tau_{1+iE} = |B| \begin{bmatrix} n \\ n-k \end{bmatrix}_q, \tag{2.2}$$

$$\sum_{i\geq 0}(1+iE)(1+iE-1)\tau_{1+iE} = |B|(|B|-1) \begin{bmatrix} n-1 \\ n-k-1 \end{bmatrix}_q. \tag{2.3}$$

Since $\sum_{i\geq 0} i(i-1)E^2\tau_{1+iE} \geq 0$, we obtain

$$|B|(|B|-1)-(1+E)|B|\left(\frac{q^n-1}{q^{n-k}-1}\right)+(1+E)\left(\frac{(q^{n+1}-1)(q^n-1)}{(q^{n-k+1}-1)(q^{n-k}-1)}\right) \geq 0.$$

Putting $|B| = q^k + \frac{2q^k}{E} + 1$ or $B = 2q^k + 1$ in the previous inequality, we get a contradiction under the condition $3 < E$. This implies that

$$|B| \leq q^k + \frac{2q^k}{E},$$

from which it follows that $|B| < 3(q^k+1)/2$. □

2.4 A unique reducibility property for k-blocking sets in $\mathrm{PG}(n,q)$

If B is a blocking set in $\mathrm{PG}(n,q)$, it is clear that by subsequently removing non-necessary points, one obtains a minimal blocking set $\tilde{B}$. However, if one starts by removing a different non-necessary point, one might end up with a different minimal blocking set. For example, let B be the union of two lines L and M in $\mathrm{PG}(2,q)$. If one removes a point of $L \setminus M$ first, $\tilde{B}$ will be the line M. On the other hand, if one removes a point of $M \setminus L$ first, $\tilde{B}$ will be the line L.

Remark. Note that in this example, $|B| = 2q+1$. The next theorem of Szőnyi shows that a blocking set B in $\mathrm{PG}(2,q)$ of smaller size is *uniquely reducible* to a minimal blocking set, by which we mean that there are no two different

minimal blocking sets contained in B. Szőnyi shows this reducibility result as a corollary of the Jamison/Brouwer-Schrijver theorem on the size of an affine blocking set, see Chapter 5.

Theorem 2.4.1. [139, Remark 3.3] *If B is a blocking set in* PG$(2,q)$ *with $|B| \leq 2q$, then B can be reduced in a unique way to a minimal blocking set.*

The remainder of this section is devoted to the extension of Theorem 2.4.1. This result is also a corollary of Theorem 5.2.2 and Theorem 5.2.3 of Chapter 5, but we choose to include both proofs.

We first extend this theorem to 1-blocking sets in PG(n,q), $n \geq 3$, by associating an algebraic hypersurface to a blocking set in PG(n,q). A combinatorial proof will enable us to extend the theorem further to k-blocking sets.

Let B be a 1-blocking set in PG(n,q), $n \geq 3$, with $|B| \leq 2q-1$. Let the coordinates of the points be $(x_0,\ldots,x_n)$, where $X_n = 0$ defines the hyperplane at infinity H_∞, and let U be the set of affine points of B. Let $|B| = q+k+N$, $N \geq 1$, where N is the number of points of B in H_∞. Furthermore we assume that $(0,\ldots,0,1,0) \in B$. The hyperplanes not passing through $(0,\ldots,0,1,0)$ have equations $m_0X_0+\cdots+m_{n-2}X_{n-2}-X_{n-1}+m_nX_n = 0$ and they intersect H_∞ in the $(n-2)$-dimensional space $X_n = m_0X_0+\cdots+m_{n-2}X_{n-2}-X_{n-1} = 0$. We call the $(n-1)$-tuple $\bar{m} = (m_0,\ldots,m_{n-2})$ the *slope* of the hyperplane. We also identify a slope $\bar{m}$ with the corresponding $(n-2)$-dimensional subspace of H_∞.

Remark. By abuse of notation, we say that the hyperplanes not passing through $(0,\ldots,0,1,0)$ have equations $m_0X_0+\cdots+m_{n-2}X_{n-2}-X_{n-1}+b = 0$, for some $b \in \mathbb{F}_q$, by putting $X_n = 1$ in the equation $m_0X_0+\cdots+m_{n-2}X_{n-2}-X_{n-1}+m_nX_n = 0$. To obtain the intersection of a hyperplane of the form $m_0X_0+\cdots+m_{n-2}X_{n-2}-X_{n-1}+b = 0$ with the hyperplane H_∞, clearly, one has to homogenise the equation to $m_0X_0+\cdots+m_{n-2}X_{n-2}-X_{n-1}+bX_n = 0$, and then put $X_n = 0$.

Definition 2.4.2. *Define the* Rédei polynomial *of U as*

$$\begin{aligned} H(X,X_0,\ldots,X_{n-2}) &= \prod_{(a_0,\ldots,a_{n-1})\in U} (X + a_0X_0 + \cdots + a_{n-2}X_{n-2} - a_{n-1}) \\ &= X^{q+k} + h_1(X_0,\ldots,X_{n-2})X^{q+k-1} + \cdots \\ &+ h_{q+k}(X_0,\ldots,X_{n-2}). \end{aligned}$$

For all $j = 1, \ldots, q+k$, $\deg h_j \leq j$. For simplicity of notations, we will also write $H(X, X_0, \ldots, X_{n-2})$ as $H(X, \bar{X})$.

Definition 2.4.3. *Let C be the affine hypersurface, of degree k, of $\mathrm{AG}(n,q) = \mathrm{PG}(n,q) \setminus H_\infty$, defined by*

$$f(X, \bar{X}) = X^k + h_1(\bar{X})X^{k-1} + \cdots + h_k(\bar{X}) = 0.$$

Theorem 2.4.4. *(i) For a fixed slope $\bar{m}$ defining an $(n-2)$-dimensional subspace at infinity not containing any point of B, the polynomial $X^q - X$ divides $H(X, \bar{m})$, $\forall \bar{m}$. Moreover, if $k < q-1$, then $H(X, \bar{m})/(X^q - X) = f(X, \bar{m})$ and $f(X, \bar{m})$ splits into linear factors over $\mathbb{F}_q$.*

(ii)For a fixed slope $\bar{m} = (m_0, \ldots, m_{n-2})$, the element x is an r-fold root of $H(X, \bar{m})$ if and only if the hyperplane with equation $m_0X_0 + \cdots + m_{n-2}X_{n-2} - X_{n-1} + x = 0$ intersects U in exactly r points.

(iii) If $k < q-1$ and $\bar{m}$ defines an $(n-2)$-dimensional subspace at infinity not containing any point of B, such that the line $X_0 = m_0, \ldots, X_{n-2} = m_{n-2}$ intersects $C : f(X, \bar{X}) = 0$ at $(x, m_0, \ldots, m_{n-2})$ with multiplicity r, then the hyperplane with equation $m_0X_0 + \cdots + m_{n-2}X_{n-2} - X_{n-1} + x = 0$ intersects B in exactly $r+1$ points.

Proof. (i) For every value of b, the hyperplane $m_0X_0 + \cdots + m_{n-2}X_{n-2} - X_{n-1} + b = 0$ contains a point $(a_0, \ldots, a_{n-1})$ of U. So $X - b$ is a factor of $H(X, \bar{m})$. If $k < q-1$, then $H(X, \bar{m}) = X^{q+k} + h_1(\bar{m})X^{q+k-1} + \cdots + h_{q+k}(\bar{m}) = (X^k + h_1(\bar{m})X^{k-1} + \cdots + h_k(\bar{m}))(X^q - X) = f(X, \bar{m})(X^q - X)$. Since $H(X, \bar{m})$ splits into linear factors over $\mathbb{F}_q$, this is also true for $f(X, \bar{m})$.

(ii)The multiplicity of a root $X = x$ is the number of linear factors in the product defining $H(X, \bar{m})$ that vanish at $(x, \bar{m})$. This is the number of points of U lying on the hyperplane $m_0X_0 + \cdots + m_{n-2}X_{n-2} - X_{n-1} + x = 0$.

(iii) The slope $(m_0, \ldots, m_{n-2})$ defines an $(n-2)$- subspace at infinity not containing a point of B. If the intersection multiplicity is r, then x is an $(r+1)$-fold root of $H(X, \bar{m})$. Hence, the result follows from (1) and (2). □

Since $|B| \leq 2q - 1 < q^2 + q + 1$, B is not a 2-blocking set in $\mathrm{PG}(n,q)$. Hence, we find an $(n-2)$-space α, skew to B. Since $|B| \leq 2q - 1$, B has a tangent hyperplane because all hyperplanes through α must contain at least one point of B. Assume that $X_n = 0$ is a tangent hyperplane to B in the

point $(0,\dots,0,1,0)$. The following theorem links the problem of minimality of the blocking set B to that of the problem of finding linear factors of the affine hypersurface $C : f(X,\bar{X}) = 0$.

Theorem 2.4.5. *(i) If a point $P = (a_0,\dots,a_{n-1}) \in U$ is not essential, then the linear factor $a_0X_0 + \cdots + a_{n-2}X_{n-2} - a_{n-1} + X$ divides $f(X,\bar{X})$.*

(ii) If the linear factor $X + a_0X_0 + \cdots + a_{n-2}X_{n-2} - a_{n-1}$ divides $f(X,\bar{X})$, then $P = (a_0,\dots,a_{n-1}) \in U$ and this point is not essential.

Proof. $\underline{(i) \to (ii)}$ Let $P = (a_0,\dots,a_{n-1}) \in U$ be a non-essential point in B and consider an arbitrary slope $\bar{m} = (m_0,\dots,m_{n-2})$. For this slope $\bar{m}$, there are at least two points of B in the hyperplane $m_0X_0 + \cdots + m_{n-2}X_{n-2} - X_{n-1} + b = 0$ through $(a_0,\dots,a_{n-1})$. Hence, by Theorem 2.4.4, the hyperplane $H : a_0X_0 + \cdots + a_{n-2}X_{n-2} - a_{n-1} + X = 0$ shares the point $(a_{n-1} - (a_0m_0 + \cdots + a_{n-2}m_{n-2}), m_0,\dots,m_{n-2})$ with $C : f(X,\bar{X}) = 0$.

Suppose that $a_0X_0 + \cdots + a_{n-2}X_{n-2} - a_{n-1} + X$ does not divide $f(X,\bar{X})$, and let R be a point of the hyperplane H not lying in C. There are $q^{n-2} + \cdots + q + 1$ lines through R in the hyperplane H, and none of them is contained in C since $R \notin C$. Since such lines contain at most k points of C, H contains at most $k(q^{n-2} + \cdots + q + 1) < (q-1)(q^{n-2} + \cdots + q + 1) = q^{n-1} - 1$ points of C. This is a contradiction since the number of possibilities for $\bar{m}$ is $q^{n-1} - 1$, and each slope corresponds to a distinct point of $H \cap C$.

$\underline{(ii) \to (i)}$ If the linear factor $X + a_0X_0 + \cdots + a_{n-2}X_{n-2} - a_{n-1}$ divides $f(X,\bar{X})$, then for all $\bar{m} = (m_0,\dots,m_{n-2})$, the hyperplane with slope $\bar{m}$ through the point $(a_0,\dots,a_{n-1})$ intersects U in at least two points (Theorem 2.4.4). Here, we use that $X_n = 0$ is a tangent hyperplane to B in the point $(0,\dots,0,1,0)$, so $\bar{m}$ defines an $(n-2)$-dimensional subspace at infinity not containing a point of B. Suppose that $(a_0,\dots,a_{n-1}) \notin U$. Let L be a line in H_∞ then $|U \cup L| \leq q + k + q + 1 < q^2 + q + 1$, hence, it is not a 2-blocking set. This implies that there is an $(n-2)$-space π, skew to $U \cup L$, and since $L \subset H_\infty$, $\pi \not\subset H_\infty$. Consider all hyperplanes through π. One of them passes through $(0,\dots,0,1,0)$; the other ones contain at least two points of B. So $|B| \geq 2q+1$, which is false.

Hence, $P = (a_0,\dots,a_{n-1}) \in U$. Since all hyperplanes through P, including those through $(0,\dots,0,1,0)$, contain at least two points of B, the point P is not essential. □

Corollary 2.4.6. *A 1-blocking set B of size smaller than $2q$ in $\mathrm{PG}(n,q)$ is uniquely reducible to a minimal 1-blocking set.*

Proof. The non-essential points of B correspond to the linear factors over $\mathbb{F}_q$ of the polynomial $f(X,\bar{X})$, and this polynomial is uniquely reducible. □

We will extend this unique reducibility property to k-blocking sets, but for this, we need an easy lemma.

Lemma 2.4.7. *Let μ be an $(n-k)$-space in $\mathrm{PG}(n,q)$ and embed $\mathrm{PG}(n,q)$ in $\mathrm{PG}(n,q^k)$. For every $i=1,\ldots,k-1$, there is an $(n-k+i)$-dimensional subspace of $\mathrm{PG}(n,q^k)$ through μ, meeting $\mathrm{PG}(n,q)$ only in μ. In particular, there exists a hyperplane through μ, meeting $\mathrm{PG}(n,q)$ only in μ.*

Proof. The number of $(n-k+1)$-spaces through μ in $\mathrm{PG}(n,q^k)$ is $\frac{(q^k)^k-1}{q^k-1}$, which is larger than θ_{k-1}, the number of $(n-k+1)$-spaces through μ in $\mathrm{PG}(n,q)$. This proves the lemma for $i=1$. Suppose by induction that the lemma holds for all $1\leq j<k-1$, and let π be an $(n-k+j)$-space, meeting $\mathrm{PG}(n,q)$ only in μ. The number of $(n-k+j+1)$-dimensional subspaces of $\mathrm{PG}(n,q^k)$ through π is $\frac{(q^k)^{k-j}-1}{q^k-1}$, which is larger than the number θ_{k-1} of $(n-k+1)$-spaces through μ in $\mathrm{PG}(n,q)$ if $j<k-1$. Hence, there exists a $(n-k+j+1)$-space ν, meeting $\mathrm{PG}(n,q)$ only in μ. The lemma follows. □

Theorem 2.4.8. *A k-blocking set in $\mathrm{PG}(n,q)$ of size smaller than $2q^k$ is uniquely reducible to a minimal k-blocking set.*

Proof. [10] Let B be a k-blocking set of size smaller than $2q^k$ in $\mathrm{PG}(n,q)$. Embed $\mathrm{PG}(n,q)$ in $\mathrm{PG}(n,q^k)$. Let H be a hyperplane of $\mathrm{PG}(n,q^k)$. Let $H^{q^i}=\{(x_0^{q^i},\ldots,x_n^{q^i})|(x_0,\ldots,x_n)\in H\}$. The space $H\cap H^q\cap H^{q^2}\cap\cdots\cap H^{q^{k-1}}$ is the intersection of H with $\mathrm{PG}(n,q)$. Since it is the intersection of k (not necessarily distinct) hyperplanes, it has dimension at least $n-k$. This implies that the k-blocking set B in $\mathrm{PG}(n,q)$ is also a 1-blocking set in $\mathrm{PG}(n,q^k)$. If B' is a minimal k-blocking set in $\mathrm{PG}(n,q)$, contained in B, then B' is a minimal 1-blocking set in $\mathrm{PG}(n,q^k)$: since B' is minimal, there is a tangent $(n-k)$-space μ in $\mathrm{PG}(n,q)$ for every point P of B', and by Lemma 2.4.7, μ can be extended to a tangent hyperplane in $\mathrm{PG}(n,q^k)$ through P to B'. If

[10] The method used in this proof, namely embedding $\mathrm{PG}(n,q)$ in $\mathrm{PG}(n,q^k)$, is used by Szőnyi and Weiner in the proof of Theorem 2.2.2. It is very useful to extend results for 1-blocking sets to results for k-blocking sets (see also the proof of Theorem 5.3.5).

B' and B'' are two different minimal k-blocking sets, contained in B, then B' and B'' are two different minimal 1-blocking set in $\mathrm{PG}(n, q^k)$, contained in B. Since $|B| < 2q^k$, this is a contradiction. □

3

Linear sets on a projective line

Linear sets generalise the concept of subgeometries in a projective space. They have many applications in finite geometry; linear sets have been intensively used in recent years in order to classify, construct or characterise various geometric structures, e.g. blocking sets (see Chapter 4), translation ovoids of orthogonal spaces [98], and semifields. Finite semifields are division algebras that are not necessarily associative, and can be geometrically constructed using linear sets (see [88] or the chapter *Finite Semifields* in [44]). Despite the fact that linear sets are frequently used, not much is known about them. The only general treatment of linear sets is by Polverino [123]. In this chapter we address three problems on linear sets, contained in a projective line: the equivalence problem, the representation problem and the intersection problem. The solution of the last problem for sublines will be of importance in the proof of the linearity conjecture for k-blocking sets in $\mathrm{PG}(n, p^3)$, p prime (see Chapter 4). The results of this chapter are joint work with Michel Lavrauw, and will appear in *Designs, Codes, and Cryptography* [93].

3.1 A different view on linear sets

Linear sets were introduced in Chapter 1. We will now introduce a different view on linear sets, namely as the quotient geometry of a canonical subgeometry.

It is clear that a canonical subgeometry is a linear set, but a linear set is not necessarily a canonical subgeometry. However, the following theorem by Lunardon and Polverino shows that every linear set is a projection of a canonical subgeometry. For the particular case of linear blocking sets, this was proven in [120]. Let $\Sigma = \mathrm{PG}(m, q)$ be a canonical subgeometry of $\Sigma^* = \mathrm{PG}(m, q^t)$ and suppose there exists an $(m - n - 1)$-dimensional subspace Ω^* of Σ^* disjoint from Σ. Let $\Omega = \mathrm{PG}(n, q^t)$ be an n-dimensional subspace of Σ^* disjoint from Ω^*. Let $p_{\Omega^*,\Omega}$ denote the projection map defined by $x \mapsto \langle \Omega^*, x\rangle \cap \Omega$ for each point $x \in \Sigma^* \setminus \Omega^*$. The point set $\Gamma = p_{\Omega^*,\Omega}(\Sigma)$, i.e., the image of Σ under the projection map $p_{\Omega^*,\Omega}$ is simply called the *projection* of Σ from Ω^* into Ω.

Theorem 3.1.1. [98] *If Γ is a projection of $\mathrm{PG}(m, q)$ into $\Omega = \mathrm{PG}(n, q^t)$, then Γ is an $\mathbb{F}_q$-linear set of rank $m + 1$ and $\langle\Gamma\rangle = \Omega$. Conversely, if L is an $\mathbb{F}_q$-linear set of Ω of rank $m + 1$ and $\langle L\rangle = \Omega = \mathrm{PG}(n, q^t)$, then either L is a canonical subgeometry of Ω or there are an $(m - n - 1)$-dimensional subspace Ω^* of $\Sigma^* = \mathrm{PG}(m, q^t)$ disjoint from Ω and a canonical subgeometry Σ of Σ^* disjoint from Ω^* such that $L = p_{\Omega^*,\Omega}(\Sigma)$.*

If we consider the quotient space Σ^*/Ω^* instead of the projection we obtain the following.

Theorem 3.1.2. *If Γ is the quotient of $\mathrm{PG}(m, q)$ in $\Sigma^*/\Omega^* \cong \mathrm{PG}(n, q^t)$, then Γ is an $\mathbb{F}_q$-linear set of rank $m + 1$ and $\langle\Gamma\rangle = \Sigma^*/\Omega^*$. Conversely, if L is an $\mathbb{F}_q$-linear set of rank $m+1$ and $\langle L\rangle = \mathrm{PG}(n, q^t)$, then there are an $(m-n-1)$-dimensional subspace Ω^* of $\Sigma^* = \mathrm{PG}(m, q^t)$ and a canonical subgeometry Σ of Σ^* disjoint from Ω^* such that L is the quotient of Σ in $\Sigma^*/\Omega^* \cong \mathrm{PG}(n, q^t)$.*

Using this view on linear sets we derive the following equivalences which will be used in this chapter. For the particular case of $\mathbb{F}_q$-linear sets of rank $n + 1$ in $\mathrm{PG}(2, q^n)$, this was proven in [24].

Theorem 3.1.3. *Let S_i be the $\mathbb{F}_q$-linear set of rank $m+1$ in $\mathrm{PG}(n, q^t)$, defined as the quotient of $\Sigma_i \cong \mathrm{PG}(m, q)$ in Σ^*/Ω_i^*, where $\langle\Sigma_i\rangle = \Sigma^* \cong \mathrm{PG}(m, q^t)$, $i = 1, 2$, and suppose that S_i is not a linear set of rank s with $s < m + 1$. The following statements are equivalent.*

(i) There exists an element $\alpha \in \mathrm{P\Gamma L}(n+1, q^t)$ *such that* $S_1^\alpha = S_2$.

(ii) There exists an element $\beta \in \mathrm{Aut}(\Sigma^*)$ *such that* $\Sigma_1^\beta = \Sigma_2$ *and* $(\Omega_1^*)^\beta = \Omega_2^*$.

(iii) For all canonical subgeometries $\Sigma \cong \mathrm{PG}(m, q)$ *in* Σ^*, *skew to* Ω_1^* *and* Ω_2^*, *there exist elements* $\delta, \varphi, \psi \in \mathrm{Aut}(\Sigma^*)$, *such that* $\Sigma^\delta = \Sigma$ *and* $(\Omega_1^*)^{\varphi\delta} = (\Omega_2^*)^\psi$, $\Sigma_1^\varphi = \Sigma$ *and* $\Sigma_2^\psi = \Sigma$.

Proof. (ii)⇒(i) Define $\alpha : S_1 \to S_2$: $\langle \Omega_1^*, x\rangle/\Omega_1^* \mapsto \langle \Omega_2^*, x^\beta\rangle/\Omega_2^*$ with $x \in \Sigma_1$. The map α is well defined: every element of S_1 can be written as $\langle \Omega_1^*, z\rangle/\Omega_1^*$ for some $z \in \Sigma_1$. Suppose that $\langle \Omega_1^*, z\rangle/\Omega_1^* = \langle \Omega_1^*, z'\rangle/\Omega_1^*$ for some z, z' in Σ_1, then, since $\dim\langle z, z', \Omega_1^*\rangle = \dim\langle z^\beta, z'^\beta, (\Omega_1^*)^\beta\rangle$, $(\langle \Omega_1^*, z\rangle/\Omega_1^*)^\alpha = (\langle \Omega_1^*, z'\rangle/\Omega_1^*)^\alpha$. The map α is a collineation: if the points $\langle \Omega_1^*, z\rangle/\Omega_1^*$, $\langle \Omega_1^*, z'\rangle/\Omega_1^*$, and $\langle \Omega_1^*, z''\rangle/\Omega_1^*$ are collinear, then $\dim\langle z, z', z'', \Omega_1^*\rangle = m - r + 2 = \dim\langle z^\beta, z'^\beta, z''^\beta, \Omega_2^*\rangle$, hence, the points $(\langle \Omega_1^*, z\rangle/\Omega_1^*)^\alpha$, $(\langle \Omega_1^*, z'\rangle/\Omega_1^*)^\alpha$, and $(\langle \Omega_1^*, z''\rangle/\Omega_1^*)^\alpha$ are collinear. Moreover, $S_1^\alpha = (\langle \Omega_1^*, \Sigma\rangle/\Omega_1^*)^\alpha = \langle \Omega_2^*, \Sigma\rangle/\Omega_2^* = S_2$.

(i)⇒ (ii) Let Ω_i be an n-dimensional space in Σ^*, skew to Ω_i^*, and denote the projection of the point $x \notin \Omega_i^*$ from Ω_i^* on Ω_i, i.e. $\langle \Omega_i^*, x\rangle \cap \Omega_i$, by $p_i(x)$, $i = 1, 2$.

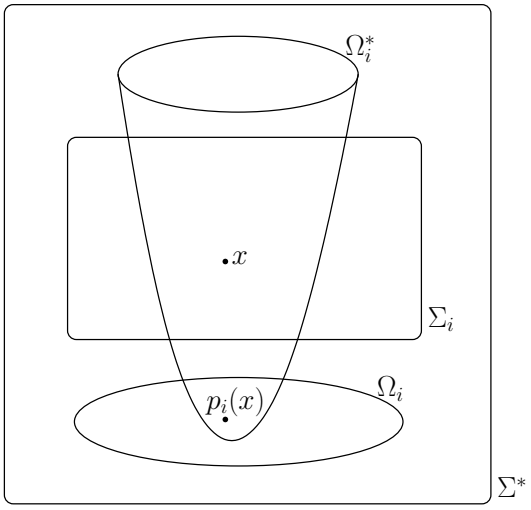

Figure 3.1: The construction of $p_i(x)$.

The collineation α induces a collineation χ of Σ^*, with $\Omega_1^{*\chi} = \Omega_2^*$. Part 1 of this proof, applied to χ, implies that $\Sigma_1/\Omega_1^* \cong \Sigma_1^\chi/\Omega_1^{*\chi} = \Sigma_1^\chi/\Omega_2^*$. Hence, $\Sigma_1^\chi/\Omega_2^* \cong \Sigma_2/\Omega_2^*$.

We claim that there exist $m+1$ linearly independent points $a_0, \ldots, a_m$ in Σ_1^χ and $m+1$ linearly independent points $b_0, \ldots, b_m$ in Σ_2 such that $p_2(a_i) = p_2(b_i)$. Note that, since $\Sigma_1^\chi/\Omega_2^* \cong \Sigma_2/\Omega_2^*$, for every x in Σ_1^χ, there is at least one point x' in Σ_2 with $p_2(x) = p_2(x')$. Suppose that for every choice for a generating set $\{x_0, \ldots, x_m\}$, the set $\{x'_0, \ldots, x'_m\}$ (of possibly coinciding points) does not span the space Σ_2. Let $\{a_0, \ldots, a_m\}$ be a generating set for Σ_1^χ such that $\dim\langle a'_0, \ldots, a'_m\rangle = \mu < m$ is maximal. W.l.o.g. the set $\{a'_0, \ldots, a'_\mu\}$ is a generating set for $\langle a'_0, \ldots, a'_m\rangle$. Denote the space $\langle a_0, \ldots, a_\mu\rangle$ by π_μ, and $\langle a'_0, \ldots, a'_\mu\rangle$ by π'_μ. Let $\{a'_0, \ldots, a'_\mu, b_{\mu+1}, \ldots, b_m\}$ be a generating set of Σ_2. Define the projectivity γ from Σ_1^χ to Σ_2, with $a_i^\gamma = a'_i$ for all $i = 0, \ldots, \mu$, and $a_i^\gamma = b_i$ for all $i = \mu+1, \ldots, m$. Every $x \in \pi_\mu$ can be written as $\sum_{i=0}^{\mu} \lambda_i a_i$, so

$$p_2(x^\gamma) = p_2(\sum_{i=0}^{\mu} \lambda_i a_i^\gamma) = \sum_{i=0}^{\mu} \lambda_i p_2(a_i^\gamma) =$$

$$\sum_{i=0}^{\mu} \lambda_i p_2(a'_i) = \sum_{i=0}^{\mu} \lambda_i p_2(a_i) = p_2(\sum_{i=0}^{\mu} \lambda_i a_i) = p_2(x).$$

Suppose that there is a point $z \in \Sigma_1^\chi \setminus \langle a_0, \ldots, a_\mu\rangle$, such that there is a point z' in $\Sigma_2 \setminus \langle a'_0, \ldots, a'_\mu\rangle$ with $p_2(z) = p_2(z')$. Let $\{a_0, \ldots, a_\mu, z, c_{\mu+1}, \ldots, c_m\}$ be a generating set of Σ_1^χ, then $p_2(a_i) = p_2(a'_i)$ for all $i = 0, \ldots, \mu$, $p_2(z) = p_2(z')$, and $\dim\langle a'_0, \ldots, a'_\mu, z'\rangle > \mu$, a contradiction. Hence, for all points $z \in \Sigma_1^\chi \setminus \langle a_0, \ldots, a_\mu\rangle$, there is a point z' in $\langle a'_0, \ldots, a'_\mu\rangle$ with $p_2(z) = p_2(z')$. As shown before, for all points $t \in \langle a_0, \ldots, a_\mu\rangle$, there is a point $t' \in \langle a'_0, \ldots, a'_\mu\rangle$ with $p_2(t) = p_2(t')$. But this implies that $\langle a'_0, \ldots, a'_\mu\rangle/\Omega_2^* = \Sigma_1^\chi/\Omega_2^*$, a contradiction since S_2 is a linear set of rank $m+1$ with the property that it is not a linear set of lower rank. This proves our claim.

Let δ be the projectivity from Σ_1^χ onto Σ_2 with $a_i^\delta = b_i$, where $\{a_0, \ldots, a_m\}$ is a generating set for Σ_1^χ and $\{b_0, \ldots, b_m\}$ for Σ_2, for which $p_2(a_i) = p_2(b_i)$, $i = 0, \ldots, m$.

Since $\langle\Sigma_1^\chi\rangle = \Sigma^*$, a point x of Σ^* can be written as a linear combination $\sum_{i=0}^{m} \lambda_i a_i$ of points a_i of Σ_1^χ, with $\lambda_i \in \mathbb{F}_{q^n}$. If $x \notin \Omega_2^*$, $p_2(x)$ is well defined, and

$$p_2(x) = \sum_{i=0}^{m} \lambda_i p_2(a_i) = \sum_{i=0}^{m} \lambda_i p_2(a_i^\delta).$$

If $x \notin \Omega_2^*$ and $x^\delta \notin \Omega_2^*$, then

$$p_2(x^\delta) = \sum_{i=0}^{m} \lambda_i p_2(a_i^\delta) = p_2(x). \tag{3.1}$$

Let P be a point of Ω_2^*. We will show that $P^\delta \in \Omega_2^*$. Let P_1 and P_2 be different points of Ω_2. Let $x \neq P, P_1$ be a point of PP_1 and let $y \neq P, P_2$ be a point of PP_2. Either $x^\delta \in \Omega_2^*$, or, by (3.1), $p_2(x^\delta) = p_2(x) = P_1$, and either $P_1^\delta \in \Omega_2^*$, or, by (3.1), $p_2(P_1^\delta) = p_2(P_1) = P_1$. In any case, $x^\delta P_1^\delta \in \langle \Omega_2^*, P_1 \rangle$ and similarly $y^\delta P_2^\delta \in \langle \Omega_2^*, P_2 \rangle$. Now $P^\delta = x^\delta P_1^\delta \cap y^\delta P_2^\delta$, hence, $P^\delta \in \langle \Omega_2^*, P_1 \rangle \cap \langle \Omega_2^*, P_2 \rangle$. Since $P_1 \neq P_2$, the spaces $\langle \Omega_2^*, P_1 \rangle$ and $\langle \Omega_2^*, P_2 \rangle$ are distinct, so $P^\delta \in \Omega_2^*$. This implies that $P^\delta \in \Omega_2^*, \forall P \in \Omega_2^*$, and since the collineation δ maps an $(m-r)$-space to an $(m-r)$-space, we get that ${\Omega_2^*}^\delta = \Omega_2^*$.

Let $\beta := \delta \circ \chi$, then ${\Omega_1^*}^\beta = ({\Omega_1^*}^\chi)^\delta = {\Omega_2^*}^\delta = \Omega_2^*$ and $\Sigma_1^\beta = (\Sigma_1^\chi)^\delta = \Sigma_2$.

(ii)⇒(iii) Let Σ be a canonical subgeometry in Σ^*, skew to Ω_i^*, $i = 1, 2$. Let φ, resp. ψ, be the collineation of Σ^* mapping Σ_1, resp. Σ_2, onto Σ. The first part shows that the linear sets $\Sigma/{\Omega_1^*}^\varphi$ and Σ_1/Ω_1^* are isomorphic, and the linear sets $\Sigma/{\Omega_2^*}^\psi$ and Σ_2/Ω_2^* are isomorphic. Let $\delta := \psi \circ \beta \circ \varphi^{-1}$, then δ is a collineation of Σ^* with $\Sigma^\delta = \Sigma$ and $({\Omega_1^*}^\varphi)^\delta = {\Omega_2^*}^\psi$.

(iii)⇒(ii) The collineation $\beta := \psi^{-1} \circ \delta \circ \varphi$ maps Σ_1 onto Σ_2 and Ω_1^* onto Ω_2^*.□

3.2 Isomorphic linear sets

In this section, we determine in which cases linear sets of rank 3 on a projective line of the same size are projectively equivalent or isomorphic. Let $\mathcal{D}$ be the Desarguesian $(t-1)$-spread in $\mathrm{PG}(2t-1, q)$ and consider the linear set $\mathcal{B}(\pi)$ of rank 3, with $\pi \notin \mathcal{D}$ a plane of $\mathrm{PG}(2t-1, q)$. If there is a spread element H intersecting π in a line, using the terminology introduced by Fancsali and Sziklai in [54], then $\mathcal{B}(\pi)$ is called a *club* and H is called the *head* of $\mathcal{B}(\pi)$. If all elements of $\mathcal{D}$ intersecting π, intersect π in a point, then $\mathcal{B}(\pi)$ is a *scattered linear set of rank* 3, as introduced in Chapter 1.

Remark 1.6 of [54] states without proof that a club in $\mathrm{PG}(1, q^3)$ is projectively equivalent to the set of points $\{x \in \mathbb{F}_{q^3} | \mathrm{Tr}(x) = x + x^q + x^{q^2} = 0\} \cup \{\infty\}$. In Corollary 3.2.2, we show that indeed in the case $t = 3$, all clubs of $\mathrm{PG}(1, q^t)$

are projectively equivalent, and that all scattered linear sets of rank 3 are projectively equivalent too.

If $t > 3$ however, the situation is different and linear sets of the same size are not necessarily projectively equivalent nor isomorphic (see Theorem 3.2.2).

Some parts of the following lemma already appear in the paper of 1982 [57], where Figueroa introduces a class of non-Desarguesian projective planes of order q^3.

Remark. Figueroa planes admit an easy construction. Consider the plane $\mathrm{PG}(2, q^3)$. Applying the automorphism $\sigma : x \mapsto x^q$ to all coordinates induces a collineation of $\mathrm{PG}(2, q^3)$, fixing a subplane $\pi = \mathrm{PG}(2, q)$. Let S be the set of points P such that $P, P^\sigma, P^{\sigma^2}$ are not collinear (these are exactly the points lying on no secant to π) and let T be the set of lines L such that L, L^σ and L^{σ^2} are not concurrent. We now define a bijection μ between the points of S and the lines of T: let $P^\mu = P^\sigma P^{\sigma^2}$ for a point $P \in S$ and let $L^\mu = L^\sigma \cap L^{\sigma^2}$.

Let $\mathcal{P}$ be the set of points of $\mathrm{PG}(2, q^3)$ and let $\mathcal{L}$ be the set of lines of $\mathrm{PG}(2, q^3)$. We change the incidence I of $\mathrm{PG}(2, q^3)$ to the following for $P \in \mathcal{P}$ and $L \in \mathcal{L}$:

$$P\mathrm{I}'L \iff \begin{cases} L^\mu \mathrm{I} P^\mu & \text{if } P \in S \text{ and } L \in T, \\ P\mathrm{I}L & \text{otherwise.} \end{cases}$$

The incidence structure $(\mathcal{P}, \mathcal{L}, \mathrm{I}')$ is the projective Figueroa plane of order q^3 and is not Desarguesian for $q > 2$.

Lemma 3.2.1. *Let $H \leq \mathrm{P\Gamma L}(3, q^3)$ denote the setwise stabiliser of a subplane $\pi \cong \mathrm{PG}(2, q)$ of $\mathrm{PG}(2, q^3)$, and put $H' := H \cap \mathrm{PGL}(3, q)$, let T denote the set of points that do not lie on a secant line of π, and let S denote the set of points of $\mathrm{PG}(2, q^3) \setminus \pi$ that lie on a secant line of π.*

(i) For each point X of π, the stabiliser H'_X of X in H' acts regularly on the set T, and for each point R of T, the stabiliser H'_R of R in H' acts transitively on the points of π.

(ii) The group H' acts transitively on the set S. The stabiliser H'_Z of a point $Z \in S$ acts transitively on the points of π not lying on the secant line through Z.

Proof. (i) The set T has size

$$t := q^6 + q^3 + 1 - (q^2 + q + 1) - (q^2 + q + 1)(q^3 - q) = q^6 - q^5 - q^4 + q^3.$$

Let $X \in \pi$. Since H' acts transitively on the points of π and has size $(q^2+q+1)t$, we have $|H'_X| = t$. We show that H'_X acts regularly on the points of T, by proving that H'_{XY} is trivial, for each $Y \in T$. An element of H'_{XY} corresponds to a matrix A with entries in $\mathbb{F}_q$ with an eigenvalue in $\mathbb{F}_q$, with eigenvector X, and an eigenvalue in $\mathbb{F}_{q^3} \setminus \mathbb{F}_q$, corresponding to Y. But Y^q and Y^{q^2} are also fixed by A. Since $Y \in T$, Y, Y^q and Y^{q^2} are linearly independent. Since a matrix A can have at most three eigenvalues which correspond to linearly independent points, and there are already three linearly independent points with eigenvalue in $\mathbb{F}_{q^3} \setminus \mathbb{F}_q$, there cannot be an eigenvector with eigenvalue in $\mathbb{F}_q$. This implies that H'_{XY} is trivial.

For each point $R \in T$, there exists an element $\alpha \in \mathrm{PGL}(3,q)$ of order q^2+q+1 (generating a Singer cycle) that fixes R. This implies that the size of H'_R is at least q^2+q+1. Since the stabiliser H'_{RX} of a point $X \in \pi$ is trivial, and the orbit of a point of π can have length at most q^2+q+1, from $|H'_R| = |H'_{RX}||X^{H'_R}|$, we derive that $|X^{H'_R}| = q^2+q+1$. So H'_R acts transitively on the points of π.

(ii) The number of points in S is equal to

$$s := (q^2+q+1)(q^3-q).$$

Let Z be a point of S, and let L be the secant line to $\mathrm{PG}(2,q)$ through Z. Since an element of H'_Z fixes three different points Z, Z^q, Z^{q^2} on L, it must fix L pointwise. It follows that an element of H'_{ZX}, with $X \in \pi \setminus L$, is a homology with center X and axis L, and each homology with center X and axis L clearly belongs to H'_{ZX}. It follows that $|H'_{ZX}| = q-1$. Since the group of elations of π with axis L acts transitively on the points not on L, $|X^{H'_Z}| = q^2$. Now $|H'_Z| = |H'_{ZX}||X^{H'_Z}| = (q-1)q^2$, $|H'| = |H'_Z||Z^{H'}|$ and $|H'| = (q^2+q+1)(q^6-q^5-q^4+q^3)$, hence $|Z^{H'}| = (q^2+q+1)(q^3-q) = s$. This implies that H' acts transitively on the points of S. □

Theorem 3.2.2. *(i) All clubs in* $\mathrm{PG}(1,q^3)$ *and all scattered linear sets of rank* 3 *in* $\mathrm{PG}(1,q^3)$ *are projectively equivalent.*

(ii) All scattered linear sets of rank 3 *in* $\mathrm{PG}(1,q^4)$ *are projectively equivalent.*

(iii) All clubs and all scattered linear sets of rank 3 *in* $\mathrm{PG}(1,2^5)$ *are isomorphic, but there exist projectively inequivalent clubs and projectively inequivalent scattered linear sets of rank* 3 *in* $\mathrm{PG}(1,2^5)$.

(iv) In all other cases, there exist non-isomorphic clubs and non-isomorphic scattered linear sets of rank 3.

Proof. Let H be the setwise stabiliser in $\mathrm{P\Gamma L}(3,q^t)$ of a subplane $\pi \cong \mathrm{PG}(2,q)$ of $\mathrm{PG}(2,q^t)$. Let T denote the set of points that do not lie on a secant line of π, and let S denote the set of points of $\mathrm{PG}(2,q^3) \setminus \pi$ that lie on a secant line of π. By the equivalent view on linear sets using quotient geometries and Theorem 3.1.3, it suffices to study the transitivity of the action of H on the sets T and S. Since the group $H' = \mathrm{PGL}(3,q)$ acts regularly on the frames of $\mathrm{PG}(2,q)$ and the only element of $\mathrm{PGL}(3,q^t)$ fixing a frame is the identity element, it follows that

$$|H| = t|\mathrm{P\Gamma L}(3,q)| = thq^3(q^3-1)(q^2-1),$$

where $q = p^h$, p prime. Calculating the size of T and S we get

$$|T| = q^{2t} - q^{t+2} - q^{t+1} + q^3 \text{ and } |S| = q^{t+2} + q^{t+1} + q^t - q^3 - q^2 - q.$$

Using Theorem 3.1.3, it follows that there are non-isomorphic scattered linear sets of rank 3 in $\mathrm{PG}(1,q^t)$, $t \geq 6$, and in $\mathrm{PG}(1,q^5)$, for $q > 2$, and that there are non-isomorphic clubs in $\mathrm{PG}(1,q^t)$, $t > 7$, and in $\mathrm{PG}(1,q^7)$ for $q > 5$. If $t = 3$, then H acts transitively on both T and S by Lemma 3.2.1. If H acts transitively on S, then $|S|$ has to divide $|H|$. If $t = 5$, this yields that $p^{2h}+1$ has to divide $5h(p^h-1)$. This is only possible in the cases $h = 1, p = 2, 3$. If $t = 7$, this argument yields that $p^{4h}+p^{2h}+1$ has to divide $7h(p^{3h}-p^h)$, which is not possible.

If t is not a prime and $t > 4$, then by the induced action of H on subplanes of order q^s, $s|t$, containing π, it follows that H does not act transitively on S neither on T. If $t = 4$, the same argument shows that H does not act transitively on S. Let X be a point of T in $\mathrm{PG}(2,q^t)$, $t = 3, 4$. An element of H'_X corresponds to a 3×3-matrix A with entries in $\mathbb{F}_q$, having t eigenvectors, three of which are independent, each corresponding to an eigenvalue of A in $\mathbb{F}_{q^t} \setminus \mathbb{F}_q$, a contradiction unless A is the identity matrix. Hence, $|H'_X| = 1$. If $t = 4$, then $|X^{H'}| = |H'| = q^8 - q^6 - q^5 + q^3 = |T|$, and we conclude that H' acts transitively on the points of T in this case.

This leaves only the cases $\mathrm{PG}(2,q^5)$ with $q = 2, 3$. Let Z be a point of S on a secant L of π. Since H_Z fixes $Z, Z^q, Z^{q^2}, Z^{q^3}, Z^{q^4}$ on L, L is fixed pointwise. The elements of H_Z consist of an element φ of $\mathrm{PGL}(3,q)$ and an element α of $\mathrm{Aut}(\mathbb{F}_{q^t})$ and since L is fixed pointwise, α is trivial and $H_Z = H'_Z$, with $H' = \mathrm{PGL}(3,q)$. As in the proof of Lemma 3.2.1, one shows that the size of H'_Z is equal to $(q-1)q^2$. If $q^t = 2^5$, then $|H| = 840 = |H_Z|.|Z^H| = 4.|Z^H|$. Since $|S| = 210$, H acts transitively on the points of S. Together with Theorem 3.1.3

this shows that all clubs in $\mathrm{PG}(1, 2^5)$ are isomorphic. Since $|H_Z| = |H'_Z| = 4$ and $|H'| = 168$, it follows that $|Z^{H'}| = 42 < 210$, hence, not all clubs in $\mathrm{PG}(1, 2^5)$ are projectively equivalent.

If $q = 3^5$, then $|H_Z| = 18$ and $|H| = 28080$, from which it follows that $|Z^H| = 1560 < |S| = 3120$, which implies that there are non-isomorphic clubs in $\mathrm{PG}(1, 3^5)$.

Let X be a point of T in $\mathrm{PG}(2, 2^5)$. Since $|H'_X| = 1$, $|X^{H'}| = |H'| = 168 < |T| = 840$. So H' does not act transitively on the points of T, and H' has five orbits $\mathcal{O}_1, \ldots, \mathcal{O}_5$ of length 168 on the points of T. The element $\sigma : x \mapsto x^2$ of $\mathrm{P\Gamma L}(3, 2^5)$ has order five. Since 5 is not a divisor of 168, σ permutes the orbits $\mathcal{O}_i$. We conclude that all scattered linear sets in $\mathrm{PG}(2, 2^5)$ are isomorphic, but not necessarily projectively equivalent. □

3.3 The intersection of subgeometries in $\mathrm{PG}(n, q^t)$

Subgeometries provide examples of linear sets. The study of the intersection of two subgeometries started in 1980 when Bose, Freeman and Glynn determined the possibilities for the intersection of two Baer subplanes in $\mathrm{PG}(2, q)$ [27]. In 2003, Jagos, Kiss and Pór settled the case of intersecting Baer subgeometries in $\mathrm{PG}(n, q)$ [78]. Only recently, the problem of the intersection of subgeometries was solved in general by Donati and Durante [50] where they proved the following.

Theorem 3.3.1. [50, Theorem 1.3] *Let G and G' be two subgeometries of order p^t and $p^{t'}$ respectively of $\mathrm{PG}(n, q)$, $q = p^h$, with $t \leq t'$ and let $m = \gcd(t, t')$. If $G \cap G'$ is non-empty, then $G \cap G' = G_1 \cup \ldots \cup G_k$, with $k \leq \frac{q-1}{p^{t'}-1}$ and with $G_1, \ldots, G_k$ subgeometries of order p^m of independent subspaces of $\mathrm{PG}(n, q)$.*

They also showed the converse:

Theorem 3.3.2. [50, Theorem 1.4] *Let t and t' be two positive divisors of h with $t|t'$. Let $k \leq \min\{n + 1, \frac{q-1}{p^{t'}-1}\}$ and let $G_1, \ldots, G_k$ be subgeometries of order p^t of independent subspaces of $\mathrm{PG}(n, q)$, $q = p^h$. Then there exist two subgeometries G and G' of order p^t and $p^{t'}$, respectively, of $\mathrm{PG}(n, q)$ such that $G \cap G' = G_1 \cup \ldots \cup G_k$.*

The intersection of linear sets in general is more difficult: it will not be the union of linear sets contained in independent subspaces. In Section 3.4, we determine the possible intersection of a subline with a linear set, and in Section 3.6, we determine the intersection of two linear sets of rank 3.

3.4 The intersection of a subline and an $\mathbb{F}_q$-linear set in $\mathrm{PG}(1, q^t)$

The intersection of an $\mathbb{F}_q$-*subline* (an $\mathbb{F}_q$-linear set of rank 2 with $q+1$ points) and a club of $\mathrm{PG}(1, q^t)$ was first investigated in [54]. However, in this proof, the authors used the 'fact' that all clubs of $\mathrm{PG}(1, q^t)$ are projectively equivalent, which is in general not true (see Corollary 3.2.2). Theorem 3.4.4 shows that their result is correct and Lemma 3.4.2 gives a description of the geometric structure of the intersection points of the subline and the linear set. In the meantime, Sz.L. Fancsali and P. Sziklai provided a correct proof for this theorem, using coordinates, in [55] .

To our knowledge, the only other result on the intersection of linear sets is the following theorem, which gives an upper bound on the size of the intersection of an $\mathbb{F}_q$-linear set and an $\mathbb{F}_{q\sqrt{q}}$-linear set in $\mathrm{PG}(n, q^3)$ where q is a square.

Theorem 3.4.1. [107, Lemma 4.4, 4.5, 4.6] *Let q be a square. A subline $\mathrm{PG}(1, q)$ and a Baer subline $\mathrm{PG}(1, q\sqrt{q})$ of $\mathrm{PG}(1, q^3)$ share at most a subline $\mathrm{PG}(1, \sqrt{q})$[1]. A Baer subline $\mathrm{PG}(1, q\sqrt{q})$ and an $\mathbb{F}_q$-linear set of q^2+1 or q^2+q+1 points in $\mathrm{PG}(1, q^3)$ share at most $q+\sqrt{q}+1$ points.*

The following lemma determines the intersection of a subline and a linear set of rank 3 in $\mathrm{PG}(n, q^t)$.[2] In Theorem 3.4.4, this is proved for general k. We treat the case $k=3$ separately because it gives information on the structure of the intersection points.

Remark. We like to mention that K. Metsch provided us with a short proof of the first part of this lemma using coordinates. A similar argument can be used to prove Theorem 3.4.4. We do not incorporate these proofs here since they do not give us a method to construct all possible intersection sizes (see Theorem 3.4.5), and do not provide much geometrical insight.

[1] This part of the theorem follows also from Theorem 3.3.2.

[2] This is exactly the case we will use in Chapter 4 to prove the linearity conjecture for k-blocking sets in $\mathrm{PG}(n, p^3)$.

Lemma 3.4.2. *Let $\mathcal{R}=\{\sigma_1,\dots,\sigma_{q+1}\}$ be a $(t-1)$-regulus in $\mathrm{PG}(2t-1,q)$, $q>2$, and let π be a plane in $\mathrm{PG}(2t-1,q)$ such that $\pi\cap\sigma_i$ is a point P_i, $i=1,\dots,4$, where no three points of $\{P_1,P_2,P_3,P_4\}$ are collinear. Then $\pi\cap\sigma_i$ is a point P_i for all $1\le i\le q+1$ and $\{P_1,\dots,P_{q+1}\}$ are the points of a conic in π.*

Proof. Let $\mathcal{R}=\{\sigma_1,\dots,\sigma_{q+1}\}$ be a $(t-1)$-regulus, and let π be a plane such that $\pi\cap\sigma_i$ is a point P_i, $i=1,\dots,4$, where no three points of $\{P_1,P_2,P_3,P_4\}$ are collinear. Let T be the transversal line to $\mathcal{R}$ through P_1. Let $P_1'=P_1$ and let P_j' be the points $\sigma_j\cap T$, $j=2,\dots,q+1$. The 3-dimensional space $\langle T,\pi\rangle$ intersects σ_j in the line $\ell_j=P_jP_j'$, $j=2,3,4$. Hence, T is a transversal line to the 1-regulus $\mathcal{R}(\ell_2,\ell_3,\ell_4)$. The transversal line T' through P_2 to the regulus $\mathcal{R}(\ell_2,\ell_3,\ell_4)$ intersects the spread elements σ_i in points P_i'', with $i=1,5,6,\dots,q+1$ if $q\ge4$ and $i=1$ if $q=3$. This implies that the line $P_i'P_i''$, contained in σ_i, with $i=1,5,6,\dots,q+1$ if $q\ge4$ and $i=1$ if $q=3$, is a line of the regulus $\mathcal{R}(\ell_2,\ell_3,\ell_4)$. Hence, the elements of $\mathcal{R}$ intersect the 3-dimensional space $\langle T,\pi\rangle$ in the lines of a regulus of a hyperbolic quadric. Since π is a plane of $\langle T,\pi\rangle$, not containing a line of an element of $\mathcal{R}$, the line $P_i'P_i''$, with $i=1,5,6,\dots,q+1$ if $q\ge4$ and $i=1$ if $q=3$, meets π in a point P_i and $\{P_1,\dots,P_{q+1}\}$ are the points of a conic. □

Lemma 3.4.3. *If a $(2k-1)$-space π intersects three elements of a $(t-1)$-regulus $\mathcal{R}$ in a $(k-1)$-dimensional subspace, then $\mathcal{R}$ intersects π in a $(k-1)$-regulus.*

Proof. Let σ_i, with $i=1,2,3$, be the three elements of $\mathcal{R}$, with $\mathcal{R}$ a $(t-1)$-regulus, intersecting some $(2k-1)$-space π in a $(k-1)$-space S_i. The spaces S_1,S_2,S_3 determine a unique $(k-1)$-regulus $\mathcal{R}'$. Let S_l be an element of $\mathcal{R}'$. A transversal line T through a point P of S_l to $\mathcal{R}'$ intersects the elements $\sigma_i, i=1,2,3$, in a point of S_i. Hence, T is the unique transversal line through P to $\mathcal{R}$ and it follows that every element of the regulus through S_1,S_2,S_3 is contained in an element of the regulus $\mathcal{R}$, and conversely every element of $\mathcal{R}$ contains an element of the $(k-1)$-regulus $\mathcal{R}'$ through S_1,S_2,S_3. □

Theorem 3.4.4. *An $\mathbb{F}_q$-subline intersects an $\mathbb{F}_q$-linear set of rank k of $\mathrm{PG}(1,q^t)$ in $0,1,\dots,\min\{q+1,k\}$ or $q+1$ points.*

Proof. We proceed by induction on the rank k. For $k=2$, the theorem follows from the observation that three points determine a unique $\mathbb{F}_q$-subline. So now suppose $k>2$ and assume that the statement holds for $k'<k$. Let π be a

$(k-1)$-dimensional space. Let $\mathcal{B}(L_1)$ be an $\mathbb{F}_q$-subline of $\mathrm{PG}(1,q^t)$, intersecting $\mathcal{B}(\pi)$ in at least $k+1$ points. Let $\sigma_1,\ldots,\sigma_{k+1}$ be elements of $\mathcal{B}(L_1)$, intersecting π. We may choose L_1 to go through a point R_1 of $\sigma_1\cap\pi$. Let R_i be a point in $\sigma_i\cap\pi$. If one of the intersections $\sigma_i\cap\pi$, say $\sigma_2\cap\pi$, contains a line M, then the space $\mu=\langle R_1,R_3,\ldots,R_k\rangle$ intersects M in a point, and we have that $\mathcal{B}(L_1)$ intersects $\mathcal{B}(\mu)$, which has rank $k-1$, in k points. By induction, $\mathcal{B}(L_1)$ is contained in $\mathcal{B}(\mu)\subset\mathcal{B}(\pi)$.

So from now on, we assume that all intersections $\sigma_i\cap\pi$, $i=1,\ldots,k+1$, are points R_i. Suppose that $r+1$ points of $\{R_1,\ldots,R_{k+1}\}$ are contained in an $(r-1)$-dimensional subspace ν of π, $r<k$, then again by induction on k, $\mathcal{B}(L_1)$ is contained in $\mathcal{B}(\nu)\subset\mathcal{B}(\pi)$.

Hence, from now on, we also assume that no $r+1$ points of $\{R_1,\ldots,R_{k+1}\}$ are contained in an $(r-1)$-dimensional space, $r<k$.

Let L_i be the transversal line through R_i, $i=2,\ldots,k-2$, to the regulus $\mathcal{B}(L_1)$. Let φ_i be the space $\langle L_1\cap\sigma_i,\ldots,L_{k-2}\cap\sigma_i\rangle$, with $\dim\varphi_i=k-3-x$, for all $1\leq i\leq q+1$. The $(k-3)$-space $\psi=\langle R_1,\ldots,R_{k-2}\rangle$ is contained in the $(2k-2x-5)$-space $\langle\varphi_1,\varphi_2\rangle$. Hence, if $x>0$, $\varphi_i\subset\sigma_i$ meets $\psi\subset\pi$ for all $i\leq q+1$, so, $\mathcal{B}(L_1)\subset\mathcal{B}(\pi)$. Assume that $\dim\varphi_i=k-3$. If one of the points $R_j\in\varphi_j$ for some $j\in\{k-1,k,k+1\}$, then $\dim\langle\pi,L_1,\ldots,L_{k-2}\rangle\leq 2k-4$, and hence π intersects each φ_i, i.e., $\mathcal{B}(L_1)\subset\mathcal{B}(\pi)$.

If $R_j\notin\varphi_j$ for all $j\in\{k-1,k,k+1\}$, the $(k-2)$-spaces $\langle R_i,\varphi_i\rangle$, $i=k-1,k,k+1$, contained in the $(2k-3)$-space $\nu=\langle\pi,L_1,\ldots,L_{k-2}\rangle$, determine a $(k-2)$-regulus $\{\tau_1,\ldots,\tau_{q+1}\}$, by Lemma 3.4.3. Since for all $1\leq i\leq q+1$, the $(k-2)$-space $\tau_i\subset\sigma_i$ and the $(k-1)$-space π, contained in the $(2k-3)$-space ν, intersect in a point, $\mathcal{B}(L_1)\subset\mathcal{B}(\pi)$. □

In the previous theorem, we determined the possible intersection sizes of a subline and an $\mathbb{F}_q$-linear set of rank k. The next theorem shows that all possibilities do occur.

Theorem 3.4.5. *For every subline $L\cong\mathrm{PG}(1,q)$ of $\mathrm{PG}(1,q^t)$, there is a linear set S of rank k, $k\leq t$ and $k\leq q+1$, intersecting L in exactly j points, for all $0\leq j\leq k$.*

Proof. Let $\mathcal{B}(L)=\{\sigma_1,\ldots,\sigma_{q+1}\}$ be a subline of $\mathrm{PG}(1,q^t)$. Let t_P denote the transversal line to $\mathcal{B}(L)$ through a point P that is contained in one of the

elements of the regulus $\mathcal{B}(L)$. Throughout the proof we will use the notation

$$\mu_i := \langle P_1, \ldots, P_i \rangle, \text{ and } \tau_i := \langle t_{P_1}, \ldots, t_{P_i} \rangle.$$

(i) First we show that whenever we choose j points $\{P_i, \ldots, P_j\}$, $j \leq t$, such that P_i is a point in $\sigma_i \setminus \tau_{i-1}$, it holds that

$$\mathcal{B}(\mu_j) \cap \mathcal{B}(L) = \{\sigma_1, \ldots, \sigma_j\}.$$

This statement is trivial for $j \in \{1,2\}$. We proceed by induction on j, i.e., suppose that the statement is true for less than j points. By way of contradiction, suppose μ_j intersects more than j elements of $\mathcal{B}(L)$. Then, by Theorem 3.4.4, $\mathcal{B}(L)$ is contained in $\mathcal{B}(\mu_j)$.

Suppose $\mu_j \cap \sigma_i$ is contained in τ_{j-2}, for all $i \in \{j+1, \ldots, q+1\}$. If $\mu_j \cap \sigma_i$ is contained in μ_{j-2}, for all $i \in \{j+1, \ldots, q+1\}$, then

$$|\mathcal{B}(\mu_{j-2}) \cap \mathcal{B}(L)| > j-2,$$

contradicting the induction hypothesis. Hence there is at least one point

$$P_l \in (\sigma_l \cap \mu_j) \setminus \mu_{j-2}, \ l \in \{j+1, \ldots, q+1\}.$$

If $P_{j-1} \in \langle \mu_{j-2}, P_l \rangle$, then $P_{j-1} \in \tau_{j-2}$, a contradiction. Hence $P_{j-1} \notin \langle \mu_{j-2}, P_l \rangle$, and it follows that $\mu_j = \langle \mu_{j-1}, P_l \rangle$. But then $P_j \in \mu_j \subset \tau_{j-1}$, again a contradiction.

We have shown that there exists an $l \in \{j+1, \ldots, q+1\}$, for which $P_l \in \mu_j \cap \sigma_l$ is not contained in τ_{j-2}. It follows from Lemma 3.4.3 that the $(2j-3)$-space $\langle \tau_{j-2}, P_{j-1}, P_j \rangle = \langle \tau_{j-2}, \mu_j \rangle$, which intersects each of the spread elements σ_{j-1}, σ_j, and σ_l in a $(j-2)$-space, intersects the $(t-1)$-regulus $\mathcal{B}(L)$ in a $(j-2)$-regulus. But this implies that $P_j \in \tau_{j-1}$, a contradiction.

(ii) Now, we show that there exists a linear set of rank k, $k \leq t$ and $k \leq q+1$, intersecting L in exactly j points, for all $0 \leq j \leq k$. The statement is trivial for $j \in \{0,1,2\}$, so fix $3 \leq j \leq k$.

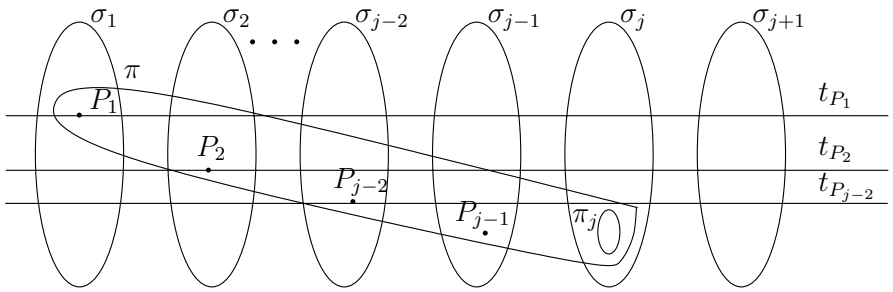

Figure 3.2: The construction appearing in the proof of Theorem 3.4.5.

Let P_1 be the point $\sigma_1 \cap L$, let P_i be a point in $\sigma_i \setminus \tau_{i-1}$, for $2 \leq i \leq j-1$, and let π_j be a $(k-j)$-space in σ_j, skew to τ_{j-1}. Let π be the subspace

$$\pi := \langle \mu_{j-1}, \pi_j \rangle,$$

hence $\mathcal{B}(\pi)$ is a linear set of rank k. We show that $\mathcal{B}(\pi) = \{\sigma_1, \ldots, \sigma_j\}$.

Suppose that one extra element of $\mathcal{B}(L)$, say σ_l, is contained in $\mathcal{B}(\pi)$ and let P_l be a point in the intersection of σ_l with π. By the first part of the proof, it follows that the dimension of $\mu := \langle P_1, \ldots, P_{j-1}, P_l \rangle$ is $j-1$, and since μ and π_j are contained in π, there is a point $P_j \in \mu \cap \pi_j$. This implies that $P_l \in \langle P_1, \ldots, P_j \rangle$. This contradicts the first part of the proof. □

3.5 Sublines contained in a linear set

Throughout this section, we let $\mathcal{D} = \{\sigma_1, \ldots, \sigma_{q^t+1}\}$ denote the Desarguesian $(t-1)$-spread of $\mathrm{PG}(2t-1, q)$ and by a subline, we mean an $\mathbb{F}_q$-subline $\mathrm{PG}(1, q)$. If π is a subspace of $\mathrm{PG}(2t-1, q)$ and s and r are points of π, then the subline $\mathcal{B}(rs)$ is clearly contained in $\mathcal{B}(\pi)$. Here, we investigate the possibility of other sublines through $\mathcal{B}(r)$ and $\mathcal{B}(s)$, contained in $\mathcal{B}(\pi)$. A subline $\mathcal{B}(L)$ of $\mathcal{B}(\pi)$ is called *irregular* if there is no line M of π such that $\mathcal{B}(M) = \mathcal{B}(L)$ and *regular* otherwise.

Lemma 3.5.1. *Let π be a 3-dimensional space in $\mathrm{PG}(2t-1, q)$. The intersection of the elements of $\mathcal{D}$ with π is one of the following:*

1. *π is contained in an element of $\mathcal{D}$,*
2. *π is scattered with respect to $\mathcal{D}$,*
3. *one element of $\mathcal{D}$ intersects π in a plane, and q^3 elements of $\mathcal{D}$ intersect π in a point,*
4. *one or two elements of $\mathcal{D}$ intersect π in a line and the other elements of $\mathcal{D}$ that intersect π, intersect π in a point,*
5. *$q+1$ elements of $\mathcal{D}$ intersect π in a line, and q^3-q elements of $\mathcal{D}$ intersect π in a point. In this case, the $q+1$ lines that are the intersection of an element of $\mathcal{D}$ with π form a (line-)regulus in π, or*

6. *all elements of $\mathcal{D}$, intersecting π, intersect π in a line and in this case, the elements intersecting π define a subline* $\mathrm{PG}(1, q^2)$.

Moreover, if t is odd, possibility 6 *cannot occur and if $t = 3$, only the possibilities* 3 *and* 5 *occur.*

Proof. If there is an element of $\mathcal{D}$ that intersects π in a plane, it is clear that all other non-empty intersections of an element of $\mathcal{D}$ with π are points. Suppose now that only lines and points occur as intersection of an element of $\mathcal{D}$ with π. Let L_1, L_2, L_3 be three lines in π that occur as the intersection of $\sigma_1, \sigma_2, \sigma_3 \in \mathcal{D}$ with π and let T be a transversal line to L_1, L_2, L_3, which exists since the lines L_i are contained in a 3-dimensional space. The line T is a transversal line to $\sigma_1, \sigma_2, \sigma_3$, hence, intersects $q-2$ other spread elements of $\mathcal{D}$, say $\sigma_4, \ldots, \sigma_{q+1}$. A transversal line $T' \neq T$ to $\mathcal{B}(T)$ intersects $\sigma_1, \sigma_2, \sigma_3$, hence, also $\sigma_4, \ldots, \sigma_{q+1}$, which implies that the intersection of σ_i, $i = 1, \ldots, q+1$, with π is a line L_i, and that the lines L_i form a regulus. Suppose now that there is a line $M \neq L_i$ contained in π, with $\mathcal{B}(M) \cap \pi = M$. Since the regulus through three of the lines $\{L_1, \ldots, L_{q+1}, M\}$ is contained in π, we easily see that in that case, every element of $\mathcal{D}$ that intersects π, intersects π in a line. The q^2+1 elements of $\mathcal{D}$ intersecting π in the Desarguesian line spread form a $\mathrm{PG}(1, q^2)$, embedded in $\mathrm{PG}(1, q^t)$, hence, t is even.

Let A be the number of elements of $\mathcal{D}$ intersecting π in a line, and suppose that no element of $\mathcal{D}$ intersects π in a plane. If $t = 3$, then $A(q+1)+(q^3+1-A) = q^3+q^2+q+1$ since all q^3+1 elements of the plane spread $\mathcal{D}$ in $\mathrm{PG}(5, q)$ intersect the 3-dimensional space π. If follows that $A = q+1$. □

3.5.1 Sublines contained in a club

In this section, we show that there are no irregular sublines contained in a club $S \ncong \mathrm{PG}(1, q^2)$.

Lemma 3.5.2. *If $S \cong \mathrm{PG}(1, q^2)$ is a club of $\mathrm{PG}(1, q^t)$, then there are exactly $q+1$ different sublines through two points of S, contained in S.*

Proof. If $S = \mathcal{B}(\pi) \cong \mathrm{PG}(1, q^2)$, then there is a 3-dimensional space μ through π such that $\mathcal{D}$ intersects μ in q^2+1 lines, forming a line spread of μ. Let $\mathcal{B}(r)$ and $\mathcal{B}(s)$ be two different points of S, with $r, s \in \pi$, and let $\mathcal{B}(s) \cap \mu$ be the line L. Any of the $q+1$ lines T_i through r and a point of L intersects $\mathcal{D}$ in

$q+1$ elements of S, hence, $\mathcal{B}(T_i)$ is contained in S. If $\mathcal{B}(T_i) = \mathcal{B}(T_j)$ for some $i \neq j$, then $T_i = T_j$ since T_i and T_j are transversal lines to the regulus $\mathcal{B}(T_i)$ through the point r. □

Lemma 3.5.3. *Let π be a plane in $\mathrm{PG}(2t-1,q)$, such that $\mathcal{B}(\pi)$ is a club $S \ncong \mathrm{PG}(1,q^2)$. If there is a line L for which $\mathcal{B}(L) \subset \mathcal{B}(\pi)$, then there is a line $M \subset \pi$ for which $\mathcal{B}(M) = \mathcal{B}(L)$.*

Proof. Suppose that π is a plane such that $\mathcal{B}(\pi) \ncong \mathrm{PG}(1,q^2)$ and that L is a line, intersecting π in exactly one point, such that $\mathcal{B}(L) \subset \mathcal{B}(\pi)$. This implies that at least $q+1$ elements of $\mathcal{D}$ intersect $\langle \pi, L\rangle$ in a line. But then there are exactly $q+1$ elements of $\mathcal{D}$ intersecting $\langle \pi, L\rangle$ in a line (see Lemma 3.5.1), where the $q+1$ intersection lines form a regulus $\mathcal{R} = \{L_1, \ldots, L_{q+1}\}$. One of these lines L_i of $\mathcal{R}$, say L_1, is contained in π. The plane π contains one line L_1 of the regulus $\mathcal{R}$, hence, it contains a transversal line M to this regulus. □

If $\mathcal{B}(\pi)$ is a club $\ncong \mathrm{PG}(1,q^2)$ with head H and $\mathcal{B}(r)$ and $\mathcal{B}(s)$, $r, s \in \pi$, are two non-head points, then the line rs meets H in a point p. Hence, the subline $\mathcal{B}(rs)$ through $\mathcal{B}(r)$ and $\mathcal{B}(s)$ always contains the head H. It follows from the previous lemma that every subline contained in $\mathcal{B}(\pi)$ is regular and contains the head.

Corollary 3.5.4. *If S is a club of $\mathrm{PG}(1,q^t)$, where $S \ncong \mathrm{PG}(1,q^2)$, then there are no irregular sublines contained in S. Hence, through two non-head points of a club $S \ncong \mathrm{PG}(1,q^2)$ of $\mathrm{PG}(1,q^t)$, there is exactly one subline contained in S, which contains the head of the club.*

3.5.2 Sublines contained in a scattered linear set of rank 3

We show that there are irregular sublines contained in a linear set of rank 3.

Lemma 3.5.5. *Let π be a plane in $\mathrm{PG}(2t-1,q)$, let $\mathcal{B}(r)$ and $\mathcal{B}(s)$ be two different points of $\mathcal{B}(\pi)$, with $r, s \in \pi$. Then the following statements hold.*

(i) There is exactly one 3-dimensional space μ through π such that μ intersects $\mathcal{B}(r)$ and $\mathcal{B}(s)$ in a line.

(ii) If there is a line L through r, $L \not\subset \pi$, such that $\mathcal{B}(s) \in \mathcal{B}(L)$ and $\mathcal{B}(L)$ is contained in $\mathcal{B}(\pi)$, then $\langle \pi, L\rangle$ intersects $\mathcal{B}(s)$ and $\mathcal{B}(r)$ in a line.

Proof. (i) Let π be a plane in $\mathrm{PG}(2t-1,q)$, let $\mathcal{B}(r)$ and $\mathcal{B}(s)$ be two different points of $\mathcal{B}(\pi)$, with $r,s \in \pi$. Since $\langle \mathcal{B}(s), \pi\rangle$ is a $(t+1)$-space, it intersects the $(t-1)$-space $\mathcal{B}(r)$ in a subspace L_r of dimension at least 1. It is not possible that $\langle \mathcal{B}(s), \pi\rangle \cap \mathcal{B}(r)$ has dimension more than one, because then the spread elements $\mathcal{B}(r)$ and $\mathcal{B}(s)$ would intersect, so L_r is a line.

Now $\langle L_r, \pi\rangle$ meets $\mathcal{B}(s)$ in a line L_s since the 3-dimensional space $\langle L_r, \pi\rangle$ is contained in the $(t+1)$-space $\langle \pi, \mathcal{B}(s)\rangle$ and $\mathcal{B}(s)$ is $(t-1)$-dimensional. Using the same reasoning as above, we get that $\langle L_r, \pi\rangle \cap \mathcal{B}(s)$ cannot have dimension larger than one. Hence, $\langle \pi, L_r\rangle$ intersects both $\mathcal{B}(s)$ and $\mathcal{B}(r)$ in a line. Suppose that there is a 3-dimensional space μ' through π, intersecting $\mathcal{B}(r)$ in the line L'_r and $\mathcal{B}(s)$ in the line L'_s, then L'_r is the intersection L_r of $\langle \mathcal{B}(s), \pi\rangle$ with $\mathcal{B}(r)$ and L'_s is the intersection L_s of $\langle \mathcal{B}(r), \pi\rangle$ with $\mathcal{B}(s)$. Hence, μ is uniquely determined.

(ii) Suppose that there is a line L through r, $L \not\subset \pi$, such that $\mathcal{B}(s) \in \mathcal{B}(L)$ and $\mathcal{B}(L)$ is contained in $\mathcal{B}(\pi)$. An element $\mathcal{B}(x) \in \mathcal{B}(L)$, $x \in L \setminus \{r\}$, intersects $\langle \pi, L\rangle$ in the line $L_x = \langle L \cap \mathcal{B}(x), \pi \cap \mathcal{B}(x)\rangle$. The q lines L_x, $x \in L \setminus \{r\}$, belong to a 1-regulus with transversal line L, so $\mathcal{B}(r) \in \mathcal{B}(L)$ intersects $\langle \pi, L\rangle$ in a line too (see Lemma 3.5.1). □

Corollary 3.5.6. *Through two points of a scattered linear set $\mathcal{B}(\pi)$ of rank 3 in $\mathrm{PG}(1,q^t)$, $q>2$, there are at most two sublines contained in $\mathcal{B}(\pi)$. If $t=3$, through two points of $\mathcal{B}(\pi)$, there are exactly two sublines contained in $\mathcal{B}(\pi)$.*

Proof. Let $\mathcal{B}(\pi)$ be a scattered linear set of rank 3 and let $r,s \in \pi$. The subline $\mathcal{B}(rs)$ is contained in $\mathcal{B}(\pi)$. By Lemma 3.5.5 (1), there is a unique 3-dimensional space $\langle L_r, L_s\rangle$, $L_r \in \mathcal{B}(r), L_s \in \mathcal{B}(s)$, through π. If there are exactly two elements of $\mathcal{D}$ that intersect the space $\langle L_r, L_s\rangle$ in a line, there are no irregular sublines contained in $\mathcal{B}(\pi)$, and if there are $q+1$ elements of $\mathcal{D}$ that intersect the space $\langle L_r, L_s\rangle$ in a line, there is an irregular subline through $\mathcal{B}(r)$ and $\mathcal{B}(s)$. Lemma 3.5.5 shows that if there is an irregular subline, this irregular subline is unique.

Lemma 3.5.1 shows that if $t=3$, there are always $q+1$ elements of $\mathcal{D}$ intersecting $\langle L_r, L_s\rangle$ in a line. □

Remark. Through two points of a scattered linear set $\mathcal{B}(\pi)$ of rank 3 in $\mathrm{PG}(1,2^t)$, there are exactly five sublines contained in S. Let P,R be two points of $\mathcal{B}(\pi)$. Through every of the five points Q_i, $i=1,\ldots,5$, different from P and R, contained in $\mathcal{B}(\pi)$, there is exactly one subline containing P,R

and Q_i. Since $q = 2$, this subline only contains the points P, R, Q_i, hence, is completely contained in S.

3.5.3 Irregular sublines as the projection of a subconic in $\mathrm{PG}(2, q^3)$

Using Theorem 3.1.1, we see that a linear set S of rank 3 in $\mathrm{PG}(2, q^3)$ is the projection of a subplane $\mathrm{PG}(2, q)$ from a point in $\mathrm{PG}(2, q^3) \setminus \mathrm{PG}(2, q)$. The projection of a line of $\mathrm{PG}(2, q)$ is a subline of S. The irregular sublines are sublines that are not the projection of a line of $\mathrm{PG}(2, q)$. In this section, we show that an irregular subline is the projection of a conic, and we investigate when the projection of a conic is a subline.

Theorem 3.5.7. [71, Chapter 6] *The points* $(0, 0, 1)$,$(0, 1, x_1)$,$(0, 1, x_2)$, *and* $(0, 1, x_3)$ *of* $\mathrm{PG}(2, q^t)$, $q = p^h$, *are contained in a subline over* $\mathbb{F}_q$ *if and only if* $\frac{x_2 - x_1}{x_3 - x_1} \in \mathbb{F}_q$.

Lemma 3.5.8. *The quotient space* C/P *of an irreducible conic in* $\mathrm{PG}(2, q)$ *over a point* P, *where* P *lies on* C^*, *and not on an extended line of* $\mathrm{PG}(2, q)$, *where* C^* *denotes the extension of* C *to* $\mathrm{PG}(2, q^3)$ *in* $\mathrm{PG}(2, q^3) \setminus \mathrm{PG}(2, q)$, *is an* $\mathbb{F}_q$*-subline.*

Proof. Let C be an irreducible conic in $\mathrm{PG}(2, q)$. There is an element φ of $\mathrm{P\Gamma L}(3, q)$ that maps C onto the conic $C' = \{(1, a, a^2) | a \in \mathbb{F}_q\} \cup \{(0, 0, 1)\}$. We will project C' on the line $X_0 = 0$ from a point $P = (1, \alpha, \alpha^2)$ on C^*, where $\alpha \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$.

The projection of C' from P on the line $X_0 = 0$ consists of the set of points $\{(0, \alpha - x, \alpha^2 - x^2) | x \in \mathbb{F}_q\} \cup \{(0, 0, 1)\}$, which equals the set of points $\{(0, 1, \alpha + x) | x \in \mathbb{F}_q\} \cup \{(0, 0, 1)\}$, since $\alpha \neq x$. Theorem 3.5.7 shows that the four points $(0, 0, 1)$, $(0, 1, \alpha + x_1)$, $(0, 1, \alpha + x_2)$, and $(0, 1, \alpha + x_3)$, $x_1 \neq x_2 \neq x_3 \neq x_1$, are on an $\mathbb{F}_q$-subline iff

$$\frac{\alpha + x_2 - \alpha - x_1}{\alpha + x_3 - \alpha - x_1} \in \mathbb{F}_q.$$

Since this equality holds for all $x_i \in \mathbb{F}_q$, the lemma follows. □

Corollary 3.5.9. *(i) The quotient space* C/P *of an irreducible conic* C *in* $\mathrm{PG}(2, q)$ *over a point* P, *not on an extended line of* $\mathrm{PG}(2, q)$ *in* $\mathrm{PG}(2, q^3) \setminus \mathrm{PG}(2, q)$, *is an* $\mathbb{F}_q$*-subline if and only if* P *lies on* C^*, *where* C^* *denotes the extension of* C *to* $\mathrm{PG}(2, q^3)$.

(ii) The quotient space C/P of an irreducible conic C in $\mathrm{PG}(2,q)$ *over a point P in* $\mathrm{PG}(2,q^3)\setminus\mathrm{PG}(2,q)$ *on an extended line of* $\mathrm{PG}(2,q)$*, is not a subline.*

Proof. (i) Corollary 3.5.6, with $t=3$, shows that there is exactly one irregular subline through two points Q and R of a scattered linear set S of rank 3. It is clear that the subline through the pre-images Q' and R' in $\mathrm{PG}(2,q)$ of Q and R by the projection from P, is projected onto a subline L through Q and R, contained in S.

Since Lemma 3.5.8 shows that the unique conic through the point P, P^q and P^{q^2} and the two points Q' and R' is projected onto a subline, different from L, the statement follows.

(ii) It is shown in Corollary 3.5.4 that there is no irregular subline contained in a club. Hence, the projection of a conic C from a point on an extended line cannot be a subline. □

Remark. In Corollary 3.5.6, we have shown that through two points of a scattered $\mathbb{F}_q$-linear set $\mathcal{B}(\pi)$ of rank 3 in $\mathrm{PG}(1,q^3)$, there is exactly one irregular subline. The q^2+q+1 points of $\mathcal{B}(\pi)$ and the q^2+q+1 irregular sublines obtained in this way, form a projective plane. In the setting of Corollary 3.5.9, we see that the unique irregular subline through the points Q and R of $\mathcal{B}(\pi)$, where $\mathcal{B}(\pi)$ is obtained by projecting the subplane $\mathrm{PG}(2,q)$ from the point $P\in\mathrm{PG}(2,q^3)$, is obtained by projecting the unique subconic of $\mathbb{F}_q$ through the points P, P^q, P^{q^2} and the pre-images of Q and R. In this way, we obtain a set of q^2+q+1 conics, which is called a *packing* [62] or *bundle* [7] *of conics*. The packing appearing here is a so-called *circumscribed* packing.

3.5.4 Irregular sublines contained in a linear set

In the following theorem, we show that every subline is an irregular subline of some linear set.

Theorem 3.5.10. *For every $2\le k\le t+1$ and for every subline $\mathcal{B}(L)$ in* $\mathrm{PG}(1,q^t)$*, there is a linear set $\mathcal{B}(\pi)$ of rank k such that $\mathcal{B}(L)\subset\mathcal{B}(\pi)$, $L\not\subset\pi$, and such that $\mathcal{B}(L)\not\subset\mathcal{B}(\pi')$ for every proper subspace π' of π.*

Proof. Let $\mathcal{B}(L)=\{\sigma_1,\dots,\sigma_{q+1}\}$ be an $\mathbb{F}_q$-subline of $\mathrm{PG}(1,q^t)$. Let t_P denote the transversal line through a point P to $\mathcal{B}(L)$. Let P_1 be a point of σ_1, let P_2 be a point in $\sigma_2\setminus t_{P_1}$, let P_3 be a point in $\sigma_3\setminus\langle t_{P_1},t_{P_2}\rangle$, let P_i, $i\le k-1$, be

a point in $\sigma_i \setminus \langle t_{P_1}, \ldots, t_{P_{i-1}} \rangle$. Let P_k be a point in $\sigma_k \cap \langle t_{P_1}, \ldots, t_{P_{k-1}} \rangle$, not in $\langle P_1, \ldots, P_{k-1} \rangle$.

The $(k-2)$-dimensional space $\langle t_{P_1} \cap \sigma_i, \ldots, t_{P_{k-1}} \cap \sigma_i \rangle \subset \sigma_i$ and the $(k-1)$-space $\pi = \langle P_1, \ldots, P_k \rangle$ are both contained in the $(2k-3)$-dimensional space $\langle \langle t_{P_1} \cap \sigma_1, \ldots, t_{P_{k-1}} \cap \sigma_1 \rangle, \langle t_{P_1} \cap \sigma_k, \ldots, t_{P_{k-1}} \cap \sigma_k \rangle \rangle$. Hence, σ_i meets π for all i.

The same arguments as in the proof of Theorem 3.4.5 show that $\mathcal{B}(L)$ cannot be contained in $\mathcal{B}(\pi')$ with π' a proper subspace of π. □

3.6 The intersection of two linear sets of rank 3

In [56], the authors show that two different linear sets of rank 3 in $\mathrm{PG}(1, q^3)$ share at most $2q+2$ points, where $q = p^h$, $p \geq 7$, using coordinates and the fact that linear sets of the same size in $\mathrm{PG}(1, q^3)$ are projectively equivalent. Now, we prove this in a geometric way and extend this result, at least for odd q, to $\mathrm{PG}(1, q^t)$. Moreover, we show that the bound is sharp.

Lemma 3.6.1. *Let π and π' be two planes in $\mathrm{PG}(t(n+1)-1, q)$ that meet in a line. Let $\mathcal{D}$ be a Desarguesian $(t-1)$-spread in $\mathrm{PG}(t(n+1)-1, q)$. If $\mathcal{B}(\pi) \neq \mathcal{B}(\pi')$, then $|\mathcal{B}(\pi) \cap \mathcal{B}(\pi')| \in \{1, 2, q+1, q+2, q+3, 2q, 2q+1, 2q+2\}$.*

Proof. By Lemma 3.5.1, the number of elements of $\mathcal{D}$ intersecting the 3-space $\langle \pi, \pi' \rangle$ in a line is $0, 1, 2$ or $q+1$ since $\mathcal{B}(\pi) \neq \mathcal{B}(\pi')$. If $|\mathcal{B}(\pi \cap \pi')| = 1$, this implies that $\mathcal{B}(\pi)$ and $\mathcal{B}(\pi')$ have 1, 2 or $q+1$ elements in common. If $|\mathcal{B}(\pi \cap \pi')| = q+1$, and no element of $\mathcal{B}(\pi \cap \pi')$ meets π or π' in a line, then $|\mathcal{B}(\pi) \cap \mathcal{B}(\pi')| = q+1, q+2, q+3$ or $2q+2$. If $|\mathcal{B}(\pi \cap \pi')| = q+1$, and there is an element of $\mathcal{B}(\pi \cap \pi')$ that meets π or π' in a line, then $|\mathcal{B}(\pi) \cap \mathcal{B}(\pi')| = q+1, q+2, 2q$ or $2q+1$. □

Theorem 3.6.2. *Two $\mathbb{F}_q$-linear sets of rank 3 in $\mathrm{PG}(1, q^t)$, $q > 3$, intersect in at most $2q+2$ points if q is odd, and in at most $2q+3$ points if q is even.*

Proof. Let $\mathcal{D}$ be a Desarguesian $(t-1)$-spread in $\mathrm{PG}(t(n+1)-1, q)$, $q > 3$. Let π and π' be two planes (in $\mathrm{PG}(t(n+1)-1, q)$) and suppose that $|\mathcal{B}(\pi) \cap \mathcal{B}(\pi')| \geq 2q+3$. By Lemma 1.10.2, we may assume $\pi \cap \pi' \neq \emptyset$. Let $X = \{P \text{ a point of } \pi | \mathcal{B}(P) \subset \mathcal{B}(\pi')\}$ and $X' = \{P \text{ a point of } \pi' | \mathcal{B}(P) \subset \mathcal{B}(\pi)\}$. From Theorem 3.4.4, we get that if a line contains four points of X

(resp. X'), then this line is contained in X (resp. X'). If $\pi \cap \pi'$ is a line, the theorem follows from Lemma 3.6.1, hence, suppose that π intersects π' in a point.

Suppose first that there are no lines in X or X', say in X. Then every line in π contains at most three points of X. In that case, $|X| = 2q + 3$, and every line intersects X in zero or three points and $q = 3^h$. But a maximal arc in a plane of odd order does not exist (Theorem 1.5.4), a contradiction. Hence, from now on, we assume that there is a line L_X in X and a line $L_{X'}$ in X'.

Case 1: $|\mathcal{B}(L_X)| = 1$**.** If $|\mathcal{B}(L_{X'})| = 1$ and $L_X \cap L_{X'} = \emptyset$, the plane $\langle L_X, \mathcal{B}(L_X) \cap \pi' \rangle$, contained in $\mathcal{B}(L_X)$ and $\langle L_{X'}, \mathcal{B}(L_{X'}) \cap \pi \rangle$ contained in $\mathcal{B}(L_{X'})$, are contained in the 4-space $\langle \pi, \pi' \rangle$, a contradiction. If $|\mathcal{B}(L_{X'})| = 1$ and $L_X \cap L_{X'} = \pi \cap \pi'$, either $|\mathcal{B}(\pi) \cap \mathcal{B}(\pi')| = 1, 2$, or $q+1$, or there is a point P in $X \setminus L_X$. In the latter case, the plane π'' through P with $\mathcal{B}(\pi') = \mathcal{B}(\pi'')$ does not contain a line M of X through P with $|\mathcal{B}(M)| = 1$, so the problem reduces to one of the other cases.

Hence, we may suppose that the $q + 1$ elements of $\mathcal{B}(L_{X'})$ meet the plane π in points of a conic C. Since $|X| \geq 2q + 3$, there is a point P_1 contained in $X \setminus (C \cup L_X)$ lying on a secant line M to C which meets L_X in a point not on C, hence containing four points of X, which implies that $M \subset X$. Now if $q > 3$, every point of π lies on a secant line to C, intersecting L_X and M in distinct points. This shows that $\pi = X$.

Case 2: $|\mathcal{B}(L_X)| = q+1$**.** Hence, the elements of $\mathcal{B}(L_X)$ meet π' in the points of a conic C.

Let P_1 be a point of C, and let Q be the point on the line L_X such that $\mathcal{B}(Q) = \mathcal{B}(P_1)$. There is a plane π'', through P_1, such that $\mathcal{B}(\pi) = \mathcal{B}(\pi'')$, moreover, the plane π'' contains a line L through P_1 with $\mathcal{B}(L) = \mathcal{B}(L_X)$. The elements of $\mathcal{B}(L_{X'})$ meet π'' in the points of a conic C'. Since $|X| \geq 2q+3$, X contains a point Q, not on $L \cup C'$. Let π'' play the role of π.

If there is a secant line M through Q to C', not through the possible intersection of L with C', containing four points of X, then M is contained in X. It is easy to see that if $q > 3$, every point R of π, different from the nucleus n of C' if q is even, lies on a secant line through C', meeting M and L. But then R lies on a line with four points of X, and we conclude that $X = \pi$. If q is odd, the secant line M always exists. If q is even, it is possible that Q is the nucleus of C'. In the latter case, if $|X| \geq 2q + 4$, there is a point $Q' \in X$,

lying on a secant line M to C' and we can repeat the previous arguments with $Q = Q'$ to show that $X = \pi$. The statement follows. □

Remark. For general q, there are two linear sets of rank 3, intersecting in $2q + 2$ points. Let μ be a 3-dimensional space, such that there are $q + 1$ elements of $\mathcal{D}$, say σ_i intersecting μ in a line L_i. Let M be a line in μ, skew to all lines L_i. Let π and π' be two different planes through M. The sets $\mathcal{B}(\pi)$ and $\mathcal{B}(\pi')$ have exactly $2q + 2$ points in common.

3.7 The representation of a linear set of rank 3

By the *representation of a linear set*, we mean the different ways in which a linear set can be written as $\mathcal{B}(\pi)$, with π a subspace. In Lemma 1.10.2, we showed that through every point P of $\mathcal{B}(\pi)$, there is a subspace π' with $\mathcal{B}(\pi) = \mathcal{B}(\pi')$. We want to answer the question how many different subspaces $\pi' \neq \pi$ through a fixed point Q of π satisfy $\mathcal{B}(\pi) = \mathcal{B}(\pi')$. It is clear that in the case that π is a line meeting $q+1$ different spread elements (i.e. $\mathcal{B}(\pi)$ is a regulus), the answer is zero. The following results only give a complete answer to the representation problem for $\mathbb{F}_q$-linear sets of rank 3 in $\mathrm{PG}(n, q^3)$ and for clubs in $\mathrm{PG}(1, q^t)$; more work needs to be done in the general case.

Theorem 3.7.1. *Let $\mathcal{D}$ be a Desarguesian $(t-1)$-spread in $\mathrm{PG}(2t-1, q)$. Let π and π' be two planes, intersecting in a line, such that $\mathcal{B}(\pi) = \mathcal{B}(\pi')$ and $|\mathcal{B}(\pi)| > 1$. If $\mathcal{B}(\pi) \ncong \mathrm{PG}(1, q^2)$, then $\pi = \pi'$.*

Proof. Let π and π' be two planes such that $\mathcal{B}(\pi) = \mathcal{B}(\pi')$, intersecting in a line. Since $\mathcal{B}(\pi) \ncong \mathrm{PG}(1, q^2)$, the number of elements of $\mathcal{D}$ intersecting the 3-space $\langle \pi, \pi' \rangle$ is at most $q+1$ (see Lemma 3.5.1). Since $\mathcal{B}(\pi) = \mathcal{B}(\pi')$, at least $q^2 > q + 1$ elements of $\mathcal{D}$ intersect $\langle \pi, \pi' \rangle$ in a line, a contradiction. □

3.7.1 The representation of a club

Theorem 3.7.2. [3] *Let $\mathcal{D}$ be a Desarguesian $(t-1)$-spread in $\mathrm{PG}(2t-1, q)$. Let $\mathcal{B}(\pi)$ be a club in $\mathrm{PG}(1, q^t)$, $q > 2$. If $\mathcal{B}(\pi) \ncong \mathrm{PG}(1, q^2)$, the head of $\mathcal{B}(\pi)$ is uniquely determined. If $\mathcal{B}(\pi) \cong \mathrm{PG}(1, q^2)$, every point of $\mathcal{B}(\pi)$ can play the role of the head.*

[3] This theorem also appears in [55], where the authors use a different method.

Proof. Let $\mathcal{B}(\pi)$ be a club of $\mathrm{PG}(1,q^t)$ with head H and $H\cap\pi=L$. Let π' be a plane such that $\mathcal{B}(\pi')=\mathcal{B}(\pi)$ and let H' be the head of $\mathcal{B}(\pi')$, $H'\cap\pi'=L'$. Suppose that $H\neq H'$. Let P be the point $H'\cap\pi$ and let P' be the point $H\cap\pi'$. Let Q be a point of L. By Lemma 1.10.2, there is an element φ that maps P' to the point Q on L; $\varphi(\pi')$ is a plane π'' and $\varphi(L')$ is a line L'' in π''. Hence, the head of $\mathcal{B}(\pi'')$ is $\mathcal{B}(L'')=\mathcal{B}(L')=H'$ and the point Q is in the intersection of π and π''.

If $\pi\cap\pi''$ is a line, Theorem 3.7.1 proves that either $\pi=\pi''$, and then the head is uniquely determined, or $\mathcal{B}(\pi)$ is a subline $\mathrm{PG}(1,q^2)$. In the latter case, $\mathcal{D}\cap\langle\pi,\pi''\rangle$ is a Desarguesian line spread and every plane μ through a line of this spread in $\langle\pi,\pi''\rangle$ intersects the same q^2+1 elements, hence, every element of $\mathcal{B}(\pi)$ can be chosen to be the head.

Hence, suppose that $\pi\cap\pi''$ is the point Q. Let R and S be different points on the line PQ, different from P and Q. Since $\mathcal{B}(\pi)=\mathcal{B}(\pi'')$, the element $\mathcal{B}(R)$ intersects π'' in a point R', $\mathcal{B}(S)$ intersects π'' in a point S'. Let $R'S'\cap L'$ be the point P''. The lines $R'S'P''$ and RSP are transversal lines to the same regulus, containing H. Hence, the line $R'S'P$", contained in π'', has to intersect H in the point Q of π''. But then there are two different transversal lines through Q to the same regulus, a contradiction. □

Corollary 3.7.3. *Let $\mathcal{B}(\pi)\ncong\mathrm{PG}(1,q^2)$ be a club in $\mathrm{PG}(1,q^t)$, $q>2$.*

(i) If $\mathcal{B}(\pi')=\mathcal{B}(\pi)$ for some plane π', intersecting π not in a point of the head H of $\mathcal{B}(\pi)$, then $\pi=\pi'$.

(ii) If H is the head of $\mathcal{B}(\pi)$, then there are exactly $q+1$ planes π_i through every point of H, such that $\mathcal{B}(\pi_i)=\mathcal{B}(\pi)$.

Proof. Let H be the head of $\mathcal{B}(\pi)$ and let L_1 be the line in π such that $\mathcal{B}(L_1)=H$.

(i) Let $\mathcal{B}(\pi)=\mathcal{B}(\pi')$. If $\pi\cap\pi'$ is a line, then $\pi=\pi'$ by Theorem 3.7.1, hence, suppose that $\pi\cap\pi'$ is a point P. By the assumption, $H\neq\mathcal{B}(P)$. It follows from Theorem 3.7.2 that there is a line L' in π' such that $\mathcal{B}(L')=H$. Let R be a point of π, different from P and not on L_1. If $\dim\langle L_1,L'\rangle=3$, then the line through R and $\mathcal{B}(R)\cap\pi'$, which is contained in $\mathcal{B}(R)$, intersects H, a contradiction. Hence, $\dim\langle L_1,L'\rangle=2$, and the line through P and $L_1\cap L'$ is contained in π and π'. By Theorem 3.7.1, $\pi=\pi'$.

(ii) Let $\mathcal{B}(P_1) \neq H$ be an element of $\mathcal{B}(\pi)$. By Lemma 1.10.2, through every point P_i of $\mathcal{B}(P_1)$, there is a plane π_i, intersecting H in a line L_i, such that $\mathcal{B}(\pi_i) = \mathcal{B}(\pi)$ (note that $\pi_1 = \pi$). It follows from the first part that this plane π_i is unique and that all lines M in H with the property that there is a plane μ through M with $\mathcal{B}(\mu) = \mathcal{B}(\pi)$ are in $\{L_1, \ldots, L_{\frac{q^t-1}{q-1}}\}$. By Theorem 3.7.1, the lines L_i are all distinct.

Let Q be a point of H. For every point R_i, $i = 1, \ldots, q+1$, of L_1, there is, by Lemma 1.10.2, an element φ_i of the elementwise stabiliser of $\mathcal{D}$ with $R_i^{\varphi_i} = Q$. The $q+1$ different lines L^{φ_i}, $i = 1, \ldots, q+1$, all go through Q. By the number of points in H and the number of lines L_i, we see that the number of lines L_i through Q is exactly $q+1$. □

3.7.2 The representation of a scattered linear set of rank 3

In the previous subsection, we showed that if $\mathcal{B}(\pi) = \mathcal{B}(\pi')$ is a club and $\pi \cap \pi'$ is not the head of this club, then $\pi = \pi'$. In the case of a scattered linear set of rank 3, $\mathcal{B}(\pi) = \mathcal{B}(\pi')$ with $\pi \cap \pi' \neq \varnothing$ does not imply $\pi = \pi'$. In the case $t = 3$, we prove that there are exactly two different planes through a point defining the same scattered linear set of rank 3.

Theorem 3.7.4. *Let $\mathcal{D}$ be the Desarguesian 2-spread in $\mathrm{PG}(5, q)$, $q > 4$. Let $\mathcal{B}(\pi)$ be a scattered linear set of rank 3 in $\mathrm{PG}(1, q^3)$. Let P be a point of π. Then there is exactly one plane $\pi' \neq \pi$ through P such that $\mathcal{B}(\pi) = \mathcal{B}(\pi')$.*

Proof. Let π be a plane in $\mathrm{PG}(5, q)$ such that $\mathcal{B}(\pi)$ is a scattered linear set, and let P and R be different points of π. Theorem 3.5.6 shows that through $\mathcal{B}(P)$ and $\mathcal{B}(R)$ there is exactly one subline $\mathcal{B}(L')$ contained in $\mathcal{B}(\pi)$, different from $\mathcal{B}(PR)$. Let L be the transversal line through P to $\mathcal{B}(L')$. Let S be a point of π, such that $\mathcal{B}(S)$ is not contained in $\mathcal{B}(L)$ and let M denote the transversal line through P to the unique regulus in $\mathcal{B}(\pi)$ containing $\mathcal{B}(R)$ and $\mathcal{B}(S)$, such that M is not contained in π.

We claim that $\mathcal{B}(\pi) = \mathcal{B}(\langle M, L\rangle)$. It follows from Theorem 3.4.2 that the intersection points of the elements of $\mathcal{B}(L)$, resp. $\mathcal{B}(M)$, with π form a conic C_L, resp. C_M, through P. Let $Q_1 \neq P$ be a point of C_L. Since $q > 3$, there is a secant line N, through Q_1 to C_M, intersecting C_L in the points Q_1 and Q_2. The subline $\mathcal{B}(N)$ contains four points of the linear set $\mathcal{B}(\langle L, M\rangle)$, hence, it is contained in $\mathcal{B}(\langle L, M\rangle)$ (see Theorem 3.4.2). The linear sets $\mathcal{B}(\pi)$ and

$\mathcal{B}(\langle M, L\rangle)$ have $2q+1+q+1-4$ points in common. If $q > 5$, then $3q-2 > 2q+3$, so Theorem 3.6.2 proves our claim. If $q = 5$, then $3q + 2 > 2q + 2$, and again by Theorem 3.6.2, our claim holds.

Suppose now that there is a plane $\pi' \neq \pi, \langle M, L\rangle$, through P, with $\mathcal{B}(\pi') = \mathcal{B}(\pi)$, and let M' be a line through P in π'. The subline $\mathcal{B}(M')$ is contained in $\mathcal{B}(\pi)$, hence, it is an irregular subline, say through the point R. Let $\mathcal{B}(R) \cap \langle L, M\rangle = \{R'\}$, then $\mathcal{B}(PR')$ is contained in $\mathcal{B}(\pi)$, hence, it is an irregular subline. But this implies that there are three different sublines through P and R contained in $\mathcal{B}(\pi)$, a contradiction by Corollary 3.5.6. □

For $q = 3$ and 4, the construction in the previous proof gives a plane $\pi' \neq \pi$ through P. One can check that also in these cases, the plane π' is such that $\mathcal{B}(\pi') = \mathcal{B}(\pi)$, and it follows by the same arguments as in the previous proof that π' is unique.

Remark. The previous theorem gives another view on the projective packing of conics associated with the scattered linear set of rank 3 in $\mathrm{PG}(1, q^3)$: if π and π' are the planes through the point P for which $\mathcal{B}(\pi) = \mathcal{B}(\pi')$, found in the previous proof, then it is clear that a line in the plane π correponds to a conic in π' (and conversely). If $\mathcal{P}$ is the set of points in π', and $\mathcal{L}$ is the set of all conics in π', obtained in this way, the incidence structure $(\mathcal{P}, \mathcal{L}, \mathrm{I})$ forms a projective plane.

4

The linearity conjecture for k-blocking sets and a proof in PG(n, p^3)

For a long time, all constructed small minimal blocking sets were of Rédei-type, what led people to believe and conjecture that all small minimal blocking sets were of Rédei-type. A counterexample was given in 1998 by Polito and Polverino [119], who noticed that the construction for linear blocking sets, introduced by Lunardon [96] can give a blocking set not of Rédei-type[1]. This construction of linear blocking sets was given in Chapter 1 in a slightly different form.

The construction of linear blocking sets opened up a new perspective on blocking sets and soon people conjectured that all small minimal k-blocking sets in PG(n, q) must be linear. However, it took until 2008 for this so-called 'Linearity conjecture' to be formally stated in the literature, see Sziklai [138].

(LC) *All small minimal k-blocking sets in* PG(n, q) *are linear.*

In this chapter, we give an overview of the cases in which the linearity conjecture is proven. Except for these cases, the linearity conjecture is still open.

[1] At the same time, they extended their construction to construct blocking sets that are not of Rédei-type in André planes, which are a type of translation planes [120].

We also give a new proof for the fact that Rédei-type k-blocking sets are linear using the corresponding result in the plane, and prove the linearity conjecture for k-blocking sets in $\mathrm{PG}(n,p^3)$, p prime. The latter proof is joint work with Leo Storme and Michel Lavrauw, see [91].

Throughout this chapter, the parameters k and n will satisfy $n \geq 2$, $1 \leq k \leq n-1$, unless indicated otherwise.

4.1 Instances for which the linearity conjecture is proven

If B is a linear set, then every line intersects B in a linear set. The following theorem of Sziklai shows that this property holds if $|\ell \cap B| = p^e + 1$ for some line ℓ, where e is the exponent of B as defined in Section 2.2.

Theorem 4.1.1. [138, Corollary 5.2] *Let B be a small minimal k-blocking set with exponent e in $\mathrm{PG}(n,q)$. If for a certain line ℓ, $|\ell \cap B| = p^e + 1$, then $\mathbb{F}_{p^e}$ is a subfield of $\mathbb{F}_q$ and $\ell \cap B$ is $\mathbb{F}_{p^e}$-linear.*

We give an overview of the instances for which the linearity conjecture has been proven.

4.1.1 Blocking sets in $\mathrm{PG}(n,p)$ and $\mathrm{PG}(n,p^2)$, p prime

It is easy to check that the *Fano plane* $\mathrm{PG}(2,2)$ does not contain a non-trivial blocking set.

Blokhuis showed in [16] that a small minimal blocking set in a plane of prime order is trivial.

Theorem 4.1.2. [16, Theorem 1] *The size of a minimal non-trivial blocking set in $\mathrm{PG}(2,p)$, $p > 2$ prime, is at least $3(p+1)/2$.*

Remark. This theorem solved a 25-year old conjecture by Di Paola [48], already mentioned in Chapter 2. Note that the bound $3(p+1)/2$ is sharp, since there exists a projective triangle of side $(p+1)/2$ which forms a non-trivial blocking set in $\mathrm{PG}(2,p)$ (see Theorem 2.1.1). Already in 1975, Bruen showed that the size of a non-trivial minimal blocking set of Rédei-type in $\mathrm{PG}(2,p)$, p prime, has size at least $3(p+1)/2$ [31].

Theorem 2.2.2 by Szőnyi and Weiner shows that a line meets a small minimal k-blocking set B in $\mathrm{PG}(n,p)$ in 0,1, or $p+1$ points. This implies that B is a subspace. Since every $(n-k)$-space has to intersect B in a point, B is a k-space. This proves the linearity conjecture for $\mathrm{PG}(n,p)$, p prime, since a k-space is a linear set.

Szőnyi shows in [139] that the only non-trivial example of a small minimal blocking set in $\mathrm{PG}(2,p^2)$, p prime, is a Baer subplane. For 1-blocking sets in $\mathrm{PG}(n,p^2)$, p prime, Storme and Weiner [137] showed that a Baer subplane is the only example of a small minimal non-trivial blocking set. The majority of work for the general case of small minimal k-blocking sets in $\mathrm{PG}(n,p^2)$ was done by Bokler in [22]. Using the Theorem 2.2.2, Weiner was able to extend the results of Bokler to a complete proof of the linearity conjecture in $\mathrm{PG}(n,p^2)$, p prime [149].

4.1.2 Blocking sets of Rédei-type

Let H_∞ be a hyperplane of $\mathrm{PG}(n,q)$ and consider $\mathrm{AG}(n,q)$ as the affine space obtained by taking H_∞ as the hyperplane at infinity. A subset U of $\mathrm{AG}(n,q)$ is identified with its image under the natural embedding of $\mathrm{AG}(n,q)$ in $\mathrm{PG}(n,q)$. We say that a set of points $U \subset \mathrm{AG}(n,q)$ *determines* the set of *directions* $\{d_1,\ldots,d_N\}$ of H_∞, iff through every d_i in this set, there is a line meeting U in at least two points.

The linearity of planar minimal blocking sets of Rédei-type was proven in 1999 in the following theorem.

Theorem 4.1.3. [17, Theorem 1.1] *Let $U \subset \mathrm{AG}(2,q)$ be a point set of size q containing the origin, let D be the set of its determined directions, and put $N := |D|$. Let e (with $0 \le e \le h$) be the largest integer such that each line with direction in D meets U in a multiple of p^e points. Then we have one of the following cases:*

(i) $e = 0$ *and* $(q+3)/2 \le N \le q+1$,

(ii) $e = 1$, $p = 2$, *and* $(q+5)/3 \le N \le q-1$,

(iii) $p^e > 2$, $e|h$, *and* $q/p^e + 1 \le N \le (q-1)/(p^e-1)$,

(iv) $e = h$ *and* $N = 1$.

Moreover, if $p^e > 3$ or ($p^e = 3$ and $N = q/3+1$), then U is $\mathbb{F}_{p^e}$-linear, and all possibilities for N can be determined explicitly (in principle).

Corollary 4.1.4. *Every minimal blocking set of Rédei-type in $\mathrm{PG}(2,p^h)$, $p > 2$, is linear.*

Proof. A minimal blocking set of Rédei-type in $\mathrm{PG}(2,q)$ can be written a set $U \cup D$, where U is an affine set of size q containing the origin and D is its set of determined directions. The previous theorem shows that $U = \langle e_1, \ldots, e_h \rangle_{\mathbb{F}_{p^e}}$, where $e_i = (x_i, y_i)$. We embed this set in $\mathrm{PG}(2,q)$ by using the map $\phi : (x_i, y_i) \to (x_i, y_i, 1)$. We write $f_i := \phi(e_i)$. Every determined direction can be written as $(x_i' - x_j', y_i' - y_j', 0)$, with $(x_i', y_i') \in U$, $i = 1, 2$. This implies that $U \cup D = \mathcal{B}(\langle f_1, \ldots, f_h, (0,0,1) \rangle_{\mathbb{F}_{p^e}})$, and hence, $U \cup D$ is a linear set. □

In [136], Storme and Sziklai prove the following theorem.

Theorem 4.1.5. [136, Theorem 11] *Let $U \subset \mathrm{AG}(n,q)$, $q = p^h$, $|U| = q^k$ and let $D \subseteq H_\infty$ be the set of directions determined by U with $|D| \leq \frac{(q+3)}{2} q^{k-1} + q^{k-2} + \ldots + q^2 + q$ if $k > 1$ and $|D| < (q+3)/2$ if $k = 1$. Then every line ℓ intersects U either in one point, or $|U \cap \ell| = 0 \bmod p^e$, for some $e|h$. Moreover, the set $U \cap \ell$ is $\mathbb{F}_{p^e}$-linear.*

Remark. In the statement of [136, Theorem 9], the authors do not explicitly mention the case $k = 1$. However, it follows from the same arguments that the statement holds for $k = 1$ if $|D| < (q+3)/2$. From now on, we work with the weaker bound $|D| < (q^k+3)/2$, since all small blocking sets of Rédei-type have $|D| < (q^k+3)/2$, and in this way, we do not have to make a distinction between $k = 1$ and $k \neq 1$.

Lemma 4.1.6. *Let $U \subset \mathrm{AG}(n,q)$, $q = p^h$, $|U| = q^k$, and let $D \subseteq H_\infty$ be the set of directions determined by U, with $|D| < (q^k+3)/2$. If ℓ is a line intersecting U in at least two points, then $|U \cap \ell| = p^x$ for some $x \geq 1$.*

Proof. Let ℓ be a secant line to U. This line ℓ can be embedded in a plane π, with $|\pi \cap U| = q$, and such that $U \cap \pi$ forms, together with the set of its determined directions, a blocking set of Rédei-type in π, where the number of directions, contained in the line $L_\infty = \pi \cap H_\infty$, is at most $(q+1)/2$ (see the proof of Theorem 4.1.5 in [136]). By Corollary 4.1.4, the set $(U \cup D) \cap \pi$ is $\mathbb{F}_{p^{e'}}$-linear. Let e be the maximal integer for which $(U \cup D) \cap \pi$ is $\mathbb{F}_{p^e}$-linear. Looking at the spread representation, one sees that $(U \cup D) \cap \pi$ corresponds to $p^{e(h/e)}$ spread

elements of the Desarguesian $(h/e-1)$-spread $\mathcal{D}$ in $\mathrm{PG}(h(n+1)/e-1,p^e)$, intersecting a fixed subspace μ of $\mathrm{PG}(h(n+1)/e-1,p^e)$ in a point, and one spread element $\mathcal{B}(L_\infty)$ intersecting μ in a hyperplane. Recall that $\mathcal{S}(\nu)$ denotes the set of spread elements corresponding to a subspace ν of $\mathrm{PG}(n,q)$. Because a line ℓ of $\mathrm{PG}(n,q)$ contains exactly one point p_∞ of L_∞ in $\mathrm{PG}(n,q)$, $\mathcal{S}(p_\infty)\cap\mu$ is a hyperplane of $\langle\mathcal{S}(\ell)\rangle\cap\mu$. This implies that $|U\cap\ell|=p^x$ for some $x\geq e$, $e|x$. □

The next theorem will provide a complete proof for the fact that all small blocking sets of Rédei-type are linear.[2]

Theorem 4.1.7. *Let $B=U\cup D$, with $U\subset\mathrm{AG}(n,q)$, $q=p^h$, $|U|=q^k$, and with $D\subseteq H_\infty$ the set of directions determined by U, and with $|D|<(q^k+3)/2$. Then B is $\mathbb{F}_{p^e}$-linear for some $e\geq 1$.*

Proof. For $h=1$, this is a Corollary of the 1 mod p-theorem of Szőnyi and Weiner (Theorem 2.2.2). Let $h\geq 2$. By Theorem 4.1.5, $|\ell\cap U|=0 \bmod p^{e_\ell}$ and $\ell\cap U$ is $\mathbb{F}_{p^{e_\ell}}$-linear for some e_ℓ. Let e be the greatest common divisor of the numbers $\{e_\ell|\ell\cap U \text{ is } \mathbb{F}_{p^{e_\ell}}\text{-linear for some line } \ell\}$. It follows from Theorem 4.1.5 that the value of e is at least 1 and that $e|h$. Let $\mathcal{D}$ be the Desarguesian $(h/e-1)$-spread of $\mathrm{PG}(h(n+1)/e-1,p^e)$.

Let ℓ be the line in $\mathrm{PG}(n,q)$ through two points P and Q of U and let P_∞ be the direction determined by ℓ. By Theorem 4.1.5, ℓ intersects $U\cup P_\infty$ in an $\mathbb{F}_{p^{e'}}$-linear set, $e|e'$, which is also an $\mathbb{F}_{p^e}$-linear set. By Lemma 4.1.6, $|\ell\cap U|=p^x$, where x is a multiple of e, so the elements of $\mathcal{D}$ corresponding to this linear set intersect a fixed x/e-dimensional space π, contained in $\langle\mathcal{S}(P),\mathcal{S}(Q)\rangle$, in a point. Let P_∞ be the direction determined by ℓ, then $\mathcal{S}(P_\infty)$ intersects π in a hyperplane H of π. Let X be the point $\mathcal{S}(P)\cap\pi$.

Let ℓ' be the line through the points P and $Q'\neq P$, where $Q'\in U\setminus(U\cap\ell)$, let P'_∞ be the direction determined by ℓ'. Again, by Theorem 4.1.5, ℓ' intersects $U\cup P'_\infty$ in an $\mathbb{F}_{p^e}$-linear set. Hence, the elements of $\mathcal{D}$ corresponding to this linear set intersect a fixed k'-space π' in a point where we can choose π' through X by Lemma 1.10.2. It follows that $\mathcal{S}(P'_\infty)$ intersects π' in a hyperplane H' of π'.

Let Y be the point $\mathcal{S}(Q)\cap\pi$, and let Y' be the point $\mathcal{S}(Q')\cap\pi'$. By Theorem 4.1.5, QQ' intersects B in a linear set, hence, there is a subspace π'', through

[2] This theorem is stated as a Corollary of Theorem 4.1.5 in [136], but its proof is not completely clear to me.

Y, such that $\mathcal{B}(\pi'') = U \cap QQ'$. The line YY' is contained in $\langle \pi, \pi' \rangle$, so it intersects the hyperplane $\langle H, H' \rangle$ of $\langle \pi, \pi' \rangle$ in a point Z. The spread element $\mathcal{B}(Z)$ intersects π'' in a hyperplane of π''.

This implies that the line YY' is contained in π'', otherwise, there would be two transversal lines through Y to the regulus through $\mathcal{B}(Y), \mathcal{B}(Y')$ and $\mathcal{B}(Z)$, hence, $\mathcal{B}(YY') \subset B$, and $\mathcal{B}(\langle \pi, \pi' \rangle) \subset B$.

Repeating this argument for all lines ℓ' through P shows that $B = \mathcal{B}(\mu)$ for some subspace μ, hence, B is linear. □

Corollary 4.1.8. *A small minimal k-blocking set in $\mathrm{PG}(n,p^h)$, p prime, of Rédei-type is $\mathbb{F}_p$-linear.*

4.1.3 1-Blocking sets in $\mathrm{PG}(n,p^3)$, p prime

In 2000, Polverino showed that a small minimal blocking set in $\mathrm{PG}(2,p^3)$, p prime, is of Rédei-type, and hence, by Theorem 4.1.7, linear [122]. This result was extended to point sets meeting every line in 1 mod q points in $\mathrm{PG}(2,q^3)$ in [124].

For 1-blocking sets in $\mathrm{PG}(n,q^3)$, we have the following theorem of Storme and Weiner ($n \geq 3$).

Theorem 4.1.9. [137, Theorem 5.11] *A minimal 1-blocking set in $\mathrm{PG}(n,q^3)$, $q = p^h$, $h \geq 1$, p prime, $p \geq 7$, $n \geq 2$, of size at most q^3+q^2+q+1, is either:*

(i) a line;

(ii) a Baer subplane when q is square;

(iii) a minimal blocking set of cardinality q^3+q^2+1 in a plane of $\mathrm{PG}(n,q^3)$, projectively equivalent to the set $K = \{(x,T(x),1)|x \in \mathbb{F}_{q^3}\} \cup \{(x,T(x),0)|x \in \mathbb{F}_{q^3} \setminus \{0\}\}$, with T the trace function from $\mathbb{F}_{q^3}$ to $\mathbb{F}_q$ (i.e. $T : \mathbb{F}_{q^3} \to \mathbb{F}_q : x \mapsto x + x^q + x^{q^2}$);

(iv) a minimal blocking set of cardinality q^3+q^2+q+1 in a plane of $\mathrm{PG}(n,q^3)$, projectively equivalent to $\{(x,x^q,1)|x \in \mathbb{F}_{q^3}\} \cup \{(x,x^q,0)|x \in \mathbb{F}_{q^3} \setminus \{0\}\}$;

(v) a subgeometry $\mathrm{PG}(3,q)$ in a 3-dimensional subspace of $\mathrm{PG}(n,q^3)$.

The five possibilities appearing in the previous theorem are linear point sets. In Corollary 4.2.4 we will enlargen the upper bound on B for which Theorem 4.1.9 is valid to prove the linearity conjecture for 1-blocking sets in $\mathrm{PG}(n,p^3)$.

4.1.4 Blocking sets that are a subgeometry

A (naturally embedded) subgeometry $\mathrm{PG}(hk,p)$ is clearly a k-blocking set in $\mathrm{PG}(n,q)$, $q=p^h$, $n\geq hk$. The fourth case in which the linearity conjecture has been proven shows that if the k-blocking set B spans a hk-dimensional space contained in $\mathrm{PG}(n,q)$, then B is always a subgeometry $\mathrm{PG}(hk,p)$.

Theorem 4.1.10. [140, Theorem 3.14] *Let B be a small minimal k-blocking set in $\mathrm{PG}(n,q)$, $q=p^h$, $p>2$ prime. Suppose that $\langle B\rangle = hk$, then B is projectively equivalent to $\mathrm{PG}(hk,p)$.*

4.2 A proof of the linearity conjecture in $\mathrm{PG}(n,p^3)$

In this section we prove the linearity conjecture for small minimal k-blocking sets in $\mathrm{PG}(n,p^3)$, $p\geq 7$, as a corollary of the following theorem.

Theorem 4.2.1. *A small minimal k-blocking set in $\mathrm{PG}(n,q^3)$, $q=p^h$, p prime, $h\geq 1$, $p\geq 7$, intersecting every $(n-k)$-space in $1 \bmod q$ points is linear.*

4.2.1 Some bounds and the case $k=1$

In the following lemma, we show that the size of the intersection of a small minimal blocking set with a subspace of dimension s lies in one of two disjoint intervals.

Lemma 4.2.2. *If B is a subset of $\mathrm{PG}(n,q^3)$, $q\geq 7$, intersecting every $(n-k)$-space, $k\geq 1$, in $1 \bmod q$ points, and π is an $(n-k+s)$-space, $s\leq k$, then either*

$$|B\cap\pi| < q^{3s}+q^{3s-1}+q^{3s-2}+3q^{3s-3}$$

or

$$|B\cap\pi| > q^{3s+1}-q^{3s-1}-q^{3s-2}-3q^{3s-3}.$$

Proof. Let π be an $(n-k+s)$-space of $\mathrm{PG}(n,q^3)$, and put $B_\pi := B \cap \pi$. Let x_i denote the number of $(n-k)$-spaces of π intersecting B_π in i points. Counting the number of $(n-k)$-spaces, the number of incident pairs (P,σ) with $P \in B_\pi, P \in \sigma, \sigma$ an $(n-k)$-space, and the number of triples (P_1,P_2,σ), with $P_1,P_2 \in B_\pi$, $P_1 \neq P_2$, $P_1,P_2 \in \sigma$, σ an $(n-k)$-space yields:

$$\sum_i x_i = \begin{bmatrix} n-k+s+1 \\ n-k+1 \end{bmatrix}_{q^3}, \tag{4.1}$$

$$\sum_i i x_i = |B_\pi| \begin{bmatrix} n-k+s \\ n-k \end{bmatrix}_{q^3}, \tag{4.2}$$

$$\sum i(i-1)x_i = |B_\pi|(|B_\pi|-1) \begin{bmatrix} n-k+s-1 \\ n-k-1 \end{bmatrix}_{q^3}. \tag{4.3}$$

Since we assume that every $(n-k)$-space intersects B in 1 mod q points, it follows that every $(n-k)$-space of π intersects B_π in 1 mod q points, and hence

$$\sum_i (i-1)(i-1-q)x_i \geq 0.$$

Using Equations (4.1), (4.2), and (4.3), this yields that

$$|B_\pi|(|B_\pi|-1)(q^{3n-3k}-1)(q^{3n-3k+3}-1)-(q+1)|B_\pi|(q^{3n-3k+3s}-1)(q^{3n-3k+3}-1)$$
$$+(q+1)(q^{3n-3k+3s+3}-1)(q^{3n-3k+3s}-1) \geq 0.$$

Putting $|B_\pi| = q^{3s}+q^{3s-1}+q^{3s-2}+3q^{3s-3}$ or $|B_\pi| = q^{3s+1}-q^{3s-1}-q^{3s-2}-3q^{3s-3}$ in this inequality, with $q \geq 7$, gives a contradiction. Hence the statement follows. □

We are now ready to prove the induction basis for theorem 4.2.1 (i.e. the case $k=1$).

Theorem 4.2.3. *A small minimal* 1*-blocking set in* $\mathrm{PG}(n,q^3)$*,* $p \geq 7$*, intersecting every hyperplane in* 1 mod q *points, is linear.*

Proof. Lemma 4.2.2 implies that a small minimal 1-blocking set B in $\mathrm{PG}(n,q^3)$, intersecting every hyperplane in 1 mod q points, has at most q^3+q^2+q+3 points. Since every hyperplane intersects B in 1 mod q points, it is easy to see that $|B| = 1 \bmod q$. This implies that $|B| \leq q^3+q^2+q+1$. Theorem 4.1.9 shows that B is linear. □

Corollary 4.2.4. *A small minimal* 1*-blocking set in* $\mathrm{PG}(n,p^3)$*,* p *prime,* $p \geq 7$*, is* $\mathbb{F}_p$*-linear.*

Proof. This follows from Theorem 2.2.2 and Theorem 4.2.3. □

For the remainder of this section, we use the following assumption:

> B is a small minimal k-blocking set in $\mathrm{PG}(n,q^3)$, $p \geq 7$, intersecting every $(n-k)$-space in 1 mod q points.

For convenience let us introduce the following terminology. A *full* line of B is a line which is contained in B. An $(n-k+s)$-space S, $s<k$, is called *large* if S contains more than $q^{3s+1}-q^{3s-1}-q^{3s-2}-3q^{3s-3}$ points of B, and S is called *small* if it contains less than $q^{3s}+q^{3s-1}+q^{3s-2}+3q^{3s-3}$ points of B.

Lemma 4.2.5. *Let* π *be an* $(n-k)$*-space of* $\mathrm{PG}(n,q^3)$*,* $k>1$*.*

(1) If $B\cap\pi$ *is a point, then there are at most* $q^{3k-5}+4q^{3k-6}-1$ *large* $(n-k+1)$*-spaces through* π*.*

(2) If π *intersects* B *in* $q\sqrt{q}+1$*,* q^2+1 *or* q^2+q+1 *collinear points, then there are at most* $q^{3k-5}+5q^{3k-6}-1$ *large* $(n-k+1)$*-spaces through* π*.*

(3) If π *intersects* B *in* $q+1$ *collinear points, then there are at most* $3q^{3k-6}-q^{3k-7}-1$ *large* $(n-k+1)$*-spaces through* π*.*

Proof. Suppose there are y large $(n-k+1)$-spaces through π. Then the number of points in B is at least

$$y(q^4-q^2-q-3-|B\cap\pi|)+((q^{3k}-1)/(q^3-1)-y)x+|B\cap\pi|,\ (*)$$

where x depends on the intersection $B\cap\pi$.

(1) In this case, $x=q^3$ and $|B\cap\pi|=1$. If $y=q^{3k-5}+4q^{3k-6}$, then $(*)$ is larger than $q^{3k}+q^{3k-1}+q^{3k-2}+3q^{3k-3}$, a contradiction.

(2) In this case $x=q^3$ and $|B\cap\pi|\leq q^2+q+1$. If $y=q^{3k-5}+5q^{3k-6}$, then $(*)$ is larger than $q^{3k}+q^{3k-1}+q^{3k-2}+3q^{3k-3}$, a contradiction.

(3) By Theorem 4.1.9 we know that an $(n-k+1)$-space π' through π intersects B in at least q^3+q^2+1 points, since a $(q+1)$-secant in π' implies that the intersection of π' with B is non-trivial and not a Baer subplane, hence $x=q^3+q^2-q$, and $|B\cap\pi|=q+1$. If $3q^{3k-6}-q^{3k-7}$, then $(*)$ is larger than $q^{3k}+q^{3k-1}+q^{3k-2}+3q^{3k-3}$, a contradiction. □

Lemma 4.2.6. *Let L be a line such that $1 < |B \cap L| < q^3 + 1$.*

(1) For all $i \in \{1, \ldots, n-k\}$, there exists an i-space π_i containing L such that $B \cap \pi_i = B \cap L$.

(2) Let N be a line, skew to L. For all $j \in \{1, \ldots, k-2\}$, there exists a small $(n-k+j)$-space π_j containing L, skew to N.

Proof. (1) It follows from Theorem 2.2.2 that every subspace on L intersects $B \setminus L$ in 0 or at least p points. We proceed by induction on the dimension i. The statement obviously holds for $i = 1$. Suppose there exists an i-space π_i on L such that $\pi_i \cap B = L \cap B$, with $i \leq n-k-1$. If there is no $(i+1)$-space intersecting B only on L, then the number of points of B is at least

$$|B \cap L| + p(q^{3(n-i)-3} + q^{3(n-i)-6} + \ldots + q^3 + 1),$$

but, by Lemma 4.2.2, $|B| \leq q^{3k} + q^{3k-1} + q^{3k-2} + 3q^{3k-3}$. If $i < n-k-1$ this is a contradiction. If $i = n-k-1$ then in the above counting argument we may replace the factor p by a factor q, using the hypothesis (B), and hence also in this case we get a contradiction. We may conclude that there exists an i-space π_i on L such that $B \cap L = B \cap \pi_i$, $\forall i \in \{1, \ldots, n-k\}$.

(2) Part (1) shows that there is an $(n-k-1)$-space π_{n-k-1} on L, skew to N, such that $B \cap L = B \cap \pi_{n-k-1}$. If an $(n-k)$-space through π_{n-k-1} contains an extra element of B, it contains at least q^2 extra elements of B, since a line containing two points of B contains at least $q+1$ points of B. This implies that there is an $(n-k)$-space π_{n-k} through π_{n-k-1} with no extra points of B, and skew to N.

We proceed by induction on the dimension i. Lemma 4.2.5 (1) shows that there are at least $(q^{3k}-1)/(q^3-1) - q^{3k-5} - 5q^{3k-6} + 1 > q^3 + 1$ small $(n-k+1)$-spaces through π_{n-k} which proves the statement for $i = 1$.

Suppose that there exists an $(n-k+t)$-space π_{n-k+t} on L, skew to N, such that $B \cap \pi_{n-k+t}$ is a small minimal t-blocking set of π_{n-k+t}. An $(n-k+t+1)$-space through π_{n-k+t} contains at most $(q^{3t+4}-1)(q-1)$ or more than $q^{3t+4} - q^{3t+2} - q^{3t+1} - 3q^{3t}$ points of B (see Lemmas 4.2.2 and 4.2.8).

Suppose all $(q^{3k-3t}-1)(q^3-1) - q^3 - 1$ $(n-k+t)$-spaces through $\pi_{n-k+t-1}$, skew to N, contain more than $q^{3t+4} - q^{3t+2} - q^{3t+1} - 3q^{3t}$ points of B. Then the number of points in B is larger than $q^{3k} + q^{3k-1} + q^{3k-2} + 3q^{3k-3}$ if $t \leq k-3$, a contradiction.

We may conclude that there exists an $(n-k+j)$-space π_j on L such that $B \cap \pi_j$ is a small minimal i-blocking set, skew to N, $\forall j \in \{1, \ldots, k-2\}$. □

As seen in Theorem 4.1.1, many lines intersect a small minimal k-blocking set in a linear set. The following theorem shows that if B is a small minimal k-blocking set in $\mathrm{PG}(n, q^3)$ intersecting every $(n-k)$-space in 1 mod q points, this property holds for every line.

Theorem 4.2.7. *A line L intersects a small minimal k-blocking set B in $\mathrm{PG}(n, q^3)$, $p \geq 7$, intersecting every $(n-k)$-space in 1 mod q points, in a linear set.*

Proof. Note that it is enough to show that L is contained in a subspace of $\mathrm{PG}(n, q^3)$ intersecting B in a linear set. If $k = 1$, then B is linear by Theorem 4.2.3, and the statement follows. Let $k > 1$, let L be a line, not contained in B, intersecting B in at least two points. It follows from Lemma 4.2.6 that there exists an $(n-k)$-space π_L such that $B \cap L = B \cap \pi_L$. If each of the $(q^{3k}-1)/(q^3-1)$ $(n-k+1)$-spaces through π_L is large, then the number of points in B is at least

$$\frac{q^{3k}-1}{q^3-1}(q^4-q^2-q-3-q^3)+q^3 > q^{3k}+q^{3k-1}+q^{3k-2}+3q^{3k-3},$$

a contradiction. Hence, there is a small $(n-k+1)$-space π through L, so $B \cap \pi$ is a small 1-blocking set which is linear by Theorem 4.2.3. This concludes the proof. □

4.2.2 The proof of the Theorem 4.2.1

In the proof of the Theorem 4.2.1, we distinguish two cases. In both cases we need the following two lemmas.

We continue with the following assumption:

> B is a small minimal k-blocking set in $\mathrm{PG}(n, q^3)$, $p \geq 7$, intersecting every $(n-k)$-space in 1 mod q points;

and we consider the following properties:

(H_1) $\forall s < k$: every small minimal s-blocking set, intersecting every $(n-s)$-space in 1 mod q points, not containing a $(q\sqrt{q}+1)$-secant, is $\mathbb{F}_q$-linear;

(H_2) $\forall s < k$: every small minimal s-blocking set, intersecting every $(n-s)$-space in 1 mod q points, containing a $(q\sqrt{q}+1)$-secant, is $\mathbb{F}_{q\sqrt{q}}$-linear.

Lemma 4.2.8. *Suppose* (H_1) *or* (H_2). *If S is a small $(n-k+s)$-space, $0 < s < k$, then $B \cap S$ is a small minimal linear s-blocking set in S, and hence $|B \cap S| \leq (q^{3s+1}-1)/(q-1)$.*

Proof. Clearly $B \cap S$ is an s-blocking set in S. Theorem 2.2.2 implies that $B \cap S$ intersects every $(n-k+s-s)$-space of S in 1 mod p points, and it follows from Theorem 2.2.3 that $B \cap S$ is minimal. Now apply (H_1) or (H_2).□

Lemma 4.2.9. *Suppose* (H_1) *or* (H_2). *Let $k > 2$ and let π_{n-2} be an $(n-2)$-space such that $B \cap \pi_{n-2}$ is a non-trivial small linear $(k-2)$-blocking set, then there are at least $q^3 - q + 6$ small hyperplanes through π_{n-2}.*

Proof. Applying Lemma 4.2.8 with $s = k-2$, it follows that $B \cap \pi_{n-2}$ contains at most $(q^{3k-5}-1)/(q-1)$ points. On the other hand, from Lemmas 4.2.2 and 4.2.8 with $s = k-1$, we know that a hyperplane intersects B in at most $(q^{3k-2}-1)/(q-1)$ points or in more than $q^{3k-2}-q^{3k-4}-q^{3k-5}-3q^{3k-6}$ points. In the first case, a hyperplane H intersects B in at least $q^{3k-3}+1+(q^{3k-3}+q)/(q+1)$ points, using a theorem of Szőnyi and Weiner [140, Corollary 3.7] for the $(k-1)$-blocking set $H \cap B$. If there are at least $q-4$ large hyperplanes, then the number of points in B is at least

$$(q-4)(q^{3k-2}-q^{3k-4}-q^{3k-5}-3q^{3k-6}-\frac{q^{3k-5}-1}{q-1})+$$

$$(q^3-q+5)(q^{3k-3}+1+\frac{q^{3k-3}+q}{q+1}-\frac{q^{3k-5}-1}{q-1})+\frac{q^{3k-5}-1}{q-1},$$

which is larger than $q^{3k}+q^{3k-1}+q^{3k-2}+3q^{3k-3}$ if $q \geq 7$, a contradiction. Hence, there are at most $q-5$ large hyperplanes through π_{n-2}. □

Remark. The proof of Theorem 4.2.1 uses the same ideas in both cases. We prove first that there are many subspaces that have a linear intersection with B and then 'glue' these linear parts together to prove that B is a linear blocking set.

Case 1: there are no $(q\sqrt{q}+1)$-secants

In this case, we will use induction on k to prove that small minimal k-blocking sets in $\mathrm{PG}(n,q^3)$, intersecting every $(n-k)$-space in 1 mod q points and not containing a $(q\sqrt{q}+1)$-secant, are $\mathbb{F}_q$-linear. The induction basis is Theorem 4.2.3. We continue with the assumption (H_1) and we suppose that

> B is a small minimal k-blocking set in $\mathrm{PG}(n,q^3)$, $p \geq 7$, intersecting every $(n-k)$-space in 1 mod q points, not containing a $(q\sqrt{q}+1)$-secant.

Lemma 4.2.10. *If B is non-trivial, there exist a point $P \in B$, a tangent $(n-k)$-space π at the point P and small $(n-k+1)$-spaces H_i, through π, such that there is a $(q+1)$-secant through P in H_i, $i = 1, \ldots, q^{3k-3} - 2q^{3k-4}$.*

Proof. Since B is non-trivial, there is at least one line N with $1 < |N \cap B| < q^3+1$. Lemma 4.2.6 shows that there is an $(n-k)$-space π_N through N such that $B \cap N = B \cap \pi_N$. It follows from Theorem 4.2.7 and Lemma 4.2.5 that there is at least one $(n-k+1)$-space H through π_N such that $H \cap B$ is a small minimal linear 1-blocking set of H. In this non-trivial small minimal linear 1-blocking set, there are $(q+1)$-secants (see Theorem 4.1.9). Let M be one of those $(q+1)$-secants of B. Again using Lemma 4.2.6, we find an $(n-k)$-space π_M through M such that $B \cap M = B \cap \pi_M$.

Lemma 4.2.5 (3) shows that through π_M, there are at least $\frac{q^{3k}-1}{q^3-1} - 3q^{3k-6} + q^{3k-7}+1$ small $(n-k+1)$-spaces. Let P be a point of M. Since in each of these intersections, P lies on at least q^2-1 other $(q+1)$-secants, a point P of M lies in total on at least $(q^2-1)(\frac{q^{3k}-1}{q^3-1} - 3q^{3k-6} + q^{3k-7} + 1)$ other $(q+1)$-secants. Since each of the $\frac{q^{3k}-1}{q^3-1} - 3q^{3k-6} + q^{3k-7} + 1$ small $(n-k+1)$-spaces contains at least q^3+q^2-q points of B not on M, and $|B| < q^{3k} + q^{3k-1} + q^{3k-2} + 3q^{3k-3}$ (see Lemma 4.2.2), there are less than $2q^{3k-2} + 6q^{3k-3}$ points of B left in the large $(n-k+1)$-spaces. Hence, P lies on less than $2q^{3k-5} + 6q^{3k-6}$ full lines.

Since B is minimal, P lies on a tangent $(n-k)$-space π. There are at most $q^{3k-5} + 4q^{3k-6} - 1$ large $(n-k+1)$-spaces through π (Lemma 4.2.5 (1)). Moreover, since at least $\frac{q^{3k}-1}{q^3-1} - (q^{3k-5}+4q^{3k-6}-1) - (2q^{3k-5}+6q^{3k-6})$ $(n-k+1)$-spaces through π contain at least q^3+q^2 points of B, and at most $2q^{3k-5}+6q^{3k-6}$ of the small $(n-k+1)$-spaces through π contain exactly q^3+1 points of B, there are at most $2q^{3k-2} + 23q^{3k-3}$ points of B left. Hence, P lies on at most $2q^{3k-3} + 23q^{3k-4}$ $(q+1)$-secants of the large $(n-k+1)$-spaces through π. This

implies that there are at least $(q^2-1)(\frac{q^{3k}-1}{q^3-1} - 3q^{3k-6} + q^{3k-7} + 1) - (2q^{3k-3} + 23q^{3k-4})$ $(q+1)$-secants through P left in small $(n-k+1)$-spaces through π. Since in a small $(n-k+1)$-space through π, there can lie at most q^2+q+1 $(q+1)$-secants through P, this implies that there are at least $q^{3k-3} - 2q^{3k-4}$ $(n-k+1)$-spaces H_i through π such that P lies on a $(q+1)$-secant in H_i. □

Lemma 4.2.11. *Let π be an $(n-k)$-dimensional tangent space of B at the point P. Let H_1 and H_2 be two $(n-k+1)$-spaces through π for which $B \cap H_i = \mathcal{B}(\pi_i)$, for some 3-space π_i through $x \in \mathcal{S}(P)$, $\mathcal{B}(x) \cap \pi_i = \{x\}$ $(i = 1, 2)$ and $\mathcal{B}(\pi_i)$ not contained in a line of $\mathrm{PG}(n, q^3)$. Then $\mathcal{B}(\langle \pi_1, \pi_2 \rangle) \subseteq B$.*

Proof. Since $\langle \mathcal{B}(\pi_i) \rangle$ is not contained in a line of $\mathrm{PG}(n, q^3)$, there is at most one element Q of $\mathcal{B}(\pi_i)$ such that $\langle \mathcal{S}(P), Q \rangle$ intersects π_i in a plane. If there is such a plane, then we denote its point set by μ_i, otherwise we put $\mu_i = \varnothing$.

Let M be a line through x in $\pi_1 \setminus \mu_1$, let $s \neq x$ be a point of $\pi_2 \setminus \mu_2$, and note that $\mathcal{B}(s) \cap \pi_2 = \{s\}$.

We claim that there is a line T through s in π_2 and an $(n-2)$-space π_M through $\langle \mathcal{B}(M) \rangle$ such that there are at least four points $t_i \in T, t_i \notin \mu_2$, such that $\langle \pi_M, \mathcal{B}(t_i) \rangle$ is small and hence has a linear intersection with B, with $B \cap \pi_M = M$ if $k = 2$ and $B \cap \pi_M$ is a small minimal $(k-2)$-blocking set if $k > 2$.

If $k = 2$, the existence of π_M follows from Lemma 4.2.6 (1), and we know from Lemma 4.2.5 (1) that there are at most $q+3$ large hyperplanes through π_M. Denote the set of points of $\mathcal{B}(\pi_2)$, contained in one of those hyperplanes by F. Hence, if Q is a point of $\mathcal{B}(\pi_2) \setminus F$, $\langle Q, \pi_M \rangle$ is a small hyperplane.

Let T_1 be a line through s in $\pi_2 \setminus \mu_2$ and not through x, and suppose that $\mathcal{B}(T_1)$ contains at least $q-3$ points of F.

Let T_2 be a line in $\pi_2 \setminus \mu_2$, through s, not in $\langle x, T_1 \rangle$, and not through x. There are at most $q+3-(q-3)$ reguli through x of $\mathcal{S}(F)$, not in $\langle x, T_1 \rangle$, and if $\mu \neq \varnothing$ one element of $\mathcal{B}(\mu_2)$ is contained in $\mathcal{B}(T_2)$. Since it is possible that $\mathcal{B}(s)$ is an element of F, this gives in total at most eight points of $\mathcal{B}(T_2)$ that are contained in F. This implies, if $q > 11$, that at least 5 of the hyperplanes $\{\langle \pi_M, \mathcal{B}(t) \rangle | t \in T_2\}$ are small.

If $q = 11$, it is possible that $\mathcal{B}(T_2)$ contains at least 8 points of F. If T_3 is a line in $\pi_2 \setminus \mu_2$, through s, not in $\langle x, T_1 \rangle$, nor $\langle x, T_2 \rangle$, nor x, then there are at least five points t of T_3 such that $\langle \pi_M, \mathcal{B}(t) \rangle$ is a small hyperplane.

If $q=7$ and if $\mathcal{B}(s)\in\mathcal{B}(F)$, it is possible that $\mathcal{B}(T_2)$, $\mathcal{B}(T_3)$, and $\mathcal{B}(T_4)$, with T_i a line through s in $\pi_2\setminus\mu_2$, not in $\langle x,T_j\rangle$, $j<i$, and not through x, contain four points of F. A fifth line T_5 through s in $\pi_2\setminus\mu_2$, not in $\langle x,T_j\rangle$, $j<i$, and not through x, contains at least five points t such that $\langle\pi_M,\mathcal{B}(t)\rangle$ is a small hyperplane.

If $k>2$, let T be a line through s in $\pi_2\setminus\mu_2$, not through x. It follows from Lemma 4.2.6 (2) that there is an $(n-2)$-space π_M through $\langle\mathcal{B}(M)\rangle$ such that $B\cap\pi_M$ is a small minimal $(k-2)$-blocking set of $\mathrm{PG}(n,q^3)$, skew to $\mathcal{B}(T)$. Lemma 4.2.9 shows that at most $q-5$ of the hyperplanes through π_M are large. This implies that at least five of the hyperplanes $\{\langle\pi_M,\mathcal{B}(t)\rangle|t\in\mathcal{B}(T)\}$ are small. This proves our claim.

Since $B\cap\langle\mathcal{B}(t_i),\pi_M\rangle$ is linear, also the intersection of $\langle\mathcal{B}(t_i),\mathcal{B}(M)\rangle$ with B is linear, i.e., there exist subspaces τ_i, $\tau_i\cap\mathcal{S}(P)=\{x\}$, such that $\mathcal{B}(\tau_i)=\langle\mathcal{B}(t_i),\mathcal{B}(M)\rangle\cap B$. Since $\tau_i\cap\langle\mathcal{B}(M)\rangle$ and M are both transversals through x to the same regulus $\mathcal{B}(M)$, they coincide, hence $M\subseteq\tau_i$. The same holds for $\tau_i\cap\langle\mathcal{B}(t_i),\mathcal{S}(P)\rangle$, implying $t_i\in\tau_i$. We conclude that $\mathcal{B}(\langle M,t_i\rangle)\subseteq\mathcal{B}(\tau_i)\subseteq B$.

We show that $\mathcal{B}(\langle M,T\rangle)\subseteq B$. Let L' be a line of $\langle M,T\rangle$, not intersecting M. The line L' intersects the planes $\langle M,t_i\rangle$ in points p_i such that $\mathcal{B}(p_i)\in B$. Since $\mathcal{B}(L')$ is a subline intersecting B in at least four points, Lemma 3.4.2 shows that $\mathcal{B}(L')\subset B$. Since every point of the space $\langle M,T\rangle$ lies on such a line L', $\mathcal{B}(\langle M,T\rangle)\subseteq B$.

Hence, $\mathcal{B}(\langle M,s\rangle)\subseteq B$ for all lines M through x, M in $\pi_1\setminus\mu_1$, and all points $s\neq x\in\pi_2\setminus\mu_2$, so $\mathcal{B}(\langle\pi_1,\pi_2\rangle\setminus(\langle\mu_1,\pi_2\rangle\cup\langle\mu_2,\pi_1\rangle))\subseteq B$. Since every point of $\langle\mu_1,\pi_2\rangle\cup\langle\mu_2,\pi_1\rangle$ lies on a line N with $q-1$ points of $\langle\pi_1,\pi_2\rangle\setminus(\langle\mu_1,\pi_2\rangle\cup\langle\mu_2,\pi_1\rangle)$, Lemma 3.4.2 shows that $\mathcal{B}(N)\subset B$. We conclude that $\mathcal{B}(\langle\pi_1,\pi_2\rangle)\subseteq B$. □

Theorem 4.2.12. *A small minimal k-blocking set B in $\mathrm{PG}(n,q^3)$, $p\geq 7$, intersecting every $(n-k)$-space in 1 mod q points and not containing a $(\sqrt{q}+1)$-secant is $\mathbb{F}_q$-linear.*

Proof. If B is a k-space, then B is $\mathbb{F}_q$-linear. If B is a non-trivial small minimal k-blocking set, Lemma 4.2.10 shows that there exists a point P of B, a tangent $(n-k)$-space π at the point P and at least $q^{3k-3}-2q^{3k-4}$ $(n-k+1)$-spaces H_i through π for which $B\cap H_i$ is small and linear, where P lies on at least one $(q+1)$-secant of $B\cap H_i$, $i=1,\ldots,s$, $s\geq q^{3k-3}-2q^{3k-4}$. Let $B\cap H_i=\mathcal{B}(\pi_i)$, $i=1,\ldots,s$, with π_i a 3-dimensional space.

Lemma 4.2.11 shows that $\mathcal{B}(\langle\pi_i,\pi_j\rangle)\subseteq B$, $0\leq i\neq j\leq s$.

If $k=2$, the set $\mathcal{B}(\langle\pi_1,\pi_2\rangle)$ corresponds to a linear 2-blocking set B' in $\mathrm{PG}(n,q^3)$. Since B is minimal, $B=B'$, and the theorem is proven.

Let $k>2$. Denote the $(n-k+1)$-spaces through π, different from H_i, by $K_j, j=1,\ldots,z$ for some z. It follows from Lemma 4.2.10 that $z\leq 2q^{3k-4}+(q^{3k-3}-1)/(q^3-1)$. There are at least $(q^{3k-3}-2q^{3k-4}-1)/q^3$ different $(n-k+2)$-spaces $\langle H_1,H_j\rangle$, $1<j\leq s$. If all $(n-k+2)$-spaces $\langle H_1,H_j\rangle$, contain at least $5q^2-49$ of the spaces K_i, then $z\geq(5q^2-49)(q^{3k-3}-2q^{3k-4}-1)/q^3$, a contradiction if $q\geq 7$. Let $\langle H_1,H_2\rangle$ be an $(n-k+2)$-space containing less than $5q^2-49$ spaces K_i.

Suppose by induction that for any $1<i<k$, there is an $(n-k+i)$-space $\langle H_1,H_2,\ldots,H_i\rangle$ containing at most $5q^{3i-4}-49q^{3i-6}$ of the spaces K_i such that $\mathcal{B}(\langle\pi_1,\ldots,\pi_i\rangle)\subseteq B$.

There are at least $\frac{q^{3k-3}-2q^{3k-4}-(q^{3i}-1)/(q^3-1)}{q^{3i}}$ different $(n-k+i+1)$-spaces $\langle H_1,H_2,\ldots,H_i,H\rangle$, $H\not\subseteq\langle H_1,H_2,\ldots,H_i\rangle$. If all of these contain at least $5q^{3i-1}-49q^{3i-3}$ of the spaces K_i, then

$$\begin{aligned} z\geq\ & (5q^{3i-1}-49q^{3i-3}-5q^{3i-4}+49q^{3i-6})\tfrac{q^{3k-3}-2q^{3k-4}-(q^{3i}-1)/(q^3-1)}{q^{3i}}\\ & +5q^{3i-4}-49q^{3i-6}, \end{aligned}$$

a contradiction if $q\geq 7$. Let $\langle H_1,\ldots,H_{i+1}\rangle$ be an $(n-k+i+1)$-space containing less than $5q^{3i-1}-49q^{3i-3}$ spaces K_i. We still need to prove that $\mathcal{B}(\langle\pi_1,\ldots,\pi_{i+1}\rangle)\subseteq B$. Since $\mathcal{B}(\langle\pi_{i+1},\pi\rangle)\subseteq B$, with π a 3-space in $\langle\pi_1,\ldots,\pi_i\rangle$ for which $\mathcal{B}(\pi)$ is not contained in one of the spaces K_i, there are at most $5q^{3i-4}-49q^{3i-6}$ 6-dimensional spaces $\langle\pi_{i+1},\mu\rangle$ for which $\mathcal{B}(\langle\pi_{i+1},\mu\rangle)$ is not necessarily contained in B, giving rise to at most $(5q^{3i-4}-49q^{3i-6})(q^6+q^5+q^4)$ points t for which $\mathcal{B}(t)$ is not necessarily contained in B. Let u be a point of such a space $\langle\pi_{i+1},\mu\rangle$. Suppose that each of the $(q^{3i+3}-1)/(q-1)$ lines through u in $\langle\pi_1,\ldots,\pi_{i+1}\rangle$ contains at least $q-2$ of the points t for which $\mathcal{B}(t)$ is not in B. Then there are at least $(q-3)(q^{3i+3}-1)/(q-1)+1>(5q^{3i-4}-49q^{3i-6})(q^6+q^5+q^4)$ such points t, if $q\geq 7$, a contradiction. Hence, there is a line N through t for which for at least four points $v\in N$, $\mathcal{B}(v)\in B$. Lemma 3.4.2 yields that $\mathcal{B}(t)\in B$. This implies that $\mathcal{B}(\langle\pi_1,\ldots,\pi_{i+1}\rangle)\subseteq B$.

Hence, the space $\langle H_1,H_2,\ldots,H_k\rangle$, which spans the space $\mathrm{PG}(n,q^3)$, is such that $\mathcal{B}(\langle\pi_1,\ldots,\pi_k\rangle)\subseteq B$. But $\mathcal{B}(\langle\pi_1,\ldots,\pi_k\rangle)$ corresponds to a linear k-blocking set B' in $\mathrm{PG}(n,q^3)$. Since B is minimal, $B=B'$. □

Corollary 4.2.13. *A small minimal k-blocking set in $\mathrm{PG}(n,p^3)$, p prime, $p\geq 7$, is $\mathbb{F}_p$-linear.*

Proof. This follows from Theorems 2.2.2 and Theorem 4.2.12. □

Case 2: there are $(q\sqrt{q}+1)$-secants to B

In this case, we will use induction on k to prove that small minimal k-blocking sets in $\mathrm{PG}(n, q^3)$, intersecting every $(n-k)$-space in 1 mod q points and containing a $(q\sqrt{q}+1)$-secant, are $\mathbb{F}_{q\sqrt{q}}$-linear. The induction basis is Theorem 4.2.3. We continue with assumption (H_2) and we suppose that

> B is a small minimal k-blocking set in $\mathrm{PG}(n, q^3)$ intersecting every $(n-k)$-space in 1 mod q points, containing a $(q\sqrt{q}+1)$-secant.

In this case, $\mathcal{S}$ maps $\mathrm{PG}(n, q^3)$ onto $\mathrm{PG}(2n+1, q\sqrt{q})$ and the Desarguesian spread consists of lines.

Lemma 4.2.14. *If B is non-trivial, there exist a point $P \in B$, a tangent $(n-k)$-space π at P and small $(n-k+1)$-spaces H_i through π, such that there is a $(q\sqrt{q}+1)$-secant through P in H_i, $i = 1, \ldots, q^{3k-3} - q^{3k-4} - 2\sqrt{q}q^{3k-5}$.*

Proof. There is a $(q\sqrt{q}+1)$-secant M. Lemma 4.2.6 (1) shows that there is an $(n-k)$-space π_M through M such that $B \cap M = B \cap \pi_M$.

Lemma 4.2.5 (3) shows that there are at least $\frac{q^{3k}-1}{q^3-1} - q^{3k-5} - 5q^{3k-6} + 1$ small $(n-k+1)$-spaces through π_M. Moreover, the intersections of these small $(n-k+1)$-spaces with B are Baer subplanes $\mathrm{PG}(2, q\sqrt{q})$, since there is a $(q\sqrt{q}+1)$-secant M. Let P be a point of $M \cap B$.

Since in any of these intersections, P lies on $q\sqrt{q}$ other $(q\sqrt{q}+1)$-secants, a point P of $M \cap B$ lies in total on at least $q\sqrt{q}(\frac{q^{3k}-1}{q^3-1} - q^{3k-5} - 5q^{3k-6} + 1)$ other $(q\sqrt{q}+1)$-secants. Since any of the $\frac{q^{3k}-1}{q^3-1} - q^{3k-5} - 5q^{3k-6} + 1$ small $(n-k+1)$-spaces through π_M contains q^3 points of B not in π_M, and $|B| < q^{3k} + q^{3k-1} + q^{3k-2} + 3q^{3k-3}$ (see Lemma 4.2.2), there are less than $q^{3k-1} + 4q^{3k-2}$ points of B left in the other $(n-k+1)$-spaces through π_M. Hence, P lies on less than $q^{3k-4} + 4q^{3k-5}$ full lines.

Since B is minimal, there is a tangent $(n-k)$-space π through P. There are at most $q^{3k-5} + 4q^{3k-6} - 1$ large $(n-k+1)$-spaces through π (Lemma 4.2.5 (1)). Moreover, since at least $\frac{q^{3k}-1}{q^3-1} - (q^{3k-5} + 4q^{3k-6} - 1) - (q^{3k-4} + 4q^{3k-5})$ small $(n-k+1)$-spaces through π contain $q^3 + q\sqrt{q} + 1$ points of B, and at most

$q^{3k-4}+4q^{3k-5}$ of the small $(n-k+1)$-spaces through π contain exactly q^3+1 points of B, there are at most $q^{3k-1}-q^{3k-2}\sqrt{q}+4q^{3k-2}$ points of B left. Hence, P lies on at most $(q^{3k-1}-q^{3k-2}\sqrt{q}+4q^{3k-2})/(q\sqrt{q}+1)$ different $(q\sqrt{q}+1)$-secants of the large $(n-k+1)$-spaces through π. This implies that there are at least $q\sqrt{q}(\frac{q^{3k}-1}{q^3-1}-q^{3k-5}-5q^{3k-6}+1)-(q^{3k-1}-q^{3k-2}\sqrt{q}+4q^{3k-2})/(q\sqrt{q}+1)$ different $(q\sqrt{q}+1)$-secants left through P in small $(n-k+1)$-spaces through π. Since in a small $(n-k+1)$-space through π, there lie $q\sqrt{q}+1$ different $(q\sqrt{q}+1)$-secants through P, this implies that there are certainly at least $q^{3k-3}-q^{3k-4}-2\sqrt{q}q^{3k-5}$ small $(n-k+1)$-spaces H_i through π such that P lies on a $(q\sqrt{q}+1)$-secant in H_i. □

Lemma 4.2.15. *Let π be an $(n-k)$-dimensional tangent space of B at the point P. Let H_1 and H_2 be two $(n-k+1)$-spaces through π for which $B\cap H_i=\mathcal{B}(\pi_i)$, for some plane π_i through $x\in\mathcal{S}(P)$, $\mathcal{B}(x)\cap\pi_i=\{x\}$ $(i=1,2)$ and $\mathcal{B}(\pi_i)$ not contained in a line of $\mathrm{PG}(n,q^3)$. Then $\mathcal{B}(\langle\pi_1,\pi_2\rangle)\subseteq B$.*

Proof. Let M be a line through x in π_1, let $s\neq x$ be a point of π_2.

We claim that there is a line T through s, not through x, in π_2 and an $(n-2)$-space π_M through $\langle\mathcal{B}(M)\rangle$ such that there are at least $q\sqrt{q}-q-2$ points $t_i\in T$, such that $\langle\pi_M,\mathcal{B}(t_i)\rangle$ is small and hence has a linear intersection with B, with $B\cap\pi_M=M$ if $k=2$ and $B\cap\pi_M$ is a small minimal $(k-2)$-blocking set if $k>2$. From Lemma 4.2.5 (1), we know that there are at most $q+3$ large hyperplanes through π_M if $k=2$, and at most $q-5$ if $k>2$ (see Lemma 4.2.9).

Let T be a line through s in π_2, not through x. The existence of π_M follows from Lemma 4.2.6 (1) if $k=2$, and Lemma 4.2.6 (2) if $k>2$. Since $\mathcal{B}(T)$ contains $q\sqrt{q}+1$ spread elements, there are at least $q\sqrt{q}-q-2$ points $t_i\in T$ such that $\langle\pi_M,\mathcal{B}(t_i)\rangle$ is small. This proves our claim.

Since $B\cap\langle\mathcal{B}(t_i),\pi_M\rangle$ is linear, also the intersection of $\langle\mathcal{B}(t_i),\mathcal{B}(M)\rangle$ with B is linear, i.e., there exist subspaces τ_i, $\tau_i\cap\mathcal{S}(P)=\{x\}$, such that $\mathcal{B}(\tau_i)=\langle\mathcal{B}(t_i),\mathcal{B}(M)\rangle\cap B$. Since $\tau_i\cap\langle\mathcal{B}(M)\rangle$ and M are both transversals through x to the same regulus $\mathcal{B}(M)$, they coincide, hence $M\subseteq\tau_i$. The same holds for $\tau_i\cap\langle\mathcal{B}(t_i),\mathcal{S}(P)\rangle$, implying $t_i\in\tau_i$. We conclude that $\mathcal{B}(\langle M,t_i\rangle)\subseteq\mathcal{B}(\tau_i)\subseteq B$.

We show that $\mathcal{B}(\langle M,T\rangle)\subseteq B$. Let L' be a line of $\langle M,T\rangle$, not intersecting M. The line L' intersects the planes $\langle M,t_i\rangle$ in points p_i such that $\mathcal{B}(p_i)\subseteq B$. Since $\mathcal{B}(L')$ is a subline intersecting B in at least $q\sqrt{q}-q-2$ points, Theorem 3.4.1 shows that $\mathcal{B}(L')\subseteq B$. Since every point of the space $\langle M,T\rangle$ lies on such

a line L', $\mathcal{B}(\langle M,T\rangle)\subseteq B$.

Hence, $\mathcal{B}(\langle M,s\rangle)\subseteq B$ for all lines M through x in π_2, and all points $s\neq x\in\pi_2$. We conclude that $\mathcal{B}(\langle\pi_1,\pi_2\rangle)\subseteq B$.

Theorem 4.2.16. *A small minimal k-blocking set in $\mathrm{PG}(n,q^3)$, intersecting every $(n-k)$-space in 1 mod q points, containing a $(q\sqrt{q}+1)$-secant is $\mathbb{F}_{q\sqrt{q}}$-linear.*

Proof. Lemma 4.2.14 shows that there exists a point P of B, a tangent $(n-k)$-space π at the point P and at least $q^{3k-3}-q^{3k-4}-2\sqrt{q}q^{3k-5}$ $(n-k+1)$-spaces H_i through π for which $B\cap H_i$ is a Baer subplane, $i=1,\ldots,s$, $s\geq q^{3k-3}-q^{3k-4}-2\sqrt{q}q^{3k-5}$. Let $B\cap H_i=\mathcal{B}(\pi_i), i=1,\ldots,s$, with π_i a plane.

Lemma 4.2.15 shows that $\mathcal{B}(\langle\pi_i,\pi_j\rangle)\subseteq B$, $0\leq i\neq j\leq s$.

If $k=2$, the set $\mathcal{B}(\langle\pi_1,\pi_2\rangle)$ corresponds to a linear 2-blocking set B' in $\mathrm{PG}(n,q^3)$. Since B is minimal, $B=B'$, and the theorem is proven.

Let $k>2$. Denote the $(n-k+1)$-spaces through π different from H_i by K_j, $j=1,\ldots,z$. There are at least $(q^{3k-3}-q^{3k-4}-2\sqrt{q}q^{3k-5}-1)/q^3$ different $(n-k+2)$-spaces $\langle H_1,H_j\rangle$, $1<j\leq s$. If all $(n-k+2)$-spaces $\langle H_1,H_j\rangle$ contain at least $2q^2$ of the spaces K_i, then $z\geq 2q^2(q^{3k-3}-q^{3k-4}-2\sqrt{q}q^{3k-5}-1)/q^3$, a contradiction if $q\geq 49$. Let $\langle H_1,H_2\rangle$ be an $(n-k+2)$-space containing less than $2q^2$ spaces K_i.

Suppose, by induction, that for any $1<i<k$, there is an $(n-k+i)$-space $\langle H_1,H_2,\ldots,H_i\rangle$ containing at most $2q^{3i-4}$ of the spaces K_i, such that $\mathcal{B}(\langle\pi_1,\ldots,\pi_i\rangle)\subseteq B$.

There are at least $\frac{q^{3k-3}-q^{3k-4}-2\sqrt{q}q^{3k-5}-(q^{3i}-1)/(q^3-1)}{q^{3i}}$ different $(n-k+i+1)$-spaces $\langle H_1,H_2,\ldots,H_i,H\rangle$, $H\not\subseteq\langle H_1,H_2,\ldots,H_i\rangle$.

If all of these contain at least $2q^{3i-1}$ of the spaces K_i, then

$$z\geq(2q^{3i-1}-2q^{3i-4})\frac{q^{3k-3}-q^{3k-4}-2\sqrt{q}q^{3k-5}-(q^{3i}-1)/(q^3-1)}{q^{3i}}+2q^{3i-4},$$

a contradiction if $q\geq 49$. Let $\langle H_1,\ldots,H_{i+1}\rangle$ be an $(n-k+i+1)$-space containing less than $2q^{3i-1}$ spaces K_i. We still need to prove that $\mathcal{B}(\pi_1,\ldots,\pi_{i+1})\subseteq B$.

Since $\mathcal{B}(\langle\pi_{i+1},\pi\rangle)\subseteq B$, with π a plane in $\langle\pi_1,\ldots,\pi_i\rangle$ for which $\mathcal{B}(\pi)$ is not contained in one of the spaces K_i, there are at most $2q^{3i-4}$ 4-dimensional spaces

$\langle \pi_{i+1}, \mu\rangle$ for which $\mathcal{B}(\langle \pi_{i+1}, \mu\rangle)$ is not necessarily contained in B, giving rise to at most $2q^{3i-4}(q^6+q^4\sqrt{q})$ points Q_i for which $\mathcal{B}(Q_i)$ is not necessarily in B. Let Q be a point of such a space $\langle \pi_{i+1}, \mu\rangle$.

There are $((q\sqrt{q})^{2i+2}-1)/(q\sqrt{q}-1)$ lines through Q in $\langle \pi_1,\ldots,\pi_{i+1}\rangle \cong \mathrm{PG}(2i+2,q\sqrt{q})$, and there are at most $2q^{3i-4}(q^6+q^4\sqrt{q})$ points Q_i for which $\mathcal{B}(Q_i)$ is not necessarily in B. Suppose all lines through Q in $\langle \pi_1,\ldots,\pi_{i+1}\rangle \cong \mathrm{PG}(2i+2,q\sqrt{q})$ contain at least $q\sqrt{q}-q-\sqrt{q}$ points Q_i for which $\mathcal{B}(Q_i)$ is not necessarily in B, then there are at least $(q\sqrt{q}-q-\sqrt{q}-1)((q\sqrt{q})^{2i+2}-1)/(q\sqrt{q}-1)+1 > 2q^{3i-4}(q^6+q^4\sqrt{q})$ points Q_i for which $\mathcal{B}(Q_i)$ is not necessarily in B, a contradiction.

Hence, there is a line N through Q in $\langle \pi_1,\ldots,\pi_{i+1}\rangle$ with at most $q\sqrt{q}-q-\sqrt{q}-1$ points Q_i for which $\mathcal{B}(Q_i)$ is not necessarily contained in B, hence, for at least $q+\sqrt{q}+2$ points $R\in N$, $\mathcal{B}(R)\in B$. Theorem 3.4.1 yields that $\mathcal{B}(Q)\in B$. This implies that $\mathcal{B}(\langle \pi_1,\ldots,\pi_{i+1}\rangle)\subseteq B$.

Hence, the space $\mathcal{B}(\langle H_1,H_2,\ldots,H_k\rangle)$ is such that $\mathcal{B}(\langle \pi_1,\ldots,\pi_k\rangle)\subseteq B$. But $\mathcal{B}(\langle \pi_1,\ldots,\pi_k\rangle)$ corresponds to a linear k-blocking set B' in $\mathrm{PG}(n,q^3)$. Since B is minimal, $B=B'$. □

The combination of Theorem 4.2.12 and Theorem 4.2.16 proves Theorem 4.2.1.

Remark. The fact that small 1-blocking sets in $\mathrm{PG}(n,q^2)$, intersecting every hyperplane in 1 mod q points, are lines or Baer subplanes, was already noticed in 2000 by Storme and Weiner in [137]. The techniques used in this chapter also prove that *a small k-blocking set in* $\mathrm{PG}(n,q^2)$*, intersecting every* $(n-k)$*-space in* 1 mod q *points is* $\mathbb{F}_q$*-linear.* This latter theorem, implying the truth of the linearity conjecture for small minimal k-blocking sets in $\mathrm{PG}(n,p^2)$, p prime, was proven by Weiner [149] (see Subsection 4.1.1).

5

Partial covers of PG(n, q): 'almost' blocking sets

It is easy to cover all points of a projective plane by lines. For example, one can take all $q + 1$ lines through a fixed point. If one takes a small number of lines, say $q + \epsilon$, is it possible to cover all points but one? If we look at the dual plane, this question is equivalent to finding the smallest size of a blocking set in the affine plane AG$(2, q)$. Brouwer and Schrijver, and Jamison proved the following theorem.

Theorem. [79, Theorem 1], [28, Theorem 1] *If B is a minimal blocking set of* AG$(2, q)$*, then* $|B| \geq 2q - 1$.

From this, we get that the minimum number of lines to cover all but one point of PG$(2, q)$ is at least $2q - 1$. This bound is attained when we take q lines through a point P and $q - 1$ other lines, not through P, intersecting the $(q + 1)$th line through P in different points.

This chapter deals with the following problem: if we take a small number of hyperplanes, and we request that there is at least one point that is not covered, how many non-covered points are there, and what can we say about their configuration? Dually, we have a small number of points blocking almost all

hyperplanes, i.e., an *almost* 1-*blocking set*. We finish this chapter by extending the results for almost 1-blocking sets to *almost* k-*blocking sets* and comparing these to results found by K. Metsch in [106].

The results concerning partial covers of PG(n,q), or almost 1-blocking sets, are joint work with Stefan Dodunekov and Leo Storme and will appear in *European Journal of Combinatorics* [49].

Throughout this section, the parameters n and k will satisfy $n \geq 2$, $1 \leq k \leq n-1$, unless indicated otherwise.

5.1 Introduction

We start by giving the necessary definitions. Let $\mathcal{C}$ be a set of $q+b$ hyperplanes of PG(n,q). Denote by $\mathcal{C}(P)$ the set of hyperplanes of $\mathcal{C}$ containing the point P. A *partial* cover $\mathcal{S}$ is a set of hyperplanes such that there is at least one point Q in PG(n,q) with $|\mathcal{S}(Q)| = 0$. A point H for which $|\mathcal{S}(H)| = 0$, is called a *hole of* $\mathcal{S}$. We denote the set of holes of $\mathcal{S}$ by $\mathcal{H}(\mathcal{S})$.

Dualising this definition, we get that a partial cover corresponds to a set of points $\mathcal{K}$ such that there is at least one hyperplane of PG(n,q), not containing a point of $\mathcal{K}$. The latter kind of hyperplanes are called 0-*secants* and we say that a 0-secant *misses* the set $\mathcal{K}$. The set of 0-secants is denoted by $\mathcal{Z}(\mathcal{K})$. If the number of 0-secants is small, then the set $\mathcal{K}$ is 'almost' a 1-blocking set in PG(n,q). If $\mathcal{K}$ has size τ, then we say that $\mathcal{K}$ is an *almost* 1-*blocking* τ-*set* in PG(n,q). These definitions extend in a straightforward way to *almost* k-*blocking sets*. In what follows, the terms 'small' and 'almost' will always be made explicit.

In [19], Blokhuis, Brouwer and Szőnyi proved the following theorem on partial covers.

Theorem 5.1.1. [19] *If $\mathcal{S}$ is a partial cover of size $q+b$ in* PG$(2,q)$, *$b < (q-2)/3$, with $|\mathcal{H}(\mathcal{S})| \leq q+b$, then $q-b \leq |\mathcal{H}(\mathcal{S})| \leq q$ and the holes are collinear.*

The bound on b in Theorem 5.1.1 is sharp: let $b = (q-2)/3$ and let $\mathcal{S}$ be a set of $q-1$ lines L_i through a point P, and $b+1$ other lines through a fixed point, lying on one of the lines L_i. In this case, the number of holes is $2(q-b-1) = q+b$, and the holes lie on two lines.

Remark. Theorem 5.1.1 was independently proven around the same time as our results (Theorem 5.1.2) for $\mathrm{PG}(n,q)$ in [49], but improves them in the planar case. In this chapter, instead of working with our original bound, $b \leq (q-10)/4$, we extend Theorem 5.1.1 to general dimension. For completeness, we include Theorem 5.1.2 and its original proof.

Theorem 5.1.2. *If $\mathcal{S}$ is a partial cover of size $q+b$ in $\mathrm{PG}(2,q)$, $b \leq (q-10)/4$, $q > 13$, with $|\mathcal{H}(\mathcal{S})| \leq q+b$, then $|\mathcal{H}(\mathcal{S})| \leq q$ and the holes are collinear.*

Proof. Let $|\mathcal{H}(\mathcal{S})| = x \leq q+b$ and suppose that there are three non-collinear points in $\mathcal{H}(\mathcal{S})$. We will derive a contradiction. The set $\mathcal{H}(\mathcal{S})$ can be covered by a set $\mathcal{L}$ of at most $(x+1)/2$ lines. The set $\mathcal{S} \cup \mathcal{L}$ is a cover of $\mathrm{PG}(2,q)$ of size at most

$$q + b + \frac{q+b+1}{2} \leq 2q.$$

Hence, there is a unique minimal cover $\mathcal{S}' \cup \mathcal{L}'$ contained in $\mathcal{S} \cup \mathcal{L}$ (see Theorem 2.4.1), where $\mathcal{S}' \subseteq \mathcal{S}$ and $\mathcal{L} \subseteq \mathcal{L}'$. Denote the cover $\mathcal{S} \cup \mathcal{L}'$ by $\mathcal{C}$ and note that $\mathcal{H}(\mathcal{S}) = \mathcal{H}(\mathcal{C})$ Suppose that there exists a y-secant $\ell_y \in \mathcal{L}'$ to $\mathcal{H}(\mathcal{S})$ with $y \leq (q-3b-1)/2$. Removing the line ℓ_y from $\mathcal{C}$ and replacing it by y lines, different from ℓ_y, one through each hole of ℓ_y, yields a cover $\mathcal{C}'$ of $\mathrm{PG}(2,q)$. Since $|\mathcal{C} \cup \mathcal{C}'| \leq q+b+(q+b+1)/2+(q-3b-1)/2 \leq 2q$, by Theorem 2.4.1, there is a unique minimal cover contained in $\mathcal{C} \cup \mathcal{C}'$. Since ℓ_y is essential to the cover $\mathcal{C}$, but ℓ_y is not contained in the minimal cover contained in $\mathcal{C}'$, we obtain a contradiction.

Hence $\mathcal{L}'$ contains only lines with at least $(q-3b-1)/2$ holes. We call a line with at least $(q-3b-1)/2$ holes a *long* secant. Suppose that the set $\mathcal{T}$ of long secants in $\mathcal{L}'$ has size z. If $z = 1$, then all holes are collinear, a contradiction, so $z > 1$.

There is a long secant L in $\mathcal{T}$ with less than $(q+b+1+\binom{z}{2})/z$ holes, since otherwise

$$|\mathcal{H}(\mathcal{S})| \geq z(q+b+1+\binom{z}{2})/z - \binom{z}{2} = q+b+1 > q+b.$$

The cover $\mathcal{C}''$ is obtained from $\mathcal{C}$ by removing the line L and replacing it with at most $(q+b+1+\binom{z}{2})/z$ lines, each through one hole of L. Then $\mathcal{C} \cup \mathcal{C}''$ has at most

$$q + b + (q+b+1+\binom{z}{2})/z + z \tag{5.1}$$

lines.

If the expression of (5.1) is at most $2q$, then, by the unique reducibility property, there is a unique minimal cover in $\mathcal{C} \cap \mathcal{C}''$. Since L is essential to the cover $\mathcal{C}$, but L is not contained in the minimal cover contained in $\mathcal{C}''$, we obtain a contradiction.

If the expression in (5.1) is larger than $2q$, then replacing $z = 2, \ldots, 8$ in (5.1) and considering $b \leq (q-10)/4$ and $q > 13$, gives a contradiction[1]. Hence, there are at least 9 long secants in $\mathcal{C}$, yielding

$$|\mathcal{H}(\mathcal{S})| \geq 9(q - 3b - 1)/2 - 36. \tag{5.2}$$

But the right hand side of (5.2) is larger than $q + b$ if $b \leq (q-10)/4$, a final contradiction. □

Remark. The fact that the number of holes of the partial cover, considered in Theorem 5.1.2, is at least $q - b$ follows in the same way as we will prove it for the hyperplane case in Lemma 5.3.1.

In this chapter, we generalise Theorem 5.1.1 to general dimension in Theorem 5.3.3 and we extend the dual of this theorem to almost k-blocking sets in Theorem 5.3.5.

5.2 The number of tangent $(n-k)$-spaces through an essential point of a k-blocking set in PG(n, q)

We extend the following theorem, proven by Blokhuis and Brouwer, to general dimension for $k = 1$ in Theorem 5.2.2 and for general k in Theorem 5.2.3.

Theorem 5.2.1. [18] *Let B be a blocking set in* PG$(2, q)$. *If $|B| = 2q - s$, then there are at least $s + 1$ tangent lines through each essential point of B.*

Theorem 5.2.2. *The number of tangent hyperplanes through an essential point of a 1-blocking set B of size $q + b + 1$, $|B| \leq 2q$, in* PG(n, q) *is at least $q^{n-1} - bq^{n-2}$.*

[1]The bound on b arises from considering the case $z = 3$ in (5.1).

Proof. [2] For $n = 2$, Theorem 5.2.1 proves this statement. Assume by induction that the theorem holds for all dimensions $i \leq n-1$. Let B be a 1-blocking set in $\pi = \mathrm{PG}(n, q)$. Since $|B| \leq 2q$, there is an $(n-2)$-space L in π that is skew to B. Let H be a hyperplane through L. Embed π in $\mathrm{PG}(2n-2, q)$. Let P be an $(n-3)$-space, skew to π, in $\mathrm{PG}(2n-2, q)$. The cone C with vertex P and base B, is an $(n-1)$-blocking set in $\mathrm{PG}(2n-2, q)$ (Theorem 2.1.3). Let $H^* \neq H$ be a hyperplane through L only sharing one point Q with B. Since $|B|$ is at most $2q$, there are at least two tangent hyperplanes to B through L, hence H^* can be chosen different from H.

Let $\mathcal{D}$ be a Desarguesian $(n-2)$-spread through L and $\langle Q, P\rangle$ in W, the $(2n-3)$-dimensional space spanned by L and $\langle Q, P\rangle$. Using the André-Bruck-Bose construction (see Chapter 1), this yields a projective plane $\mathrm{PG}(2, q^{n-1}) = \Pi^W$.

Since C is an $(n-1)$-blocking set in $\mathrm{PG}(2n-2, q)$, and every line of Π^W corresponds to an $(n-1)$-space (through an element of $\mathcal{D}$), C corresponds to a 1-blocking set C' in Π^W.

We claim that H defines a line ℓ in Π^W, only having essential points of C'. Let R be a point of $C' \cap \ell$. Since B is minimal, there exists an $(n-1)$-space H_R through R, contained in $\mathrm{PG}(n, q)$ and tangent to B. The $(2n-3)$-space $\langle H_R, P\rangle$ meets W in a $(2n-4)$-dimensional space, hence, $\langle H_R, P\rangle$ contains exactly one element $\mathcal{S}$ of $\mathcal{D}$. To prove our claim, it is sufficient to show that $\langle \mathcal{S}, R\rangle \cap C = \{R\}$, since it follows from this that $\langle \mathcal{S}, R\rangle$ defines a line in Π^W, tangent to C' at the point R, hence, R is an essential point of C'.

If P does not intersect the space $\langle \mathcal{S}, R\rangle$, then the projection from P of $\langle \mathcal{S}, R\rangle$ on H_R yields a bijection between the points of $\langle \mathcal{S}, R\rangle \cap C$ and $H_R \cap C$, so in this case, $\langle \mathcal{S}, R\rangle \cap C = \{R\}$.

If P intersects the space $\langle \mathcal{S}, R\rangle$ in the point S, then clearly $S \neq R$ and the line RS meets $\mathcal{S}$. Since RS is contained in C, $\mathcal{S}$ meets C, but $\langle P, Q\rangle$ is the only element of $\mathcal{S}$ meeting C since $C \cap W = \langle P, Q\rangle$. Hence, $H_R \cap W = \langle P, Q\rangle$, so $\langle P, Q\rangle \cap H_R$ is a point, different from R, contained in C, a contradiction. This proves our claim.

Now C' has size $1 + (q+b)q^{n-2} = q^{n-1} + bq^{n-2} + 1$ (the element $\langle Q, P\rangle \in \mathcal{D}$ corresponds to one point of C', and the $q+b$ affine points R_i of B lie all on a cone $\langle R_i, P\rangle$ with q^{n-2} affine points, each corresponding to a point of C').

[2] The arguments of this proof are based on the proof of Proposition 2.5 in [140].

Theorem 5.2.1 shows that every essential point of C' lies on at least $q^{n-1}-bq^{n-2}$ tangent lines to the blocking set C' in Π^W. We will show that the number of tangent lines through an essential point of the blocking set C' in Π^W is a lower bound on the number of tangent hyperplanes through an essential point of B in PG(n,q).

A tangent line through an affine essential point R of C' corresponds to an $(n-1)$-space $\langle R,\mathcal{S}\rangle$, with $\mathcal{S}$ a spread element of $\mathcal{D}$. Note that $\Omega \neq \langle Q,P\rangle$, since both are spread elements and cannot coincide since $\langle Q,P\rangle$ is an element of the blocking set, hence $\langle R,Q,P\rangle$ cannot correspond to a tangent line to C'.

The projection of $\langle R,\mathcal{S}\rangle$ from P onto PG(n,q) is an $(n-1)$-dimensional space through R in PG(n,q) which is skew to Q since $\mathcal{S}\cap\langle Q,P\rangle=\varnothing$, and which only has R in common with B since $\langle\mathcal{S},R\rangle\cap\langle B,P\rangle=\{R\}$. Hence, this projection is a tangent $(n-1)$-space through R to B in PG(n,q). So we have shown that every tangent line through R to C' in Π^W gives rise to a tangent hyperplane through R to B in PG(n,q). We will now show that the obtained tangent hyperplanes are all distinct.

Let η be a tangent hyperplane to B in R which is the projection of two tangent lines $\langle\mathcal{S},R\rangle$ and $\langle\mathcal{S}',R\rangle$. The dimension of $\langle\eta,P\rangle$ is $2n-3$, and $\dim(\langle\eta,P\rangle\cap W)=2n-4$. A hyperplane of PG$(2n-3,q)$ contains exactly one element of $\mathcal{D}$. Since it contains $\mathcal{S}$ and $\mathcal{S}'$, $\mathcal{S}=\mathcal{S}'$. So η is the projection of at most one such $(n-1)$-space.

For every essential point Q of B, it is possible to select a tangent hyperplane H through Q, and to let this tangent hyperplane H play the role described in the preceding paragraphs. Since Q is an affine essential point, this implies that Q lies in at least $q^{n-1}-bq^{n-2}$ tangent hyperplanes to B. □

We now extend the previous theorem to k-blocking sets.

Theorem 5.2.3. *The number of tangent $(n-k)$-spaces through an essential point of a k-blocking set B of size q^k+b+1, $|B|\leq 2q^k$, in* PG(n,q) *is at least* $q^{k(n-2)}(q^k-b)(q^k-1)/(q^{k^2}-1)$.

Proof. Embed PG(n,q) in PG(n,q^k). As shown in Theorem 2.4.8, a k-blocking set B in PG(n,q) is a 1-blocking set in PG(n,q^k). We count the number Z of couples (μ,H), where μ is a tangent $(n-k)$-space to B in PG(n,q) and H is a tangent hyperplane to B through μ in PG(n,q^k). Let X be the number of tangent hyperplanes to B in PG(n,q^k) and let Y be the number of tangent $(n-k)$-spaces to B in PG(n,q).

The number of hyperplanes through an $(n-k)$-space in $\mathrm{PG}(n,q^k)$ is $(q^{k^2}-1)/(q^k-1)$. Hence, if π is a tangent $(n-k)$-space in $\mathrm{PG}(n,q)$ to B, then there are at most $(q^{k^2}-1)/(q^k-1)$ tangent hyperplanes H through π in $\mathrm{PG}(n,q^k)$. Let H be a tangent hyperplane to B in $\mathrm{PG}(n,q^k)$. Since every hyperplane intersects $\mathrm{PG}(n,q)$ in a subspace of dimension at least $n-k$, there is at least one tangent $(n-k)$-space π to B in $\mathrm{PG}(n,q)$ contained in H.

This implies that $Y\cdot(q^{k^2}-1)/(q^k-1)\geq Z\geq X$. Since $|B|=q^k+b+1\leq 2q^k$, Theorem 5.2.2 shows that $X\geq q^{k(n-1)}-bq^{k(n-2)}$. It follows that $Y\geq q^{k(n-2)}(q^k-b)(q^k-1)/(q^{k^2}-1)$. □

Remark. As noted in Chapter 2, the unique reducibility theorem for k- blocking sets (Theorem 2.4.8) of size smaller than $2q^k$ follows also from Theorem 5.2.3. The latter theorem also incorporates the case where the size of the k-blocking set is exactly $2q^k$.

5.3 Almost 1-blocking sets and almost k-blocking sets in $\mathrm{PG}(n,q)$

The statements and proofs of this section will be formulated in terms of partial covers or almost 1-blocking sets, depending on which point of view is most convenient.

Lemma 5.3.1. *Let $\mathcal{K}$ be an almost 1-blocking $(q+b)$-set of $\mathrm{PG}(n,q)$, $b<q$. If all 0-secants $\mathcal{Z}(\mathcal{K})$ go through a common point P of $\mathrm{PG}(n,q)$, then $|\mathcal{Z}(\mathcal{K})|\geq q^{n-1}-bq^{n-2}$.*

Proof. The set $\mathcal{K}$, together with the common point P of all 0-secants, forms a 1-blocking set B of size $q+b+1$, where P is an essential point. Theorem 5.2.2 shows that P lies on at least $q^{n-1}-bq^{n-2}$ tangent hyperplanes to B. Removing P from B shows that there are at least $q^{n-1}-bq^{n-2}$ different 0-secants to $\mathcal{K}$.

Remark. The lower bound in Lemma 5.3.1 is sharp; let $\mathcal{K}$ be the set of q points on a line L, different from the point $P\in L$ together with a set A of b points, different from P, in a fixed plane π through L, such that every line through P in π is tangent to A. Then there are exactly $q^{n-1}-bq^{n-2}$ different 0-secants since there are $q-b$ lines in π, not containing a point of $\mathcal{K}$ and each of these lines is contained in exactly q^{n-2} different hyperplanes, not containing π.

Theorem 5.3.2. *Let $\mathcal{S}$ be a partial cover of* PG(n,q)*, $n \geq 3$, of size $q+b$, $b < (q-2)/3$, and assume that $|\mathcal{H}(\mathcal{S})| \leq q^{n-1}$. The following statements are valid.*

(i) A line that contains 2 holes of $\mathcal{S}$ contains at least $b+3$ holes of $\mathcal{S}$.

(ii) Every hole of $\mathcal{S}$ lies on more than $q^{n-2}/2$ lines with at least $q-b$ holes.

(iii) The holes of $\mathcal{S}$ are contained in one hyperplane of PG(n,q)*.*

Proof. (i) Let L be a line with t holes, $t < q-b$, and let π be a plane through L. Theorem 5.1.1 shows that if π contains at most $q+b$ holes, there are at least $q-b$ holes, which are all collinear, a contradiction. Hence, every plane through L contains at least $q+b+1$ holes, which implies that there are at least

$$\theta_{n-2}(q+b+1-t)+t$$

holes in PG(n,q), which has to be at most q^{n-1}. If $t = b+2$, $\theta_{n-2}(q+b+1-b-2)+b+2 > q^{n-1}$, a contradiction. Hence, t is at least $b+3$.

(ii) Let R be a hole. There is a line L through R containing only covered points and R, otherwise there would be at least $\theta_{n-1}+1$ holes. Using Theorem 5.1.1, we see that a plane through L contains either at most $q-1$ holes on a line through R, different from L, or it contains at least $q+b$ holes different from R.

Suppose that there are X planes through L with at most $q-1$ holes different from R, then the number of holes is at least

$$X(q-b-1)+(\theta_{n-2}-X)(q+b)+1,$$

which has to be at most q^{n-1}. Putting $X = q^{n-2}/2$ yields a contradiction. Hence, there are more than $q^{n-2}/2$ planes with at most q holes and in each of these X planes, there is a line through R containing at least $q-b-1$ other holes, and all holes in such a plane lie on this line.

(iii) For $n = 2$, this follows from Theorem 5.1.1. Suppose by induction that the theorem holds for any dimension $i \leq n-1$.

We show that $\forall j = 1,\ldots,n-1$, there is a j-space π_j through a hole R, with at most q^{j-1} holes. Let R be a hole. There is a line L through R containing only covered points and R, otherwise there would be at least $\theta_{n-1}+1$ holes. This proves the case $j = 1$. Let $j > 1$ and suppose by induction that for all $k = 1,\ldots,j-1$, there is a space π_k through R with at most q^{k-1} holes. The

number of $(k+1)$-dimensional spaces through π_k is θ_{n-k-1}. If every $(k+1)$-space through π_k contains more than q^k holes, the number of holes is at least

$$\theta_{n-k-1}(q^k+1-q^{k-1})+q^{k-1},$$

a contradiction if $k<n-1$. We conclude that there exists a hyperplane π of PG(n,q) with at most q^{n-2} holes.

Using the induction hypothesis, all holes in π are contained in an $(n-2)$-dimensional space μ of π and by Lemma 5.3.1, the number of holes in μ is at least $q^{n-2}-bq^{n-3}$. There are at least $\theta_{n-2}(q-b-1)+1$ holes in PG(n,q) since every plane through L contains at least $q-b-1$ extra holes. Hence, there is certainly a hole R' that is not contained in μ.

Now we distinguish between two cases.

Case 1: All lines through R' with at least $q-b$ holes intersect μ. Part (ii) shows that there are at least $q^{n-2}/2$ lines through R' with at least $q-b$ holes. Since a line through two holes contains at least $b+3$ holes (see (i)), counting the holes in $\langle R',\mu\rangle$ yields that this number is at least

$$Z:=q^{n-2}(q-b-1)/2+(q^{n-2}-bq^{n-3}-q^{n-2}/2)(b+2)+1.$$

Suppose now that not all holes are contained in the hyperplane $\langle R',\mu\rangle$. Let R'' be a hole not in $\langle R',\mu\rangle$. Connecting R'' with all the holes in $\langle R',\mu\rangle$ yields at least $(b+2)Z+1$ holes, which is more than q^{n-1}, a contradiction. Hence, all holes are contained in $\langle R',\mu\rangle$, and the theorem follows.

Case 2: There is a line through R', skew to μ, with at least $q-b$ holes. Since a line through two holes, contains at least $b+3$ holes (see (i)), this yields at least

$$(q-b)(q^{n-2}-bq^{n-3})(b+1)+q^{n-2}-bq^{n-3}+q-b>q^{n-1}$$

holes, a contradiction. □

Theorem 5.3.3. *Let $\mathcal{K}$ be an almost 1-blocking $(q+b)$-set in PG(n,q), with $b<(q-2)/3$ and assume that $|\mathcal{Z}(\mathcal{K})|\leq q^{n-1}$. Then the number of 0-secants is at least $q^{n-1}-bq^{n-2}$ and they all go through a fixed point.*

Proof. This follows immediately from Theorem 5.3.2 (iii) and Lemma 5.3.1.□

Theorem 5.3.4. *Let $\mathcal{K}$ be an almost 1-blocking $(p+b)$-set in PG(n,p), p prime, with $b<(p-2)/3$ and assume $|\mathcal{Z}(\mathcal{K})|\leq p^{n-1}$. Then $\mathcal{K}$ consists of p points on a line and b other points, not on L.*

Proof. By Theorem 5.3.2 (iii), the 0-secants contain a fixed point P. Hence, the set $\mathcal{K} \cup \{P\}$ is a 1-blocking set B of size $q+b+1 < 3(q+1)/2$. Theorem 2.2.2, together with Theorem 2.4.6, shows that the unique minimal 1-blocking set in B is a line L. Clearly, the point P belongs to L. The other b points lie in $\mathrm{PG}(n,q) \setminus L$. □

We now extend Theorem 5.3.3 to almost k-blocking sets.

Theorem 5.3.5. *If $\mathcal{K}$ is an almost k-blocking (q^k+b)-set in* PG(n,q), *$b < (q^k-2)/3$, with at most $(q^{k(n-1)})(q^k-1)/(q^{k^2}-1)$ 0-secants, then it has at least $q^{k(n-2)}(q^k-b)(q^k-1)/(q^{k^2}-1)$ 0-secants and all 0-secants go through a common point.*

Proof. Embed PG(n,q) in PG(n,q^k). An $(n-k)$-space in PG(n,q) that misses $\mathcal{K}$ gives rise to at most $(q^{k^2}-1)/(q^k-1)$ hyperplanes in PG(n,q^k) that miss $\mathcal{K}$. Since the number of 0-secants in PG(n,q) is smaller than $(q^{k(n-1)})(q^k-1)/(q^{k^2}-1)$, the number of hyperplanes missing $\mathcal{K}$ in PG(n,q^k) is at most $q^{k(n-1)}$. By Theorem 5.3.2 (iii), the hyperplanes missing $\mathcal{K}$ go through a common point, say P, hence $\mathcal{K} \cup \{P\}$ is a 1-blocking set in PG(n,q^k). Let H be a hyperplane missing $\mathcal{K}$. Since $\mathcal{K} \cup \{P\}$ has to block the hyperplanes $H, H^q, \ldots, H^{q^{k-1}}$, the point P has to be contained in PG(n,q). This implies that all $(n-k)$-spaces missing $\mathcal{K}$ in PG(n,q) contain the point P, hence $\mathcal{K} \cup \{P\}$ is a k-blocking set in PG(n,q). Since P is essential, by Theorem 5.2.3, the number of tangent $(n-k)$-spaces to $\mathcal{K} \cup \{P\}$ is at least $q^{k(n-2)}(q^k-b)(q^k-1)/(q^{k^2}-1)$. Hence, the number of 0-secants to $\mathcal{K}$ is at least $q^{k(n-2)}(q^k-b)(q^k-1)/(q^{k^2}-1)$. □

The lower bound on the number of 0-secants in Theorem 5.2.3 can be improved in some cases by the following theorem of Metsch.

Theorem 5.3.6. [106, Theorem 1.2][3] *Let s, d, n be integers with $s, d \geq 1$ and $n \geq d+s$. Let B be a set of points of* PG(n,q) *and suppose that $|B| \leq \theta_d$.*

(a) The number of s-spaces missing B is at least

$$q^{(s+1)(d+1)} \begin{bmatrix} n-d \\ s+1 \end{bmatrix}_q + (\theta_d - |B|) q^{sd} \begin{bmatrix} n-d \\ s \end{bmatrix}_q .$$

[3] Note that this theorem gives no information on the configuration of the 0-secants, as opposed to Theorems 5.3.3 and 5.3.5.

(b) Equality holds in (a) if and only if there exists a d-space D such that $B \subseteq D$ and B meets all lines of D (this implies that $|B| \geq \theta_{d-1}$).

(c) Suppose that the set B generates a subspace of dimension at least $d+1$. If $|B| \geq \theta_{d-1}+1$, then the bound in (a) can be improved by a term

$$(|B| - 1 - \theta_{d-1}) q^{(s-1)d} \begin{bmatrix} n-d-1 \\ s-1 \end{bmatrix}_q .$$

If $|B| = \theta_{d-1}+1$, then the bound in (a) can be improved by a term

$$(q^{d-1} - 1) q^{(s-1)d} \begin{bmatrix} n-d-1 \\ s-1 \end{bmatrix}_q .$$

Applying this theorem with $s = n-k$ and $d = k$ yields the following lower bound.

Corollary 5.3.7. *If B is an almost k-blocking (q^k+b)-set in $\mathrm{PG}(n,q)$, $b \leq \theta_{k-1}$, then the number of 0-secants is at least*

$$(\theta_{k-1} - b) q^{k(n-k)}.$$

One can check that for $k > 1$ and $|B| < \theta_k$, this theorem improves on Theorem 5.3.5. For $k = 1$ or $\theta_k \leq |B| < (q^k - 2)/3$, Theorem 5.3.5 gives the best bound on the minimum number of 0-secants.

6

The code of points and k-spaces and its dual

The code of points and lines in a projective plane has been intensively studied and the nature of the codewords of minimum weight in this code has been known since the late 1960's. Later, in the mid-1980's, the study of codewords of small weight and of the weight enumerator of codes from a projective plane turned out to be very useful in the computer proof of the non-existence of a projective plane of order 10. The reference [86] provides an excellent overview of how Lam, Schwierz and Thiel found this proof. Later, codewords of small weight of (not necessarily Desarguesian) projective planes were studied and the minimum weight of the dual code arising from them was investigated. However, up to today, even the minimum weight of the dual code of the Desarguesian projective plane $\mathrm{PG}(2, q)$ is not known, except for the cases where q is prime or q is even.

Already in the 1970's, the code of points and k-spaces was studied in a similar way, but apart from the determination of the codewords of minimum weight, nothing was known.

The mentioned codes belong to a broader class of codes, the so called *Reed-Muller codes*. These codes are well studied, e.g. by Delsarte [45] and Delsarte,

Goethals and MacWilliams [46]. For more information, we refer to the chapter *The standard geometric codes* in [4].

In this chapter, we investigate the code of points and k-spaces and show that there is a gap in the weight enumerator. We derive a lower and upper bound on the minimum weight of the dual code. To our knowledge, this upper bound is currently still the best known. The results of this chapter are published in [89, 90, 92]. These papers are joint work with Michel Lavrauw and Leo Storme, the last paper is joint work with Peter Sziklai as well.

In Chapter 1, we introduced $\mathrm{C}_k(n,q)$, $q=p^h$, p prime, $h\geq 1$, as the p-ary linear code of points and k-spaces in $\mathrm{PG}(n,q)$. It follows from the definitions that $c\in \mathrm{C}_k(n,q)^\perp$ if and only if $(c,\pi)=0$ for all k-spaces π of $\mathrm{PG}(n,q)$. In what follows, we often identify the support of a codeword c with the corresponding set of points of $\mathrm{PG}(n,q)$ and this point set will always be denoted by $\mathcal{S}$. Furthermore, if T is a set of points of $\mathrm{PG}(n,q)$, then the incidence vector of this set is also denoted by T. If c is a codeword of $\mathrm{C}_k(n,q)$ and R is a point of $\mathrm{PG}(n,q)$, then c_R denotes the coordinate of the codeword c at the position corresponding to the point R. The parameters k and n will always satisfy $n\geq 2$, $1\leq k\leq n-1$, unless indicated otherwise.

6.1 Earlier results

The codes of points and k-spaces in $\mathrm{PG}(n,q)$, $q=p^h$, p prime, are generated *over the field* $\mathbb{F}_p$, and one might wonder why these codes are not always taken over $\mathbb{F}_2$, or over some other finite field. The reason why the only possible interesting cases occur precisely for the q'-ary codes where q' divides the order of the projective space, is shown in Theorem 6.1.1.

Theorem 6.1.1. *Let* C *be the q'-ary code of points and k-spaces in a projective space* Π *of order q, where $q'\not| q$. Then* C *is either the $[\theta_n,\theta_n-1,2]$-code which is the dual of the all-one vector* $\mathbf{1}$*, or* C *is the $[\theta_n,\theta_n,1]$-code which is the entire vector space.*

Proof. [1] Let π_i be the k-spaces contained in $\mathrm{PG}(n,q)$, then $c=\sum_i \pi_i = \begin{bmatrix} n \\ k \end{bmatrix}_q \mathbf{1}$

[1] This is a straightforward extension of the proof given in [40, Proposition 8] for the case of finite projective planes. This theorem also holds for non-Desarguesian planes and planes where the order is not a prime power. Note that the latter kind of planes are conjectured not to exist.

is a codeword of the q'-ary code C of points and k-spaces of $\mathrm{PG}(n,q)$. Let c^x be the codeword which is the sum of all the k-spaces through a point x. The codeword $c^{xy} := c^x - c^y$, for $x \neq y$, has $c^{xy}_x = \begin{bmatrix} n \\ k \end{bmatrix}_q - \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q$, $c^{xy}_y = -\begin{bmatrix} n \\ k \end{bmatrix}_q + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q$ and $c^{xy}_z = 0$ for all $z \neq x, y$, so codewords $c^{x_i x_j}$ clearly belong to the code $\mathbf{1}^\perp$. The code $\mathbf{1}^\perp$ has dimension at most $\theta_n - 1$. Since $c^{x_1 x_i}$, $i \neq 1$ are $\theta_n - 1$ independent codewords, contained in $\mathbf{1}^\perp$, the dimension of $\mathbf{1}^\perp$ is equal to $\theta_n - 1$. The generators $c^{x_1 x_i}$, $i \neq 1$, of the code $\mathbf{1}^\perp$ are contained in C, hence, $\mathbf{1}^\perp \subseteq \mathrm{C}$ and the theorem follows. □

6.1.1 The parameters of $\mathrm{C}_k(n,q)$

The parameters of the code of points and k-spaces $\mathrm{C}_k(n,q)$ are known since the 1960's. Clearly, the length of $\mathrm{C}_k(n,q)$ equals θ_n. The minimum weight, hence also the minimum distance, is determined by Assmus and Key.

Theorem 6.1.2. [4, Proposition 5.7.3] *The minimum weight vectors of* $\mathrm{C}_k(n,q)$ *are the scalar multiples of the* k*-spaces.*

This theorem also follows from the following, more general, result on the code $\mathrm{C}_{s,t}(n,q)$ of s-spaces and t-spaces in $\mathrm{PG}(n,q)$.

Theorem 6.1.3. [6, Theorem 1] *The minimum weight of* $\mathrm{C}_{s,t}(n,q)$ *is* $\begin{bmatrix} t+1 \\ s+1 \end{bmatrix}_q$.

Remark. Theorem 6.1.2 will be an easy consequence of our approach of the codewords of small weight of $\mathrm{C}_k(n,q)$ using blocking sets (see Theorem 6.3.3).

The dimension of $\mathrm{C}_k(n,q)$ is determined by Hamada in [67], where he gives the following explicit formula for the p-rank of the incidence matrix of points and k-spaces, i.e. the dimension of $\mathrm{C}_k(n,q)$.

Theorem 6.1.4. [67] (see also [4, Theorem 5.8.1]) *The* p*-rank of the incidence matrix of points and* k*-spaces in* $\mathrm{PG}(n,q)$, $q = p^h$, *is given by:*

$$\sum_{s_0} \cdots \sum_{s_{h-1}} \prod_{j=0}^{h-1} \sum_{i=0}^{L(s_{j+1},s_j)} (-1)^i \binom{k+1}{i} \binom{k + s_{j+1}p - s_j - ip}{k},$$

where $s_h = s_0$ and summations are taken over all integers s_j (for $j = 0, \ldots, h-1$) such that

$$k+1 \leq s_j \leq n+1, \text{ and } 0 \leq s_{j+1}p - s_j \leq (n+1)(p-1),$$

and

$$L(s_{j+1}, s_j) = \lfloor \frac{s_{j+1}p - s_j}{p} \rfloor.$$

In the case of points and hyperplanes, this formula simplifies to the following formula, which was already independently deduced by Goethals and Delsarte [63] and Smith [134].

Theorem 6.1.5. *The p-rank of the incidence matrix of points and hyperplanes of $\mathrm{PG}(n,q)$, $q = p^h$, is*

$$\binom{n+p-1}{n}^h + 1.$$

In [75], Inamdar and Sastry deduce the following easier formula for the dimension of the code $\mathrm{C}_k(n,q)$.

Theorem 6.1.6. [75, Theorem 2.13] *The dimension of the p-ary code of $\mathrm{C}_k(n,q)$, $q = p^h$, is given by:*

$$1+\sum_{i=1}^{n-k} \sum_{\substack{1 \leq r_1, \ldots, r_{l-1} \leq n-k \\ r_0 = r_l = i}} \prod_{j=0}^{h-1} \sum_{t=0}^{r_{j+1}-1} (-1)^h \binom{n+1}{t} \binom{n+pr_{j+1}-r_j-ph}{n}.$$

Remark. The p-rank of the incidence matrix of points and lines of $\mathrm{PG}(2,q)$, $q = p^h$, is $\binom{p+1}{2}^h + 1$. This was already proven in 1966 by Graham and MacWilliams [65]. Hamada and Sachar conjecture that Desarguesian projective planes can be characterised by this property; they conjecture that every projective plane π of order p^h has p-rank at least $\binom{p+1}{2}^h + 1$ and that equality holds if and only if the plane π is Desarguesian. Moreover, Salwach proved that the p-rank of an arbitrary projective plane of order p, p prime, is $\binom{p+1}{2}+1$ [128]. Thus, if one can prove the Hamada-Sachar conjecture, one has proved another - much more famous - conjecture, namely the conjecture that *the projective plane of order p is unique.*

6.1.2 Bounds on the weight of $\mathrm{C}_k(n,q)^\perp$

For the dual code, the situation is different: the dimension of the code follows easily from the dimension of $\mathrm{C}_k(n,q)$, but the minimum weight of the dual code of points and k-spaces is not known in general. The following bound is derived by Calkin, Key and de Resmini in [37]. For $n = 2$, this result was long since known (see [4, Theorem 6.4.2]).

Theorem 6.1.7. [37, Proposition 1] *The minimum weight of* $\mathrm{C}_k(n,q)^\perp$, $q = p^h$, *satisfies the following:*

$$(q+p)q^{n-k-1} \leq d \leq 2q^{n-k}.$$

The following corollary follows easily.

Corollary 6.1.8. *The minimum weight of* $\mathrm{C}_k(n,p)^\perp$, p *prime, is* $2p^{n-k}$.

Remark. This result was also proved in [6, Proposition 2], where Bagchi and Inamdar conjecture that, if p is prime, the minimum weight of the dual code $\mathrm{C}_{s,t}(n,p)^\perp$ is $2p^{n-t}$ too[2].

Calkin et al. also show that for $p = 2$, the lower bound derived in Theorem 6.1.7 is sharp.

Theorem 6.1.9. [37, Theorem 1] *The minimum weight of* $\mathrm{C}_k(n,q)^\perp$, q *even, is* $(q+2)q^{n-k-1}$.

6.1.3 The hull of $\mathrm{C}_k(n,q)$

Assmus and Key define the *hull* of a code C as the intersection $\mathrm{C} \cap \mathrm{C}^\perp$ and prove the following theorem. Recall that $\mathrm{C}(2,q) = \mathrm{C}_1(2,q)$.

Theorem 6.1.10. [4, Corollary 6.4.4] *The hull* $\mathrm{C}(2,q) \cap \mathrm{C}(2,q)^\perp$ *has minimum weight* $2q$ *and the minimum weight vectors are the scalar multiples of the differences of the incidence vectors of any two distinct lines of* $\mathrm{PG}(2,q)$.

In this chapter, this result will be extended to the code of points and hyperplanes of $\mathrm{PG}(n,q)$.

[2] For $s+1 = t$, the truth of the conjecture follows from the bound in Theorem 6.2.14.

6.1.4 Codewords of small weight in $\mathrm{C}_k(n,q)$

The first results on codewords of small weight in the p-ary linear code of points and lines in $\mathrm{PG}(2,p)$, p prime, were proved by McGuire and Ward [101]; they proved that there are no codewords of $\mathrm{C}(2,p)$, p an odd prime, in the interval $[p+2, 3(p+1)/2]$. This result was extended by Chouinard in [40, 41], where he proved the following theorem.

Theorem 6.1.11. [40], [41] *There are no codewords in* $\mathrm{C}(2,p)$*, p prime, with weight in the closed interval* $[p+2, 2p-1]$*.*

In [53], we extended the result of Chouinard to a larger interval for p prime.

Theorem 6.1.12. [53, Theorem 4] *The only codewords c, with* $0 < wt(c) \leq 2p + (p-1)/2$*, in* $\mathrm{C}(2,p)$*, $p \geq 11$, are:*

(i) codewords with weight $p+1$: $\alpha\ell$, with ℓ a line of $\mathrm{PG}(2,p)$*, $\alpha \in \mathbb{F}_p \setminus \{0\}$,*

(ii) codewords with weight $2p$: $\alpha(\ell_1 - \ell_2)$, with ℓ_1 and ℓ_2 two distinct lines of $\mathrm{PG}(2,p)$*, $\alpha \in \mathbb{F}_p \setminus \{0\}$,*

(iii) codewords with weight $2p+1$: $\alpha\ell_1 + \beta\ell_2$, $\beta \neq -\alpha, \alpha, \beta \in \mathbb{F}_p \setminus \{0\}$, with ℓ_1 and ℓ_2 two distinct lines of $\mathrm{PG}(2,p)$*.*

In [4, Proposition 6.6.4], it was shown that the incidence vector of a Baer subplane $\mathrm{PG}(2,q)$ is not a codeword in $\mathrm{C}(2,q^2)$. Together with some lemmas proven in the same book, one can easily prove that a codeword in $\mathrm{C}(2,p^2)$ of weight at most $2p^2$ has to be a line or the incidence vector of a Baer subplane. Using the same arguments and the fact that small minimal blocking sets in $\mathrm{PG}(2,p^3)$, p prime, are classified (see Subsection 4.1.3), we proved the following result in [53].

Theorem 6.1.13. [53, Theorem 6] *There are no codewords in* $\mathrm{C}(2,p^3)$ *with weight in the interval* $[p^3+2, 2p^3-1]$*.*

In Section 6.3, we will show that Theorem 6.1.13 can be extended to fields of arbitrary order, and can be extended partially to the code of points and k-spaces in $\mathrm{PG}(n,q)$.

For $\mathrm{C}(2,q)$, this theorem was recently improved by Gács, Szőnyi and Weiner in [58] where they show the following result.

Theorem 6.1.14. *A codeword c in $\mathrm{C}(2,q)$, $q=p^h$, with $wt(c)<\sqrt{q}q+1$ is a linear combination of at most $\lceil \frac{wt(c)}{q+1} \rceil$ lines, when q is large and $h>2$.*

Remark. We believe that the techniques developed by Gacs, Szőnyi and Weiner to characterise codewords of small weight of $\mathrm{C}(2,q)$ might be extended to find similar results for the code $\mathrm{C}_k(n,q)$. This makes it plausible that codewords of small weight in $\mathrm{C}_k(n,q)$ can be characterised up to much larger weights.

6.2 The dual code of $\mathrm{C}_k(n,q)$

In this section, we consider codewords in the code $\mathrm{C}_k(n,q)^\perp$ and we derive new upper and lower bounds on the minimum weight of the code $\mathrm{C}_k(n,q)^\perp$. A trivial upper bound is given by the following lemma. In the case that q is a prime, Corollary 6.1.8 shows that this trivial upper bound is sharp.

Lemma 6.2.1. $d(\mathrm{C}_k(n,q)^\perp) \leq 2q^{n-k}$.

Proof. Let $c=\mu_1-\mu_2$, with μ_1 and μ_2 two $(n-k)$-spaces intersecting in an $(n-k-1)$-space. Since $(\mu_i,\pi)=1$ for every k-space π, $i=1,2$, c is a codeword of $\mathrm{C}_k(n,q)^\perp$; it has weight $2q^{n-k}$. □

6.2.1 A reduction theorem for the minimum weight of $\mathrm{C}_k(n,q)^\perp$

In Lemma 6.2.2 and Theorem 6.2.3, we reduce the problem of finding the minimum weight of $\mathrm{C}_k(n,q)^\perp$ to finding the minimum weight of $\mathrm{C}_1(n-k+1,q)^\perp$.

Lemma 6.2.2. *The following inequalities hold:*

$$d(\mathrm{C}_k(n,q)^\perp) \geq d(\mathrm{C}_{k-1}(n-1,q)^\perp) \geq \cdots \geq d(\mathrm{C}_1(n-k+1,q)^\perp).$$

Proof. Let c be a codeword of $\mathrm{C}_k(n,q)^\perp$ of minimum weight. If $k=1$, the statement holds trivially, so we assume that $k>1$. Let P be a point of $\mathcal{S}=supp(c)$ and suppose that every line through P contains another point of $\mathcal{S}$, then $|\mathcal{S}| \geq \theta_{n-1}+1$, a contradiction since $wt(c) \leq 2q^{n-k}$ according to Lemma 6.2.1. Hence, there exists a point R of $\mathrm{PG}(n,q)\backslash\mathcal{S}$, lying on a tangent line to $\mathcal{S}$. Let H be a hyperplane of $\mathrm{PG}(n,q)$ not containing R. For each

point $Q \in H$, define $c'_Q = \sum c_{Q_i}$, with Q_i the points of $\mathcal{S}$ on the line $\langle R, Q\rangle$, and let c' denote the vector with coordinates c'_Q, $Q \in H$. It follows that $c' \in \mathrm{C}_{k-1}(n-1,q)^\perp$, and $supp(c')$ is contained in the projection of $\mathcal{S}$ from the point R onto the hyperplane H. Clearly, $wt(c') \leq wt(c)$, hence $d(\mathrm{C}_{k-1}(n-1,q)^\perp) \leq d(\mathrm{C}_k(n,q)^\perp)$. Continuing this process proves the statement. □

Theorem 6.2.3. $d(\mathrm{C}_k(n,q)^\perp) = d(\mathrm{C}_1(n-k+1,q)^\perp)$.

Proof. Embed $\mu = \mathrm{PG}(n-k+1,q)$ in $\mathrm{PG}(n,q)$, $n > 2$, and extend each codeword c of $\mathrm{C}_1(\mu)^\perp$ to a vector $c^{(n)}$ of $V(\theta_n, p)$ by putting a zero at each point $P \in \mathrm{PG}(n,q)\backslash\mu$. The all one vector $\mathbf{1}$ is a codeword of $\mathrm{C}_1(n-k+1,q)$ since it is the sum of the incidence vectors of all lines of $\mathrm{PG}(n-k+1,q)$. It follows that $\sum_{P\in\mu} c_P^{(n)} = 0$ for each $c^{(n)}$. This implies that $(c^{(n)}, \pi) = 0$, for each k-space π of $\mathrm{PG}(n,q)$ which contains μ. If a k-space π of $\mathrm{PG}(n,q)$ does not contain μ, then $(c^{(n)}, \pi \cap \mu) = 0$, since $\mu \cap \pi$ is a line or can be described as a pencil of lines through a given point, and $(c, \ell) = 0$ for each line ℓ of μ. It follows that $c^{(n)}$ is a codeword of $\mathrm{C}_k(n,q)^\perp$ with $wt(c^{(n)}) = wt(c)$. This implies that $d(\mathrm{C}_k(n,q)^\perp) \leq d(\mathrm{C}_1(n-k+1,q)^\perp)$. By Lemma 6.2.2, $d(\mathrm{C}_k(n,q)^\perp) = d(\mathrm{C}_1(n-k+1,q)^\perp)$. □

Lemma 6.2.4. *Let $\mathcal{S}$ be a set of points in $\mathrm{PG}(n,q)$, with the property that those points of $\mathrm{PG}(n,q)\backslash\mathcal{S}$ that are incident with a secant line to $\mathcal{S}$ are incident with no tangent lines to $\mathcal{S}$. If $\dim\langle\mathcal{S}\rangle \geq n-k+2$, then $|\mathcal{S}| \geq \theta_{n-k+1}$.*

Proof. Let $\mathcal{S}$ be a set of points in $\mathrm{PG}(n,q)$, with the property that those points of $\mathrm{PG}(n,q) \setminus \mathcal{S}$ that are incident with a secant line to $\mathcal{S}$ are incident with no tangent lines to $\mathcal{S}$. We claim that if P is a point of $\mathcal{S}$ and L is a line through P, lying in a plane π through P, R, S, with $R, S \in \mathcal{S}$ and $P \notin RS$, then L is a secant line to $\mathcal{S}$. This claim is true because if L were a tangent line to $\mathcal{S}$, then the point $RS \cap L$ would lie on the secant line L to $\mathcal{S}$ and on the tangent line L to $\mathcal{S}$, a contradiction.

By induction, we prove that for each point $P \in \mathcal{S}$, there exists an r-space π_r, with $r \leq n-k+2$, such that all lines through P in π_r are secant lines. The case $r = 2$ is already settled, so suppose that the statement is true for r, $r < n-k+2$. There is a point $T \in B \notin \pi_r$ since $\dim\langle\mathcal{S}\rangle \geq n-k+2$. If M is a line through P in $\langle\pi_r, T\rangle$, then $\langle M, T\rangle$ intersects π_r in a line N through P, which is a secant line according to the induction hypothesis. Hence, we find three non-collinear points in $\mathcal{S}$ in the plane $\langle N, T\rangle$, from which it follows that M is a secant line, so there is an $(r+1)$-space for which any line through P is

a secant line. This implies that there is an $(n-k+2)$-space π_{n-k+2} through P such that every line through P in π_{n-k+2} is a secant line. Counting the points of $\mathcal{S}$ on lines through P in π_{n-k+2} yields that $|\mathcal{S}| \geq \theta_{n-k+1}$. □

Theorem 6.2.5. *If c is a codeword of $\mathrm{C}_k(n,q)^\perp$ of minimal weight, then $\mathcal{S} = supp(c)$ is contained in an $(n-k+1)$-space of $\mathrm{PG}(n,q)$.*

Proof. If $k = 1$, the statement holds. Hence, assume $k > 1$. Let c be a codeword of $\mathrm{C}_k(n,q)^\perp$ of minimum weight. We know from Lemma 6.2.1 that $wt(c) \leq 2q^{n-k}$. Suppose now that $\dim\langle\mathcal{S}\rangle \geq n-k+2$. Since $2q^{n-k} < \theta_{n-k+1}$, Lemma 6.2.4 shows that there exists a point $R \notin \mathcal{S}$ lying on a tangent line to $\mathcal{S}$ and lying on at least one secant line to $\mathcal{S}$. It follows from Theorem 6.2.3 that

$$wt(c) = d(\mathrm{C}_k(n,q)^\perp) = d(\mathrm{C}_{k-1}(n-1,q)^\perp) = d(\mathrm{C}_1(n-k+1,q)^\perp).$$

Let c' be defined as in the proof of Lemma 6.2.2. Since R lies on at least one secant line to $\mathcal{S}$, we have that $0 < wt(c') < wt(c)$. But this implies that c' is a codeword of $\mathrm{C}_{k-1}(n-1,q)^\perp$ satisfying $0 < wt(c') \leq wt(c) - 1 < d(\mathrm{C}_{k-1}(n-1,q)^\perp)$, a contradiction. □

6.2.2 An upper bound on the minimum weight

When q is not a prime, Corollary 6.1.8 does not hold and we present some counterexamples.

Remark. In [6, p. 130], the authors write that they have no examples of codewords of $\mathrm{C}(2,q)^\perp$, with weight smaller than $2q$, where q is odd. The next theorem provides numerous examples of such codewords for even and odd q.

Theorem 6.2.6. *Let B be a minimal $(n-k)$-blocking set in $\mathrm{PG}(n,q)$ of size $q^{n-k}+x$, with $x < (q^{n-k}+3)/2$, such that there exists an $(n-k)$-space μ intersecting B in x points. The difference of the incidence vectors of B and μ is a codeword of $\mathrm{C}_k(n,q)^\perp$ with weight $2q^{n-k} + \theta_{n-k-1} - x$.*

Proof. If $x < (q^{n-k}+3)/2$, then B is a small minimal $(n-k)$-blocking set, hence every k-space intersects B in 1 mod p points (see Theorem 2.2.2). If μ is an $(n-k)$-space π intersecting B in x points, then $(B-\mu,\pi) = (B,\pi) - (\mu,\pi) = 0$ for all k-spaces π since $(\mu,\pi = 1 \bmod p)$ and Theorem 2.2.2 shows that $(B,\pi) = 1 \bmod p$. Hence $B-\mu$ is a codeword of $\mathrm{C}_k(n,q)^\perp$, with weight $|B| + \theta_{n-k} - 2|B \cap \mu| = 2q^{n-k} + \theta_{n-k-1} - x$. □

We can use this theorem to lower the upper bound on the possible minimum weight of codewords of $\mathrm{C}_k(n,q)^\perp$. For this we need to find a small minimal $(n-k)$-blocking set B of size $q^{n-k}+x$ such that there exists an $(n-k)$-space μ with $|\mu \cap B| = x$ with x as large as possible.

Theorem 6.2.7. *There exists a small minimal $(n-k)$-blocking set B of size $q^{n-k}+x$ such that there is a $(n-k)$-space μ with $|B \cap \mu| = x$ and with $x = q^{n-k-1}(q-1)/(p-1) + \theta_{n-k-2}$.*

Proof. We first construct a Rédei-type blocking set of size $q+(q-1)/(p-1)$ in $\mathrm{PG}(2,q)$. Let $\mathcal{D}$ be the Desarguesian $(h-1)$-spread corresponding to $\mathrm{PG}(2,q)$. Let H be a $(2h-1)$-space spanned by spread elements. It follows from Theorem 1.10.1 that there exists a scattered $(h-1)$-space ν in H, i.e., $|\mathcal{B}(\nu)| = (p^h - 1)/(p-1)$. Let S be an element of $\mathcal{D} \notin H$ and let P be a point of S. The space $\nu' = \langle P, \nu\rangle$ has dimension h and $|\mathcal{B}(\nu')| = p^h + \frac{p^h-1}{p-1} = q + \frac{q-1}{p-1}$. Since $B' = \mathcal{B}(\nu')$ meets H in $(q-1)/(p-1)$ points, B' is a blocking set of Rédei-type. If we denote the line corresponding to H by L, then $|L \cap B'| = (q-1)/(p-1)$.

Embed $\mathrm{PG}(2,q)$ in $\mathrm{PG}(n-k+1,q)$ and let ψ be an $(n-k-2)$-dimensional space skew to $\mathrm{PG}(2,q)$. Let B be the cone with vertex ψ and base B'. The set B has size $q^{n-k-1}(q+(q-1)/(p-1)) + \theta_{n-k-2} = q^{n-k} + x$ with $x = q^{n-k-1}(q-1)/(p-1) + \theta_{n-k-2}$, and hence, B is small. The $(n-k)$-space $\langle \psi, L\rangle$ meets B in x points. Embed $\mathrm{PG}(n-k+1,q)$ in $\mathrm{PG}(n,q)$. It follows from Theorem 2.1.3 that the set B is a minimal $(n-k)$-blocking set in $\mathrm{PG}(n,q)$.□

Using this, together with Theorem 6.2.6, yields the following corollary.

Corollary 6.2.8. *The minimum weight $d(\mathrm{C}_k(n,q)^\perp)$ of $\mathrm{C}_k(n,q)^\perp$ satisfies the following inequality:*

$$d(\mathrm{C}_k(n,q)^\perp) \leq 2q^{n-k} - q^{n-k-1}(q-p)/(p-1).$$

Remark. For $k=1$ and $n=2$, this bound was derived by Key, McDonough, and Mavron in [81].

6.2.3 Lower bounds on the minimum weight

We first derive a trivial lower bound on the minimum weight of $\mathrm{C}_k(n,q)^\perp$.

Lemma 6.2.9. $d(\mathrm{C}_k(n,q)^\perp) \geq \theta_{n-k} + 1$.

Proof. The minimum weight of $C_1(n-k+1,q)^\perp$, hence of $C_k(n,q)^\perp$ (see Theorem 6.2.3), is at least $\theta_{n-k}+1$ since every line in $PG(n-k+1,q)$ through a point of $\mathcal{S} = supp(c)$, with $c \neq 0 \in C_1(n-k+1,q)^\perp$, has to contain at least one other point of $\mathcal{S}$. □

If q is odd, Theorems 6.2.12, 6.2.13 and 6.2.14 will improve on this lower bound. For q even, the minimum weight of $C_k(n,q)^\perp$ is known (Theorem 6.1.9).

We will derive a lower bound on the minimum weight of $C_k(n,q)^\perp$, q not a prime, q odd, by extending the bound of Sachar [127, Proposition 2.4] on the minimum weight of $C(2,q)^\perp$. Lemma 6.2.11 establishes a connection between the number of symbols used in a codeword and its minimum weight. But we first prove a useful lemma.

Lemma 6.2.10. *If S is a set of at most $2q^k$ points in $PG(n,q)$, then, for every point $R \in S$, there is a tangent i-dimensional space to S in R, $i = 0,\ldots,n-k-1$.*

Proof. Let R be a point of S. For $i=0$, the statement is trivial. Suppose by induction that the statement holds for all $j = 0,\ldots,s$, where $s < n-k-1$. Let π be the s-dimensional space meeting S only in R. The number of $(s+1)$-spaces through π is $(q^{n-s}-1)/(q-1)$, so if they all contain an extra element of S,

$$|S| \geq (q^{n-s}-1)/(q-1)+1 > 2q^k, \text{ if } s < n-k-1,$$

a contradiction. This proves the statement. □

Lemma 6.2.11. *The number of different non-zero symbols used in the codeword $c \in C_k(n,q)^\perp$, q odd, is even, say $2m$, and if there are $2m$ different non-zero symbols, then*

$$wt(c) \geq \frac{4m}{2m+1}\theta_{n-k} + \frac{2m}{2m+1}.$$

Proof. [3]Let c be a non-zero codeword in $C_k(n,q)^\perp$. Assume that $wt(c) \leq 2q^{n-k}$, and write $wt(c)$ as $\theta_{n-k}+x$. For simplicity of notations, we use the terminology 2-*secant* for a k-space having two points of $\mathcal{S}$. By Lemma 6.2.10, for every $P \in \mathcal{S} = supp(c)$, there is a $(k-1)$-space which intersects $\mathcal{S}$ only in the point P. The number of 2-secants through a given $(k-1)$-space intersecting $\mathcal{S}$ in exactly one point, is at least $\theta_{n-k}-x+1$. Since c is a codeword of $C_k(n,q)^\perp$,

[3] The ideas of this proof come from [127, Proposition 2.3].

$(c, \pi) = 0$, for all k-spaces π. So if ν is a 2-secant through the points R and R' of $\mathcal{S}$, then $c_R + c_{R'} = 0$, which implies that the symbol $c_{R'}$ occurs at least X times in c, where X denotes the minimum of the number of 2-secants through a tangent $(k-1)$-space to $\mathcal{S}$ for all tangent $(k-1)$-spaces. This implies that the number of non-zero symbols used in c must be even and that the number of occurrences of a certain non-zero symbol is always at least X. If we denote the number of different non-zero symbols by $2m$, then it follows that

$$2m(\theta_{n-k} - x + 1) \leq \theta_{n-k} + x.$$

Hence,

$$x \geq \frac{2m-1}{2m+1}\theta_{n-k} + \frac{2m}{2m+1},$$

and

$$wt(c) \geq \frac{4m}{2m+1}\theta_{n-k} + \frac{2m}{2m+1}.$$

□

Theorem 6.2.12. *If $p \neq 2$, then $d(\mathrm{C}_k(n,q)^\perp) \geq (4\theta_{n-k} + 2)/3$.*

Proof. This follows from Lemma 6.2.11 by putting $m = 1$. □

Theorem 6.2.13. *The minimum weight of $\mathrm{C}_k(n,q)^\perp$ is at least $(12\theta_{n-k}+2)/7$ if $p = 7$, and at least $(12\theta_{n-k} + 6)/7$ if $p > 7$.*

Proof. [4] Let c be a codeword of minimum weight of $\mathrm{C}_k(n,q)^\perp$ and suppose to the contrary that $wt(c) < (12\theta_{n-k} + 6)/7$. It follows from Lemma 6.2.11 that there are at most four different non-zero symbols used in the codeword c. Suppose first that there are exactly two non-zero symbols used in c, say 1 and -1. Suppose that the symbol -1 occurs the least, say y times. By Lemma 6.2.10, there is a $(k-1)$-space ν through a point R of $\mathcal{S} = supp(c)$, where $c_R = 1$ and $\nu \cap \mathcal{S} = \{R\}$. Every k-space π through ν contains at least a second point of $\mathcal{S}$. At most y of those k-spaces contain a point R' of $\mathcal{S}$ with $c_{R'} = -1$, so at least $\theta_{n-k} - y$ of those k-spaces only contain points R' of $\mathcal{S}$ with $c_{R'} = 1$. Since $(c, \pi) = 0$, such k-spaces contain 0 mod p points of $\mathcal{S}$. This yields

$$wt(c) \geq (\theta_{n-k} - y)(p-1) + y + 1.$$

[4] We use the same techniques as in the proof of Proposition 2.4 in [127].

Using that $wt(c) < (12\theta_{n-k}+2)/7$ implies that

$$p\theta_{n-k} - 7\theta_{n-k} - p + 7 < 0,$$

a contradiction if $p = 7$. Using that $wt(c) < (12\theta_{n-k}+6)/7$ implies that

$$(p-7)\theta_{n-k} + 7 - 3p < 0,$$

a contradiction if $p > 7$.

So we may assume that there are four non-zero symbols used in c, say $1, -1, a, -a$. Using the same notations as in the proof of Lemma 6.2.11, we see that

$$wt(c) \geq 4X_R. \tag{6.1}$$

We call a k-space through one of the $(k-1)$-spaces ν, with $\nu \cap \mathcal{S} = \{R\}$, that has exactly two extra points of $\mathcal{S}$, a 3-*secant*. Let X_3 denote the number of 3-secants through ν, and let X_w denote the number of k-spaces through ν that intersect $\mathcal{S}$ in more than three points. We have the following equations:

$$wt(c) \geq 1 + X_R + 2X_3 + 3X_w, \tag{6.2}$$
$$\theta_{n-k} = X_R + X_3 + X_w. \tag{6.3}$$

Suppose first that there are no 3-secants, then substituting (6.1) in (6.2) and (6.3) gives

$$wt(c) \geq 4\theta_{n-k} - 4X_w, \tag{6.4}$$
$$wt(c) \geq 1 + \theta_{n-k} + 2X_w. \tag{6.5}$$

Eliminating X_w using (6.4) and (6.5) gives

$$3wt(c) \geq 6\theta_{n-k} + 2,$$

a contradiction. This implies that $X_3 \neq 0$. Let π be a 3-secant through ν. The sum of the symbols used in π has to be zero, hence

$$(*)\ \begin{array}{l} 0 = 1 + 1 + a \text{ and } a = -2, \text{ or} \\ 0 = 1 + a + a \text{ and } a = -1/2. \end{array}$$

For each point P with $c_P = -a$, the k-space through ν containing P has to intersect $\mathcal{S}$ in more than three points, since otherwise

$$\begin{array}{l} 1 - a - a = 0 \text{ and } a = 1/2 \text{ or} \\ 1 + 1 - a = 0 \text{ and } a = 2. \end{array}$$

This contradicts $(*)$ since $p > 5$ implies that $\{2, -2\}$ cannot be the same as $\{1/2, -1/2\}$. There are at least X_R points with coefficient $-a$ and we see that they all must be on k-spaces contributing to X_w. We have

$$\begin{aligned} wt(c) &\geq 1 + X_R + 2X_3 + X_R \\ &= 1 + 2(\theta_{n-k} - X_3 - X_w) + 2X_3 \\ &= 1 + 2\theta_{n-k} - 2X_w. \end{aligned} \tag{6.6}$$

Substituting (6.3) in (6.1) and (6.2) gives

$$wt(c) \geq 4(\theta_{n-k} - X_3 - X_w) \tag{6.7}$$

$$wt(c) \geq 1 + \theta_{n-k} + X_3 + 2X_w. \tag{6.8}$$

Eliminating X_3 and X_w using (6.6), (6.7) and (6.8) yields

$$7wt(c) \geq 12\theta_{n-k} + 6;$$

a contradiction since we assumed that $wt(c) < (12\theta_{n-k} + 6)/7$. This finishes our proof. □

In [6], Bagchi and Inamdar derive a lower bound on the minimum weight of the dual code $\mathrm{C}_{s,t}(n,q)^{\perp}$, generated by the incidence matrix of s-spaces and t-spaces.

Theorem 6.2.14. [6, Theorem 3] *The minimum weight d of $\mathrm{C}_{s,t}(n,q)^{\perp}$ satisfies*

$$2\left(\frac{q^{n-s}-1}{q^{t-s}-1}(1-\frac{1}{p})+\frac{1}{p}\right) \leq d \leq 2q^{n-t}.$$

p	h	d
2	$h \geq 1$	$(q+2)q^{n-k-1}$
p	1	$2p^{n-k}$
p	$h \geq 1$	$2\left(\frac{q^n-1}{q^k-1}(1-\frac{1}{p})+\frac{1}{p}\right) \leq d$
		$\leq 2q^{n-k} - q^{n-k-1}(q-p)/(p-1)$

Table 6.1: The minimum weight d of $\mathrm{C}_k(n,q)^\perp$, $q=p^h$, p prime, $h \geq 1$

If we put $s=0$ in this theorem, we get that $d(\mathrm{C}_k(n,q)^\perp) \geq 2\left(\frac{q^n-1}{q^k-1}(1-\frac{1}{p})+\frac{1}{p}\right)$ and one can check that this improves on the lower bound derived earlier.[5]

We summarise the results on the minimum weight of $\mathrm{C}_k(n,q)^\perp$ in Table 6.1.

6.3 A gap in the weight enumerator of $\mathrm{C}_k(n,q)$

Lemma 6.3.1. *If μ_1 and μ_2 are subspaces of dimension at least $n-k$ in $\mathrm{PG}(n,q)$, then $\mu_1 - \mu_2 \in \mathrm{C}_k(n,q)^\perp$.*[6]

Proof. For every subspace μ_i of dimension at least $n-k$ and every k-space π, $(\pi, \mu_i) = 1$, hence $(\pi, \mu_1 - \mu_2) = 0$, so $\mu_1 - \mu_2 \in \mathrm{C}_k(n,q)^\perp$. □

Lemma 6.3.2. *Let c be a codeword of $\mathrm{C}_k(n,q)$. There exists a constant $a \in \mathbb{F}_p$ such that $(c,\mu) = a$, for all subspaces μ of dimension at least $n-k$.*

Proof. Lemma 6.3.1 yields $\mu_1 - \mu_2 \in \mathrm{C}_k(n,q)^\perp$, for all subspaces μ_1, μ_2 with $\dim(\mu_i) \geq n-k$, hence $(c, \mu_1 - \mu_2) = 0$, so $(c,\mu_1) = (c,\mu_2)$. □

The minimum weight of $\mathrm{C}_k(n,q)$ is θ_k, which was already proved in [4] (see Theorem 6.1.2). As promised, we give an alternative and easier proof, similar to the proof given in [6, Proposition 1].

Theorem 6.3.3. *The minimum weight of $\mathrm{C}_k(n,q)$ is θ_k, and a codeword of weight θ_k is a scalar multiple of the incidence vector of a k-space.*

[5] Unfortunately, we did not know about this theorem when submitting the articles [89, 90, 92]. This theorem allows us to derive a better bound in Theorem 6.3.9 than the one that appeared in [92].

[6] Note that $\dim \mu_1 \neq \dim \mu_2$ is allowed.

Proof. According to Lemma 6.3.2, there are two possibilities for a codeword $c \in \mathrm{C}_k(n,q)$ with $wt(c) < 2q^k$. Either $(c,\mu) \neq 0$ for every $(n-k)$-dimensional space μ, and then $\mathcal{S}$ is a k-blocking set or $(c,\mu) = 0$ for all $(n-k)$-spaces μ which implies that $c \in \mathrm{C}_{n-k}(n,q)^{\perp}$, which has weight at least $\theta_k + 1$ (see Lemma 6.2.9).

Theorem 2.1.4 shows that the minimum weight of a k-blocking set in $\mathrm{PG}(n,q)$ is equal to θ_k, and that this minimum is reached if and only if the blocking set is a k-space. □

The aim of this section is to prove that there is a gap in the weight enumerator of the code $\mathrm{C}_k(n,q)$.[7]

The next theorem establishes the connection between certain codewords of small weight in $\mathrm{C}_k(n,q)$ and small minimal blocking sets.

Remark. For the planar case, the link between codewords and blocking sets was used by Chouinard [40]. Already in 1982, Bierbrauer made use of this connection for binary codes in [15].

Theorem 6.3.4. *If c is a codeword of $\mathrm{C}_k(n,q)$, $p > 3$, with weight smaller than $2q^k$, for which $(c,\mu) \neq 0$ for some $(n-k)$-space μ, then c is a scalar multiple of an incidence vector of a small minimal k-blocking set in $\mathrm{PG}(n,q)$.*

Proof. If c is a codeword with weight smaller than $2q^k$, and $(c,\mu) = a \neq 0$ for some $(n-k)$-space μ, then, according to Lemma 6.3.2, $(c,\mu_i) = a$ for all $(n-k)$-spaces μ_i, so $\mathcal{S} = supp(c)$ defines a k-blocking set B.

Suppose that every $(n-k)$-space contains at least two points of the k-blocking set B. Counting the number of incident pairs $(P \in B, (n-k)$-space through $P)$ yields

$$|B| \begin{bmatrix} n \\ n-k \end{bmatrix}_q \geq \begin{bmatrix} n+1 \\ n-k+1 \end{bmatrix}_q 2.$$

Using $|B| \leq 2q^k$ gives a contradiction. So there is a point $R \in B$ on a tangent $(n-k)$-space. Since c_R is equal to a, according to Lemma 6.3.2, $c_{R'} = a$ for every essential point R' of B.

Suppose B is not minimal, i.e. suppose there is a point $R \in B$ that is not essential. By induction on the dimension, we find an $(n-k-1)$-dimensional

[7] This theorem was proven in [92], although most of the ideas for the proof appear already in [89] (for $\mathrm{C}_{n-1}(n,q)$) and [90]. Here, we improve on this result, using the bound of Theorem 6.2.14.

space ν tangent to B in R. If every $(n-k)$-space through ν contains two extra points of B, then $|B| > 2q^k$, a contradiction. Hence, there is an $(n-k)$-space μ, containing besides R only one extra point R' of $\mathcal{S}$, such that $(c,\mu) = c_R + c_{R'} = a$. But since B is uniquely reducible to a minimal blocking set B (see Theorem 2.4.8), R' is essential, hence, $c_{R'} = a$. But this implies that $c_R = 0$, a contradiction. We conclude that the k-blocking set B is minimal.

Since all the elements R of $\mathcal{S}$ have the coordinate value $c_R = a$, and since $(c,\mu) = a$ for every $(n-k)$-dimensional space μ, necessarily $\mathcal{S}$ intersects every $(n-k)$-dimensional space in 1 mod p points. Theorem 2.3.4 shows that if $p > 3$, B is small. □

Lemma 6.3.5. *If B_1 and B_2 are small minimal $(n-k)$-blocking sets in $\mathrm{PG}(n,q)$, then $B_1 - B_2 \in \mathrm{C}_k(n,q)^\perp$.*

Proof. It follows from Theorem 2.2.2 that $(B_i,\pi) = 1$ for all k-spaces π, $i = 1,2$. Hence $(B_1 - B_2,\pi) = 0$ for all k-spaces π. This implies that $B_1 - B_2 \in \mathrm{C}_k(n,q)^\perp$.

Lemma 6.3.6. *Let c be a codeword of $\mathrm{C}_k(n,q)$, $p > 3$, with weight smaller than $2q^k$, for which $(c,\mu) \neq 0$ for some $(n-k)$-space μ, and let B be a small minimal $(n-k)$-blocking set. Then $\mathcal{S} = supp(c)$ intersects B in 1 mod p points.*

Proof. Let c be a codeword of $\mathrm{C}_k(n,q)$, with weight smaller than $2q^k$, for which $(c,\mu) \neq 0$ for some $(n-k)$-space μ. Lemma 6.3.5 shows that $(c, B_1 - B_2) = 0 = (c,B_1) - (c,B_2)$ for all small minimal $(n-k)$-blocking sets B_1 and B_2. Hence (c,B), with B a small minimal $(n-k)$-blocking set, is a constant. Theorem 6.3.4 shows that c is a codeword only taking values from $\{0,a\}$ for some $a \in \mathbb{F}_p$, so $(c,B) = a(supp(c),B)$, hence $(supp(c),B)$ is a constant too. Let B_1 be an $(n-k)$-space, then Theorem 2.2.2 shows that $(supp(c),B_1) = 1$. This implies that the number of intersection points of $\mathcal{S}$ and B is equal to 1 mod p for every small minimal blocking set B. □

Theorem 6.3.7. *If B is a minimal k-blocking set in $\mathrm{PG}(n,p^h)$, $p > 2$, $|B| \leq 3(p^{hk} - p^{hk-1})/2$, intersecting every $\mathbb{F}_p$-linear $(n-k)$-blocking set in 1 mod p points, then B is trivial.*

Proof. Let $\mathcal{D}$ be the Desarguesian $(h-1)$-spread in $\mathrm{PG}(h(n+1)-1,p)$ and let $\mathcal{B}(\pi)$, with π an $h(n-k)$-space in $\mathrm{PG}(h(n+1)-1,p)$, be a small minimal k-blocking set. Let B be a small minimal k-blocking set, $|B| \leq 3(p^{hk} - p^{hk-1})/2$,

intersecting every $\mathbb{F}_p$-linear $(n-k)$-blocking set in 1 mod p points. Since B and $\mathcal{B}(\pi)$ intersect in 1 mod p points, there are 1 mod p spread elements of B that intersect π.

This property holds for every $h(n-k)$-space π' in $\mathrm{PG}(h(n+1)-1,p)$, since any $h(n-k)$-space π' corresponds to a small minimal $\mathbb{F}_p$-linear $(n-k)$-blocking set $\mathcal{B}(\pi')$ in $\mathrm{PG}(n,q)$.

Let $\tilde{B}$ be the set of points contained in the spread elements of B. Since a spread element that intersects a subspace of $\mathrm{PG}(h(n+1)-1,p)$ intersects it in 1 mod p points, $\tilde{B}$ intersects every $h(n-k)$-space in 1 mod p points. Moreover, $|\tilde{B}| = |B| \cdot (p^h-1)/(p-1) < 3(p^{h(k+1)-1}+1)/2$. This implies that $\tilde{B}$ is a small $(h(k+1)-1)$-blocking set in $\mathrm{PG}(h(n+1)-1,p)$.

Moreover, $\tilde{B}$ is minimal. This can be proved in the following way. Let R be a point of $\tilde{B}$. Since B is a minimal k-blocking set in $\mathrm{PG}(n,q)$, there is a tangent $(n-k)$-space S in $\mathrm{PG}(n,q)$ through the point $\mathcal{B}(R)$. Now S corresponds to an $(h(n-k+1)-1)$-space π' in $\mathrm{PG}(h(n+1)-1,p)$, such that $\mathcal{B}(R)$ is the only element of B in π'. This implies that through R, there is an $h(n-k)$-space in π' containing only the point R of $\tilde{B}$. This shows that through every point of $\tilde{B}$, there is a tangent $h(n-k)$-space, hence that $\tilde{B}$ is a minimal $(h(k+1)-1)$-blocking set.

Theorem 2.2.2 implies that $\tilde{B}$ intersects any subspace of $\mathrm{PG}(h(n+1)-1,p)$ in 1 mod p or zero points. This implies that a line is skew, tangent or entirely contained in $\tilde{B}$, hence $\tilde{B}$ is a subspace of $\mathrm{PG}(h(n+1)-1,p)$, with at most $3(p^{h(k+1)-1}+1)/2$ points, intersecting every $h(n-k)$-space. Moreover, it is the point set of a set of $|B|$ spread elements. Hence, B is a k-space in $\mathrm{PG}(n,q)$.□

Remark. Note that every small minimal k-blocking set in $\mathrm{PG}(n,p^h)$, p prime, $p>5$ satisfies the condition $|B| \leq 3(p^{hk}-p^{hk-1})/2$ since $q^k + \frac{2q^k}{p} \leq 3(p^{hk}-p^{hk-1})/2$ if $p>5$ and every small minimal blocking set, $p>5$ has size at most $q^k + \frac{2q^k}{p}$ (Theorem 2.3.4).

Lemma 6.3.2 shows that, for $c \in \mathrm{C}_k(n,q)$ and μ an $(n-k)$-space, (c,μ) is a constant. Hence, either $(c,\mu) \neq 0$ for all $(n-k)$-spaces μ, or $(c,\mu)=0$ for all $(n-k)$-spaces μ. In this latter case, $c \in \mathrm{C}_{n-k}(n,q)^\perp$.

Theorem 6.3.8. *There are no codewords in* $\mathrm{C}_k(n,q)\backslash\mathrm{C}_{n-k}(n,q)^\perp$*, with weight in the open interval* $]\theta_k, 2q^k[$*,* $p>5$.

Proof. Let c be a codeword of $\mathrm{C}_k(n,q) \setminus \mathrm{C}_{n-k}(n,q)^\perp$, $p > 5$, with weight at most $2q^k - 1$. Theorem 6.3.4 and Lemma 6.3.6 show that $\mathcal{S}$ is a small minimal k-blocking set B intersecting every $\mathbb{F}_p$-linear $(n-k)$-blocking set in 1 mod p points. Theorem 6.3.7 shows that $wt(c) = \theta_k$. □

The following theorem shows that there is a gap in the weight enumerator of the code $\mathrm{C}_k(n,q)$.

Theorem 6.3.9. *There are no codewords in* $\mathrm{C}_k(n,q)$, $p > 5$, *with weight in the open interval* $]\theta_k, 2\left(\frac{q^n-1}{q^{n-k}-1}(1-\frac{1}{p})+\frac{1}{p}\right)[$.

Proof. This follows immediately from Theorem 6.3.8 and 6.2.14. □

We will now study the hull of the code $\mathrm{C}_k(n,q)$ to prove that in the case $\mathrm{C}_{n-1}(n,q)$, we find a sharp interval on the weights for which there are no codewords in $\mathrm{C}_k(n,q)$.

Lemma 6.3.10. *Assume that* $k \geq n/2$. *A codeword* c *of* $\mathrm{C}_k(n,q)$ *is in* $\mathrm{C}_k(n,q) \cap \mathrm{C}_k(n,q)^\perp$ *if and only if* $(c,\mu) = 0$ *for all subspaces* μ *with* $\dim(\mu) \geq n-k$.

Proof. Let c be a codeword of $\mathrm{C}_k(n,q) \cap \mathrm{C}_k(n,q)^\perp$. Since $c \in \mathrm{C}_k(n,q)^\perp$, $(c,\pi) = 0$ for all k-spaces π. Lemma 6.3.2 yields that $(c,\mu) = 0$ for all subspaces μ with dimension at least $n-k$ since $k \geq n-k$. Now suppose $c \in \mathrm{C}_k(n,q)$ and $(c,\mu) = 0$ for all subspaces μ with dimension at least $n-k$. Applying this to a k-space yields that $c \in \mathrm{C}_k(n,q) \cap \mathrm{C}_k(n,q)^\perp$ since $k \geq n-k$. □

Remark. If $k < n/2$, the previous lemma is false. Let c be $\pi_1 - \pi_2$, with π_1 and π_2 two skew k-spaces. It is clear that $c \in \mathrm{C}_k(n,q)$ and that $(c,\mu) = 0$ for all $(n-k)$-spaces μ. But $c \notin \mathrm{C}_k(n,q)^\perp$ since $(c,\pi_1) = 1 \neq 0$. Note that the lemma is still valid in one direction: if $c \in \mathrm{C}_k(n,q) \cap \mathrm{C}_k(n,q)^\perp$, then $(c,\mu) = 0$ for all $(n-k)$-spaces μ. For, let μ be an $(n-k)$-space, and let π_i, $i = 1, \ldots, \theta_{n-2k}$, be the θ_{n-2k} k-spaces through a fixed $(k-1)$-space μ' contained in μ. Since $(c,\pi) = 0$ for all k-spaces π, it follows that $(c,\mu) = \sum_{i=1}^{\theta_{n-2k}} (c,\pi_i) - (\theta_{n-2k} - 1) \cdot (c,\mu') = \sum_{i=1}^{\theta_{n-2k}} (c,\pi_i) = 0$.

Corollary 6.3.11. *If* $k \geq n/2$, $\mathrm{C}_k(n,q) \setminus \mathrm{C}_{n-k}(n,q)^\perp = \mathrm{C}_k(n,q) \setminus \mathrm{C}_k(n,q)^\perp$.

Proof. It follows from Lemma 6.3.10 that $\mathrm{C}_k(n,q) \cap \mathrm{C}_{n-k}(n,q)^\perp = \mathrm{C}_k(n,q) \cap \mathrm{C}_k(n,q)^\perp$ if $k \geq n/2$. □

Theorem 6.3.12. *The minimum weight of* $\mathrm{C}_{n-1}(n,q) \cap \mathrm{C}_{n-1}(n,q)^{\perp}$ *is equal to* $2q^{n-1}$.

Proof. It follows from Lemma 6.3.10 that the support of a codeword c in $\mathrm{C}_{n-1}(n,q) \cap \mathrm{C}_{n-1}(n,q)^{\perp}$ corresponds to a set of points such that every line contains zero or at least two of them. Suppose that $wt(c) < 2q^{n-1}$. There is a line L containing exactly two points of $\mathcal{S}$, since otherwise all lines through a point $P \in \mathcal{S}$ would have two extra intersection points with $\mathcal{S}$, which would imply that $wt(c) \geq 1 + 2\theta_{n-1}$, a contradiction.

Since the intersection of a hyperplane H with a plane π is a line (if $\pi \nsubseteq H$) or the sum of the lines of a pencil (if $\pi \subseteq H$), it follows that the restriction of the codeword c to a plane π is a codeword in the code $\mathrm{C}_1(\pi)$ of points and lines in π.

In all planes π through L, $\mathcal{S}$ has at least two points and $(c,\ell) = 0$ for all lines ℓ in π, so the restriction of c to π lies in $\mathrm{C}_1(\pi) \cap \mathrm{C}_1(\pi)^{\perp}$, which has minimum weight $2q$ (see Theorem 6.1.10).

This implies that $\mathcal{S}$ has at least $\theta_{n-2}(2q-2)+2$ points which is equal to $2q^{n-1}$, a contradiction since we assumed that $wt(c) < 2q^{n-1}$. Hence, the minimum weight of $\mathrm{C}_{n-1}(n,q) \cap \mathrm{C}_{n-1}(n,q)^{\perp}$ is at least $2q^{n-1}$.

The bound can be attained when we take the difference of two hyperplanes H_1 and H_2. This vector has weight $2q^{n-1}$, it is a codeword of $\mathrm{C}_{n-1}(n,q)$ since it is a linear combination of hyperplanes, and it belongs to $\mathrm{C}_{n-1}(n,q)^{\perp}$ since $(H_1 - H_2, H) = (H_1, H) - (H_2, H) = 0$ for all hyperplanes H. □

Theorem 6.3.8 and 6.3.12 and Corollary 6.3.11 yield the following corollary, which gives an empty interval on the size of small weight codewords of $\mathrm{C}_{n-1}(n,q)$. This interval is sharp since θ_{n-1} is the weight of a codeword arising from the incidence vector of a hyperplane and $2q^{n-1}$ is the weight of a codeword arising from the difference of the incidence vectors of two hyperplanes.

Corollary 6.3.13. *There are no codewords with weight in the open interval* $]\theta_{n-1}, 2q^{n-1}[$ *in the code* $\mathrm{C}_{n-1}(n,q)$, $p > 5$.

In the planar case, this yields the following corollary, which improves on Theorem 6.1.11 of Chouinard.

Corollary 6.3.14. *There are no codewords with weight in the open interval* $]q+1, 2q[$ *in* $\mathrm{C}(2,q)$, $p > 5$.

Theorem 6.3.8 and Corollary 6.1.8 have the following corollary, extending Theorem 6.1.11 of Chouinard to general dimensions.

Corollary 6.3.15. *There are no codewords with weight in the open interval* $]\theta_k, 2p^k[$ *in the code* $\mathrm{C}_k(n,p)$, $p > 5$.

7

LDPC codes from linear representations and polar spaces

Apart from their nice geometric properties, the motivation for the study of codes from linear representations and polar spaces is their possible application when viewed as an LDPC code. If the 0-1 parity check matrix of a code C is sparse, roughly speaking if there are 'few' 1s and 'many' 0s, then we say that C is a *Low Density Parity Check code* or *LDPC code*. Sparsity is mathematically defined for sequences of matrices: a sequence of $m \times n$-matrices is called *sparse* if whenmn tends to infinity, then the number of non-zero elements is bounded by a polynomial function in m, or n, where the highest degree coefficient has degree k for some $k < 2$.[1]

LDPC codes were introduced by Gallager [60], who invented an easy decoding method for these codes in the early 1960's. LDPC codes were forgotten for more than 30 years due to the fact that the computer power in those days was unsufficient to decode codes with a useful length. They were rediscovered in the

[1] There are several definitions for the term 'sparse'. According to Shokrollahi [133], a sequence of matrices is sparse if when mn tends to infinity, then the number of non-zero elements in these matrices is always less than $\max(m, n)$. However, most codes arising from geometric objects do not satisfy this definition, and are still considered to be LDPC codes by various authors; hence this alternative definition.

1990's by MacKay and Neal [99], who showed that their empirical performance is excellent; given a communication channel, Shannon proved in 1948 that there exists a number, called the capacity of the channel, such that reliable transmission is possible for rates (in our setting, the rate is k/n) arbitrarily close to the capacity, and reliable transmission is not possible for rates above the capacity [132]. However, this theoretical approach did not give a method to construct codes ensuring a rate close to the capacity of a channel. But it turns out that there exist practical constructions of LDPC codes coming very close to this *Shannon-limit* [99]. Moreover, using iterative *belief propagation* techniques, LDPC codes can be decoded in time linearly proportional to their length. These two advantages explain the interest in LDPC codes. For more information on the encoding and decoding of LDPC codes and an extended introduction to the subject, we refer to [133].

The problem is, however, to give explicit constructions for LDPC codes. One of the methods is to construct LDPC codes using the incidence matrix of some finite incidence structure. Constructions of LDPC codes based on various types of incidence structures are studied, for example, based on generalised quadrangles [148], conics [51], or a Hermitian curve [116]. This method has as an advantage that, if the incidence structure is a partial linear space (i.e. if there is at most one block through two different points), the associated graph has girth at least 6, which forces these codes to behave better under iterative decoding via belief propagation.

Using the definition, we see that the dual codes of projective spaces[2], of linear representations and of polar spaces are LDPC codes.

In this chapter, we derive upper and lower bounds on the minimum weight of the codes arising from linear representations and polar spaces. The results concerning the codes arising from linear representations are published in [117] and the codes concerning polar spaces will appear in [118]. Both are joint work with Valentina Pepe and Leo Storme.

[2] In [85], Kou, Lin and Fossorier study the binary dual code of projective spaces $\mathrm{PG}(n,q)$, q even, from the point of view of LDPC codes. They show that these codes are easier to encode than randomly constructed LDPC codes and perform simulations on their performance.

7.1 A geometric condition

In this chapter, we denote the support of a codeword by $\mathcal{S}$ and we identify this set with the set of points it defines. We denote the point set corresponding to the complement of the support of c by $\mathcal{B}$. Recall that the p-ary code $\mathrm{C}(\mathcal{I})$, where $\mathcal{I}$ is embedded in a projective space of order q, where $q = p^h$, p prime, is the $\mathbb{F}_p$-span of the incidence matrix of $\mathcal{I}$, where the rows correspond to the blocks of $\mathcal{I}$ and the columns correspond to the points of $\mathcal{I}$. The following geometric conditions are used to find examples of codewords in the p-ary code $\mathrm{C}(\mathcal{I})^\perp$, where $\mathcal{I}$ is an incidence structure. They follow easily from the definitions.

(C1) The support of a codeword c of $\mathrm{C}(\mathcal{I})^\perp$ defines a set $\mathcal{S}$ of points of $\mathcal{I}$ such that every block of $\mathcal{I}$ contains zero or at least two points of $\mathcal{S}$.

If $p = 2$, we have the following necessary and sufficient condition for a codeword of $\mathrm{C}(\mathcal{I})^\perp$.

(C2) The support of a codeword c of the binary code $\mathrm{C}(\mathcal{I})^\perp$ defines a set $\mathcal{S}$ of points of $\mathcal{I}$ such that every block of $\mathcal{I}$ contains an even number of points of $\mathcal{S}$ and any such set defines a codeword of $\mathrm{C}(\mathcal{I})^\perp$.

(C3) If every block has an odd number of points, then the complement of the support of a codeword c of the binary code $\mathrm{C}(\mathcal{I})^\perp$ defines a blocking set $\mathcal{B}$ with respect to the blocks of $\mathcal{I}$, intersecting every block in an odd number of points.

If we dualise the incidence structure $\mathcal{I}$, we get the following condition.

(C4) The support of a codeword c of the binary code $\mathrm{C}(\mathcal{I}^D)^\perp$ defines a set $\mathcal{S}$ of blocks of $\mathcal{I}$ such that every point of $\mathcal{I}$ lies on an even number of blocks of $\mathcal{S}$, and any such set defines a codeword of $\mathrm{C}(\mathcal{I}^D)^\perp$.

7.2 Introductory results

Small weight codewords

Bagchi and Sastry were the first to investigate the code of points and lines of a generalised quadrangle. In 1988, they showed that for $X = \mathcal{W}(q)$ or $X = \mathcal{H}(3, q^2)$, the following holds[3]. For the notations, we refer to Chapter 1.

Theorem 7.2.1. [5, Theorem 2.8] *Let* $\mathrm{C}(X)$ *be the code of points and lines of* $X = \mathcal{W}(q)$, $q = p^h$ *or* $X = \mathcal{H}(3, q^2)$, *generated over the field* $\mathbb{F}_p$, *and let us denote the order of* X *by* (s, t).

(i) The minimum weight of $\mathrm{C}(X)$ *is* $s + 1$ *and any codeword of weight* $s + 1$ *is a scalar multiple of a line of* X.

(ii) The minimum weight of $\mathrm{C}(X)^\perp$ *is* $2t + 2$ *and any codeword of weight* $2t + 2$ *is a scalar multiple of a generalised subquadrangle of order* $(1, t)$.

Remark. Theorem 7.2.1 (i) also follows from the fact that $\mathrm{C}(\mathcal{W}(q))$ is a subcode of $\mathrm{C}_1(3, q)$ (resp. $\mathrm{C}(\mathcal{H}(3, q^2))$ is a subcode of $\mathrm{C}_1(3, q^2)$), and Theorem 6.1.2.

Liu and Pados [95] show that all codewords in the binary dual code of a generalised quadrangle have even weight. They also show that the minimum weight of $\mathrm{C}(\mathcal{Q}(4, q))^\perp$ is at least $2(q+1)$ if q is odd, which was greatly improved in [82], where Kim, Mellinger and Storme derive a lower bound on the minimum weight of the dual of the code of points and lines of certain classical generalised quadrangles (some coinciding with the results of Theorem 7.2.1). These results can be found in Table 7.1.

Furthermore, they characterise the codewords of small weight in the codes of some generalised quadrangles.[4]

Theorem 7.2.2. [82, Propositions 3.5 and 3.7] *In the LDPC code defined by* $\mathcal{H}(3, q^2)$, $\mathcal{W}(q)$ *for* q *even, or* $\mathcal{Q}(4, q)$ *for* q *even, every codeword of weight at most* $\sqrt{q}(q + 1)/2$ *is a linear combination of codewords of minimum weight* $2(q + 1)$.

[3] The results of Bagchi and Sastry are more general: they are also valid for some particular classes of generalised polygons, but it goes beyond the scope of this thesis to include them here.

[4] These are precisely the generalised quadrangles for which Theorem 7.2.1 of Bagchi and Sastry gives the minimum weight of the code.

Generalised quadrangle	Minimum weight
$\mathcal{W}(q)$	$2(q+1)$
$\mathcal{Q}(4,q)$, q even	$2(q+1)$
$\mathcal{Q}(4,q)$, q odd	$\geq (q+1)\sqrt{q}/2$
$\mathcal{Q}^-(5,q)$	$\geq (q+1)(q^2-q+2)$
$\mathcal{H}(3,q^2)$	$2(q+1)$
$\mathcal{H}(4,q^2)$	$\geq (q^2+1)(q^3-q^2+2)$

Table 7.1: Lower bounds on the minimum weight of the dual code of some GQ's.

Results on the dimension

Here, we do not investigate the dimension of the code of a generalised quadrangle, a linear representation, or a polar space. In the first case, the dimension was investigated by Bagchi and Sastry [5], and in the second case by Vandendriessche [144].

Remark. To our knowledge, the dimension of the code arising from points and k-spaces of a polar space $\mathcal{P}$ of rank at least 3 has not yet been investigated, unless in the symplectic case (see below). A trivial upper bound on the dimension is the dimension of the code of points and k-spaces in the projective space in which the polar space $\mathcal{P}$ is embedded, which is known (see Section 6.1).

The dimension of the p-ary code of the generalised quadrangle $\mathcal{W}(q)$ is derived by Chandler, Sin and Xiang in the following theorem.

Theorem 7.2.3. [38, Theorem 1.1] *The p-rank of the incidence matrix of points and lines of $\mathcal{W}(q)$, $q = p^h$, p odd, is equal to*

$$1 + \alpha_1^h + \alpha_2^h,$$

where $\alpha_1, \alpha_2 = \frac{p(p+1)^2}{4} \pm \frac{p(p+1)(p-1)}{12}\sqrt{17}$.

Bagchi and Sastry consider the code of a generalised quadrangle, generated over an arbitrary finite field. Under a condition on the characteristic of the field,[5] they determine the dimension of the code $\mathrm{C}(X)$.

[5] This condition is quite severe: it excludes the p-ary code of points and lines of a generalised quadrangle, embedded in $\mathrm{PG}(n,q)$ which is the case we are interested in.

Theorem 7.2.4. [5, Theorem 3.6] *Let* $\mathrm{C}(X)$ *be the code of points and lines in the generalised quadrangle* X *of order* (s,t)*, generated over the field* $\mathbb{F}_q$ *with characteristic* p*. Then* $\dim(\mathrm{C}(X)) \leq (st+1)(s+t+st)/(s+t)$ *and equality holds if* p *does not divide* $s+t$*.*

Theorem 7.2.5. [5, Theorem 3.10] *Let* $\mathrm{C}(X)$ *be the code of points and lines of* $X = \mathcal{W}(q)$ *or* $X = \mathcal{H}(3,q^2)$*, generated over the field* $\mathbb{F}_{q'}$ *with characteristic* p'*, where* X *is a generalised quadrangle of order* (s,t)*. If* p' *does not divide* $(s+1)(s+t)$*, then* $\mathrm{C}(X)^{\perp}$ *is generated by the set of minimum weight codewords in* $\mathrm{C}(X)^{\perp}$*.*

The dimension of the LDPC code generated by a linear representation $T_2^*(\mathcal{K})$, where $\mathcal{K}$ is a k-arc, was determined by Vandendriessche in 2009. He proves the following result.

Theorem 7.2.6. [144, Theorems 3.3 and 4.10] *If* $\mathcal{K}$ *is a* k*-arc in* $\mathrm{PG}(2,q)$*,* $q = p^h$*, that can be extended to an oval for* q *odd or an hyperoval for* q *even, then the code* $\mathrm{C}(T_2^*(\mathcal{K}))$ *generated over the finite field* $\mathbb{F}_{q'}$*,* $q' = p'^h$*,* p' *prime, where* $p' \neq p$*, has dimension* $\frac{(k-1)(qk-k+2)}{2}$ *and this code is generated by the codewords of minimum weight*[6] $2q$*.*

Remark. Most of the incidence structures discussed in this chapter are examples of *partial geometries* or *semipartial geometries*. A *semipartial geometry* is an incidence structure $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathrm{I})$ satisfying the following axioms.

(i) Each point is incident with $t+1$ lines and two distinct points are incident with at most one line.

(ii) Each line is incident with $s+1$ points and two distinct lines are incident with at most one point.

(iii) If P is a point and ℓ is a line not incident with P, then the number of pairs $(Q,m) \in \mathcal{P} \times \mathcal{B}$ for which $P\mathrm{I}m\mathrm{I}Q\mathrm{I}\ell$ is either 0 or a constant $\alpha > 0$.

(iv) For any pair of non-collinear points (P,Q), there are $\mu > 0$ points R such that R is collinear with both P and Q.

[6] The fact that the minimum weight of $\mathrm{C}(T_2^*(\mathcal{K}))$ is $2q$, and the nature of the codewords of weight $2q$ will be derived in this chapter. Note that this theorem excludes the case that we are interested in, namely the p-ary code of points and lines of the linear representation of $\mathcal{K}$, where $\mathcal{K} \subset \mathrm{PG}(2,q)$, $q = p^h$.

A *partial geometry* is a semipartial geometry for which the possibility 0 in condition (iii) does not occur. Note that a generalised quadrangle is a partial geometry with $\alpha = 1$. The LDPC codes of general semipartial geometries are not yet studied in a geometric way. In [80], Johnson and Weller study the LDPC code of points and lines in partial geometries. They give bounds on the minimum weight and the dimension of these LDPC codes, and in [94, Lemma 3.3], Li, Zhang and Shen investigate the LDPC codes from semipartial geometries and derive a lower bound on the minimum weight. Both of these papers use eigenvalue techniques, based on a result of Brouwer and Van Eijl [29]. In all of the cases discussed in this chapter, the bounds derived by us (using the geometric structure) are better than the ones derived in [80] or [94], that hold for arbitrary partial or semipartial geometries.

7.3 Bounds on the minimum weight

7.3.1 Bounds on the minimum weight of the dual code of a linear representation

In this subsection, we derive an upper bound on the minimum weight of the binary code $\mathrm{C}(T_2^*(\Theta))^\perp$, Θ a translation hyperoval, and the p-ary code $\mathrm{C}(T_2^*(\mathcal{K})^D)^\perp$ by giving examples of codewords of small weight. Codewords of weight at most $2q$ in the p-ary code $\mathrm{C}(T_2^*(\mathcal{K})^D)^\perp$, where $\mathcal{K} \subset H_\infty = \mathrm{PG}(2,q)$ will be characterised. Recall that if the incidence structure is embedded in a projective space of order q, $q = p^h$, p prime then the associated code is considered over the prime field $\mathbb{F}_p$. Hence, with the notation $\mathrm{C}(T_2^*(\Theta))^\perp$, Θ a translation hyperoval, we mean the *binary* code, since hyperovals only exist in the case that q is even (see Section 1.5).

Lemma 7.3.1. *There is a codeword of weight* $4q$ *in the binary code* $\mathrm{C}(T_2^*(\Theta))^\perp$, Θ *a translation hyperoval.*

Proof. Let Θ be a translation hyperoval of $\mathrm{PG}(2,q)$, $q = 2^h$. We construct a set $\mathcal{S}$ of points that satisfies condition (C2) using the coordinate description by Pambianco and Storme [110] of a construction of complete caps due to Segre [131]. Suppose that H_∞ has equation $x_2 = x_3$ and let Θ be the set $\{(t^\beta, t, 1, 1) | t \in \mathbb{F}_q\} \cup \{(1,0,0,0), (0,1,0,0)\}$, where $\beta = 2^v, \gcd(v,h) = 1$. Let $\mathcal{S}$ be the set $\mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_1' \cup \mathcal{C}_2'$, where $\mathcal{C}_1 = \{(t^\beta, t, 1, 0) | t \in \mathbb{F}_q\}$, $\mathcal{C}_2 = \{(t^\beta, t, 0, 1) | t \in \mathbb{F}_q\}$, $\mathcal{C}_1' = \{(t^\beta + \mu, t + \mu, 1, 0) | t \in \mathbb{F}_q\}$ and $\mathcal{C}_2' = \{(t^\beta + \mu, t +$

$\mu, 0, 1)|t \in \mathbb{F}_q\}$, with $\mu \neq 0, 1$. Then every affine line through Θ contains zero or two points of $\mathcal{S}$. More precisely, there are four possibilities for a line of $T_2^*(\Theta)$ that intersects $\mathcal{S}$: a line can intersect $\mathcal{C}_1$ and $\mathcal{C}_2$, or $\mathcal{C}_1'$ and $\mathcal{C}_2'$, or $\mathcal{C}_1$ and $\mathcal{C}_1'$, or $\mathcal{C}_2$ and $\mathcal{C}_2'$. The lines through a point of $\mathcal{C}_1$ and a point of $\mathcal{C}_2'$, and the lines through a point of $\mathcal{C}_1'$ and a point of $\mathcal{C}_2$ are not in the geometry $T_2^*(\Theta)$. Every affine line through the point at infinity $(1, 0, 0, 0)$ or $(0, 1, 0, 0)$, containing an affine point of $\mathcal{C}_1$ (resp. $\mathcal{C}_2$), contains an affine point of $\mathcal{C}_1'$ (resp. $\mathcal{C}_2'$). Let c be the vector with 1 in the coordinates corresponding to the affine points of $\mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_1' \cup \mathcal{C}_2'$, and 0 in the other positions. Clearly, the vector c is a codeword of the code $\mathrm{C}(T_2^*(\Theta))^\perp$ of weight $4q$. □

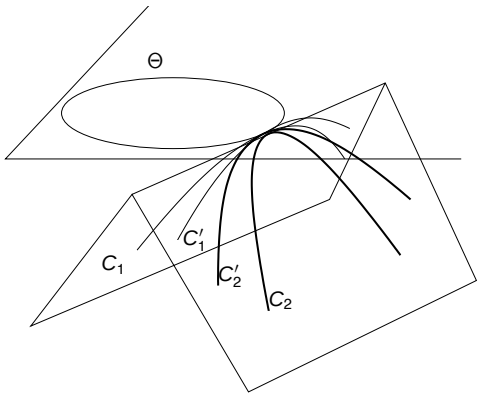

Figure 7.1: The configuration of Lemma 7.3.1.

From now on, we denote $(q+1)$-arcs $\mathcal{C}_1$, $\mathcal{C}_2$ satisfying the condition that any line that intersects $\mathcal{C}_1$ and $\mathcal{C}_2$, meets a $(q+1)$-arc $\mathcal{C}$ of Θ, by *corresponding* $(q+1)$-arcs w.r.t. $T_2^*(\Theta)$.

In the dual code of points and lines in the dual of $\mathcal{K}$, there is an easy construction of a codeword of weight $2q$.

Lemma 7.3.2. *For all point sets $\mathcal{K}$, $|\mathcal{K}| \geq 2$, $\mathcal{K} \subset \mathrm{PG}(2, q)$, there is a codeword of weight $2q$ in the p-ary code $\mathrm{C}(T_2^*(\mathcal{K})^D)^\perp$.*

Proof. Let $\pi \neq H_\infty$ be a plane of $\mathrm{PG}(3, q)$ that intersects $\mathcal{K}$ in at least two points P_1 and P_2, and let $\mathcal{S}_i$ be the set of all the affine lines of π through P_i, $i = 1, 2$. The vector c with $(-1)^i$ in the coordinate positions corresponding to $\mathcal{S}_i$, and 0 in the other positions is a codeword of weight $2q$ of the code arising from $T_2^*(\mathcal{K})$. □

If the set $\mathcal{K}$ contains a conic, for example if $\mathcal{K} = \Theta$ is a regular hyperoval, the following lemma shows how to construct a codeword with weight $2(q+1)$ in $\mathrm{C}(T_2^*(\Theta)^D))^\perp$.

Lemma 7.3.3. *If $\mathcal{K}$ contains a conic, then there is a codeword of weight $2q+2$ in the p-ary code $\mathrm{C}(T_2^*(\mathcal{K})^D)^\perp$.*

Proof. Suppose that $\mathcal{K}$ contains the conic $\mathcal{C}$ and let $\mathcal{S}$ be the set of lines of a hyperbolic quadric $\mathcal{Q} = \mathcal{Q}^+(3,q)$ intersecting H_∞ in $\mathcal{C}$. Let $\mathcal{Q}$ be the union of the two reguli $\mathcal{R}_1$ and $\mathcal{R}_2$, and let c be the vector with 1 in the coordinate positions corresponding to the lines of $\mathcal{R}_1$, -1 in the coordinate positions corresponding to the lines of $\mathcal{R}_2$, and 0 in the other positions. It is clear that c is a codeword of weight $2(q+1)$ of $\mathrm{C}(T_2^*(\mathcal{K})^D)^\perp$. □

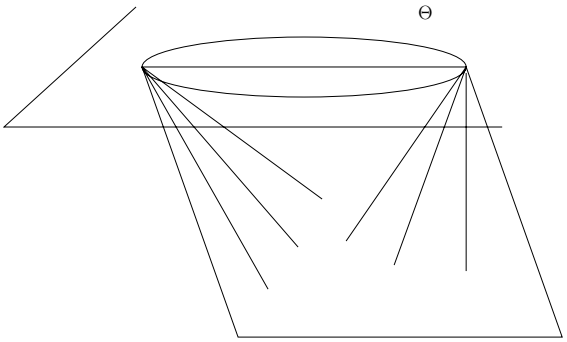

Figure 7.2 (a):
The example of Lemma 7.3.2

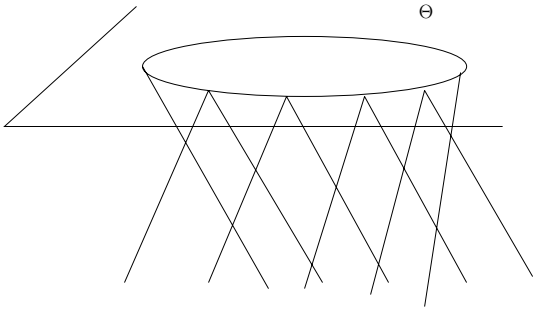

Figure 7.2 (b):
The example of Lemma 7.3.3

In Theorem 7.4.3, we will show that in the code $\mathrm{C}(T_2^*(\Theta)^D)^\perp$, where Θ is a hyperoval, the codewords of small weight arise from the examples given in Lemmas 7.3.2 and 7.3.3. The following theorem shows that codewords of weight $< 2q$ in $\mathrm{C}(T_2^*(\mathcal{K})^D)^\perp$ arise from a planar configuration and characterises codewords of weight $2q$.

Theorem 7.3.4. *Let $\mathcal{K}$ be an arbitrary set of points in $H_\infty = \mathrm{PG}(2,q)$ and let c be a codeword in the p-ary code $\mathrm{C}(T_2^*(\mathcal{K})^D)^\perp$. If $wt(c) < 2q$, then $\mathcal{S}$ is contained in a plane. If $wt(c) = 2q$ and $\mathcal{S}$ is not contained in a plane, then either:*

(i) $\mathcal{S}$ consists of $2q$ lines of a hyperbolic quadric intersecting $\mathcal{K}$ in two lines, or

(ii) $\mathcal{S} = S_1 \cup S_2$, *where* S_i, $i = 1, 2$, *is a dual* q*-arc contained in the plane* π_i, *extended by the line* $\pi_i \cap H_\infty$ *to a dual oval. If* $\pi_1 \cap \pi_2$ *is a line of* $T_2^*(\mathcal{K})^D$, *then* S_i, *the line at infinity of* π_i, *and* $\pi_1 \cap \pi_2$ *form a dual hyperoval,* $i = 1, 2$, *and* q *is even.*

Proof. Let c be a codeword of weight at most $2q$ in the code $\mathrm{C}(T_2^*(\mathcal{K})^D)^\perp$. Let $\pi_1 \neq H_\infty$ be a plane containing at least one line of $\mathcal{S}$ and let $X = \{\ell_1, \ldots, \ell_i\}$ be the set of lines of $\mathcal{S}$ contained in π_1. In order to satisfy condition (C4), every line of X has at least $q - i + 1$ affine points that lie on a line of $\mathcal{S} \setminus X$, hence

$$i(q - i + 1) \leq 2q - i,$$

from which we get: $i \geq q$ or $i \leq 2$. Hence, a plane contains either at most two or at least q lines of $\mathcal{S}$.

Suppose first that $i \geq q + 1$. If $\mathcal{S}$ is not contained in π_1, then there exists a line of $\mathcal{S}$, say ℓ, that is not contained in π_1. This line ℓ has at least $q - 1$ affine points that must lie on a second line of $\mathcal{S}$ not contained in π_1, hence $\mathcal{S} \setminus X$ contains at least $q - 1$ lines different from ℓ. This yields

$$|\mathcal{S}| = |X| + |\mathcal{S} \setminus X| \geq q + 1 + 1 + q - 1 \geq 2q + 1,$$

a contradiction.

Suppose that $i = q$, then the line ℓ_k of X has at least one affine point contained in a line of $\mathcal{S} \setminus X$, $\forall k \in \{1, \ldots, q\}$. Since $|\mathcal{S} \setminus X| \leq q$, ℓ_k has exactly one affine point contained in a line of $\mathcal{S} \setminus X$ and intersects the lines ℓ_j, $j \neq k$, in different affine points, $\forall j, k \in \{1, \ldots, q\}$. The set $\{\ell_\infty = H_\infty \cap \pi_1, \ell_1, \ldots, \ell_q\}$ is a dual oval of π_1. The lines of $\mathcal{S} \setminus X$, say $m_1, \ldots, m_q$, must intersect each other in an affine point, hence, they all lie in the same plane π_2 and, using the same arguments, the lines $m_1, \ldots, m_q$, and the line $m_\infty := \pi_2 \cap H_\infty$ form a dual oval.

If $\ell := \pi_1 \cap \pi_2$ is a line of $T_2^*(\mathcal{K})$, then $\{\ell_\infty, \ell_1, \ldots, \ell_q, \ell\}$ and $\{m_\infty, m_1, \ldots, m_q, \ell\}$ are two dual hyperovals and necessarily q is even. The sets $\{\ell_1, \ldots, \ell_q, \ell\}$ and $\{m_1, \ldots, m_q, \ell\}$ give rise to two codewords of weight $q + 1$, say c' and c'', because of condition (C4). If ℓ is not a line of $T_2^*(\mathcal{K})$, then the set $\{\ell_1, \ldots, \ell_q, m_1, \ldots, m_q\}$ gives rise to a codeword of weight $2q$.

Suppose now that every plane contains at most two lines of $\mathcal{S}$. Let ℓ_1 be a line of $\mathcal{S}$ and let P be an affine point of ℓ_1. At least one line m_1 of $\mathcal{S}$, different from ℓ_1, contains P. Let π be the plane $\langle \ell_1, m_1 \rangle$. There are $2(q - 1)$ points on the lines ℓ_1 and m_1 that must lie on a line of $\mathcal{S} \setminus X$. Let $\{\ell_2, \ldots, \ell_q\}$ be the lines of $\mathcal{S}$

intersecting m_1 and let $\{m_2, \ldots, m_q\}$ be the lines of $\mathcal{S}$ intersecting ℓ_1. If there are two lines of $\{\ell_2, \ldots, \ell_q\}$, say ℓ_2 and ℓ_3, intersecting in a point, then the plane $\langle \ell_2, \ell_3 \rangle$ contains three lines m_1, ℓ_2, ℓ_3 of $\mathcal{S}$, a contradiction. This implies that the lines in the set $\{\ell_1, \ldots, \ell_q\}$ and the lines in the set $\{m_1, \ldots, m_q\}$, are pairwise skew. Moreover, the line ℓ_i intersects the line m_j, $\forall i, j = 1, \ldots, q$. Hence, the lines of $\mathcal{S}$ form a hyperbolic quadric intersecting $\mathcal{K}$ in two lines. □

Using Theorem 7.3.4, we can derive a lower bound on the minimum weight of $\mathrm{C}(T_2^*(\mathcal{K})^D)^\perp$.

Corollary 7.3.5. *Let c be a codeword of the p-ary code $\mathrm{C}(T_2^*(\mathcal{K})^D)^\perp$ with $wt(c) < 2q$. Let x be the number of points of $\pi \cap \mathcal{K}$, where π is the plane containing all the lines of $\mathcal{S}$. Then we have*

$$wt(c) \geq q + q/(x-1).$$

Proof. Let $wt(c) = q + k$, with $1 \leq k < q$. Theorem 7.3.4 shows that $\mathcal{S}$ is contained in a plane π. Let $\pi \cap \mathcal{K} = \{P_1, \ldots, P_x\}$. The average number of lines of $\mathcal{S}$ through a point of $\pi \cap \mathcal{K}$ is $(q+k)/x$, hence there exists a point of $\mathcal{K}$, say P_1, through which there pass at least $(q+k)/x$ lines of $\mathcal{S}$. Let ℓ be a line of $\mathcal{S}$ through P_1; every affine point of ℓ is contained in at least another line of $\mathcal{S}$, hence, there are at least q lines of $\mathcal{S}$ not through P_1. This implies that the following inequality must hold:

$$\frac{q+k}{x} + q \leq q + k,$$

from which we derive $k \geq q/(x-1)$. □

If x is the minimum integer, larger than one, such that $x = |\pi \cap \mathcal{K}|$ for a plane $\pi \neq H_\infty$, then we can find a number of cases in which the lower bound of the previous corollary is sharp.

1. If $x = 2$; then $wt(c) \geq 2q$. The lower bound is sharp because of Lemma 7.3.2.

2. If $x = q + 1$ and q is even; then $wt(c) \geq q + 1$. Let $\mathcal{S}$ be a dual oval of the plane π extended by the line at infinity to a dual hyperoval. The codeword c corresponding to $\mathcal{S}$ has weight $q + 1$.

Remark. In general, the lower bound $q+q/(x-1)$, $x>2$, is sharp if we find a set $\mathcal{S}$ of lines that is a dual $(0,2,t)$-arc of size $q+t$ in $\mathrm{PG}(2,q)$ such that the line at infinity is the dual t-nucleus and $t=q/(x-1)$. Theorem 1.5.5 shows that a $(0,2,t)$-arc of size $q+t$ always has a t-nucleus. If such an arc exists, then q is even. The following example of a $(q+\sqrt{q})$-arc of type $(0,2,\sqrt{q})$ is based on a construction due to Korchmáros and Mazzocca (see [84]). The set

$$\{(z^2+z^{2\sqrt{q}},z,1)|z\in\mathbb{F}_q\}\cup\{(1,z',0)|z'\in\mathbb{F}_{\sqrt{q}}\}$$

is a $(q+\sqrt{q})$-arc of type $(0,2,\sqrt{q})$ with $(0,1,0)$ as $\sqrt{q}$-nucleus. The points

$$(z^2+z^{2\sqrt{q}}=\rho,z,1),\ \text{with } z\in\mathbb{F}_q,$$

belong to $X=\rho Z$, for some $\rho\in\mathbb{F}_{\sqrt{q}}$. The points $(1,z',0)$, with $z'\in\mathbb{F}_{\sqrt{q}}$, are on $Z=0$. So the $\sqrt{q}$-secants through $(0,1,0)$ are $X=\rho Z$, with $\rho\in\mathbb{F}_{\sqrt{q}}$, and $Z=0$, and these $\sqrt{q}+1$ lines l_i form a dual Baer subline. When we dualise, this gives a line l_∞ with $P_1,\ldots,P_{\sqrt{q}+1}$ the $\sqrt{q}+1$ points of a Baer subline, where we denoted the dual of the line l_i by P_i. There are $\sqrt{q}$ lines of $\mathcal{S}$ through every point P_i intersecting all the lines with a different direction in an affine point. The set $\mathcal{S}$ corresponds to a codeword of $T_2^*(\mathcal{K})$ with weight $q+\sqrt{q}$.

7.3.2 A lower bound on the minimum weight of the dual code of a polar space

In this subsection, we derive a lower bound on the minimum weight of the p-ary code $\mathrm{C}_k(\mathcal{P})^\perp$, $\mathcal{P}$ a classical polar space embedded in a projective space over $\mathbb{F}_q$, $q=p^h$, p prime, using an easy counting argument.

Theorem 7.3.6. *Let d be the minimum weight for the p-ary code $\mathrm{C}_k(\mathcal{P})^\perp$.*

(i) If $\mathcal{P}=\mathcal{Q}^+(2n+1,q)$, then

$$d\geq 1+\frac{q^n-1}{q^k-1}(q^{n-1}+1).$$

(ii) If $\mathcal{P}=\mathcal{Q}(2n,q)$, then

$$d\geq 1+\frac{q^{n-1}-1}{q^k-1}(q^{n-1}+1).$$

(iii) If $\mathcal{P} = \mathcal{Q}^-(2n+1,q)$, *then*

$$d \geq 1 + \frac{q^{n-1}-1}{q^k-1}(q^n+1).$$

(iv) If $\mathcal{P} = \mathcal{H}(n,q^2)$, *then*

$$d \geq 1 + \frac{(q^{n-1}-(-1)^{n-1})(q^{n-2}-(-1)^{n-2})}{q^{2k}-1}.$$

Proof. (i) Let c be a codeword of $\mathrm{C}_k(\mathcal{Q}^+(2n+1,q))^\perp$. If P is a point of $\mathcal{S}$, then every k–space of $\mathcal{Q}^+(2n+1,q)$ through P must contain at least another point of $\mathcal{S}$ (condition (C1)). The number of k–spaces of $\mathcal{Q}^+(2n+1,q)$ through P is the number of $(k-1)$–spaces of $\mathcal{Q}^+(2n-1,q)$, and this number equals (see [73, Chapter 22])

$$M := \prod_{i=0}^{k-1} \frac{q^{n-i}-1}{q^{i+1}-1} \cdot \prod_{i=n-k}^{n-1} (q^i+1)$$

and the number of k–spaces of $\mathcal{Q}^+(2n+1,q)$ through two collinear points of $\mathcal{Q}^+(2n+1,q)$ is

$$N := \prod_{i=0}^{k-2} \frac{q^{n-i-1}-1}{q^{i+1}-1} \cdot \prod_{i=n-k}^{n-2} (q^i+1),$$

hence

$$|\mathcal{S}| \geq 1 + \frac{M}{N} = 1 + \frac{q^n-1}{q^k-1}(q^{n-1}+1).$$

(ii) The same reasoning as in case (a), with $M := \prod_{i=0}^{k-1} \frac{q^{n-1-i}-1}{q^{i+1}-1} \cdot \prod_{i=n-k}^{n-1} (q^i+1)$ and $N := \prod_{i=0}^{k-2} \frac{q^{n-2-i}-1}{q^{i+1}-1} \cdot \prod_{i=n-k}^{n-2} (q^i+1)$ proves the proposition.

(iii) In this case, $M := \prod_{i=0}^{k-1} \frac{q^{n-1-i}-1}{q^{i+1}-1} \cdot \prod_{i=n-k+1}^{n} (q^i+1)$ and $N := \prod_{i=0}^{k-2} \frac{q^{n-2-i}-1}{q^{i+1}-1} \cdot \prod_{i=n-k+1}^{n-1} (q^i+1)$.

(iv) It follows from [73, Chapter 23] that $M := \prod_{i=n-2k}^{n-1}(q^i-(-1)^i)/\prod_{j=1}^{k}(q^{2j}-1)$ and $N := \prod_{i=n-2k}^{n-3}(q^i-(-1)^i)/\prod_{j=1}^{k-1}(q^{2j}-1)$. □

7.4 Characterisations of codewords of small weight

7.4.1 Small weight codewords in $\mathrm{C}(T_2^*(\Theta)^D)^\perp$

In this section, we investigate the *binary* dual code of the linear representation $T_2^*(\Theta)^D$, where Θ is a (not necessarily regular) hyperoval. We characterise small weight codewords in the binary code $\mathrm{C}(T_2^*(\Theta)^D)^\perp$.

Remark. The reason to characterise codewords of $\mathrm{C}(T_2^*(\Theta)^D)^\perp$ first is that condition (C4) is easier to work with than condition (C2). For this reason, the codes from linear representations were defined in [117] in a different way: the parity check matrix of the code defined there is the transpose of the parity check matrix defined here. Using the definition from [117], the codewords in the code of $\mathrm{C}(T_2^*(\Theta))^\perp$ are easier to determine than those in $\mathrm{C}(T_2^*(\Theta)^D)^\perp$, and a characterisation of codewords of small weight of $\mathrm{C}(T_2^*(\Theta)^D)^\perp$ is obtained by using the results for $\mathrm{C}(T_2^*(\Theta))^\perp$. Our choice for the definition is consistent with the definition of the code of projective planes (see Chapter 6) and the code of a generalised quadrangle as introduced by Liu and Pados in [95], but has as disadvantage that the method of determining the small weight codewords of $\mathrm{C}(T_2^*(\Theta))^\perp$ by using the results for $\mathrm{C}(T_2^*(\Theta)^D)^\perp$ seems a bit artificial.

Lemma 7.4.1. *Let c be a codeword of $\mathrm{C}(T_2^*(\Theta)^D)^\perp$, $\Theta \subset \mathrm{PG}(2,q)$, $q>2$. If $wt(c) \le 2(q+1)$, then either:*

(i) $\mathcal{S}$ defines a set of $2q$ lines in a plane, or

(ii) $\mathcal{S}$ defines a set of $2(q+1)$ lines of a hyperbolic quadric $\mathcal{Q}$, intersecting Θ in a conic.

Proof. By Theorem 7.3.4 and the fact that there are no lines in Θ, a codeword c of weight at most $2q$ in $\mathrm{C}(T_2^*(\Theta)^D)^\perp$ corresponds to a set $\mathcal{S}$ of $2q$ lines in a plane. Suppose that $wt(c) = 2q+1$ or $2q+2$. If every plane has at most two

lines of $\mathcal{S}$, the same argument as in the proof of Theorem 7.3.4 shows that $\mathcal{S}$ is a hyperbolic quadric $\mathcal{Q}$. In this case, $\mathcal{Q}$ meets $\mathrm{PG}(2,q) = H_\infty$ in a conic contained in Θ. Suppose that there is a plane π with more than two lines, say that π contains x lines. The number of points in π, lying on exactly one line of $\mathcal{S}$ contained in π, is at least $xq - x(x-1)/2$. It follows that the number of lines in $\mathcal{S}$ is at least $xq - x(x-1)/2 + x$, which has to be equal to $2q+1$ or $2q+2$, from which it follows for $q > 2$ that $x \leq 2$ or $x \geq 2q$. But it is clearly not possible that $2q$ of the $2q+1$ or $2q+2$ lines of $\mathcal{S}$ are contained in a plane, which proves the theorem. □

From now on, let c be a codeword of the code $\mathrm{C}(T_2^*(\Theta)^D)^\perp$, let $wt(c) = 2\delta(q+1) \leq 2\sqrt[3]{q}(q+1)/3$, and let $\mathcal{S}$ be the set of lines corresponding to $supp(c)$.

Lemma 7.4.2. *(i) For every line ℓ of $\mathcal{S}$, there exists a plane $\pi \neq H_\infty$ containing ℓ such that π contains at least $2(q-2\delta+1)$ lines of $\mathcal{S}$, or there exists a hyperbolic quadric $\mathcal{Q} \cong \mathcal{Q}^+(3,q)$ containing ℓ and intersecting Θ in a conic, such that each regulus of $\mathcal{Q}$ contains at least $q-4\delta+2$ lines of $\mathcal{S}$.*

(ii) The set $\mathcal{S}$ is contained in at most $\lceil \delta \rceil$ planes or hyperbolic quadrics sharing at least $2(q-2\delta+1)$ or $2(q-4\delta+2)$ lines with $\mathcal{S}$, respectively.

Proof. (i) Let ℓ_1 be a line of $\mathcal{S}$. The affine points of ℓ_1, say $P_1, \ldots, P_q$ need to lie on a second line of $\mathcal{S}$ to satisfy condition (C4). Denote the line of $\mathcal{S}$ through P_i, different from ℓ_1 by m_i, for all $i = 1, \ldots, q$. The lines m_i do not intersect each other affinely since $T_2^*(\Theta)$ is a generalised quadrangle, hence, there are $q(q-1)$ affine points on the lines $m_1, \ldots, m_q$ that must lie on a second line of $\mathcal{S}$. The average number of points of $m_1, \ldots, m_q$ on one of the lines of $\mathcal{S} \setminus \{\ell_1, m_1, \ldots, m_q\}$ is

$$y = \frac{q(q-1)}{(2\delta-1)(q+1)} > \frac{q-2}{2\delta}.$$

Hence, there exists a line ℓ_2 in $\mathcal{S}$ that intersects at least y of the lines $m_1, \ldots, m_q$, say $m_1, \ldots, m_k$, with $k \geq y > (q-2)/(2\delta)$. The lines ℓ_1 and ℓ_2 are either skew or intersect at infinity.

Case 1: The lines ℓ_1 and ℓ_2 intersect at infinity.

The lines $\ell_1, \ell_2, m_1, \ldots, m_k$ are contained in a plane π. Let $\Theta \cap \pi = \{P_1\} \cup \{P_2\}$, let $\mathcal{S}_i$ be the set of lines of $\mathcal{S}$ contained in π_i that go through P_i, let $x_i = |\mathcal{S}_i|$, $i = 1, 2$, and suppose that $x_1 \leq x_2$. There are $x_2(q-x_1) + x_1(q-x_2)$ affine

points on the lines of $\mathcal{S}_1 \cup \mathcal{S}_2$ that have to lie on a second line of $\mathcal{S}$. A line not in π can contain at most one affine point of π, so, to avoid a contradiction, we must have that

$$x_2(q - x_1) + x_1(q - x_2) \leq 2\delta(q + 1) - x_1 - x_2, \tag{7.1}$$

which implies that

$$x_1 + x_2 \leq 2\delta + \frac{2x_1x_2}{q+1} < 2\delta + 2x_1.$$

Let c be $x_2 - x_1$, then $c < 2\delta$. Replacing x_2 by $x_1 + c$ in (7.1) yields:

$$2x_1^2 - 2x_1(q + 1 - c) + (2\delta - c)(q + 1) \geq 0.$$

Recall that $\delta \leq \sqrt[3]{q}/3$ and that $c < 2\delta$. This implies that $x_1 \leq \delta + 1/2$ or $x_1 \geq q - 2\delta + 1$. Since x_2 is at least $k \geq (q-2)/(2\delta)$, $x_1 = x_2 - c$ must be at least $q - 2\delta + 1$. So there exists a plane π through ℓ_1 containing at least $2(q - 2\delta + 1)$ lines of $\mathcal{S}$.

Case 2: The lines ℓ_1 and ℓ_2 are skew.

There are $k(q-2)$ affine points on the lines $m_1, \ldots, m_k$ that must lie on a second line of $\mathcal{S}$, and the average number of these $k(q-2)$ points on the lines of $\mathcal{S} \setminus \{\ell_1, \ell_2, m_1, \ldots, m_k\}$ is

$$z = \frac{k(q-2)}{(2\delta - 1)(q+1) - 1} > \frac{(q-2)^2}{4\delta^2(q+1)},$$

hence, there exists a line ℓ_3 of $\mathcal{S}$ that intersects $t \geq z > (q-2)^2/(4\delta^2(q+1))$ lines of $m_1, \ldots, m_k$, say $m_1, \ldots, m_t$. The lines ℓ_1, ℓ_2 and ℓ_3 are pairwise skew, hence they define a hyperbolic quadric $\mathcal{Q} \cong \mathcal{Q}^+(3, q)$. Denote the lines of $\mathcal{S}$, contained in the first (resp. second) regulus of $\mathcal{Q}$ by $\mathcal{S}_1$ (resp. $\mathcal{S}_2$), let $x_i = |\mathcal{S}_i|$, $i = 1, 2$, and suppose that $x_1 \leq x_2$. There are $x_1(q - x_2) + x_2(q - x_1)$ affine points on the lines of $\mathcal{S}_1 \cup \mathcal{S}_2$ that must lie on a second line of $\mathcal{S}$. A line not contained in $\mathcal{Q}$ can meet the quadric $\mathcal{Q}$ in at most two points, hence

$$x_2(q - x_1) + x_1(q - x_2) \leq 4\delta(q + 1) - 2(x_1 + x_2) \tag{7.2}$$

which yields that

$$x_1 + x_2 < 4\delta + 2x_1. \tag{7.3}$$

Replacing x_2 by $x_1 + c$ in (7.2) gives the following inequality

$$2x_1^2 - 2x_1(q + 2 - c) + 4\delta(q + 1) - c(q + 2) \geq 0.$$

Recall that $c < 4\delta$ from (7.3), $\delta \leq \sqrt[3]{q}/3$ and x_2 must be at least $t > (q - 2)^2/(4\delta^2(q+1))$, so the inequality (7.2) is only satisfied if $x_1 > q - 4\delta + 2$. This implies that there exists a hyperbolic quadric $\mathcal{Q}^+(3, q)$ that contains at least $q - 4\delta + 2$ lines of $\mathcal{S}$ in each of its reguli. Moreover, Θ is a regular hyperoval since it contains already at least $q - 4\delta + 2$ points of a conic (see Lemma 1.5.2).

(ii) Part (i) implies that the lines of $\mathcal{S}$ are contained in planes and hyperbolic quadrics with 'many' lines of $\mathcal{S}$ in them. Let $\mathcal{S}$ be contained in k planes with at least $2(q - 2\delta + 1)$ lines of $\mathcal{S}$ and k' hyperbolic quadrics with at least $2(q - 4\delta + 2)$ lines of $\mathcal{S}$. Two planes have at most one line in common, a plane and a hyperbolic quadric have at most two lines in common, and two hyperbolic quadrics containing at least $2(q - 4\delta + 2)$ lines of $\mathcal{S}$ share the same conic contained in Θ and therefore share at most two lines. Since $wt(c) \leq 2\delta(q+1)$, we get that

$$2k(q - 2\delta + 1) + 2k'(q - 4\delta + 2) - (k + k' - 1)(k + k') \leq 2\delta(q + 1).$$

For simplicity, we replace the term $(q - 2\delta + 1)$ by the smaller term $(q - 4\delta + 2)$ and substitute λ for $k + k'$. We obtain that

$$-\lambda^2 + \lambda(2q - 8\delta + 5) \leq 2\delta(q + 1). \tag{7.4}$$

Replacing λ by $\delta + 1$ in inequality (7.4) gives a contradiction, hence, λ is at most $\lceil \delta \rceil$.

□

The previous lemma enables us to characterise the codewords of small weight in the dual code of $T_2^*(\Theta)^D$.

Theorem 7.4.3. *Every codeword in* $\mathrm{C}(T_2^*(\Theta)^D)^\perp$ *of weight at most* $2\sqrt[3]{q}(q + 1)/3$ *is a linear combination of* $\lceil \frac{wt(c)}{2q+2} \rceil$ *codewords of weight* $2q$ *or* $2(q + 1)$.

Proof. Lemma 7.4.1 shows that every codeword in $\mathrm{C}(T_2^*(\Theta)^D)^\perp$ of weight at most $2q+2$ is either a codeword of weight $2q$ or a codeword of weight $2q+2$, and hence, a (trivial) linear combination of codewords of weight $2q$ and $2q+2$. We proceed by induction on the weight of the codewords to show that a codeword in $\mathrm{C}(T_2^*(\Theta)^D)^\perp$ of weight at most $2\sqrt[3]{q}(q+1)/3$ is a linear combination of codewords of weight $2q$ or $2q+2$: let c be a codeword of $\mathrm{C}(T_2^*(\Theta)^D)^\perp$ of weight $2\delta(q+1)$, $\delta \leq \sqrt[3]{q}/3$, and assume that all the codewords of C of weight smaller than $wt(c)$ have already been characterised as being linear combinations of codewords of weight $2q$ and $2(q+1)$.

Let $\{X_1, \ldots, X_t\}$, $t \leq \lceil \delta \rceil$, be the set of planes and hyperbolic quadrics in which $\mathcal{S}$ is contained (see Lemma 7.4.2 (ii)). Since X_i, $i \neq j$, meets X_j in at most two lines, every X_i contains at least $2q - 8\delta + 4 - 2\lceil \delta \rceil$ lines of $\mathcal{S}$ that are not contained in X_j, $j \neq i$. Let ℓ_1 be a line of $\mathcal{S}$ contained in X_1 and not contained in X_j, $j \neq 1$. There exist z points $R_1, \ldots, R_z$, with $z \geq q - 2\lceil \delta \rceil$, on ℓ_1 lying on exactly two lines of $\mathcal{S}$. Denote the line of $\mathcal{S}$ through R_i, different from ℓ_1, by ℓ_{i+1}, $i = 1, \ldots, z+1$. Since there are at most $10\delta + 2$ lines of X_1 that are either not contained in $\mathcal{S}$ or contained in $\{X_2, \ldots, X_t\}$, and $q - 2\lceil \delta \rceil > 10\lceil \delta \rceil + 2$, at least one of the lines ℓ_{i+1}, say ℓ_2 is an element of $\mathcal{S}$, not belonging to $\{X_2, \ldots, X_t\}$. On the line ℓ_2, we find points $R'_1, \ldots, R'_{z'}$, $z' \geq q - 2\lceil \delta \rceil$, lying on exactly two lines of $\mathcal{S}$, and we denote the lines of $\mathcal{S}$ in X_1 through R'_i, different from ℓ_2, by $m_1, \ldots, m_{z'}$, $z' \geq q - 2\lceil \delta \rceil$.

Hence, the codeword c has 1 in the $z + z' \geq 2q - 4\lceil \delta \rceil$ positions corresponding to $\ell_1, \ldots, \ell_z, m_1, \ldots, m_{z'}$.

Let c' be the codeword defined by taking all symbols in the positions corresponding to lines of X_1 equal to 1, then c and c' share at least $2q - 4\lceil \delta \rceil$ non-zero positions. Now

$$\begin{aligned} wt(c - c') &= wt(c) + wt(c') - 2wt(c \cap c') \\ &\leq wt(c) + 2q + 2 - 2(2q - 4\lceil \delta \rceil) < wt(c). \end{aligned}$$

By the induction hypothesis, $c - c'$ is a linear combination of codewords of weight $2q$ and $2q+2$. Hence, $c = (c - c') + c'$ is a linear combination of such codewords too.

From the preceding arguments, it also follows that every X_i corresponds to a codeword that occurs in the linear combination defining the codeword c. Hence, c is a linear combination of at most $\lceil \delta \rceil$ codewords of weight $2q$ and $2q+2$. We will now show that a codeword c with $wt(c) \leq 2\sqrt[3]{q}(q+1)/3$ is a

linear combination of $\lceil \frac{wt(c)}{2q+2} \rceil$ codewords of weight $2q$ and $2q+2$. A codeword arising from the sum of x planes and hyperbolic quadrics has weight at least $2xq - \frac{x(x-1)}{2} \cdot 2$, and weight at most $x(2q+2)$. Since

$$2q(x+1) - (x+1)x > x(2q+2), \ \forall x \leq \lceil \delta \rceil \leq \sqrt[3]{q}/3,$$

we conclude that there are gaps in the weight enumerator of $\mathrm{C}(T_2^*(\Theta)^D)^\perp$ and that a codeword c, with $wt(c) \leq 2\sqrt[3]{q}(q+1)/3$, is a linear combination of $\lceil \frac{wt(c)}{2q+2} \rceil$ codewords of weight $2q$ and $2q+2$.

□

7.4.2 Small weight codewords in $\mathrm{C}(T_2^*(\Theta))^\perp$

In this section, we investigate the small weight codewords of $\mathrm{C}(T_2^*(\Theta))^\perp$, Θ a translation hyperoval. Since we already investigated the code of the dual of $T_2^*(\Theta)$, we will describe $T_2^*(\Theta)$ as the dual of $T_2^*(\Theta)^\mathcal{D}$ and use Theorem 7.4.3. For this, we need a detailed study of the relation between $T_2^*(\Theta)$ and $T_2^*(\Theta)^D$.

We distinguish between the case where Θ is a non-regular translation hyperoval and the case where Θ is a regular hyperoval, which is a conic and its nucleus to find a description of $T_2^*(\Theta)^D$. In the latter case, the alternative description will enable us to derive a larger bound on the weight of the codewords that can be characterised.

The case $T_2^*(\Theta)^D$, with Θ a translation hyperoval

We explicitly describe the dual generalised quadrangle $T_2^*(\Theta)^D$.

Let Θ be the translation hyperoval

$$\left\{(1, x, x^\beta) | x \in \mathbb{F}_q\right\} \cup \left\{(0,0,1), (0,1,0)\right\},$$

embedded in the plane $X_0 = 0$ of $\mathrm{PG}(3,q)$, with β a generator of $\mathrm{Aut}(\mathbb{F}_q)$.

Theorem 7.4.4. *$T_2^*(\Theta)^D$ can be described as an incidence structure $(\mathcal{P}, \mathcal{L}, \mathrm{I})$ with*

$$\mathcal{P} = \begin{cases} \textit{Affine points of } T_2^*(\Theta). \\ \textit{Affine planes through } (0,0,1,0) \textit{ and } (0,1,a,a^\beta), a \in \mathbb{F}_q. \\ \textit{Affine planes through } (0,0,0,1) \textit{ and } (0,1,a,a^\beta), a \in \mathbb{F}_q. \end{cases}$$

$\mathcal{L}=$ *Affine lines through the points* $(0,1,a,a^\beta)$ *of* Θ.

$$\mathrm{I}=\begin{cases} \textit{An affine point } P \textit{ lies on an affine line } L \textit{ if } P\in L.\\ \textit{An affine plane } \Pi \textit{ through } (0,1,a,a^\beta),\textit{ and } (0,0,0,1) \textit{ or } (0,0,1,0),\\ \textit{ is incident with the affine lines of } \Pi \textit{ through } (0,1,a,a^\beta). \end{cases}$$

Proof. The map φ with $\varphi(1,a,b,c)=\langle(1,0,c,b^\beta),(0,1,a,a^\beta)\rangle$ is a bijection that maps points onto objects that will be the lines of the geometry $T_2^*(\Theta)^D$. From the definition of φ, we get that $\mathcal{L}$ consists of all affine lines through the points $(0,1,u,u^\beta), u\in\mathbb{F}_q$.

We obtain the points of $T_2^*(\Theta)^D$ by determining the images of the lines of $T_2^*(\Theta)$ under φ.

A line $\langle(0,0,0,1),(1,a,b,c)\rangle$ through $R=(0,0,0,1)$ corresponds to the set

$$\left\{\langle(1,0,c+\lambda,b^\beta),(0,1,a,a^\beta)\rangle|\lambda\in\mathbb{F}_q\right\}.$$

All lines of this set are contained in a plane π_1 through $(0,0,1,0)$ and $(0,1,a,a^\beta)$, so we can identify this set of lines with π_1.

A line $\langle(0,0,1,0),(1,a,b,c)\rangle$ through $N=(0,0,1,0)$ corresponds to the set

$$\{\langle(1,0,c,b^\beta+\lambda^\beta),(0,1,a,a^\beta)\rangle|\lambda\in\mathbb{F}_q\}.$$

All lines of this set are contained in a plane π_2 through $(0,0,0,1)$ and $(0,1,a,a^\beta)$, so we can identify this set of lines with π_2.

A line through $(1,a,b,c)$ and $(0,1,u,u^\beta)$ corresponds to the set

$$\left\{\langle(1,0,c+\lambda u^\beta,b^\beta+\lambda^\beta u^\beta),(0,1,a+\lambda,a^\beta+\lambda^\beta)\rangle|\lambda\in\mathbb{F}_q\right\}.$$

Note that the lines of this set all pass through the point P with coordinates $(1,u^\beta,c+au^\beta,b^\beta+u^\beta a^\beta)$. So we can identify this set of lines with the point P.

Using these relations, it is clear that φ maps collinear points to intersecting lines, and intersecting lines to collinear points. □

We first have a closer look at the duality φ^{-1}, where φ is the duality between $T_2^*(\Theta)$ and $T_2^*(\Theta)^D$ defined in the proof of Theorem 7.4.4. When $\varphi(x)=y$, or $\varphi(y)=x$, then x and y are called *corresponding*.

Lemma 7.4.5. *(i) The duality φ^{-1} maps lines of $T_2^*(\Theta)^D$ through the same point at infinity to points in the same plane in $T_2^*(\Theta)$.*

(ii) All planes in $T_2^*(\Theta)$ with points corresponding to lines in $T_2^*(\Theta)^D$ contain the points $R = (0,0,0,1)$ and $N = (0,0,1,0)$.

(iii) The duality φ^{-1} maps q coplanar lines of $T_2^*(\Theta)^D$ through a point $(0,1,u,u^\beta)$, $u \in \mathbb{F}_q$, to a q-arc in a plane through R and N.

Proof. (i) The line passing through $(1,0,x,y^\beta)$ and $(0,1,a,a^\beta)$ is mapped by φ^{-1} to the point $(1,a,y,x)$. So all lines of $T_2^*(\Theta)^D$ through $(0,1,a,a^\beta)$ are mapped to points lying in the plane $aX_0 + X_1 = 0$.

(ii) As seen in (i), all these planes have equation $\alpha X_0 + X_1 = 0$, hence contain the points R and N.

(iii) All points of the plane Π through $(0,1,u,u^\beta)$, $(0,1,v,v^\beta)$ and $(1,0,a,b^\beta)$ have coordinates $(1,\lambda+\mu,a+\lambda u+\mu v, b^\beta+\lambda u^\beta+\mu v^\beta)$.

It follows that the affine lines through $(0,1,u,u^\beta)$ and the q points $(1,0,a+\lambda(u+v), b^\beta+\lambda(u^\beta+v^\beta))$, $\lambda \in \mathbb{F}_q$, in Π are mapped to the q points $(1,u,b+\lambda^{\beta^{-1}}(u+v), a+\lambda(u+v))$, with $\lambda \in \mathbb{F}_q$. It is easy to see that this set forms a q-arc. From (i) and (ii), we get that this q-arc lies in the plane $uX_0 + X_1 = 0$ through R and N. □

Lemma 7.4.6. *Under the duality φ^{-1}, $2q$ coplanar lines in $T_2^*(\Theta)^D$ correspond to two corresponding q-arcs in two planes through RN.*

Proof. Consider $2q$ lines $\ell_1, \ldots, \ell_q, m_1, \ldots, m_q$ of $T_2^*(\Theta)^D$ lying in the same plane, say π, where $\ell_1, \ldots, \ell_q$ meet Θ in the point P and $m_1, \ldots, m_q$ meet Θ in the point Q. By the previous lemmas, $\ell_1, \ldots, \ell_q$ and $m_1, \ldots, m_q$ correspond to q-arcs $\mathcal{A}_1, \mathcal{A}_2$, lying in a plane through R and N. The duality φ^{-1} gives us the following correspondences.

By Theorem 7.4.4, a line through R in $T_2^*(\Theta)$ corresponds to a tangent plane in $T_2^*(\Theta)^D$ (which is a point of $T_2^*(\Theta)^D$); a line through N in $T_2^*(\Theta)$ corresponds to a plane through R in $T_2^*(\Theta)^D$ (which is a point of $T_2^*(\Theta)^D$).

A tangent plane in $T_2^*(\Theta)^D$ through P contains only one line of $T_2^*(\Theta)^D$. So a line through R in the plane defined by P in $T_2^*(\Theta)$ contains only one point of B. The affine planes through R and P contain only one line of π of $T_2^*(\Theta)^D$, so, applying φ^{-1}, every line through N in $T_2^*(\Theta)$ in the plane defined by P contains only one point of B. The same holds for the plane defined by Q.

The points R and N do not lie on secants to $\mathcal{A}_i$, $i = 1, 2$, which means that R and N extend $\mathcal{A}_1$ and $\mathcal{A}_2$ to $(q+2)$-arcs.

A point of $T_2^*(\Theta)^D$ lies on zero or exactly two lines of $\{\ell_1, \ldots, \ell_q, m_1, \ldots, m_q\}$. So a line of $T_2^*(\Theta)$ not through R or N contains zero or exactly two points of $\mathcal{A}_1 \cup \mathcal{A}_2$. Connecting a point of $\Theta \backslash \{R, N\}$ with the q points of the q-arc $\mathcal{A}_1$ gives rise to the q-arc $\mathcal{A}_2$ in the second plane through RN and vice versa. We conclude that the two q-arcs $\mathcal{A}_1$ and $\mathcal{A}_2$ are corresponding. □

Theorem 7.4.7. *The minimum weight of* $\mathrm{C}(T_2^*(\Theta))^\perp$*, with* Θ *a non-regular translation hyperoval, is equal to* $4q$*. The minimum weight vectors correspond to the incidence vectors of a set of all lines of* $T_2^*(\Theta)^D$ *in two planes, where these two planes pass through the same line at infinity, with the line at infinity not through* R *nor* N*.*

A codeword c *of* $\mathrm{C}(T_2^*(\Theta))^\perp$*, of weight* $2\delta q$*, with* $\delta \leq \sqrt[3]{q}/3$*, is a linear combination of* $\lceil \frac{wt(c)}{2q} \rceil$ *codewords of* $\mathrm{C}(T_2^*(\Theta)^D)^\perp$*, with weight* $2q$*, which are coming from* $2q$ *lines of* $T_2^*(\times)$ *in planes through two points of* $\Theta \backslash \{R, N\}$*, where the number of lines through a point of* $\Theta \backslash \{R, N\}$ *has to be even.*

Throughout this proof, we use $R = (0, 0, 0, 1)$ and $N = (0, 0, 1, 0)$, and as usual, $\mathcal{S}$ is the set of lines defined by $supp(c)$, with c a codeword of $\mathrm{C}(T_2^*(\Theta))^\perp$.

Proof. Codewords of $\mathrm{C}(T_2^*(\Theta))^\perp = \mathrm{C}((T_2^*(\Theta)^D)^D)^\perp$ satisfy condition (C4). There is only one kind of lines in $T_2^*(\Theta)^D$, the affine lines through the points with coordinates $(0, 1, u, u^\beta)$, and there are three kinds of points of $T_2^*(\Theta)^D$ that have to lie on an even number of lines of $\mathcal{S}$.

A: The affine points.

When we only use the condition (C4) that every affine point has to lie on an even number of lines, we can copy the proof for the code of $\mathrm{C}(T_2^*(\Theta)^D)^\perp$. In that case, the minimum weight of the code equals $2q$ and this weight occurs when taking all lines of $T_2^*(\Theta)$ in a fixed plane.

For every line ℓ of $\mathcal{S}$, there are two possibilities: either there exists a plane through ℓ with at least $2(q - 2\delta + 1)$ lines of $\mathcal{S}$, or there is a hyperbolic quadric through ℓ with at least $2(q - 4\delta + 1)$ lines of $\mathcal{S}$. But in this case, there are no codewords consisting of hyperbolic quadrics, since there is no conic lying at infinity in Θ. So the initial description of the codewords becomes: *Every*

possible codeword of weight $\leq 2\delta q$*, with* $\delta \leq \sqrt[3]{q}/3$*, in* $\mathrm{C}(T_2^*(\Theta))^\perp$ *is a linear combination of codewords of* $\mathrm{C}(T_2^*(\Theta)^D)^\perp$ *of weight* $2q$*, consisting of the* $2q$ *lines of* $T_2^*(\Theta)$ *in a plane containing two points* $(0,1,u,u^\beta)$ *and* $(0,1,v,v^\beta)$. All lines in such a plane have a 1 in the corresponding codeword and it also follows, since

$$(x+1)2q - \frac{(x+1)x}{2}2 > 2qx \ \forall x \leq \lceil \delta \rceil \leq \sqrt[3]{q}/3,$$

that a codeword c of weight $\leq 2\delta q$, with $\delta \leq \sqrt[3]{q}/3$, in $\mathrm{C}(T_2^*(\Theta))^\perp$ is a linear combination of $\lceil \frac{wt(c)}{2q} \rceil$ codewords of $\mathrm{C}(T_2^*(\Theta)^D)^\perp$ of weight $2q$.

We need to investigate which extra conditions the other two kinds of points of $T_2^*(\Theta)$ impose.

B: The points arising from tangent planes to Θ (planes through $(0,0,1,0)$).

Each tangent plane through a point $(0,1,u,u^\beta)$ has to contain an even number of lines. Case A implies that the possible codewords of $\mathrm{C}(T_2^*(\Theta)^D)^\perp$ of weight $\leq 2\delta q$ are linear combinations of codewords of weight $2q$ of the dual code of $T_2^*(\Theta)^D$ in planes through two points $(0,1,u,u^\beta)$ and $(0,1,v,v^\beta)$. Take a codeword of weight $2q$, lying in the plane π, then the tangent planes at $\pi \cap \Theta$ contain only one line of $\mathcal{S}$. So at least two codewords of the dual code of $T_2^*(\Theta)^D$ (in planes π_1 and π_2) are needed to construct a codeword. Now there are three possibilities.

(i) The intersection of $\pi_1 \cap \Theta$ and $\pi_2 \cap \Theta$ is empty. In this case, in each of the points of $\pi_1 \cap \Theta$ and $\pi_2 \cap \Theta$, the tangent planes through N contain only one line, a contradiction.

(ii) There is exactly one intersection point in common in $\pi_1 \cap \Theta$ and $\pi_2 \cap \Theta$. In this case, for the two non-common intersection points, a tangent plane through them contains only one line, a contradiction.

(iii) The two intersection points of $\pi_1 \cap \Theta$ and $\pi_2 \cap \Theta$ coincide.

The only possibility for a codeword consisting of two codewords of $\mathrm{C}(T_2^*(\Theta)^D)^\perp$, hence a codeword of weight $4q$, is a codeword arising from two planes π_1 and π_2 through the same points at infinity of $\Theta \backslash \{R, N\}$.

C: The points arising from planes through $(0,0,0,1) = R$**.**

Take a possible codeword found in Case B. Then $\mathcal{S}$ has two lines in common with the planes through R and the intersection points of the planes π_1 and π_2 with Θ. Furthermore, $\mathcal{S}$ has zero lines in common with planes through R and a different point of Θ. So the possible codeword of weight $4q$ does occur.

We conclude that, from case A, every codeword of weight at most $2\delta q$, with $\delta \leq \sqrt[3]{q}/3$, is a linear combination of codewords of $\mathrm{C}(T_2^*(\Theta)^D)^\perp$ with weight $2q$. Cases B and C yield the second condition: the number of lines in each tangent plane to the q-arc $\Theta \backslash \{R, N\}$ is even. □

Remark. Note that even though we use linear combinations of codewords of weight $2q$ of $\mathrm{C}(T_2^*(\Theta)^D)^\perp$, there are no codewords of weight $2q$ in $\mathrm{C}(T_2^*(\Theta))^\perp$.

We now transfer the result on the codewords of small weight in the code $\mathrm{C}(T_2^*(\Theta))^\perp$ back to the original setting.

Theorem 7.4.8. *The codewords of the* $\mathrm{C}(T_2^*(\Theta))^\perp$*,* Θ *a non-regular translation hyperoval, with weight* $\leq 2\sqrt[3]{q}q/3$*, are linear combinations of incidence vectors of 2 corresponding q-arcs, each in a plane through* RN*, such that the number of points on a line of* $T_2^*(\Theta)$ *is even. In particular, the number of q-arcs in a fixed plane through* RN*, is even. The minimum weight is equal to* $4q$*, corresponding to two sets of corresponding q-arcs, lying in two planes through* RN*.*

Proof. This is the dual of Theorem 7.4.7, using Lemmas 7.4.5, 5.3.2, 7.4.6 to dualise. □

The case Θ **is a regular hyperoval**

We find a description of $T_2^*(\Theta)^D$ by using the following construction by Payne.

Theorem 7.4.9. [113] *Let* $S = GQ(s) = (\mathcal{P}, \mathcal{L}, \mathrm{I})$ *and let* x *be a regular point. The following incidence structure* $(\mathcal{P}', \mathcal{B}', \mathrm{I}')$ *is a* $GQ(s-1, s+1)$*.*

$$\mathcal{P}' = \mathcal{P} \backslash x^\perp$$
$$\mathcal{L}' = \begin{cases} \textit{The lines of } \mathcal{L} \textit{ not through } x. \\ \textit{The hyperbolic lines } \{x,y\}^{\perp\perp}, x \nsim y. \end{cases}$$
$$\mathrm{I}' = \textit{Natural incidence.}$$

Applying the preceding construction on $T_2(\Theta')$, Θ' a conic, gives $T_2^*(\Theta)$ for Θ the regular hyperoval containing Θ'. Note that $T_2(\Theta')$ is isomorphic to $\mathcal{Q}(4,q)$ (see [114, Theorem 3.2.2]), so we can describe $T_2^*(\Theta)$ on $Q(4,q)$. Let P be a fixed point of $\mathcal{Q}(4,q)$ and assume that q is even. In that case, all points of $\mathcal{Q}(4,q)$ are regular (see [114, Theorem 3.3.1]). The generalised quadrangle $T_2^*(\Theta)$ is the following incidence structure $(\mathcal{P},\mathcal{L},\mathrm{I})$.

$$\mathcal{P} = \text{The points of } \mathcal{Q}(4,q) \text{ not on } P^\perp.$$

$$\mathcal{L} = \begin{cases} \text{The lines of } Q(4,q) \text{ not through } P. \\ \text{The conics } C = \pi \cap \mathcal{Q}(4,q) \text{ where } \pi \text{ is a plane through } \langle N, P\rangle, \\ \quad \text{with } N \text{ the nucleus of } \mathcal{Q}(4,q). \end{cases}$$

$$\mathrm{I} = \text{Natural incidence.}$$

We dualise the incidence structure of $T_2^*(\Theta)$ described on $\mathcal{Q}(4,q)$. Since $Q(4,q)$, with q even, is self-dual (see Theorem 1.4.1), the point P becomes a line L, and conics become reguli. So $T_2^*(\Theta)^D$ described on $\mathcal{Q}(4,q)$ is an incidence structure $(\bar{\mathcal{P}},\bar{\mathcal{L}},\bar{\mathrm{I}})$ with

$$\bar{\mathcal{P}} = \begin{cases} \text{The points } P \text{ of } Q(4,q) \text{ not on } L. \\ \text{The reguli through } L. \end{cases}$$

$$\bar{\mathcal{L}} = \text{The lines } M \text{ of } Q(4,q) \text{ not in } L^\perp.$$

$$\bar{\mathrm{I}} = \text{Natural incidence.}$$

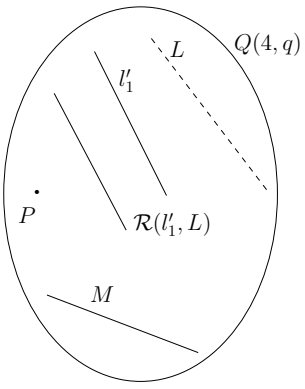

Figure 7.3: $T_2^*(\Theta)$ described on $Q(4,q)$

Using the same techniques as for Θ a non-regular hyperoval, we get a characterisation of the codewords of small weight in $\mathrm{C}(T_2^*(\Theta))^\perp$. The proof can be found in [117]. We obtain the following result.

Theorem 7.4.10. *The support of a codeword c, with $wt(c) \leq 4q^{3/2}/5$, in $\mathrm{C}(T_2^*(\Theta))^\perp$, Θ a regular hyperoval, is a linear combination of two by two corresponding conics, lying in tangent planes to the conic in Θ, such that the number of points on a line of $T_2^*(\Theta)$ is even. In particular, the number of conics in one tangent plane is even.*

Proof. See [117, Theorem 25]. □

7.4.3 Small weight codewords in $\mathrm{C}_2(\mathcal{Q}^+(5,q))^\perp$

In Section 1.11.1, we introduced the notation $\mathrm{C}_2(\mathcal{Q}^+(5,q))^\perp$ for the p-ary dual code of points and generators of $\mathcal{Q}^+(5,q)$. If c is a codeword in the p-ary code $\mathrm{C}_2(\mathcal{Q}^+(5,q))^\perp$, then $\mathcal{S}$ is a set of points of $\mathcal{Q}^+(5,q)$ such that every plane of $\mathcal{Q}^+(5,q)$ contains zero or at least two points of $\mathcal{S}$ (condition (C1)). Moreover, the sum of symbols c_P of the points P in each plane of $\mathcal{Q}^+(5,q)$ equals 0. Using the Klein correspondence, introduced in Chapter 1, this set $\mathcal{S}$ of points of $\mathcal{Q}^+(5,q)$ corresponds to a set $\mathcal{S}_L$ of lines in $\mathrm{PG}(3,q)$ such that:

(1) Every plane of $\mathrm{PG}(3,q)$ contains zero or at least two lines of $\mathcal{S}_L$.

(2) Every point of $\mathrm{PG}(3,q)$ lies on zero or on at least two lines of $\mathcal{S}_L$.

(3) The sum of the symbols of the lines of $\mathcal{S}_L$ going through a fixed point of $\mathrm{PG}(3,q)$ equals 0.

(4) The sum of the symbols of the lines of $\mathcal{S}_L$ lying in a fixed plane of $\mathrm{PG}(3,q)$ equals 0.

We first list two examples of codewords of small weight in $\mathrm{C}_2(\mathcal{Q}^+(5,q))^\perp$. In Theorem 7.4.11, we will prove that the codewords of $\mathrm{C}_2(\mathcal{Q}^+(5,q))^\perp$ of weight at most $4q+4$ arise from the examples given here.

An example of weight $2q+2$

Let $\mathcal{S}_L$ be the set of $2q+2$ lines of a hyperbolic quadric $\mathcal{Q}^+(3,q)$ in $\mathrm{PG}(3,q)$, $q = p^h$, p prime, $h \geq 1$, where the $q+1$ lines of one regulus get symbol $\alpha \in \mathbb{F}_p$, and

the $q+1$ lines of the opposite regulus get symbol $-\alpha$. It is easy to check that this set $\mathcal{S}_L$ satisfies the conditions (1)-(4). Under the Klein correspondence, the set $\mathcal{S}_L$ corresponds to a set $\mathcal{S}$ of points of $\mathcal{Q}^+(5,q)$, consisting of two conics, lying in two skew polar planes of $\mathcal{Q}^+(5,q)$.

An example of weight $4q$

Let $\mathcal{S}_L$ be the set of $4q$ lines through two fixed points P and R of $\mathrm{PG}(3,q)$, $q=p^h$, p prime, $h\geq 1$, lying in two fixed planes π_1 and π_2 through PR, different from the line PR, where all lines of $\mathcal{S}_L$ through P in π_1 and all lines of $\mathcal{S}_L$ through R in π_2 get symbol α, and all other lines of $\mathcal{S}_L$ get symbol $-\alpha$. Under the Klein correspondence, the set $\mathcal{S}_L$ corresponds to a set $\mathcal{S}$ of $4q$ points in $\mathcal{Q}^+(5,q)$, lying on four lines through a fixed point Q, where these four lines define a quadrangle on the base $\mathcal{Q}^+(3,q)$ of the cone $T_Q(\mathcal{Q}^+(5,q))\cap\mathcal{Q}^+(5,q)$, where $T_Q(\mathcal{Q}^+(5,q))$ denotes the tangent hyperplane through Q.

Remark. A linear combination of two codewords of weight $2q+2$ as given in the example can have the following weight: $4q-4$, $4q-2$, $4q$, $4q+2$ or $4q+4$. These numbers arise from the possible intersections of two hyperbolic quadrics $\mathcal{Q}^+(3,q)_1$ and $\mathcal{Q}^+(3,q)_2$ (see [31]):

(i) $\mathcal{Q}^+(3,q)_1\cap\mathcal{Q}^+(3,q)_2$ equals four lines, two contained in a regulus $\mathcal{R}_1$ of $\mathcal{Q}^+(3,q)_1$ and a regulus $\mathcal{R}_2$ of $\mathcal{Q}^+(3,q)_2$, and two contained in the opposite reguli $\mathcal{R}_1^{opp}$ and $\mathcal{R}_2^{opp}$. Let c_1 be the codeword of $\mathrm{C}(\mathcal{Q}^+(5,q))^\perp$, where the lines of $\mathcal{R}_1$ get symbol α and the lines of $\mathcal{R}_1^{opp}$ get symbol $-\alpha$, and let c_2 be the codeword of $\mathrm{C}(\mathcal{Q}^+(5,q))^\perp$ where the lines of $\mathcal{R}_2$ get symbol $-\alpha$ and the lines of $\mathcal{R}_2^{opp}$ get symbol α. Then c_1+c_2 is a codeword of $\mathrm{C}(\mathcal{Q}^+(5,q))^\perp$ with weight $4q-4$.

(ii) $\mathcal{Q}^+(3,q)_1\cap\mathcal{Q}^+(3,q)_2$ equals three lines, two contained in a regulus $\mathcal{R}_1$ of $\mathcal{Q}^+(3,q)_1$ and a regulus $\mathcal{R}_2$ of $\mathcal{Q}^+(3,q)_2$, and one (with multiplicity 2) contained in the opposite reguli $\mathcal{R}_1^{opp}$ and $\mathcal{R}_2^{opp}$. Using the same ideas as in the preceding case, we can obtain a codeword of weight $4q-2$.

(iii) $\mathcal{Q}^+(3,q)_1\cap\mathcal{Q}^+(3,q)_2$ equals two lines contained in a regulus $\mathcal{R}_1$ of $\mathcal{Q}^+(3,q)_1$ and a regulus $\mathcal{R}_2$ of $\mathcal{Q}^+(3,q)_2$. Using the same ideas, we can obtain a codeword of weight $4q$.

(iv) $\mathcal{Q}^+(3,q)_1\cap\mathcal{Q}^+(3,q)_2$ equals 1 line (with multiplicity 2) contained in a regulus $\mathcal{R}_1$ of $\mathcal{Q}^+(3,q)_1$ and a regulus $\mathcal{R}_2$ of $\mathcal{Q}^+(3,q)_2$. Now we obtain a codeword of weight $4q+2$.

(v) $\mathcal{Q}^+(3,q)_1 \cap \mathcal{Q}^+(3,q)_2$ contains no line. Now we obtain a codeword of weight $4q+4$.

In a similar way as for the small weight codewords of $\mathrm{C}(T_2^*(\Theta)^D)^\perp$, we can characterise the codewords of small weight in $\mathrm{C}(\mathcal{Q}^+(5,q))^\perp$. The proofs use the same counting techniques but get very technical and unfortunately, a rather large lower bound on q, namely $q > 124$, appears. The proof for the following theorem can be found in [117].

Theorem 7.4.11. *Let c be a codeword of weight at most $4q+4$ of $\mathrm{C}_2(\mathcal{Q}^+(5,q))^\perp$, $q > 124$, then $\mathcal{S} = supp(c)$ corresponds via the Klein correspondence to one of the following configurations of lines in $\mathrm{PG}(3,q)$:*

1. *a hyperbolic quadric $\mathcal{Q}^+(3,q)$ in $\mathrm{PG}(3,q)$, with all lines in one regulus symbol α, and all lines in the opposite regulus symbol $-\alpha$,*
2. *a linear combination of two codewords of type 1,*
3. *$4q$ lines through two fixed points R and S in two planes π_1 and π_2 through RS, the line RS not included, where the lines through R in π_1 and the lines through S in π_2 have symbol β, and the other lines have symbol $-\beta$.*

Remark. Note that there are two different kinds of codewords of weight $4q$: the codewords arising from a linear combination of two codewords of weight $2q+2$ and the codewords of the third type in Theorem 7.4.11, arising from $4q$ lines in two fixed planes.

7.5 Large weight codewords in $\mathrm{C}_k(\mathcal{P})^\perp$, q even

7.5.1 Large weight codewords in the dual code of $\mathcal{Q}(4,q)$, q even

The maximum weight of $\mathrm{C}(\mathcal{Q}(4,q))^\perp$

Theorem 7.5.1. *If c is a codeword of $\mathrm{C}(\mathcal{Q}(4,q))^\perp$, $q = 2^h$, then $wt(c) \leq q^3+q$, and if $wt(c) = q^3+q$, then $supp(c)$ is the complement of an ovoid.*

Proof. Let c be a codeword of $\mathrm{C}(\mathcal{Q}(4,q))^\perp$. By condition (C3), the complement of $\mathcal{S}$ defines a blocking set $\mathcal{B}$ of $\mathcal{Q}(4,q)$. The smallest size for a blocking set

of $\mathcal{Q}(4,q)$ is that of an ovoid, which is q^2+1. Moreover, again by condition (C3), the complement of an ovoid defines a codeword, and it has weight $(q+1)(q^2+1)-(q^2+1)=q^3+q$. □

An empty interval in the weight distribution of $\mathrm{C}(\mathcal{Q}(4,q))^\perp$, q even

We begin by extending the definition of t-fold 1-blocking sets in $\mathrm{PG}(n,q)$ to *weighted t-fold 1-blocking sets* in $\mathrm{PG}(n,q)$. A t-fold 1-blocking set in $\mathrm{PG}(n,q)$ with *weight* W [7] is a pair (B,w) where B is a set of points in $\mathrm{PG}(n,q)$ and where w is a weight function $w:\mathrm{PG}(n,q)\to\mathbb{N}:x\mapsto w(x)$ satisfying

1. $w(x)>0\iff x\in B$,
2. $\sum_{x\in B}w(x)=W$,
3. $\min\{\sum_{x\in H}w(x)|H$ is a hyperplane of $\mathrm{PG}(N,q)\}=t$.

It is clear that if the weight function w has values in $\{0,1\}$, a t-fold 1-blocking set B with weight W is a t-fold 1-blocking set, with $|B|=W$ and such that B is not a $(t+1)$-fold 1-blocking set. A t-fold blocking set is clearly an s-fold blocking set for all $s<t$. But from now on, when considering a t-fold blocking set, we assume that it is not a $(t+1)$-fold blocking set. In this way, the definition of a weighted t-fold blocking set with weight function w with values in $\{0,1\}$ coincides with the definition of a t-fold blocking set.

Lemma 7.5.2 extends [43, Lemma 3.2], that is only valid for non-weighted t-fold 1-blocking sets, to weighted t-fold 1-blocking sets, where the union of lines is replaced by a sum of lines. Consider t lines $L_1,\ldots,L_t$, where a given line may occur more than once. The *sum* $L_1+\cdots+L_t$ is the weighted set F of points with weight function w, satisfying $w(P)=j$ if P belongs to j lines in $L_1,\ldots,L_t$. For example, if $L_1=\ldots=L_t$, then all points of L_1 have weight t, and all other points have weight 0.

Lemma 7.5.2. [117, Lemma 11] *Let (B,w) be a t-fold 1-blocking set in $\mathrm{PG}(4,q)$ with weight $t(q+1), t<q/2$, contained in $\mathcal{Q}(4,q)$, then (B,w) is a sum of t lines.*

[7] Weighted t-fold 1-blocking sets in $\mathrm{PG}(n,q)$ with weight W are usually called *weighted* $\{W,t;n,q\}$-minihypers with weight function w, a definition that was introduced by Hamada in [68].

We have to introduce some more terminology. Let $\mathcal{C}$ be a cover of $\mathcal{Q}(4,q)$. The *multiplicity* $\mu(P)$ of a point P is the number of lines of $\mathcal{C}$ through it. The *excess* of a point P, denoted by $e(P)$, is equal to $\mu(P)-1$. A *multiple* point P of $\mathcal{C}$ is a point with $e(P)>0$. The excess of a line L is the sum of the excesses of the points on L. A line L of $\mathcal{Q}(4,q)$ is called a *good line* for $\mathcal{C}$ when $L \notin \mathcal{C}$ and L does not have multiple points of $\mathcal{C}$. We have the following results for covers of $\mathcal{Q}(4,q)$.

Lemma 7.5.3. [52, Lemma 2] *A cover $\mathcal{C}$ of $\mathcal{Q}(4,q)$ of size q^2+1+r, $0 \leq r \leq q$, always has a good line.*

Lemma 7.5.4. [52, Theorem 7, Part 1] *Let $\mathcal{C}$ be a cover of $\mathcal{Q}(4,q)$ of size q^2+1+r and let E be the set of multiple points of $\mathcal{C}$. Then (E,w), with $w(P)=e(P)$, is an r-fold 1-blocking set with weight $r(q+1)$.*

Theorem 7.5.5. *If $\mathcal{C}$ is a cover of $\mathcal{Q}(4,q)$, q even, of size q^2+1+r, where $0 \leq r < \frac{q+4}{6}$, then $\mathcal{C}$ contains a spread of $\mathcal{Q}(4,q)$.*

Proof. If $r=0$, the statement is trivial, hence, suppose that $r>0$. Lemma 7.5.3 shows that there exists a good line L for the cover $\mathcal{C}$. Let $M_1, M_2, \ldots, M_{q+1}$ be the lines of $\mathcal{C}$ intersecting L. Let $L^\perp$ be the plane defined by L and by the nucleus of $\mathcal{Q}(4,q)$, then the planes $L^\perp, \langle L, M_1\rangle, \langle L, M_2\rangle, \ldots, \langle L, M_{q+1}\rangle$ define a set S of $q+2$ points in the quotient geometry $\pi = \mathrm{PG}(4,q)/L \cong \mathrm{PG}(2,q)$ of L, such that every line of π intersects S in zero, one or two points, except for at most r lines which can contain, in total, at most $3r$ points of S (see Theorem 3 of [52]). Hence, at least $q+2-3r$ elements of S are internal nuclei, these are points P of S such that all lines through P meet S in at most two points. Since $q+2-3r > \frac{q}{2}$, every point of S is an internal nucleus (see [14]), which means that S is an oval, hence, it has only 0- and 2-secants. This implies that every hyperbolic quadric containing L contains zero or two lines of $\mathcal{C}$ intersecting L. By Lemmas 7.5.2 and 7.5.4, the multiple points of $\mathcal{C}$ form a sum $\mathcal{L}$ of lines.

Since $r>0$, there exist two intersecting lines M_1 and M_2 of $\mathcal{C}$. There are q hyperbolic quadrics through M_1 and M_2. Assume that one of them contains a good line M intersecting M_2, then it has another line of $\mathcal{C}$, say M_2', intersecting M. Hence, the line M_1 has at least two multiple points.

Suppose that the cover $\mathcal{C}$ is minimal. Then the lines M_1 and M_2 are not contained in $\mathcal{L}$, hence, the total excess of M_1, and M_2, is at most r. So at most $2(r-1)$ hyperbolic quadrics through M_1 and M_2 contain a good line. Let

$\mathcal{Q}^+(3,q)$ be one of the hyperbolic quadrics through M_1 and M_2, not containing a good line, and let $\mathcal{R}$ be a regulus of $\mathcal{Q}^+(3,q)$. A line of $\mathcal{R}$ cannot be a good line, hence, it is either a line of $\mathcal{C}$ or it has at least one multiple point. In any case, we have at least $q+1$ multiple points in $\mathcal{Q}^+(3,q)$. Since $q+1>r$, at least one line of the sum $\mathcal{L}$ is contained in $\mathcal{Q}^+(3,q)$, and we know that it is not M_1 nor M_2. So we find that $q-2r+2 \leq |\mathcal{L}| \leq r$, a contradiction. We conclude that $\mathcal{C}$ is not minimal.

Since for every $0 \leq r < \frac{q+4}{6}$, a cover $\mathcal{C}$ of $\mathcal{Q}(4,q)$, q even, of size q^2+1+r is not minimal, the minimal cover contained in $\mathcal{C}$ has size q^2+1, and hence, is a spread. □

Corollary 7.5.6. *Let B be a blocking set of $\mathcal{Q}(4,q)$, q even, of size q^2+1+r, where $0 \leq r < \frac{q+4}{6}$. Then B contains an ovoid of $\mathcal{Q}(4,q)$.*

Proof. This follows from Theorems 7.5.5 and 1.4.1 (2). □

Remark. Theorem 8 of Eisfeld, Storme, Sziklai and Szőnyi [52] shows that a cover of $\mathcal{Q}(4,q)$, q even, $q \geq 32$, of size q^2+1+r, $0 \leq r \leq \sqrt{q}$, contains a spread of $\mathcal{Q}(4,q)$. Theorem 7.5.5 improves on this theorem for all values of q, q even. Likewise, Corollary 7.5.6 improves on [52, Theorem 9].

Theorem 7.5.7. *There are no codewords with weight in $]q^3+\frac{5q-4}{6}, q^3+q[$ in $\mathrm{C}(\mathcal{Q}(4,q))^\perp$, q even.*

Proof. Let c be a codeword of $\mathrm{C}(\mathcal{Q}(4,q))^\perp$ with weight in $]q^3+\frac{5q-4}{6}, q^3+q[$. This implies that $\mathcal{B}$ is a blocking set of $\mathcal{Q}(4,q)$ of size less than $q^2+1+\frac{q+4}{6}$. Corollary 7.5.6 shows that $\mathcal{B}$ contains an ovoid $\mathcal{O}$ of $\mathcal{Q}(4,q)$. Let c' be the codeword of weight q^3+q of $\mathrm{C}(\mathcal{Q}(4,q))^\perp$ defined by the complement of $\mathcal{O}$. Since $\mathrm{C}(\mathcal{Q}(4,q))^\perp$ is a linear code, $c''=c+c'$ is a codeword of $\mathrm{C}(\mathcal{Q}(4,q))^\perp$. Moreover, it has weight at least 1 and less than $\frac{q+4}{6}$. This is a contradiction since the minimum weight of $\mathrm{C}(\mathcal{Q}(4,q))^\perp$ is $2(q+1)$ (see Table 7.2). □

We can translate the results about $\mathrm{C}(\mathcal{Q}(4,q))^\perp$, q even, to $\mathrm{C}(\mathcal{W}(q))^\perp$, q even, by using Theorem 1.4.1 (2).

Theorem 7.5.8. *The codewords of maximum weight of $\mathrm{C}(\mathcal{W}(q))^\perp$, q even, have weight q^3+q, and correspond to the complement of an ovoid. Moreover, there are no codewords of weight in $]q^3+\frac{5q-4}{6}, q^3+q[$.*

Remark. The lower bound in the previous theorem is not sharp; but there is an easy construction of a codeword of weight q^3+2 in $\mathrm{C}(\mathcal{W}(q))^\perp$. Let q be even and let c be the vector of weight q^3 defined by the set $\mathrm{AG}(3,q) = \mathrm{PG}(3,q)\setminus\pi$; every line of $\mathrm{PG}(3,q)$ contains zero or q points of $\mathrm{AG}(3,q)$, hence c is a codeword of $\mathrm{C}(\mathcal{W}(q))^\perp$, q even. Let c' be a codeword of weight $2(q+1)$ defined by L and $L^\perp$, where L is a not totally isotropic line (these are exactly the codewords of minimum weight, as proven in Theorem 7.2.1), such that $L\subseteq\pi$. The codeword $c+c'$ of $\mathrm{C}(\mathcal{W}(q))^\perp$, q even, has weight q^3+2.

7.5.2 Large weight codewords in the dual code of $\mathcal{Q}^+(5,q)$, q even

By condition (C3) a codeword c in the binary code $\mathrm{C}_2(\mathcal{Q}^+(5,q))^\perp$, q even, defines a set $\mathcal{S}$ of points of $\mathcal{Q}^+(5,q)$ such that every plane of $\mathcal{Q}^+(5,q)$ contains an even number of points of $\mathcal{S}$ and $\mathcal{B}=\mathcal{Q}^+(5,q)\setminus\mathcal{S}$ is a blocking set of $\mathcal{Q}^+(5,q)$. Recall that if every plane contains exactly one point of $\mathcal{B}$, $\mathcal{B}$ is an ovoid of $\mathcal{Q}^+(5,q)$. These ovoids have size q^2+1 and exist since they correspond via the Klein correspondence to a spread of $\mathrm{PG}(3,q)$. For example, the Desarguesian line spread (see Chapter 1) in $\mathrm{PG}(3,q)$ corresponds to the elliptic quadric $\mathcal{Q}^-(3,q)$, which is an ovoid of $\mathcal{Q}^+(5,q)$. This implies that the codewords of maximal weight in $\mathrm{C}_2(\mathcal{Q}^+(5,q))^\perp$, q even, correspond to the complement of an ovoid, hence have size $|\mathcal{Q}^+(5,q)|-(q^2+1)=(1+q^2)(q^2+q)$.

If $wt(c)=(1+q^2)(q^2+q)-r$, then $\mathcal{B}$ is a blocking set of size q^2+1+r meeting every plane of $\mathcal{Q}^+(5,q)$ in an odd number of points since q is even. Using the Klein correspondence, this set of points of $\mathcal{Q}^+(5,q)$ corresponds to a set $\mathcal{S}_L$ of lines in $\mathrm{PG}(3,q)$ such that:

(1) every plane of $\mathrm{PG}(3,q)$ contains an odd number of lines of $\mathcal{S}_L$.

(2) every point of $\mathrm{PG}(3,q)$ lies on an odd number of lines of $\mathcal{S}_L$.

As seen in Chapter 5, a *cover* $\mathcal{C}$ of $\mathrm{PG}(3,q)$ is a set $\mathcal{L}$ of lines such that every point of $\mathrm{PG}(3,q)$ lies on at least one line of $\mathcal{L}$.

Lemma 7.5.9. *A codeword of* $\mathrm{C}_2(\mathcal{Q}^+(5,q))^\perp$, *$q$ even, has even weight.*

Proof. Let c be a codeword of $\mathrm{C}_2(\mathcal{Q}^+(5,q))^\perp$, q even, with $wt(c)=(1+q^2)(q^2+q)-r$, then $|\mathcal{S}_L|=q^2+1+r$, and $\mathcal{S}_L$ defines a cover of size q^2+1+r. It is clear that $(q^2+1+r)(q-1)-\theta_3=r(q+1)$ is the sum of the excesses of the

multiple points. Since every point of $\mathrm{PG}(3,q)$ lies on an odd number of lines of $\mathcal{S}_L$, every point has even excess, so in total, the sum of all the excesses is even. Since q is even, this implies that r is even, hence that $wt(c)$ is even. □

Theorem 7.5.10. *There are codewords in* $\mathrm{C}_2(\mathcal{Q}^+(5,q))^\perp$, *$q$ even, of weight* $(1+q^2)(q^2+q)-2i$, *where* $i=0,1,\ldots,q/2$.

Proof. We give an explicit construction of these codewords. Let T be the Desarguesian line spread of $\mathrm{PG}(3,q)$, let L be a line of T and let $\mathcal{R}_1,\ldots,\mathcal{R}_q$ be q reguli of T through L which pairwise only share L. Replace $2i$ of the reguli $\mathcal{R}_1,\ldots,\mathcal{R}_q$ by their opposite reguli. Put the line L back. Let $\mathcal{S}_L$ be the set of $(q-2i)q+1+2i(q+1)=q^2+1+2i$ lines obtained in this way.

Let π be a plane in $\mathrm{PG}(3,q)$ through L. The plane π cannot contain another element of T. Let $\mathcal{R}$ be one of the reguli through L which is replaced by its opposite regulus. There is exactly one transversal line to $\mathcal{R}$ contained in π. Hence, a plane through L contains exactly $2i+1$ lines of $\mathcal{S}_L$.

Let π' be a plane in $\mathrm{PG}(3,q)$, not through L. It contains exactly one line L' of T, and there is exactly one regulus of $\mathcal{R}_1,\ldots,\mathcal{R}_q$ containing the line L'. If this regulus is replaced by its opposite regulus, there is a transversal line t through L and L' contained in π'. Moreover, if another regulus $\mathcal{R}'$ has a transversal line t' contained in π', t and t' intersect, and $\mathcal{R}=\mathcal{R}'$, a contradiction. We conclude that Condition (1) holds since every plane through L contains exactly $2i+1$ lines of $\mathcal{S}_L$, and a plane, not through L, contains exactly one line of $\mathcal{S}_L$.

Condition (2) holds since a point not on L lies on exactly one line of $\mathcal{S}_L$, while a point of L lies on $2i+1$ lines of $\mathcal{S}_L$.

This implies that via the Klein correspondence the complement of $\mathcal{S}_L$ is a codeword of $\mathrm{C}_2(\mathcal{Q}^+(5,q))^\perp$ of weight $(1+q^2)(q^2+q)-2i$. □

Remark. It is interesting to notice the difference between the possible large weight codewords in $\mathrm{C}(\mathcal{Q}(4,q))^\perp$, q even, and $\mathrm{C}_2(\mathcal{Q}^+(5,q))^\perp$, q even. For the code $\mathrm{C}(\mathcal{Q}(4,q))^\perp$, q even, Theorem 7.5.7 shows that there is an empty interval in the weight enumerator, whereas Theorem 7.5.10 constructs codewords in $\mathrm{C}_2(\mathcal{Q}^+(5,q))^\perp$, q even, for every even value in $[(1+q^2)(q^2+q)-q,(1+q^2)(q^2+q)]$.

7.5.3 Large weight codewords in polar spaces of higher rank

The dual code of $\mathcal{Q}^+(2n+1,q)$, q even

Large weight codewords of $\mathrm{C}_k(\mathcal{Q}^+(2n+1,q))^\perp$, q even, correspond to small blocking sets with respect to the k-subspaces of $\mathcal{Q}^+(2n+1,q)$, hence we start by considering minimal blocking sets of $\mathcal{Q}^+(2n+1,q)$ with respect to k–subspaces.

The case $k=1$.

The problem of determining the smallest blocking sets with respect to the lines of $Q^+(2n+1,q)$ is completely solved in the following result by Metsch.

Theorem 7.5.11. [105] *Let B be a minimal blocking set of $\mathcal{Q}^+(2n+1,q)$, $n \geq 3$, with respect to lines. If $|B| \leq 1+q|\mathcal{Q}^+(2n-1,q)|$, then $B = (H \setminus H^\perp) \cap \mathcal{Q}^+(2n+1,q)$ for some hyperplane H of* $\mathrm{PG}(2n+1,q)$.

This theorem has the following corollary for the maximum weight of the codewords of $\mathrm{C}_1(\mathcal{Q}^+(2n+1,q))^\perp$, q even, $n \geq 3$.

Theorem 7.5.12. *The maximum weight of* $\mathrm{C}_1(\mathcal{Q}^+(2n+1,q))^\perp$, *$q$ even, $n \geq 3$, is $(q^n+1)q^n$, the second largest weight is q^{2n}, and the codewords of weight $(q^n+1)q^n$ and q^{2n} are defined by the complement of a hyperplane with respect to $\mathcal{Q}^+(2n+1,q)$.*

Proof. Let c be a codeword of $\mathrm{C}_1(\mathcal{Q}^+(2n+1,q))^\perp$ with $wt(c) \geq q^{2n}$. Then $\mathcal{B}$ is a blocking set with respect to the lines of $\mathcal{Q}^+(2n+1,q)$ of size at most $\theta_{2n-1}+q^n$. Result 7.5.11 shows that $\mathcal{B}$ contains either a parabolic quadric $\mathcal{Q}(2n,q)$ or a cone over a hyperbolic quadric $\mathcal{Q}^+(2n-1,q)$ minus its vertex.

Suppose first that the blocking set $\mathcal{B}$ contains a parabolic quadric $\mathcal{Q} = \mathcal{Q}(2n,q)$. A line L of $\mathcal{Q}^+(2n+1,q)$ is either contained in $\mathcal{Q}$ or it intersects $\mathcal{Q}$ in one point. Hence, by condition (C2), the complement of $\mathcal{Q}$ defines a codeword c' of $\mathrm{C}_1(\mathcal{Q}^+(2n+1,q))^\perp$. But then $wt(c+c') = wt(c)+wt(c')-2wt(c\cap c') \leq q^n$, which is smaller than the minimum weight of $\mathrm{C}_1(\mathcal{Q}^+(2n+1,q))^\perp$ (see Proposition 7.3.6). Hence, in this case, $c=c'$, $wt(c) = q^{2n}+q^n$, and $\mathcal{S}$ is the complement of a parabolic quadric $\mathcal{Q}(2n,q)$.

Suppose that $\mathcal{B}$ contains a set $P^\perp \setminus \{P\}$, with $P \in \mathcal{Q}^+(2n+1,q)$, then the complement of c has size $\theta_{2n-1}+q^n-1$ or $\theta_{2n-1}+q^n$. The set $P^\perp$ is such that a line is either contained in $P^\perp$ or contains one point of $P^\perp$. Hence, by condition (C2), the complement of $P^\perp$ defines a codeword c' of $\mathrm{C}_1(\mathcal{Q}^+(2n+1,q))^\perp$. But

then $wt(c+c') \leq 1$, which implies that $c = c'$, $wt(c) = q^{2n}$, and c corresponds to the complement of a set $P^\perp$ with $P \in \mathcal{Q}^+(2n+1,q)$. □

Corollary 7.5.13. *The largest sets of even type (w.r.t. lines) in $\mathcal{Q}^+(2n+1,q)$, q even, $n \geq 3$, have size $q^{2n}+q^n$, and they correspond to the complement of a parabolic quadric $\mathcal{Q}(2n,q)$ of $\mathcal{Q}^+(2n+1,q)$, there are no sets of even type in $\mathcal{Q}^+(2n+1,q)$, q even, $n \geq 3$, with weight in $[q^{2n}+1, q^{2n}+q^n[$, and a set of even type in $\mathcal{Q}^+(2n+1,q)$, q even, $n \geq 3$, of size q^{2n} corresponds to the complement of a cone over a hyperbolic quadric $\mathcal{Q}^+(2n-1,q)$.*

The case $2 \leq k \leq n-1$.

Also in this case, Metsch has characterised the smallest blocking sets. Let $S_k\mathcal{Q}$ be a cone with a k-dimensional vertex S_k over a non–singular quadric $\mathcal{Q}$. A *truncated* cone $S_k\mathcal{Q}$ is the set $S_k\mathcal{Q} \setminus S_k$.

Theorem 7.5.14. [104] *Let B be a blocking set of the quadric $\mathcal{Q}^+(2n+1,q)$ with respect to k–subspaces, $2 \leq k \leq n-1$. Then $|B| \geq \frac{q^{n-k+1}-1}{q-1}(q^n+q^{k-2})$. If $|B| < \frac{q^{n-k+1}-1}{q-1}(q^n+q^{k-2}+1)$, then B contains the truncated cone $S_{k-3}\mathcal{Q}^-(2n+3-2k,q)$.*

Hence we can prove the following theorem.

Theorem 7.5.15. *The maximum weight of $\mathrm{C}_k(\mathcal{Q}^+(2n+1,q))^\perp$, q even, with $2 \leq k < (n+3)/2$, is $q^n(q^n+q^{n-1}+\cdots+q^{n-k+1})+q^n+q^{n-1}$ and a codeword of maximum weight corresponds to the complement of a cone $S_{k-3}\mathcal{Q}^-(2n+3-2k,q)$ in $\mathcal{Q}^+(2n+1,q)$.*

Proof. Denote the size of the complement of a cone $S_{k-3}\mathcal{Q}^-(2n+3-2k,q)$ by s. Let c be a codeword of $\mathrm{C}_k(\mathcal{Q}^+(2n+1,q))^\perp$ with $wt(c) \geq s$. The complement of c corresponds to a blocking set of size at most $|S_{k-3}\mathcal{Q}^-(2n+3-2k,q)|$. Hence, by Result 7.5.14, and since $k < (n+3)/2$, the complement of c consists of the points of a truncated cone $\mathcal{C} = S_{k-3}\mathcal{Q}^-(2n+3-2k,q)$ and some set of other points, which we will denote by T. Since $wt(c) \geq s$, $|T| \leq |S_{k-3}| = \theta_{k-3}$. Let c' be the codeword corresponding to the complement of the cone $\mathcal{C}'$, obtained by adding the vertex S_{k-3} to the truncated cone $\mathcal{C}$. Since $\mathrm{C}_k(\mathcal{Q}^+(2n+1,q))^\perp$ is a linear code, the vector $c+c'$ is in $\mathrm{C}_k(\mathcal{Q}^+(2n+1,q))^\perp$. Moreover, it has weight

$$wt(c+c') = wt(c)+wt(c')-2wt(c\cap c') \leq 2|S_{k-3}|.$$

But $2|S_{k-3}|$ is smaller than $1+\frac{q^n-1}{q^k-1}(q^{n-1}+1)$ which is the lower bound on the minimum weight by Proposition 7.3.6. This implies that $c = c'$. Hence, the maximum weight of $\mathrm{C}_k(\mathcal{Q}^+(2n+1,q))^\perp$ is $q^n(q^n+q^{n-1}+\cdots+q^{n-k+1})+q^n+q^{n-1}$ and corresponds to the complement of a cone $S_{k-3}\mathcal{Q}^-(2n+3-2k,q)$ in $\mathcal{Q}^+(2n+1,q)$. □

Remark. Note that, since $k < (n+3)/2$, the previous theorems do not cover the case $k = n$. In that case, we are looking for ovoids of $\mathcal{Q}^+(2n+1,q)$ of which the existence is dependent on the size of n and the order of q; the problem of the existence of ovoids in a hyperbolic quadric is not yet solved in general (see Chapter 1).

The dual code of $\mathcal{Q}(2n,q)$, q even, and $\mathcal{Q}^-(2n+1,q)$, q even

If we consider $\mathcal{Q}(2n,q)$ to be embedded in $\mathcal{Q}^+(2n+1,q)$, then every blocking set of $\mathcal{Q}(2n,q)$ with respect to subspaces of dimension k of $\mathcal{Q}(2n,q)$ is a blocking set of $\mathcal{Q}^+(2n+1,q)$ with respect to subspaces of dimension $k+1$ of $\mathcal{Q}^+(2n+1,q)$. So, for $1 \le k \le n-2$, a blocking set B of smallest size consists of the non–singular points of a quadric of type $S_{k-2}\mathcal{Q}^-(2n+1-2k,q)$ (Result 7.5.14; for more details, see [104]). If we consider $\mathcal{Q}^-(2n+1,q)$ embedded in $\mathcal{Q}^+(2n+3,q)$, then every blocking set of $\mathcal{Q}^-(2n+1,q)$ with respect to subspaces of dimension k of $\mathcal{Q}^-(2n+1,q)$ is a blocking set of $\mathcal{Q}^+(2n+3,q)$ with respect to subspaces of dimension $k+2$ of $\mathcal{Q}^+(2n+3,q)$. So, for $1 \le k \le n-2$, a blocking set B of smallest size consists of the non–singular points of a quadric of type $S_{k-1}\mathcal{Q}^-(2n+1-2k,q)$ [104]. From these considerations and by similar arguments of the previous section, we get the following results.

Theorem 7.5.16. *The maximum weight for $\mathrm{C}_k(\mathcal{Q}(2n,q))^\perp$, q even, $1 \le k < (n+1)/2$, is $q^n(q^{n-1}+q^{n-2}+\cdots+q^{n-k})+q^{n-1}$ and a codeword of maximum weight corresponds to the complement of a cone $S_{k-2}\mathcal{Q}^-(2n+1-2k,q)$ in $\mathcal{Q}(2n,q)$.*

Corollary 7.5.17. *The largest sets of even type (w.r.t. lines) in $\mathcal{Q}(2n,q)$, q even, have size $q^{2n-1}+q^{n-1}$, and correspond to the complement of an elliptic quadric $\mathcal{Q}^-(2n-1,q)$.*

Theorem 7.5.18. *The maximum weight for $\mathrm{C}_k(\mathcal{Q}^-(2n+1,q))^\perp$, q even, $1 \le k < (n+1)/2$, is $q^{2n-k+1}\theta_{k-1}$ and a codeword of maximum weight corresponds to the complement of a cone $S_{k-1}\mathcal{Q}^-(2n+1-2k,q)$ in $\mathcal{Q}^-(2n+1,q)$.*

Corollary 7.5.19. *The largest sets of even type (w.r.t lines) in $\mathcal{Q}^-(2n+1,q)$, q even, have size q^{2n} and correspond to the complement of a cone over an elliptic quadric $\mathcal{Q}^-(2n-1,q)$.*

A similar reasoning for the dual code of a Hermitian variety shows the following. For more details, we refer to [118].

Theorem 7.5.20. *If n is even, the maximum weight of $\mathrm{C}_k(\mathcal{H}(n,q^2))^\perp$, q even, $1 \leq k \leq (n-3)/2$, is $q^{2n-2k+1}\frac{q^{2k}-1}{q^2-1}$ and a codeword of maximum weight corresponds to the complement of a cone $S_{k-1}\mathcal{H}(n-2k,q^2)$. If n is odd, then the maximum weight of $\mathrm{C}_k(\mathcal{H}(n,q^2))^\perp$ is $q^{2n-2k+1}\frac{q^{2k}-1}{q^2-1}+q^{n-1}$ and a codeword of maximum weight corresponds to the complement of a cone $S_{k-2}\mathcal{H}(n-2k+1,q^2)$.*

Proof. See [118, Theorem 60]. □

Corollary 7.5.21. *The largest sets of even type (w.r.t. lines) of $\mathcal{H}(n,q^2)$, q even, have size q^{2n-1} and correspond to the complement of a cone over a Hermitian variety $\mathcal{H}(n-2,q^2)$ if n is even, and to the complement of a Hermitian variety $\mathcal{H}(n-1,q^2)$ if n is odd.*

A

Nederlandstalige samenvatting

A.1 Inleiding

Bij ons onderzoek tijdens de voorbije drie jaar kwamen we tot een aantal nieuwe inzichten. De door ons behaalde resultaten proberen we in deze appendix op een rijtje te zetten. We beperken ons tot het definiëren van de kernbegrippen die nodig zijn om deze samenvatting te begrijpen. Voor meer details verwijzen we naar de engelse tekst.

De titel van deze thesis maakt duidelijk dat het belangrijkste onderwerp van deze thesis *blokkerende verzamelingen* in $\mathrm{PG}(n,q)$ zijn. Het symbool $\mathrm{PG}(n,q)$ staat voor de projectieve ruimte over het eindig veld $\mathbb{F}_q$ met q elementen, waarbij q een macht van een priemgetal p is.

Een *k-blokkerende verzameling* in $\mathrm{PG}(n,q)$ is een verzameling punten die elke $(n-k)$-dimensionale ruimte snijdt (blokkeert). Een speciale klasse van de blokkerende verzamelingen in $\mathrm{PG}(n,q^t)$ zijn de *$\mathbb{F}_q$-lineaire blokkerende verzamelingen*. Een verzameling $\mathcal{S}$ van punten in $\mathrm{PG}(n,q^t)$ wordt *$\mathbb{F}_q$-lineair* genoemd als er een deelvectorruimte U bestaat van de onderliggende vectorruimte van $\mathrm{PG}(n,q^t)$ over een deelveld $\mathbb{F}_q$ van $\mathbb{F}_{q^t}$, zodat de projectieve punten die met de vectoren van deze vectorruimte U corresponderen precies de punten

van de verzameling $\mathcal{S}$ zijn. Als de ruimte U rang k heeft, zeggen we dat $\mathcal{S}$ een $\mathbb{F}_q$-lineaire verzameling is *van rang* k.

Verder noemt men een k-blokkerende verzameling B *minimaal* als geen enkele echte deelverzameling van B een k-blokkerende verzameling is. Een blokkerende verzameling wordt *klein* genoemd als ze minder dan $3(q^k+1)/2$ punten bevat.

Twee verzamelingen in $\mathrm{PG}(n,q)$ worden *isomorf* genoemd als een element van de groep $\mathrm{P\Gamma L}(n+1,q)$ de ene verzameling op de andere afbeeldt en twee verzamelingen worden *projectief equivalent* genoemd als een element van de groep $\mathrm{PGL}(n+1,q)$ de ene verzameling op de andere afbeeldt.

In de laatste twee hoofdstukken staan *lineaire codes van een meetkundige structuur* centraal. De code C van een meetkundige structuur, bestaande uit *punten* en *blokken*, wordt gedefinieerd als de vectorruimte die door de *incidentiematrix* van punten en blokken over een eindig veld voortgebracht wordt. De incidentiematrix wordt gedefinieerd als de matrix waarbij de rijen gelabeld worden door de blokken en de kolommen door de punten, en waarbij de waarde op de i-de rij en j-de kolom een 1 is als het j-de punt op het i-de blok ligt en een 0 in het andere geval. De *duale code* van C, die we als $\mathrm{C}^\perp$ noteren, is de vectorruimte die bestaat uit alle vectoren die loodrecht op alle vectoren van C staan.

A.2 Hoofdstuk 2

In Hoofdstuk 2 hebben we het over verschillende grenzen op de grootte van een minimale blokkerende verzameling. Voor kleine minimale verzamelingen, treden verschillende intervallen op waarbinnen de grootte van de minimale verzameling kan liggen. Deze intervallen volgen uit het 1 mod p-resultaat van T. Szőnyi en Zs. Weiner, dat zegt dat een deelruimte die een kleine minimale blokkerende verzameling snijdt, dat in 1 mod p punten doet. Men definieert de *exponent* e van een kleine minimale blokkerende verzameling als het grootste natuurlijk getal waarvoor elke deelruimte van $\mathrm{PG}(n,q)$ die deze minimale verzameling snijdt, in 1 mod p^e punten snijdt. Gebruikmakend van het 1 mod p-resultaat van Szőnyi en Weiner wordt de volgende stelling afgeleid:

Stelling A.2.1. *Zij B een minimale k-blokkerende verzameling in* $\mathrm{PG}(n,q)$,

met $|B| \leq 2q^k$ *en exponent* e*. Als* $p > 2$ *en* $p^e > 3$*, dan is* B *klein en*

$$|B| \leq q^k + \frac{2q^k}{p^e}.$$

Verder wordt in Hoofdstuk 2 een stelling bewezen omtrent de unieke reducibiliteit van een blokkerende verzameling. Het is namelijk evident dat, door punten te verwijderen, een blokkerende verzameling kan gereduceerd worden tot een minimale blokkerende verzameling. De volgende stelling bewijst dat als de blokkerende verzameling niet al te groot is, deze reductie op een unieke manier gebeurt.

Stelling A.2.2. *In een* k*-blokkerende verzameling met minder dan* $2q^k$ *punten is een* unieke *minimale* k*-blokkerende verzameling bevat.*

A.3 Hoofdstuk 3

In dit hoofdstuk gaan we dieper in op lineaire verzamelingen die bevat zijn in een projectieve rechte. Eerst gaan we het verband na tussen lineaire verzamelingen in een projectieve ruimte en de projectie van *canonische deelmeetkunden*. Een canonische deelmeetkunde van $\mathrm{PG}(n, q)$ is een meetkunde die, ten opzichte van een zekere basis, verkregen wordt door de coördinaten te beperken tot een deelveld van $\mathbb{F}_q$. Een resultaat van G. Lunardon en O. Polverino toont aan dat elke lineaire verzameling een canonische deelmeetkunde of een projectie daarvan is. Ruwweg gesproken bewijzen we in een eerste stelling dat een lineaire verzameling, bekomen als projectie van een ruimte π vanuit een deelruimte μ, isomorf is met de lineaire verzameling die we bekomen door het beeld van π onder een collineatie te projecteren vanuit het beeld van de deelruimte μ onder dezelfde collineatie, *en omgekeerd*.

Met behulp van deze transitiviteitseigenschappen lossen we het isomorfismeprobleem op voor lineaire verzamelingen van rang 3, die bevat zijn in een projectieve rechte. Deze lineaire verzamelingen zijn vanuit een punt op een rechte geprojecteerde vlakken. Als het punt van waaruit we projecteren op een verlengde rechte van het vlak ligt, noemen we de bekomen lineaire verzameling een *club*, anders wordt de verzameling *verstrooid* (in het engels *scattered*) genoemd.

We bewijzen het volgende:

Stelling A.3.1. *(i) Alle clubs in* $\mathrm{PG}(1,q^3)$ *en alle verstrooide lineaire verzamelingen van rang* 3 *in* $\mathrm{PG}(1,q^3)$ *zijn projectief equivalent.*

(ii) Alle verstrooide lineaire verzamelingen van rang 3 *in* $\mathrm{PG}(1,q^4)$ *zijn projectief equivalent.*

(iii) Alle clubs en alle verstrooide lineaire verzamelingen van rang 3 *in* $\mathrm{PG}(1,2^5)$ *zijn isomorf, maar er bestaan projectief inequivalente clubs en projectief inequivalente verstrooide lineaire verzamelingen van rang* 3 *in* $\mathrm{PG}(1,2^5)$.

(iv) Er bestaan niet-isomorfe clubs en niet-isomorfe verstrooide lineaire verzamelingen van rang 3 *in alle andere gevallen.*

Daarna onderzoeken we de doorsnede van een lineaire verzameling van rang k met een deelrechte (dit is een lineaire verzameling van rang 2). We bewijzen de volgende stelling.

Stelling A.3.2. *Een lineaire verzameling van rang* k *snijdt een deelrechte in* $0,1,\ldots,\min\{k,q+1\}$ *of* $q+1$ *punten en elke intersectiegrootte in de verzameling* $\{0,1,\ldots,\min\{k,q+1\},q+1\}$ *treedt daadwerkelijk op.*

Vervolgens onderzoeken we de deelrechten die volledig in een lineaire verzameling liggen. Er kunnen namelijk *reguliere* deelrechten en *irreguliere* deelrechten bevat zijn in een lineaire verzameling. Wij tonen aan dat alle deelrechten, bevat in een club, regulier zijn, maar dat in verstrooide lineaire verzamelingen irreguliere deelrechten bestaan. We tonen ook aan dat elke deelrechte kan gezien worden als een irreguliere deelrechte van een zekere lineaire verzameling van rang $k>2$. Voor een verstrooide $\mathbb{F}_q$-lineaire verzameling $\mathcal{S}$ in $\mathrm{PG}(1,q^3)$ tonen we aan dat er door twee verschillende punten van $\mathcal{S}$ juist 2 deelrechten gaan die bevat zijn in $\mathcal{S}$, een reguliere en een irreguliere. Verder onderzoeken we hoe deze irreguliere deelrechten opduiken als projectie van een bepaald soort kegelsneden.

We onderzoeken de doorsnede van twee lineaire verzamelingen van rang 3 en tonen het volgende resultaat aan.

Stelling A.3.3. *Twee* $\mathbb{F}_q$*-lineaire verzamelingen van rang* 3 *in* $\mathrm{PG}(1,q^t)$*,* q *oneven, hebben hoogstens* $2q+2$ *punten gemeen. Twee* $\mathbb{F}_q$*-lineaire verzamelingen van rang* 3 *in* $\mathrm{PG}(1,q^t)$*,* q *even, hebben hoogstens* $2q+3$ *punten gemeen.*

Tenslotte behandelen we het *representatieprobleem* voor lineaire verzamelingen van rang 3.

A.4 Hoofdstuk 4

Hoofdstuk 4 draait om het *lineariteitsvermoeden*. Dit vermoeden stelt dat elke kleine minimale blokkerende verzameling lineair is. We beginnen met een overzicht van de gevallen waarin het lineariteitsvermoeden bewezen is. Voor blokkerende verzamelingen van Rédei-type geven we een nieuw bewijs. De rest van het hoofdstuk bestaat uit het bewijs van de volgende stelling, die het lineariteitsvermoeden voor k-blokkerende verzamelingen in $\mathrm{PG}(n, p^3)$, p priem, bevestigt.

Stelling A.4.1. *Een kleine k-blokkerende verzameling in $\mathrm{PG}(n, q^3)$ die elke $(n-k)$-ruimte in 1 mod q punten snijdt, is lineair.*

A.5 Hoofdstuk 5

In Hoofdstuk 5 bestuderen we *partiële hypervlakbedekkingen*. Zoals de naam suggereert, zijn dit verzamelingen van hypervlakken die bijna alle punten bedekken. Duaal zijn zij *bijna 1-blokkerende verzamelingen*. We breiden deze definitie uit naar *bijna k-blokkerende verzamelingen* en tonen het volgende resultaat aan:

Stelling A.5.1. *Zij $\mathcal{S}$ een bijna k-blokkerende verzameling van grootte $q^k + b$, $b < (q^k - 2)/3$, die hoogstens $q^{k(n-1)}(q^k - 1)/(q^{k^2} - 1)$ $(n-k)$-ruimten niet blokkeert, dan zijn er minstens $q^{k(n-2)}(q^k - b)(q^k - 1)/(q^{k^2} - 1)$ $(n-k)$-ruimten niet geblokkeerd en al deze niet-geblokkeerde ruimten gaan door een gemeenschappelijk punt.*

Ter afsluiting van dit hoofdstuk vergelijken we onze resultaten met eerdere resultaten van K. Metsch.

A.6 Hoofdstuk 6

In Hoofdstuk 6 wordt de code $\mathrm{C}_k(n, q)$ van punten en k-ruimten in $\mathrm{PG}(n, q)$ bestudeerd. Deze code vormt een veralgemening van de code $\mathrm{C}(2, q)$ van punten en rechten in $\mathrm{PG}(2, q)$. De relevante resultaten over $\mathrm{C}(2, q)$ worden dan ook eerst uiteengezet. De parameters van de code worden besproken en we zien

dat voor de duale code van $\mathrm{C}_k(n,q)$, het minimum gewicht nog niet gekend is, behalve in de gevallen waar q even of een priemgetal is. Voor de duale code stellen we verschillende grenzen op het minimum gewicht op en we bewijzen de volgende stellingen.

Stelling A.6.1. *Het minimum gewicht van de duale code van punten en k-ruimten in* $\mathrm{PG}(n,q)$ *is gelijk aan het minimum gewicht van de duale code van punten en rechten in* $\mathrm{PG}(n-k+1,q)$.

Stelling A.6.2. *Het minimum gewicht van de p-aire code van punten en k-ruimte in* $\mathrm{PG}(n,q)$ *is minstens* $(12(q^{n-k+1}-1)/(q-1)+6)/7$ *als* $p>7$.

Stelling A.6.3. *Het minimum gewicht van de duale code van punten en k-ruimten in* $\mathrm{PG}(n,q)$ *is hoogstens* $2q^{n-k}-q^{n-k-1}(q-p)/(p-1)$.

De *romp* (engels: *hull*) van een code C wordt gedefinieerd als $\mathrm{C}\cap\mathrm{C}^{\perp}$. We veralgemenen een resultaat van Assmus en Key over de romp van $\mathrm{C}(2,q)$.

Stelling A.6.4. *Het minimum gewicht van de romp van* $\mathrm{C}_{n-1}(n,q)$ *is gelijk aan* $2q^{n-1}$.

Als hoofdresultaat bewijzen we dat er een interval bestaat waarvoor er geen codewoorden van $\mathrm{C}_k(n,q)$ met gewicht in dit interval voorkomen. Voor dit bewijs tonen we een verband aan tussen k-blokkerende verzamelingen en bepaalde codewoorden in de code $\mathrm{C}_k(n,q)$.

Stelling A.6.5. *Als c een codewoord is van* $\mathrm{C}_k(n,q)$, $q=p^h$, $p>3$, *met gewicht kleiner dan* $2q^k$, *waarvoor* $(c,\mu)\neq 0$ *voor een zekere* $(n-k)$*-ruimte* μ, *dan is c een veelvoud van een incidentievector van een kleine minimale k-blokkerende verzameling in* $\mathrm{PG}(n,q)$.

Stelling A.6.6. *Er zijn geen codewoorden in* $\mathrm{C}_k(n,q)\setminus\mathrm{C}_k(n,q)^{\perp}$, $q=p^h$, *met gewicht in het interval* $](q^{k+1}-1)/(q-1),2q^k[$, $p>5$.

Stelling A.6.7. *Er zijn geen codewoorden in* $\mathrm{C}_k(n,q)$, $q=p^h$, *met gewicht in het interval* $](q^{k+1}-1)/(q-1),2\left(\frac{q^n-1}{q^k-1}(1-\frac{1}{p})+\frac{1}{p}\right)[$.

De speciale gevallen waar q een priemgetal is of waar $k=n-1$ worden apart behandeld, omdat we in die gevallen een scherp interval kunnen afleiden voor de mogelijke gewichten van een codewoord.

A.7 Hoofdstuk 7

In het laatste hoofdstuk bespreken we de duale codes van lineaire representaties en polaire ruimten. We beginnen met enkele meetkundige voorwaarden af te leiden waaraan codewoorden van dergelijke codes moeten voldoen. Deze voorwaarden stellen ons in staat om grenzen op het minimum gewicht van deze codes af te leiden, en in sommige gevallen de codewoorden van klein gewicht te karakteriseren.

Eerst leiden we algemene ondergrenzen op het minimum gewicht van deze codes af, waarbij we in het geval van de lineaire representaties nagaan wanneer deze grens scherp is. We karakteriseren de codewoorden van klein gewicht in de duale code van de lineaire representatie $T_2^*(\Theta)$ van een hyperovaal Θ, en van de duale meetkunde $T_2^*(\Theta)^D$ in de nu volgende stellingen.

Stelling A.7.1. *Elk codewoord c uit $\mathrm{C}(T_2^*(\Theta)^D)^\perp$ met gewicht hoogstens $2\sqrt[3]{q}(q+1)/3$ is een lineaire combinatie van $\lceil \frac{wt(c)}{2q+2} \rceil$ codewoorden met gewicht $2q$ of $2(q+1)$.*

Stelling A.7.2. *Het minimum gewicht van $\mathrm{C}(T_2^*(\Theta))^\perp$ is $4q$. De codewoorden c in deze code met gewicht hoogstens $2\sqrt[3]{q}q/3$ zijn lineaire combinaties van $\lceil \frac{wt(c)}{2q} \rceil$ codewoorden van gewicht $2q$ uit $\mathrm{C}(T_2^*(\Theta)^D)^\perp$.*

In het geval dat Θ een reguliere hyperovaal is (een kegelsnede samen met zijn kern), worden de codewoorden tot op een hoger gewicht gekarakteriseerd.

We geven ook de karakterisering van de codewoorden van klein gewicht in de code van de punten en generatoren van de hyperbolische kwadriek $\mathcal{Q}^+(5,q)$.

Daarna komen de codewoorden van groot gewicht in de duale code van polaire ruimten aan bod. Voor de veralgemeende vierhoek $\mathcal{Q}(4,q)$, q even, leiden we eerst het maximum gewicht af.

Stelling A.7.3. *Als c een codewoord is van $\mathrm{C}(\mathcal{Q}(4,q))^\perp$, q even, dan is het gewicht van c hoogstens q^3+q, en als die grens bereikt wordt, correspondeert c met het complement van een ovoïde.*

Een *ovoïde* van $\mathcal{Q}(4,q)$ is een verzameling $\mathcal{O}$ van punten van $\mathcal{Q}(4,q)$ zodat elke rechte van $\mathcal{Q}(4,q)$ exact één punt van $\mathcal{O}$ bevat. Het is duidelijk dat een ovoïde een voorbeeld van een blokkerende verzameling van $\mathcal{Q}(4,q)$ is. Hieromtrent

bewijzen we de volgende stelling, waarbij we eerdere resultaten van Eisfeld, Storme, Szőnyi en Sziklai verbeteren.

Stelling A.7.4. *Als B een blokkerende verzameling is van $\mathcal{Q}(4,q)$, q even, met q^2+1+r punten, waarbij $0<r<\frac{q+4}{6}$, dan bevat B een ovoïde van $\mathcal{Q}(4,q)$.*

Hieruit kunnen we de volgende stelling afleiden die bewijst dat er een interval bestaat waarbinnen er geen codewoorden van dat gewicht in $\mathrm{C}(\mathcal{Q}(4,q))^\perp$, q even, voorkomen.

Stelling A.7.5. *Er zijn geen codewoorden met gewicht in $]q^3+\frac{5q-4}{6}, q^3+q[$ in $\mathrm{C}(\mathcal{Q}(4,q))^\perp$, q even.*

Voor de codewoorden van $\mathrm{C}(\mathcal{Q}^-(5,q))^\perp$, q even, ligt de situatie anders: hier bewijzen we dat er een interval bestaat zodat voor elke even waarde binnen dit interval er een codewoord met dat gewicht bestaat.

Stelling A.7.6. *Er bestaan codewoorden in $\mathrm{C}(\mathcal{Q}^-(5,q))^\perp$, q even, met gewicht $(1+q^2)(q^2+q)-2i$, met $i=0,1,\ldots,q/2$.*

Tenslotte leiden we nog het maximum gewicht af van de codes van polaire ruimten van hogere rang, waarbij we ook de codewoorden van grootste gewicht karakteriseren.

B

Summary

B.1 Introduction

This appendix summarises the new results obtained in this thesis. We only define the concepts that are necessary to understand this summary, and refer to the original text for more details.

The title of this thesis indicates that the main subject is *blocking sets* in $\mathrm{PG}(n,q)$, where the symbol $\mathrm{PG}(n,q)$ indicates the projective space over the finite field $\mathbb{F}_q$ with q elements, where q is a power of a prime p.

A *k-blocking set* in $\mathrm{PG}(n,q)$ is a set of points that blocks all $(n-k)$-dimensional spaces. A special class of blocking sets is provided by *linear blocking sets*. A set $\mathcal{S}$ of points in $\mathrm{PG}(n,q^t)$ is $\mathbb{F}_q$-linear if there is a vectorsubspace U of the underlying vectorspace of $\mathrm{PG}(n,q^t)$ over a subfield $\mathbb{F}_q$ of $\mathbb{F}_{q^t}$, such that the projective points corresponding to the vectors of U are precisely the projective points of $\mathcal{S}$. If the vectorspace U has rank k, then we say that $\mathcal{S}$ is an $\mathbb{F}_q$-linear set of *rank k*.

A k-blocking set B is called *minimal* if no proper subset of B is a k-blocking set. A blocking set is called *small* if it contains less that $3(q^k+1)/2$ points.

Two sets in $\mathrm{PG}(n,q)$ are called *isomorphic* if there is an element of $\mathrm{P\Gamma L}(n+1,q)$ that maps one set onto the other and two sets in $\mathrm{PG}(n,q)$ are called *projectively equivalent* if there is an element of $\mathrm{PGL}(n+1,q)$ that maps one set onto the other.

In the last two chapters we study linear codes arising from geometric structures. The code C arising from a geometric structure consisting of *points* and *blocks*, is defined as the vector space generated (over a finite field) by the *incidence matrix* of points and blocks.

The incidence matrix of points and blocks is defined as the matrix whose rows are labelled by the blocks and whose columns are labelled by the points, for which the value on the i-th row and j-th column is 1 if the j-th point lies on the i-th line, and 0 otherwise. The *dual code* of C, denoted by $\mathrm{C}^{\perp}$, is the vector space consisting of all vectors that are orthogonal to C.

B.2 Chapter 2

In Chapter 2, we discuss different bounds on the size of a minimal blocking set. There are different disjoint intervals for the possible sizes of a small minimal blocking set; these intervals follow from the 1 mod p-theorem of T. Szőnyi and Zs. Weiner, that states that a subspace that intersects a small minimal blocking set, intersects it in 1 mod p points. One defines the *exponent* e of a small minimal blocking set B as the largest natural number for which every subspace of $\mathrm{PG}(n,q)$ meets B in 1 mod p^e points. Using the 1 mod p-result by Szőnyi and Weiner, we derive the following theorem.

Theorem B.2.1. *Let B be a minimal k-blocking set in $\mathrm{PG}(n,q)$, with $|B| \leq 2q^k$ and exponent e. If $p > 2$ and $p^e > 3$, then B is small and*

$$|B| \leq q^k + \frac{2q^k}{p^e}.$$

Furthermore, we prove the following unique reducibility result.

Theorem B.2.2. *A k-blocking set in $\mathrm{PG}(n,q)$, containing less than $2q^k$ points, is uniquely reducible to a minimal k-blocking set.*

B.3 Chapter 3

In Chapter 3, we investigate linear sets contained in a projective line. We first recall the connection between linear sets in a projective space and projections of *canonical subgeometries*. A canonical subgeometry is a set of points that is obtained by restricting the coordinates points of $\mathrm{PG}(n,q)$ with repect to a certain basis, to coordinates in a subfield of $\mathbb{F}_q$. A result of G. Lunardon and O. Polverino, shows that every linear set is a canonical subgeometry or a projection thereof.

Roughly speaking, we prove that a linear set, obtained by projecting a subgeometry π from a subspace μ, is isomorphic to the linear set obtained by projecting the image of π under some collineation from the image of μ under the same collineation, *and vice versa*.

Using these transitivity properties, we solve the isomorphism problem for linear sets of rank 3, contained in a projective line. If the point from which we project lies on an extended line of the canonical subplane, we call the obtained linear set a *club*, and otherwise, we call it a *scattered linear set of rank 3*. We show the following theorem.

Theorem B.3.1. *(i) All clubs in* $\mathrm{PG}(1,q^3)$ *and all scattered linear sets of rank* 3 *in* $\mathrm{PG}(1,q^3)$ *are projectively equivalent.*

(ii) All scattered linear sets of rank 3 *in* $\mathrm{PG}(1,q^4)$ *are projectively equivalent.*

(iii) All clubs and all scattered linear sets of rank 3 *in* $\mathrm{PG}(1,2^5)$ *are isomorphic, but there exist projectively inequivalent clubs and projectively inequivalent scattered linear sets of rank* 3 *in* $\mathrm{PG}(1,2^5)$.

(iv) In all other cases, there exist non-isomorphic clubs and non-isomorphic scattered linear sets of rank 3.

Next, we determine the intersection of a linear set of rank k with a subline (which is a linear set of rank 2) and show the following theorem.

Theorem B.3.2. *An* $\mathbb{F}_q$*-subline intersects an* $\mathbb{F}_q$*-linear set of rank* k *of* $\mathrm{PG}(1,q^t)$ *in* $0,1,\ldots,\min\{q+1,k\}$ *or* $q+1$ *points.*

We investigate the sublines that are contained in a linear set. There can be *regular* and *irregular* sublines contained in a linear set. We show that all

sublines, contained in a club, are regular, but that in scattered linear sets of rank 3, there do exist irregular sublines. We show that every subline can be seen as an irregular subline of a certain linear set of rank $k > 2$, and that through two different points of a scattered $\mathbb{F}_q$-linear set $\mathcal{S}$ of rank 3, there exist exactly two sublines, contained in $\mathcal{S}$, one is regular, the other one irregular. We investigate how these irregular sublines appear as projections of a certain type of conics.

We determine the intersection of two linear sets of rank 3 in the following theorem.

Theorem B.3.3. *Two $\mathbb{F}_q$-linear sets of rank 3 in $\mathrm{PG}(1, q^t)$, $q > 3$, intersect in at most $2q + 2$ points if q is odd, and in at most $2q + 3$ points if q is even.*

Finally, we treat the *representation problem* for linear sets of rank 3.

B.4 Chapter 4

In Chapter 4, we turn our attention to the *linearity conjecture*. This conjecture states that every small minimal blocking set is linear. We start with an overview of the cases in which the linearity conjecture is proven, and reproof the case of Rédei-type blocking sets. The remainder of the chapter is devoted to the proof of the following theorem, that implies the truth of the linearity conjecture for k-blocking sets in $\mathrm{PG}(n, p^3)$, p prime, as a corollary.

Stelling B.4.1. *A small minimal k-blocking set in $\mathrm{PG}(n, q^3)$, intersecting every $(n-k)$-ruimte in 1 mod q points, is linear.*

B.5 Chapter 5

In Chapter 5, we study *partial covers*. Dually, these are almost 1-blocking sets. We extend this definition to almost k-blocking sets and show the following.

Theorem B.5.1. *If an almost k-blocking $(q^k + b)$-set $\mathcal{K}$ in $\mathrm{PG}(n, q)$, $b < (q^k - 2)/3$, misses at most $q^{k(n-1)}(q^k - 1)/(q^{k^2} - 1)$ $(n-k)$-spaces, then it misses at least $q^{k(n-2)}(q^k - b)(q^k - 1)/(q^{k^2} - 1)$ $(n-k)$-spaces and all 0-secants go through a common point.*

We end this chapter by comparing the obtained results with these of K. Metsch.

B.6 Chapter 6

In Chapter 6 we study the code $\mathrm{C}_k(n,q)$ of points and k-spaces in $\mathrm{PG}(n,q)$. This code generalises the code $\mathrm{C}(2,q)$ of points and lines in $\mathrm{PG}(2,q)$. We begin with an overview of the relevant results for $\mathrm{C}(2,q)$. The parameters of the code $\mathrm{C}_k(n,q)$ are stated and we see that for the dual code of $\mathrm{C}_k(n,q)$, the minimum weight is not known, except for the cases that q is even or a prime. For the dual code, we derive bounds on the minimum weight and prove the following theorems.

Theorem B.6.1. *The minimum weight of the dual code of points and k-spaces in $\mathrm{PG}(n,q)$ equals the minimum weight of the dual code of points and lines in $\mathrm{PG}(n-k+1,q)$.*

Theorem B.6.2. *The minimum weight of the p-ary code of points and k-spaces in $\mathrm{PG}(n,q)$ is at least $(12(q^{n-k+1}-1)/(q-1)+6)/7$ if $p>7$.*

Theorem B.6.3. *The minimum weight of the p-ary code of points and k-spaces in $\mathrm{PG}(n,q)$ is at most $2q^{n-k}-q^{n-k-1}(q-p)/(p-1)$.*

The *hull* of a code C is defined as $\mathrm{C}\cap\mathrm{C}^\perp$. We extend a result of Assmus and Key about the hull of $\mathrm{C}(2,q)$.

Theorem B.6.4. *The minimum weight of the hull of $\mathrm{C}_{n-1}(n,q)$ equals $2q^{n-1}$.*

As main result, we prove that there is an empty interval in the weight enumerator of $\mathrm{C}_k(n,q)$. To prove this, we establish a connection between small minimal k-blocking sets and certain codewords of $\mathrm{C}_k(n,q)$.

Theorem B.6.5. *If c is a codeword of $\mathrm{C}_k(n,q)$, $q=p^h$, $p>3$, with weight smaller than $2q^k$, for which $(c,\mu)\neq 0$ for some $(n-k)$-space μ, then c is a multiple of an incidence vector of a small minimal k-blocking set in $\mathrm{PG}(n,q)$.*

Theorem B.6.6. *There are no codewords in $\mathrm{C}_k(n,q)\setminus\mathrm{C}_k(n,q)^\perp$, $q=p^h$, with weight in the interval $](q^{k+1}-1)/(q-1),2q^k[$, $p>5$.*

Theorem B.6.7. *There are no codewords in $\mathrm{C}_k(n,q)$, $q=p^h$, with weight in the interval $](q^{k+1}-1)/(q-1),2\left(\frac{q^n-1}{q^k-1}(1-\frac{1}{p})+\frac{1}{p}\right)[$.*

The special cases where q is prime or $k=n-1$ are treated separately, since in these cases, we can derive a sharp interval on the possible weights of a codeword.

B.7 Chapter 7

The final chapter discusses the dual codes of linear representations and polar spaces. We start by deriving some geometric properties that have to be satisfied by a codeword of such a code. These properties provide us with a tool to derive bounds on the minimum weight of these codes and to classify the the codewords of small weight in some cases.

First we derive lower bounds on the minimum weight of these codes and in the case of linear representations, we investigate when this bound is sharp. We characterise the codewords of small weight in the dual code of the linear representation $T_2^*(\Theta)$, with Θ a hyperoval, and of the dual geometry $T_2^*(\Theta)^D$ in the following theorems.

Theorem B.7.1. *A codeword c of $\mathrm{C}(T_2^*(\Theta)^D)^\perp$ with weight at most $2\sqrt[3]{q}(q+1)/3$ is a linear combination of $\lceil \frac{wt(c)}{2q+2} \rceil$ codewords with weight $2q$ or $2(q+1)$.*

Theorem B.7.2. *The minimum weight of $\mathrm{C}(T_2^*(\Theta))^\perp$ is $4q$. A codeword c in this code with weight at most $2\sqrt[3]{q}q/3$ is a linear combination of $\lceil \frac{wt(c)}{2q} \rceil$ codewords of weight $2q$ from $\mathrm{C}(T_2^*(\Theta)^D)^\perp$.*

In the case that Θ is a regular hyperoval (a conic and its nucleus), codewords up to higher weight are characterised.

We also give a characterisation of the codewords of small weight in the code of points and generators of the hyperbolic quadric $\mathcal{Q}^+(5,q)$.

After that, we turn our attention to the codewords of large weight in the dual code of polar spaces. For the generalised quadrangle $\mathcal{Q}(4,q)$, q even, we first derive the maximum weight.

Theorem B.7.3. *If c is a codeword of $\mathrm{C}(\mathcal{Q}(4,q))^\perp$, q even, then the weight of c is at most q^3+q and if we attain this bound, c corresponds to the complement of an ovoid of $\mathcal{Q}(4,q)$.*

An *ovoid* of $\mathcal{Q}(4,q)$ is a set $\mathcal{O}$ of points of $\mathcal{Q}(4,q)$ such that every line of $\mathcal{Q}(4,q)$ meets exactly one point of $\mathcal{Q}(4,q)$. It is clear that an ovoid of $\mathcal{Q}(4,q)$ is a blocking set with respect to lines of $\mathcal{Q}(4,q)$. We prove the following theorem, improving on a result of Eisfeld, Storme, Szőnyi and Sziklai.

Theorem B.7.4. *If B is a blocking set of $\mathcal{Q}(4,q)$, q even, with q^2+1+r points, where $0 \leq r < \frac{q+4}{6}$, then B contains an ovoid of $\mathcal{Q}(4,q)$.*

From this, we derive the following theorem, proving that there is an empty interval in the spectrum of codewords in $\mathrm{C}(\mathcal{Q}(4,q))^{\perp}$, q even.

Theorem B.7.5. *There are no codewords with weight in $]q^3+\frac{5q-4}{6}, q^3+q[$ in $\mathrm{C}(\mathcal{Q}(4,q))$, q even.*

For codewords of $\mathrm{C}(\mathcal{Q}^-(5,q))^{\perp}$, q even, the situation is different: in this case, we prove that there exists an interval such that for every even value s in this interval, there exists a codeword with weight s.

Theorem B.7.6. *There are codewords in $\mathrm{C}(\mathcal{Q}^-(5,q))^{\perp}$, q even, with weight $(1+q^2)(q^2+q)-2i$, with $i=0,1,\ldots,q/2$.*

Finally, we derive the maximum weight of the codes of polar spaces, and we characterise the codewords of largest weight.

Index

Bibliography

[1] R.W. Ahrens and G. Szekeres. On a combinatorial generalization of 27 lines associated with a cubic surface. *J. Austral. Math. Soc.* **10** (1969), 485–492. (on page 12).

[2] J. André. Über nicht-Desarguessche Ebenen mit transitiver Translationsgruppe. *Math. Z.* **60** (1954), 156–186. (on page 13).

[3] M. Ashbacher. Finite Group Theory. Cambridge Studies in Advanced Mathematics **10**. *Cambridge University Press, Cambridge*, 1986. (on page 8).

[4] E.F. Assmus, Jr. and J.D. Key. Designs and their codes. *Cambridge University Press*, 1992. (on pages 96, 97, 99, 100, and 109).

[5] B. Bagchi and N.S.N. Sastry. Codes associated with generalized polygons. *Geom. Dedicata* **27** (**1**) (1988), 1–8. (on pages 120, 121, and 122).

[6] B. Bagchi and S.P. Inamdar. Projective Geometric Codes. *J. Combin. Theory, Ser. A* **99** (**1**) (2002), 128–142. (on pages 97, 99, 103, 108, and 109).

[7] R.D. Baker, J.M.N. Brown, G.L. Ebert, and J.C. Fisher. Projective Bundles. *Bull. Belg. Math. Soc.* **3** (1994), 329–336. (on page 55).

[8] S. Ball, A. Blokhuis, and F. Mazzocca. Maximal arcs in Desarguesian planes of odd order do not exist. *Combinatorica* **17** (**1**) (1997), 31–41. (on page 11).

[9] A. Barlotti. Un'estensione del teorema di Segre-Kustaanheimo. *Boll. Un. Mat. Ital. (3)* **10** (1955), 498–506. (on page 11).

[10] A. Barlotti. Some topics in Finite Geometrical Structures. *Institute of Statistics Mimeo Series* **439**. Univ. of North-Carolina, Chapel Hill, 1965. (on page 10).

[11] A. Barlotti and J. Cofman. Finite Sperner spaces constructed from projective and affine spaces. *Abh. Math. Sem. Univ. Hamburg* **40** (1974), 231–241. (on page 14).

[12] L. Berardi. Projective triangles in the four projective planes of order nine. *Riv. Mat. Pura Appl.* **6** (1990), 7–17. (on page 23).

[13] A. Beutelspacher. Blocking sets and partial spreads in finite projective spaces. *Geom. Dedicata* **9** (**4**) (1980), 425–449. (on page 25).

[14] A. Bichara and G. Korchmáros. Note on a $(q+2)$-set in a Galois plane of order q. *Ann. Discrete Math.* **14** (1982), 117–122. (on page 146).

[15] J. Bierbrauer. On the weight distribution in binary codes generated by projective planes. *Q. J. Math.* **33** (1982), 275–279. (on page 110).

[16] A. Blokhuis. On the size of a blocking set in $\mathrm{PG}(2,p)$. *Combinatorica* **14** (**1**) (1994), 111–114. (on pages 22 and 64).

[17] A. Blokhuis, S. Ball, A.E. Brouwer, L. Storme, and T. Szőnyi. On the number of slopes of the graph of a function defined on a finite field. *J. Combin. Theory, Ser. A* **86** (**1**) (1999), 187–196. (on page 65).

[18] A. Blokhuis and A.E. Brouwer. Blocking sets in Desarguesian projective planes. *Bull. London Math. Soc.* **18** (**2**) (1986), 132–134. (on page 86).

[19] A. Blokhuis, A.E. Brouwer, and T. Szőnyi. Covering all points except one. *J. Algebraic Combin.*, doi:10.1007/s10801-009-0204-1. (on page 84).

[20] A. Blokhuis and M. Lavrauw. Scattered spaces with respect to a spread in $\mathrm{PG}(n,q)$. *Geom. Dedicata* **81** (**1**–**3**) (2000), 231–243. (on page 18).

[21] A. Blokhuis, L. Storme, and T. Szőnyi. Lacunary polynomials, multiple blocking sets and Baer subplanes. *J. London Math. Soc.* **60** (**2**) (1999), 321–332. (on page 25).

[22] M. Bokler. Minimal blocking sets in projective spaces of square order. *Des. Codes Cryptogr.* **24** (**2**) (2001), 131–144. (on page 65).

[23] M. Bokler. Lower bounds for the cardinality of minimal blocking sets in projective spaces. *Discrete Math.* **270** (**1**–**3**) (2003), 13–31. (on page 24).

[24] G. Bonoli and O. Polverino. $\mathbb{F}_q$-linear blocking sets in $\mathrm{PG}(2, q^4)$. *Innov. Incidence Geom.* **2** (2005), 35–56. (on page 38).

[25] R.C. Bose. Mathematical theory of the symmetrical factorial design. *Sankhya* **8** (1947), 107–166. (on page 10).

[26] R.C. Bose and R.C. Burton. A characterization of flat spaces in a finite geometry and the uniqueness of the Hamming and the MacDonald codes. *J. Combin. Theory* **1** (1966), 96–104. (on page 25).

[27] 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), 65–77. (on page 45).

[28] A.E. Brouwer and A. Schrijver. The blocking number of an affine space. *J. Combin. Theory, Ser. A* **24 (2)** (1978), 251–253. (on page 83).

[29] A.E. Brouwer and C.A. van Eijl. On the p-rank of strongly regular graphs. *J. Algebraic Combin.* **1 (4)** (1992), 329–346. (on page 123).

[30] R.H. Bruck and R.C. Bose. The construction of translation planes from projective spaces. *J. Algebra* **1** (1964), 85–102. (on page 13).

[31] A.A. Bruen. Baer subplanes and blocking sets. *Bull. Amer. Math. Soc.* **76** (1970), 342–344. (on pages 22, 25, 64, and 143).

[32] A.A. Bruen. Blocking sets in finite projective planes. *SIAM J. Applied Math.* **21** (1971), 380–392. (on pages 23 and 25).

[33] A.A. Bruen and J.A. Thas. Blocking sets. *Geom. Dedicata* **6 (2)** (1977), 193–203. (on pages 22, 25, and 27).

[34] A. A. Bruen and J.A. Thas. Hyperplane coverings and blocking sets. *Math. Z.* **81 (3)** (1982), 407–409. (on page 27).

[35] F. Buekenhout (Editor). Handbook of incidence geometry. *North-Holland, Amsterdam*, 1995. (on page 1).

[36] F. Buekenhout and E.E. Shult. On the foundations of polar geometry. *Geom. Dedicata* **3** (1974), 155–170. (on page 6).

[37] N.J. Calkin, J.D. Key, and M.J. de Resmini. Minimum weight and dimension formulas for some geometric codes. *Des. Codes Cryptogr.* **17 (1)** (1999), 105–120. (on page 99).

[38] D.B. Chandler, P. Sin, and Q. Xiang. The permutation action of finite symplectic groups of odd characteristic on their standard modules. *J. Algebra* **318 (2)** (2007), 871–892. (on page 121).

[39] B. Cherowitzo. Hyperoval page. http://www-math.cudenver.edu/∼wcherowi/research/hyperoval/hypero.html (on page 10).

[40] K. Chouinard. Weight distributions of codes from planes (PhD Thesis, University of Virginia) (August 1998). (on pages 96, 100, and 110).

[41] K. Chouinard. On weight distributions of codes of planes of order 9. *Ars Combin.* **63** (2002), 3–13. (on page 100).

[42] A. Cossidente, A. Gács, C. Mengyán, A. Siciliano, T. Szőnyi, and Zs. Weiner. On large minimal blocking sets in $\mathrm{PG}(2,q)$. *J. Combin. Des.* **13 (1)** (2005), 25–41. (on pages 27 and 28).

[43] J. De Beule, A. Hallez, and L. Storme. A non-existence result on Cameron–Liebler line classes. *J. Combin. Des.* **16 (4)** (2007), 342–349. (on page 145).

[44] J. De Beule and L. Storme (Editors). Current research topics in Galois Geometry. *Nova Sci. Publ.*, to appear. (on pages 1, 15, and 37).

[45] P. Delsarte. A geometric approach to a class of cyclic codes. *J. Combin. Theory* **6** (1969), 340–358. (on page 95).

[46] P. Delsarte, J.M. Goethals, and F.J. MacWilliams. On generalized Reed-Muller codes and their relatives. *Information and Control* **16** (1970), 403–442. (on page 96).

[47] P. Dembowski. Finite geometries. *Springer-Verlag, Berlin-New York*, 1968. (on page 1).

[48] J. Di Paola. On minimum blocking coalitions in small projective plane games. *SIAM J. Appl. Math.* **17** (1969), 378–392. (on pages 23, 25, and 64).

[49] S. Dodunekov, L. Storme, and G. Van de Voorde. Partial covers of $\mathrm{PG}(n,q)$. *European J. Combin.*, doi:10.1016/j.ejc.2009.07.008. (on pages 84 and 85).

[50] G. Donati and N. Durante. On the intersection of two subgeometries of $\mathrm{PG}(n,q)$. *Des. Codes Cryptogr.* **46 (3)** (2008), 261–267. (on page 45).

[51] S. Droms, K.E. Mellinger, and C. Meyer. LDPC codes generated by conics in the classical projective plane. *Des. Codes Cryptogr.* **40 (3)** (2006), 343–356. (on page 118).

[52] J. Eisfeld, L. Storme, T. Szőnyi, and P. Sziklai. Covers and blocking sets of classical generalised quadrangles. *Discrete Math.* **238 (1–3)** (2001), 35–51. (on pages 146 and 147).

[53] V. Fack, Sz.L. Fancsali, L. Storme, G. Van de Voorde, and J. Winne. Small weight codewords in the codes arising from Desarguesian projective planes. *Des. Codes Cryptogr.* **46 (1)** (2008), 25–43. (on page 100).

[54] Sz.L. Fancsali and P. Sziklai. About maximal partial 2-spreads in $\mathrm{PG}(3m-1,q)$. *Innov. Incidence Geom.* **4** (2006), 89–102. (on pages 41 and 46).

[55] Sz.L. Fancsali and P. Sziklai. Description of the clubs. To appear in *Annales Univ. Sci. Sect. Mat.* (on pages 46 and 58).

[56] S. Ferret and L. Storme. Results on maximal partial spreads in $\mathrm{PG}(3,p^3)$ and on related minihypers. *Des. Codes Cryptogr.* **29** (2003), 105–122. (on page 56).

[57] R. Figueroa. A family of not (v,ℓ)-transitive projective planes of order q^3, $q \equiv \mod 3$ and $q > 2$. *Math. Z.* **81 (4)** (1982), 471–479. (on page 42).

[58] A. Gács, T. Szőnyi, and Zs. Weiner. Private communication (2009). (on page 100).

[59] A. Gács and Zs. Weiner. On $(q+t,t)$-arcs of type $(0,2,t)$. *Des. Codes Cryptogr.* **29 (1–3)** (2003), 131–139. (on page 11).

[60] R.G. Gallager. Low density parity check codes. *IRE Trans. Inform. Theory* **8** (1962), 21–28. (on page 117).

[61] GAP. Groups, Algorithms, and Programming, Version 4.4.12. *http://www.gap-system.org.* (on page iii).

[62] D.G. Glynn. Finite projective planes and related combinatorial systems. PhD thesis, Adelaide Univ., 1978. (on page 55).

[63] J.M. Goethals and P. Delsarte. On a class of majority-logic decodable cyclic codes. *IEEE Trans. Inform. Theory* **14** (1968), 182–188. (on page 98).

[64] P. Govaerts and L. Storme. The classification of the smallest nontrivial blocking sets in $\mathrm{PG}(n, 2)$. *J. Combin. Theory, Ser. A* **113** (**7**) (2006), 1543–1548. (on page 26).

[65] R.L. Graham and F.J. MacWilliams. On the number of information symbols in difference-set cyclic codes. *Bell System Tech. J.* **45** (1966), 1057–1070. (on page 98).

[66] M. Hall, Jr. Affine generalized quadrilaterals. Studies in Pure Mathematics. *Academia Press, London* (1971), 113–116. (on page 12).

[67] N. Hamada. The rank of the incidence matrix of points and d-flats in finite geometries. *J. Sci. Hiroshima Univ. Ser. A-I* **32** (1968), 381–396. (on page 97).

[68] N. Hamada. Characterization, resp. nonexistence of certain q-ary linear codes attaining the Griesmer bound. *Bull. Osaka Women's Univ.* **24** (1985), 1–47. (on page 145).

[69] U. Heim. Blockierende Mengen in endlichen projektiven Raumen. *Mitt. Math. Semin. Giessen* **226** (1996), 4–82. (on page 26).

[70] D. Hilbert. The foundations of geometry (english translation of the 1899 original). Available online at *http://www.gutenberg.org/etext/17384*. (on page 4).

[71] J.W.P. Hirschfeld. Projective Geometries over Finite Fields. *Oxford University Press*, Oxford, 1979. (on pages 1, 9, 23, and 54).

[72] J.W.P. Hirschfeld. Finite Projective Spaces of Three Dimensions. *Oxford University Press*, Oxford, 1985. (on pages 1 and 14).

[73] J.W.P. Hirschfeld and J.A. Thas. General Galois Geometries. *Oxford University Press*, Oxford, 1991. (on pages 1, 129, and 130).

[74] D.R. Hughes and F.C. Piper. Projective planes. *Springer-Verlag, New York*, 1973. (on pages 1, 4, and 14).

[75] S.P. Inamdar and N.S.N. Sastry. Codes from Veronese and Segre embeddings and Hamada's formula. *J. Combin. Theory, Ser. A* **96** (**1**) (2001), 20–30. (on page 98).

[76] S. Innamorati and A. Maturo. On irreducible blocking sets in projective planes. *Ratio Math.* **2** (1991), 151–155. (on page 28).

[77] S. Innamorati and A. Maturo. The spectrum of minimal blocking sets. *Discrete Math.* **208/209** (1999), 339–347. (on page 24).

[78] I. Jagos, G. Kiss, and A. Pór. On the intersection of Baer subgeometries of $\mathrm{PG}(n, q^2)$. *Acta Sci. Math.* **69 (1–2)** (2003), 419–429. (on page 45).

[79] R.E. Jamison. Covering finite fields with cosets of subspaces. *J. Combin. Theory, Ser. A* **22 (3)** (1977), 253–266. (on page 83).

[80] S.J. Johnson and S.R. Weller. Codes for iterative decoding from partial geometries. *IEEE Trans. Comm.* **52** (2004), 236–243. (on page 123).

[81] J.D. Key, T.P. McDonough and V.C. Mavron. An upper bound for the minimum weight of the dual codes of dearguesian planes. *European J. Combin.* **30** (2009), 220–229. (on page 104).

[82] J.L. Kim, K.E. Mellinger, and L. Storme. Small weight codewords in LDPC codes defined by (dual) classical generalised quadrangles. *Des. Codes Cryptogr.* **42 (1)** (2007), 73–92. (on page 120).

[83] C.F. Klein. Über die Transformation der allgemeinen Gleichung des zweiten Grades zwischen Linien-Koordinaten auf eine kanonische Form. PhD Dissertation, Friedrich-Wilhelms-Universität, Bonn, 1868. (on page 8).

[84] G. Korchmáros and F. Mazzocca. On $(q+t)$-arcs of type $(0, 2, t)$ in a Desarguesian plane of order q. *Math. Proc. Camb. Phil. Soc.* **108 (3)** (1990), 445–459. (on page 128).

[85] Y. Kou, S. Lin, and M. Fossorier. Low-density parity-check codes based on finite geometries: a rediscovery and new results. *IEEE Trans. Inform. Theory* **47 (7)** (2001), 2711–2736. (on page 118).

[86] C.W.H. Lam. The search for a finite projective plane of order 10. *Amer. Math. Monthly* **89 (4)** (1991), 305–318. (on page 95).

[87] M. Lavrauw. Scattered spaces with respect to spreads, and eggs in finite projective spaces. PhD Dissertation, Eindhoven University of Technology, Eindhoven, 2001. (on pages 17 and 18).

[88] M. Lavrauw. Finite semifields with a large nucleus and higher secant varieties to Segre varieties. To appear in *Adv. Geom.* (on page 37).

[89] M. Lavrauw, L. Storme, and G. Van de Voorde. On the code generated by the incidence matrix of points and hyperplanes in $\mathrm{PG}(n, q)$ and its dual. *Des. Codes Cryptogr.* **48 (3)** (2008), 231–245. (on pages 96, 109, and 110).

[90] M. Lavrauw, L. Storme, and G. Van de Voorde. On the code generated by the incidence matrix of points and k-spaces in $\mathrm{PG}(n, q)$ and its dual. *Finite Fields Appl.* **14 (4)** (2008), 1020–1038. (on pages 22, 96, 109, and 110).

[91] M. Lavrauw, L. Storme, and G. Van de Voorde. A proof of the linearity conjecture for k-blocking sets in $\mathrm{PG}(n, p^3)$, p prime. Submitted to *J. Combin. Theory, Ser. A*. (on page 64).

[92] M. Lavrauw, L. Storme, P. Sziklai, and G. Van de Voorde. An empty interval in the spectrum of small weight codewords in the code from points and k-spaces of $\mathrm{PG}(n, q)$. *J. Combin. Theory, Ser. A* **116 (4)** (2009), 996–1001. (on pages 96, 109, and 110).

[93] M. Lavrauw and G. Van de Voorde. On linear sets on a projective line. To appear in *Des. Codes Cryptogr.* (on pages 16 and 37).

[94] X. Li, C Zhang, and J. Shen. Regular LDPC codes from semipartial geometries. *Acta Appl. Math.* **102 (1)** (2008), 25–35. (on page 123).

[95] Z. Liu and D. Pados. LDPC codes from generalized polygons. *IEEE Trans. Inform. Theory* **51 (11)** (2005), 3890–3898. (on pages 120 and 130).

[96] G. Lunardon. Normal spreads. *Geom. Dedicata* **75 (3)** (1999), 245–261. (on pages 16 and 63).

[97] G.Lunardon, P. Polito, and O. Polverino. A geometric characterisation of linear k-blocking sets. *J. Geom.* **74 (1–2)** (2002), 120–122. (on pages 38 and 63).

[98] G. Lunardon and O. Polverino. Translation ovoids of orthogonal polar spaces. *Forum Math.* **16 (5)** (2004), 663–669. (on pages 37 and 38).

[99] D.J.C. MacKay and R.M. Neal. Near Shannon limit performance of low density parity check codes. *Electron. Lett.* **32 (18)** (1996), 1645–1646. (on page 118).

[100] F.J. MacWilliams and N.J.A. Sloane. The theory of error-correcting codes. *North-Holland Mathematical Library*, Amsterdam-New York-Oxford (1977). (on page 1).

[101] G. McGuire and H.N. Ward. The weight enumerator of the code of the projective plane of order 5. *Geom. Dedicata* **73 (1)** (1998), 63–77. (on page 100).

[102] J.H. Maclagan-Wedderburn. A Theorem on Finite Algebras. *Trans. Amer. Math. Soc.* **6 (3)** (1905), 349–352. (on page 4).

[103] F. Mazzocca, O. Polverino, and L. Storme. Blocking sets in $\mathrm{PG}(r, q^n)$. *Des. Codes Cryptogr.* **44 (1–3)** (2007), 97–113. (on page 24).

[104] K. Metsch. A Bose–Burton type theorem for quadrics. *J. Combin. Des.* **11 (5)** (1999), 317–338. (on pages 151 and 152).

[105] K. Metsch. On blocking sets of quadrics. *J. Geom.* **67** (2000), 188–207. (on page 150).

[106] K. Metsch. How many s-subspaces must miss a point set in $\mathrm{PG}(d, q)$? *J. Geom.* **86 (1–2)** (2007), 154–164. (on pages 84 and 92).

[107] K. Metsch and L. Storme. Partial t-spreads in $\mathrm{PG}(2t + 1, q)$. *Des. Codes Cryptogr.* **18 (1–3)** (1999), 199–216. (on page 46).

[108] C.M. O'Keefe, T. Penttila, and G.F. Royle. Classification of ovoids in $\mathrm{PG}(3, 32)$. *J. Geom.* **50 (1–2)** (1994), 143–150. (on page 12).

[109] T.G. Ostrom. Replaceable nets, net collineations, and net extensions. *Canad. J. Math.* **18** (1966), 666–672. (on page 14).

[110] F. Pambianco and L. Storme. Small Complete Caps in Spaces of Even Characteristic. *J. Combin. Theory, Ser. A* **75 (1)** (1996), 70–84. (on page 123).

[111] G. Panella. Caratterizzazione delle quadriche di uno spazio (tridimensionale) lineare sopra un corpo finito. *Boll. Un. Mat. Ital. (3)* **10** (1955), 507–513. (on page 11).

[112] K.H. Parschall. In pursuit of the finite division algebra theorem and beyond: Joseph H.M. Wedderburn, Leonard E. Dickson, and Oswald Veblen. *Archives of International History of Science* **33** (1983), 274–299. (on page 4).

[113] S.E. Payne. Nonisomorphic generalized quadrangles. *J. Algebra* **18** (1971), 201–212. (on page 140).

[114] S.E. Payne and J.A. Thas. *Finite Generalized Quadrangles*. Pitman Advanced Publishing Program, 1984. (on pages 1 and 141).

[115] T. Penttila and G.F. Royle. Classification of hyperovals in $\mathrm{PG}(2, 32)$. *J. Geom.* **50 (1–2)** (1994), 151–158. (on page 10).

[116] V. Pepe. LDPC codes from the Hermitian curve. *Des. Codes Cryptogr.* **42 (3)** (2007), 303–315. (on page 118).

[117] V. Pepe, L. Storme, and G. Van de Voorde. Small weight codewords in the LDPC codes arising from linear representations of geometries. *J. Combin. Des.* **17 (1)** (2009), 1–24. (on pages 118, 130, 142, 144, and 145).

[118] V. Pepe, L. Storme, and G. Van de Voorde. On codewords in the dual code of classical generalised quadrangles and classical polar spaces. *Discrete Math.*, doi:10.1016/j.disc.2009.06.010. (on pages 118 and 153).

[119] P. Polito and O. Polverino. On small blocking sets. *Combinatorica* **18 (1)** (1998), 133–137. (on page 63).

[120] P. Polito and O. Polverino. Blocking Sets in André Planes. *Geom. Dedicata* **75 (2)** (1999), 199–207. (on pages 38 and 63).

[121] O. Polverino. Blocking set nei piani proiettivi, PhD Thesis, University of Naples 'Federico II', Naples, 1998. (on pages 22 and 30).

[122] O. Polverino. Small blocking sets in $\mathrm{PG}(2, p^3)$. *Des. Codes Cryptogr.* **20 (3)** (2000), 319–324. (on page 68).

[123] O. Polverino. Linear sets in finite projective spaces. *Discrete Math.* (2009), doi:10.1016/j.disc.2009.04.007. (on page 37).

[124] O. Polverino and L. Storme. Small minimal blocking sets in $\mathrm{PG}(2, q^3)$. *European J. Combin.* **23 (1)** (2002), 83–92. (on page 68).

[125] L. Rédei. Lückenhafte Polynome über endlichen Körpern. (German) Lehrbücher und Monographien aus dem Gebiete der exakten Wissenschaften. Mathematische Reihe, Band 42. *Birkhäuser Verlag, Basel-Stuttgart*, 1970. (on page 22).

[126] M. Richardson. On finite projective games. *Proc. Amer. Math. Soc.* **7** (1956), 458–465. (on pages 24 and 25).

[127] H. Sachar. The $\mathbb{F}_p$-span of the incidence matrix of a finite projective plane. *Geom. Dedicata* **8 (4)** (1979), 407–415. (on pages 105 and 106).

[128] C.J. Salwach. Planes, biplanes, and their codes. *Amer. Math. Monthly* **88 (2)** (1981), 106–125. (on page 98).

[129] B. Segre. Sulle ovali nei piani lineari finiti. *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat. (8)* **17** (1954), 141–142. (on page 10).

[130] B. Segre. On complete caps and ovaloids in three-dimensional Galois spaces of characteristic two. *Acta Arith.* **5** (1959), 315–332. (on page 15).

[131] B. Segre. Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane. *Ann. Mat. Pura Appl. (4)* **64** (1964), 1–76. (on pages 12 and 123).

[132] C.E. Shannon. A mathematical theory of communication. *Bell System Tech. J.* **27** (1948), 379–423, 623–656. (on page 118).

[133] A. Shokrollahi. LDPC codes: an introduction. Coding, cryptography and combinatorics. *Progr. Comput. Sci. Appl. Logic* **23**, 85–110, *Birkhäuser*, Basel, 2004. (on pages 117 and 118).

[134] K.J.C. Smith. On the p-rank of the incidence matrix of points and hyperplanes in a finite projective geometry. *J. Combin.Theory* **7** (1969), 122–129. (on page 98).

[135] P. Sin. The p-rank of the incidence matrix of intersecting linear subspaces. *Des. Codes Cryptogr.* **31 (3)** (2004), 213–220. (on page 20).

[136] L. Storme and P. Sziklai. Linear pointsets and Rédei type k-blocking sets in $\mathrm{PG}(n,q)$. *J. Algebraic Combin.* **14 (3)** (2001), 221–228. (on pages 66 and 67).

[137] L. Storme and Zs. Weiner. On 1-blocking sets in $\mathrm{PG}(n,q)$, $n \geq 3$. *Des. Codes Cryptogr.* **21 (1–3)** (2000), 235–251. (on pages 65, 68, and 82).

[138] P. Sziklai. On small blocking sets and their linearity. *J. Combin. Theory, Ser. A* **115 (7)** (2008), 1167–1182. (on pages 63 and 64).

[139] T. Szőnyi. Blocking sets in Desarguesian affine and projective planes. *Finite Fields Appl.* **3 (3)** (1997), 187–202. (on pages 22, 28, 29, 32, and 65).

[140] T. Szőnyi and Zs. Weiner. Small blocking sets in higher dimensions. *J. Combin. Theory, Ser. A* **95** (**1**) (2001), 88–101. (on pages 22, 24, 28, 29, 30, 69, 74, and 87).

[141] J.A. Thas. Ovoidal translation planes. *Arch. Math.* **23** (1972), 110–112. (on pages 10 and 15).

[142] J. Tits. Ovoïdes et groupes de Suzuki. *Arch. Math.* **13** (1962), 187–198. (on page 12).

[143] J. Tits. Buildings of spherical type and finite BN-pairs. *Springer-Verlag, Berlin, Lecture Notes in Mathematics 386*, 1974. (on pages 6 and 8).

[144] P. Vandendriessche. Some low-density parity-check codes derived from finite geometries. *Des. Codes Cryptogr.* **54** (**3**) (2010), 287–297. (on pages 121 and 122).

[145] O. Veblen and J.W. Young. Projective geometry. *Blaisdell Publishing Co. Ginn and Co. New York-Toronto-London*, 1965. (on page 3).

[146] F.D. Veldkamp. Polar geometry. *Indag. Math.* **21** (1959), 512–551. (on page 6).

[147] J. Von Neumann, O. Morgenstern, and H. Kuhn. Theory of games and economic behavior. *Princeton University Press*, 1944. (on page 21).

[148] P.O. Vontobel and R.M. Tanner. Construction of codes based on finite generalized quadrangles for iterative decoding. *Proceedings of 2001 IEEE Intern. Symp. Inform. Theory, Washington, DC* (2001), p. 223. (on page 118).

[149] Zs. Weiner. Small point sets of $\mathrm{PG}(n, \sqrt{q})$ intersecting every k-space in 1 modulo $\sqrt{q}$ points. *Innov. Incidence Geom.* **1** (2005), 171–180. (on pages 65 and 82).

...een woordje van dank

Bedankt Leo, omdat je als lesgever en promotor van mijn licentiaatsthesis mijn interesse hebt gewekt voor blocking sets en codes. Zonder jouw inbreng in mijn onderzoeksproject voor het BOF was ik nooit aan een doctoraat begonnen. Bedankt voor de kansen die je me bood om mee te gaan op congressen, de vele uren die je voor de begeleiding van mijn doctoraat uitgetrokken hebt en je eindeloze geduld hierbij. Je deur stond altijd open voor mij, en ondanks je drukke schema maakte je toch meteen tijd om je uitgebreide wiskundige kennis met mij te delen.

Bedankt Michel, omdat je mij jouw kijk op lineaire verzamelingen uit de doeken hebt gedaan, waardoor er voor mij een nieuwe wereld vol interessante problemen openging. Samenwerken met jou was inspirerend, je gaf mij steeds de kans om zelf problemen te onderzoeken, met de zekerheid dat ik kon rekenen op je hulp wanneer die nodig was. Jouw wijze raad was onmisbaar bij het tot stand komen van deze thesis.

Bedankt Aart Blokhuis, omdat je mij tijdens mijn verblijf in Eindhoven liet proeven van jouw manier van onderzoek doen.

Bedankt Kris Coolsaet, Jan De Beule en Frank De Clerck, voor de tijd die jullie spendeerden om mijn thesis in zoveel detail te lezen, en voor de relevante opmerkingen die daaruit voortvloeiden.

Thank you, Peter Sziklai and Jenny Key, for being interested in my research, for willing to be in my jury, and for the time you spent on reading this thesis.

Bedankt Anja en Beukje, omdat jullie ervoor zorgden dat bureau 12 een fijne plek was. Bedankt ook aan alle andere collega's die het de voorbije jaren leuk maakten om hier te werken.

Bedankt aan mijn ouders, voor de steun op materieel en emotioneel vlak, de talrijke gebrande kaarsjes tijdens mijn studies en de interesse voor mijn werk.

Bedankt ook aan mijn vrienden die de wekelijkse episode van 'Het leven zoals het is: de Galglaan', niet beu werden.

Dankjewel Jurgen, voor de fantastische voedselvoorziening, en voor nog zoveel meer...