UNIVERSITEIT GENT

Faculteit Wetenschappen
Vakgroep Zuivere Wiskunde en
Computeralgebra

Finite geometrical structures having applications in coding theory and cryptography

Jeroen Schillewaert

Academiejaar 2008-2009

Promotoren: Prof. Dr. L. Storme
Prof. Dr. J.A. Thas

Proefschrift voorgelegd aan de Faculteit Wetenschappen tot het behalen van de graad van Doctor in de Wetenschappen, wiskunde.

Acknowledgements

First of all I want to thank my supervisors Leo Storme and Jef Thas, for their support and encouragement during the past three years. I got the freedom to work on the problems I liked, having the reassuring thought that I could rely on their help if I got stuck. Apart from being very good mathematicians, they patiently read my manuscripts, and greatly improved my mathematical writing skills.

I also want to thank my family, and especially my parents, for their support during all those years and for giving me the opportunity to study.

Without dropping names, since then you risk to forget someone, I would like to thank my friends and colleagues for wonderful times on all sorts of occasions.

Last but not least, I would like to thank the FWO and B-Crypt for financial support, allowing me to present my work at several wonderful places, and giving me the opportunity to meet very nice people.

Jeroen Schillewaert
November 2008

Summary

In this thesis, we study particular finite geometric structures, such as quadrics, Hermitian varieties, Veroneseans,... and their applications in research areas such as coding theory and cryptography. Characterizing these algebraically defined objects in a combinatorial way is an interesting and widely spread habit which dates back to Segre, when he proved his classical result that every oval in $\mathbf{PG}(2, q)$, q odd is a conic. Furthermore, it turns out that finite geometric structures are an excellent tool for the construction of certain cryptographic systems such as secret sharing schemes and authentication codes.

The first chapter is an introductory chapter, where we briefly discuss the geometrical background needed to read this thesis. It consists of a collection of definitions and some important theorems which are used throughout the thesis.

In Chapter 2, we study the applications of the studied finite geometric structures, namely authentication codes and secret sharing schemes. Here the construction of such cryptographic protocols by means of geometric structures is studied. The later Chapters 3 and 4 study the geometric structures themselves.

We start with authentication codes, which are cryptographic systems used to authenticate a person. We list their important parameters and properties, and give a small overview of previous geometrical constructions of them. First we show that generalized Veroneseans can be used to construct generalized dual arcs. Next, it is shown how generalized dual arcs and generalized quadrangles can be used to construct authentication codes and their performance with respect to the above described parameters is discussed.

The second part describes secret sharing schemes, protocols designed for the distribution of a secret amongst a group of people. Several geometric secret sharing schemes, including new ones using Veroneseans are described. Following Massey [40], the link with coding theory is exploited, as it is shown that one can construct secret sharing schemes based on so-called minimal codewords in a linear code.

In Chapter 3, minimal codewords in a particular code, the binary Reed-Muller codes are investigated. It is easy to show that codewords of very small weight are all minimal and codewords of very large weight are all non-minimal. In [5], Borissov, Manev and Nikova considered the first non-trivial case from the lower side. We continue in this fashion, thereby translating the problem into a geometrical one, which concerns the intersection of quadrics and other geometrical objects in projective space.

In the fourth chapter, the quadric Veronesean and the generalized Verone-

sean is studied. Several very good characterization results on the quadric Veronesean are already known for quite some time.

In the first part of the chapter, we are able to obtain an extension and a characterization result for the generalized Veronesean. The proof is quite long and technical, but it relies on and extends one of the characterization results for the quadric Veronesean.

The second part of this chapter forms the bridge to the last chapter of the thesis, since we will study geometric objects by means of their intersection numbers with respect to certain subspaces. Here, the quadric Veronesean is characterized, since we are able to prove the conditions of a structural characterization result of it from the intersection numbers.

The last chapter concerns the study of classical polar spaces by means of intersection numbers, except for the symplectic ones for obvious reasons. First, some previous characterizations using line intersection numbers are given. These are not only of general interest, but in some proofs, they are used. We state a nice characterization result of the parabolic quadric $Q(4,q)$ by Ferri and Tallini [23], which is characterized by means of its intersection numbers with planes and 3-spaces. This theorem is extended in two ways. One direction is to show that one can characterize singular classical polar spaces if one allows all possible intersection numbers with planes and 3-spaces. Only few exceptions, containing a very large singular subspace, are found. The other direction is to extend this result to higher dimension and to consider more generally the intersection numbers with hyperplanes and spaces of codimension 2. No exceptions are found here.

Contents

Chapter 1

Introduction

In this introductory chapter, we give an overview of the geometrical background needed to read this thesis, and we introduce some notations. We do not intend to be complete when discussing some of this background, but we rather try to restrict ourselves to the particular results we will use later on. For those who want to know about particular things, we have included references to standard works.

1.1 Generalized quadrangles

A *finite generalized quadrangle* (**GQ**) of *order* (s,t) is an incidence structure $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathbf{I})$ in which $\mathcal{P}$ and $\mathcal{B}$ are disjoint non-empty sets of objects called *points* and *lines* respectively, and for which $\mathbf{I}$ is a symmetric point-line incidence relation satisfying the following axioms.

(GQ1) Each point is incident with $t+1$ lines $(t \geq 1)$ and two distinct points are incident with at most one common line.

(GQ2) Each line is incident with $s+1$ points $(s \geq 1)$ and two distinct lines are incident with at most one common point.

(GQ3) If p is a point and L is a line not incident with p, then there is a unique point-line pair (q, M) such that $p \,\mathbf{I}\, M \,\mathbf{I}\, q \,\mathbf{I}\, L$.

A generalized quadrangle (**GQ**) of order (s,t) contains $(s+1)(st+1)$ points. If $s = t$, then $\mathcal{S}$ is also said to be of order s.

If $\mathcal{S}$ has a finite number of points and if $s > 1$, it is easy to show one can replace axiom (**GQ**1) by the following axioms.

(GQ1') No point is collinear with all others.

(GQ1”) There is a point on at least two lines.

Sometimes this alternative definition will be used in our proofs.

The classical generalized quadrangles. Consider a non-singular quadric of Witt index 2, that is of projective index 1, in $\mathbf{PG}(3,q)$, $\mathbf{PG}(4,q)$ and $\mathbf{PG}(5,q)$. The points and lines of these quadrics form generalized quadrangles which are denoted by $Q^+(3,q)$, $Q(4,q)$ and $Q^-(5,q)$, and of order $(q,1)$, (q,q) and (q,q^2) respectively. Next, let H be a non-singular hermitian variety in $\mathbf{PG}(3,q^2)$ or $\mathbf{PG}(4,q^2)$. The points and lines of H form a generalized quadrangle $H(3,q^2)$ or $H(4,q^2)$, which has order (q^2,q) or (q^2,q^3) respectively. The points of $\mathbf{PG}(3,q)$ together with the totally isotropic lines with respect to a symplectic polarity form a $\mathbf{GQ}$, denoted by $W(q)$, of order q. The generalized quadrangles defined here are the so-called *classical generalized quadrangles.*

Definition 1.1.1 *Let V be a vector space over some skew field, not necessarily finite-dimensional. A generalized quadrangle $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathbf{I})$ is* fully embedded *in the projective space $\mathbf{PG}(V)$ if there is a map π from $\mathcal{P}$ to the set of points and from $\mathcal{B}$ to the set of lines of $\mathbf{PG}(V)$ such that:*

(i) π is injective on points,

(ii) if $x \in \mathcal{P}$ and $L \in \mathcal{B}$ with $x \,\mathbf{I}\, L$, then $x^\pi \in L^\pi$,

(iii) the set of points x^π, where $x \in \mathcal{P}$, generates $\mathbf{PG}(V)$,

(iv) every point in $\mathbf{PG}(V)$ on the image of a line L of the quadrangle is also the image of a point of that line L of the quadrangle.

The following beautiful theorem is due to Buekenhout and Lefèvre [11].

Theorem 1.1.2 *Every finite generalized quadrangle fully embedded in projective space is classical.*

Point-Line Duality. There is a *point-line duality* for GQs of order (s,t) for which in any definition or theorem the words “point” and “line” are interchanged and also the parameters s and t. (If $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathbf{I})$ is a GQ of order (s,t), $\mathcal{S}^D = (\mathcal{B}, \mathcal{P}, \mathbf{I})$ is a GQ of order (t,s).)

Collinearity/Concurrency/Regularity. Let p and q be (not necessarily distinct) points of the GQ $\mathcal{S}$; we write $p \sim q$ and call these points *collinear*, provided that there is some line L such that $p \,\mathbf{I}\, L \,\mathbf{I}\, q$. Dually, for $L, M \in \mathcal{B}$, we write $L \sim M$ when L and M are *concurrent.*
For $p \in \mathcal{P}$, put

$$p^\perp = \{q \in \mathcal{P} \parallel q \sim p\}$$

(and note that $p \in p^\perp$). For a pair of distinct points $\{p, q\}$, we denote $p^\perp \cap q^\perp$ also by $\{p, q\}^\perp$. Then $|\{p, q\}^\perp| = s + 1$ or $t + 1$, according as $p \sim q$ or $p \not\sim q$, respectively. For $p \neq q$, we define

$$\{p, q\}^{\perp\perp} = \{r \in \mathcal{P} \parallel r \in s^\perp \text{ for all } s \in \{p, q\}^\perp\}.$$

Automorphisms. An *automorphism* of a GQ $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathbf{I})$ is a permutation of $\mathcal{P} \cup \mathcal{B}$ which preserves $\mathcal{P}$, $\mathcal{B}$ and $\mathbf{I}$. The set of automorphisms of a GQ $\mathcal{S}$ is a group, called the *automorphism group* of $\mathcal{S}$, which is denoted by $\mathrm{Aut}(\mathcal{S})$.

SubGQs. A *subquadrangle*, or also *subGQ*, $\mathcal{S}' = (\mathcal{P}', \mathcal{B}', \mathbf{I}')$ of a GQ $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathbf{I})$ is a GQ for which $\mathcal{P}' \subseteq \mathcal{P}$, $\mathcal{B}' \subseteq \mathcal{B}$, and where $\mathbf{I}'$ is the restriction of $\mathbf{I}$ to $(\mathcal{P}' \times \mathcal{B}') \cup (\mathcal{B}' \times \mathcal{P}')$.

Ovoid of a GQ. An *ovoid* of a generalized quadrangle $\mathcal{S}$ is a set $\mathcal{O}$ of points of $\mathcal{S}$ such that each line of $\mathcal{S}$ is incident with a unique point of $\mathcal{O}$.

The following results will sometimes be used without further reference.

Theorem 1.1.3 *[41, 2.2.1] Let $\mathcal{S}'$ be a proper subquadrangle of order (s', t') of the GQ $\mathcal{S}$ of order (s, t). Then either $s = s'$ or $s \geq s't'$. If $s = s'$, then each external point of $\mathcal{S}'$ is collinear with the $st' + 1$ points of an ovoid of $\mathcal{S}'$; if $s = s't'$, then each external point of $\mathcal{S}'$ is collinear with exactly $1 + s'$ points of $\mathcal{S}'$.*

Theorem 1.1.4 *[41, 2.2.2] Let $\mathcal{S}'$ be a proper subquadrangle of the GQ $\mathcal{S}$, where $\mathcal{S}$ has order (s, t) and $\mathcal{S}'$ has order (s, t') (so $t > t'$). Then we have*

(1) *$t \geq s$; if $s = t$, then $t' = 1$.*

(2) *If $s > 1$, then $t' \leq s$; if $t' = s \geq 2$, then $t = s^2$.*

(3) *If $s = 1$, then $1 \leq t' < t$ is the only restriction on t'.*

(4) *If $s > 1$ and $t' > 1$, then $\sqrt{s} \leq t' \leq s$ and $s^{3/2} \leq t \leq s^2$.*

(5) *If $t = s^{3/2} > 1$ and $t' > 1$, then $t' = \sqrt{s}$.*

(6) *Let $\mathcal{S}'$ have a proper subquadrangle $\mathcal{S}''$ of order (s, t''), $s > 1$. Then $t'' = 1$, $t' = s$ and $t = s^2$.*

A lot of information on finite generalized quadrangles can be found in the reference work [41].

1.2 Classical polar spaces

Polar spaces were first described axiomatically by Veldkamp [72]. Later on, Tits simplified Veldkamp's list of axioms and further completed the theory [71]. We recall Tits' definition of polar spaces.

A *polar space of rank* n, $n > 2$, is a point set $\mathcal{P}$ together with a family of subsets of $\mathcal{P}$ called *subspaces*, satisfying the following axioms.

(i) A subspace, together with the subspaces it contains, is a d-dimensional projective space with $-1 \leq d \leq n-1$; d is called the *dimension* of the subspace.

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

(iii) Given a subspace V of dimension $n-1$ and a point $p \in \mathcal{P} \backslash V$, there is a unique subspace W of dimension $n-1$ such that $p \in W$ and $V \cap W$ has dimension $n-2$; W contains all points of V that are joined to p by a subspace of dimension 1, also called a *line*.

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

The polar spaces of rank 2 are by definition the generalized quadrangles. The *finite classical polar spaces* are the following structures.

(i) The non-singular quadrics in odd dimension, $Q^+(2n+1,q), n \geq 1$, and $Q^-(2n+1,q), n \geq 2$, together with the subspaces they contain, give a polar space of rank $n+1$ and n, respectively. The non-singular parabolic quadrics $Q(2n,q), n \geq 2$, in even dimension, together with the subspaces they contain, give a polar space of rank n.

(ii) The non-singular hermitian varieties in $\mathbf{PG}(2n,q^2)$, $n \geq 2$, together with the subspaces they contain, give a polar space of rank n; the non-singular hermitian varieties in $\mathbf{PG}(2n+1,q^2)$, $n \geq 1$, together with the subspaces they contain, give a polar space of rank $n+1$.

(iii) The points of $\mathbf{PG}(2n+1,q), n \geq 1$, together with the totally isotropic subspaces of a non-singular symplectic polarity of $\mathbf{PG}(2n+1,q)$, give a polar space of rank $n+1$.

By theorems of Veldkamp and Tits, all polar spaces with finite rank at least 3 are classified. In the finite case, i.e. the polar space has a finite number of points, the following theorem, which can be found in [71], holds.

Theorem 1.2.1 *A finite polar space of rank at least 3 is classical.*

Buekenhout and Shult described polar spaces as point-line geometries.

Definition 1.2.2 *A* Shult space *is a point-line geometry $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathbf{I})$, with $\mathcal{B}$ a non-empty set of subsets of $\mathcal{P}$ of cardinality at least 2, such that the incidence relation $\mathbf{I}$, which is containment here, satisfies the following axiom. For each line $L \in \mathcal{B}$ and for each point $p \in \mathcal{P} \backslash L$, the point p is collinear with either one or all points of the line L.*

A Shult space is *non-degenerate* if no point is collinear with all other points. A *subspace* of a Shult space $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathbf{I})$ is a subset W of $\mathcal{P}$ such that any two points of W are on a common line and any line containing distinct points of W is completely contained in W. A Shult space is *linear* if two distinct lines have at most one common point. Buekenhout and Shult proved the following fundamental theorem [12]. A Shult space is of finite *rank n* if each chain of distinct subspaces $R_1 \subset R_2 \cdots \subset R_i$ of S has at most n elements.

Theorem 1.2.3 (i) *Every non-degenerate Shult space is linear.*

(ii) *If S is a non-degenerate Shult space of finite rank n at least 3, and if all lines contain at least three points, then the Shult space together with all its subspaces is a polar space.*

Hence we have the following theorem.

Theorem 1.2.4 *Suppose that $\mathcal{S}$ is a non-degenerate Shult space of rank at least 3, such that each line contains at least 3 points. Then $\mathcal{S}$ is isomorphic to the point-line geometry of a finite classical polar space.*

If a Shult space is fully embedded in a projective space then the following theorem follows from Buekenhout and Lefèvre [11], and Lefèvre-Percsy [37, 38].

Theorem 1.2.5 *Suppose $\mathcal{S}$ is a non-degenerate finite Shult space. If $\mathcal{S}$ is fully embedded in a projective space, then $\mathcal{S}$ consists of the points and lines of a finite classical polar space. Here fully embedded means that the set of lines of $\mathcal{S}$ is a subset of the set of lines of the projective space and that the point set of $\mathcal{S}$ is the set of all points contained in these lines.*

1.3 Veroneseans and generalized (dual) arcs

In this section, we define the generalized Veronesean. We give a construction showing that one can associate generalized dual arcs with them. These generalized dual arcs turn out to be excellent tools to construct message authentication codes and secret sharing schemes, which we will explain in Chapter 2.

We start by defining a generalized dual arc.

Definition 1.3.1 *A* generalized dual arc $\mathcal{F}$ *of* degree d *with* dimensions $n = n_0 > n_1 > n_2 > \cdots > n_{d+1} > -1$ *of* $\mathbf{PG}(n,q)$ *is a set of* n_1*-dimensional subspaces of* $\mathbf{PG}(n,q)$ *such that:*

1. *each* j *of these subspaces intersect in a subspace of dimension* n_j*,* $1 \leq j \leq d+1$*,*
2. *each* $d+2$ *of these subspaces have no common intersection.*

We call $(n = n_0, n_1, \ldots, n_{d+1})$ *the* type *of the generalized dual arc.*

An ordinary d-dimensional dual arc in $\mathbf{PG}(n,q)$ has type $(n,d,0)$. A generalized dual arc of degree 0 is a partial n_1-spread.

A (k,n)-*arc* $\mathcal{K}$ in $\mathbf{PG}(2,q)$ is a set of k points such that some line of the plane meets $\mathcal{K}$ in n points but such that no line meets $\mathcal{K}$ in more than n points, where $n \geq 2$. The dual of a (k,n)-arc is a (k,n)-*dual arc*. If $n=2$, we simply use *arc* and *dual arc* respectively.

Example 1.3.2

- *Take a dual arc in a plane* π*. Embed* π *in a 3-dimensional space. Now we have a generalized dual arc of type* $(3,1,0)$*. But the 3-space is not really used.*
- *Take a dual arc with* k *elements in a plane* π*. Embed* π *in a space of dimension* $k+2$ *and choose planes different from* π *through the* k *lines of the dual arc that span* $\mathbf{PG}(2+k,q)$*. This is a generalized dual arc of type* $(k+2,2,0)$*. Even if the planes span* $\mathbf{PG}(2+k,q)$*, the interesting part of the construction is contained in the plane* π*.*
- *The following planes of* $\mathbf{PG}(4,q)$ *form a generalized dual arc of type* $(4,2,0)$*:*

$$\begin{aligned}
\pi_1 &= \{[a,b,c,0,0] \,||\, a,b,c \in \mathbb{F}_q\},\\
\pi_2 &= \{[a,0,b,b,c] \,||\, a,b,c \in \mathbb{F}_q\},\\
\pi_3 &= \{[0,a,b,c,b] \,||\, a,b,c \in \mathbb{F}_q\},\\
\pi_4 &= \{[a,a,0,b,c] \,||\, a,b,c \in \mathbb{F}_q\}.
\end{aligned}$$

The intersection points of π_1 *with the other planes lie on the line* $X_2 = X_3 = X_4 = 0$*. So only that line of* π_1 *is a real part of the generalized dual arc.*

These examples motivate the notion of a regular generalized dual arc. In a characterization result on Veroneseans which we will prove in Chapter 4 even a stronger form of regularity is used.

Definition 1.3.3 *A generalized dual arc $\mathcal{F}$ of degree d and type $(n = n_0, \ldots, n_{d+1})$ is* regular *if, in addition, the n_1-dimensional spaces of $\mathcal{F}$ span* $\mathbf{PG}(n, q)$ *and if it satisfies the property that if π is the intersection of j elements of $\mathcal{F}$, $j \leq d$, then π is spanned by the subspaces of dimension n_{j+1} which are the intersections of π with the remaining elements of $\mathcal{F}$.*

A generalized dual arc is strongly regular *if it is regular and satisfies*

$$\langle \Omega_1, \ldots, \Omega_k \rangle \cap \bigcap_{i=1}^{k'} \Omega'_i = \left\langle \Omega_1 \cap \bigcap_{i=1}^{k'} \Omega'_i, \ldots, \Omega_k \cap \bigcap_{i=1}^{k'} \Omega'_i \right\rangle$$

for all arc elements $\Omega_1, \ldots, \Omega_k, \Omega'_1, \ldots, \Omega'_{k'}$.

Let us recall the definition of the quadric Veronesean $\mathcal{V}_n^{2^n}$.

Definition The *Veronese variety* $\mathcal{V}_n^{2^n}$ of all quadrics of $\mathbf{PG}(n, q)$, $n \geq 1$, is the variety

$$\mathcal{V}_n^{2^n} = \{p(x_0^2, x_1^2, \cdots, x_n^2, x_0x_1, x_0x_2, \cdots, x_{n-1}x_n) \mid\mid (x_0, \cdots, x_n) \in \mathbf{PG}(n, q)\}$$

of $\mathbf{PG}(\frac{n(n+3)}{2}, q)$; this variety has dimension n and order 2^n. The natural number n is called the *index* of $\mathcal{V}_n^{2^n}$.

For the basic properties of Veroneseans we refer to [28].

The image of an arbitrary hyperplane of $\mathbf{PG}(n, q)$ under the Veronesean map is a quadric Veronesean $\mathcal{V}_{n-1}^{2^{n-1}}$, and the subspace generated by it has dimension $N_{n-1} = \frac{(n-1)(n+2)}{2}$. Such a subspace is called a *$\mathcal{V}_{n-1}$-subspace.* In particular for $n = 2$, the $\mathcal{V}_1$-subspaces are called *conic planes.*

The image of a line of $\mathbf{PG}(n, q)$ is a plane conic, and if q is even, then the set of nuclei of all such conics is the Grassmannian of the lines of $\mathbf{PG}(n, q)$ and hence generates a subspace of dimension $\frac{(n-1)(n+2)}{2}$, which we call the *nucleus subspace* of $\mathcal{V}_n^{2^n}$, see [65].

One can also consider the quadric Veronesean from a matrix point of view.

Theorem 1.3.4 *The quadric Veronesean $\mathcal{V}_n^{2^n}$ of* $\mathbf{PG}(n, q)$ *consists of all points $p(y_{0,0}, \cdots, y_{n,n}, y_{0,1}, \cdots, y_{n-1,n})$ of* $\mathbf{PG}(\frac{n(n+3)}{2}, q)$ *for which $[y_{i,j}]$, with $y_{i,j} = y_{j,i}$ for $i \neq j$, is a symmetric matrix of rank 1.*

Let $\mathbf{PG}(V)$ be an n-dimensional space with basis e_i $(0 \leq i \leq n)$.

Let $\mathbf{PG}(W)$ be an $\left(\binom{n+d+1}{d+1} - 1\right)$-dimensional space with basis $e_{i_0,\ldots,i_d}$ $(0 \leq i_0 \leq i_1 \leq \cdots \leq i_d \leq n)$.

Below, we define a map which is a generalization of the quadratic Veronesean map.

The *generalized Veronesean* is the point set which is the image of this map.

We define $\zeta : \mathbf{PG}(V) \to \mathbf{PG}(W)$ by

$$\zeta : [\sum_{i=0}^{n} x_i e_i] \mapsto [\sum_{0 \leq i_0 \leq \cdots \leq i_d \leq n} x_{i_0} \cdots x_{i_d} e_{i_0,\ldots,i_d}].$$

For each permutation σ of $\{0, \ldots, d\}$, let $e_{i_{\sigma(0)},\ldots,i_{\sigma(d)}}$ be equal to $e_{i_0,\ldots,i_d}$, $i_0 \leq i_1 \leq \cdots \leq i_d$.

Construction 1.3.5 *Let $\theta : V^{d+1} \to W$ be the multilinear mapping*

$$\theta : (\sum_{i_0=0}^{n} x_{i_0}^{(0)} e_{i_0}, \ldots, \sum_{i_d=0}^{n} x_{i_d}^{(d)} e_{i_d}) \mapsto \sum_{0 \leq i_0,\ldots,i_d \leq n} x_{i_0}^{(0)} \cdot \ldots \cdot x_{i_d}^{(d)} e_{i_0,\ldots,i_d} \,. \qquad (1.1)$$

For each point $p = (x)$ of $\mathbf{PG}(V)$, we define a subspace $D(p)$ of $\mathbf{PG}(W)$ by

$$D(p) = \langle \theta(x, v_1, \cdots, v_d) \mid\mid v_1, \cdots, v_d \in V \rangle.$$

Theorem 1.3.6 *The set $\mathcal{D} = \{D(p) \mid\mid p \in \mathbf{PG}(V)\}$ is a strongly regular generalized dual arc with dimensions $d_i = \binom{n+d+1-i}{d+1-i} - 1, i = 0, \cdots, d+1$.*

Proof Since θ is a multilinear form we get

$$D(p_0) \cap \ldots \cap D(p_k) = \langle \theta(x_0, \ldots, x_k, v_{k+1}, \ldots, v_d) \mid\mid v_{k+1}, \ldots, v_d \in V \rangle$$

and hence $\mathcal{D}$ is a generalized dual arc with the specified dimensions (see also [35]).

To see that $\mathcal{D}$ is strongly regular, a calculation yields that

$$\langle D(p_1), \ldots, D(p_k) \rangle = \langle \theta(x, v_1, \ldots, v_d) \mid\mid x \in \langle x_1, \ldots, x_k \rangle, v_1, \ldots, v_d \in V \rangle$$

$$\langle D(p_1), \ldots, D(p_k) \rangle \cap (D(p'_1) \cap \ldots \cap D(p'(k'))) = \\ \langle \theta(x, x'_1, \ldots, x'_{k'}, v_{k'+1}, \ldots, v_d) \mid\mid x \in \langle x_1, \ldots, x_k \rangle, v_{k'+1}, \ldots, v_d \in V \rangle \,.$$

Since θ is a multilinear form

$$\langle \theta(x, x'_1, \ldots, x'_{k'}, v_{k'+1}, \ldots, v_d) \mid\mid x \in \langle x_1, \ldots, x_k \rangle, v_{k'+1}, \ldots, v_d \in V \rangle = \\ \langle \langle \theta(x_i, x'_1, \ldots, x'_{k'}, v_{k'+1}, \ldots, v_d) \mid\mid, v_{k'+1}, \ldots, v_d \in V \rangle \mid\mid i = 1, \ldots, k \rangle$$

and this is exactly the definition of strongly regular. □

If $\frac{q^{n+1}-1}{q-1} \geq \binom{n+d+1}{d+1}$ there is an alternative construction. That these two constructions are equivalent is proved in Lemma 6 of [73] for the case $d = 1$. The general proof is completely similar.

Construction 1.3.7 *With b and B respectively, we denote the standard scalar product of V and W, i.e.,*

$$b(\sum_{i=0}^{n} x_i e_i, \sum_{i=0}^{n} y_i e_i) = \sum_{i=0}^{n} x_i y_i,$$

and

$$B(\sum_{0\leq i_0 \leq \cdots \leq i_d \leq n} x_{i_0,\ldots,i_d} e_{i_0,\ldots,i_d}, \sum_{0\leq i_0 \leq \cdots \leq i_d \leq n} y_{i_0,\ldots,i_d} e_{i_0,\ldots,i_d}) =$$

$$\sum_{0\leq i_0 \leq \cdots \leq i_d \leq n} x_{i_0,\ldots,i_d} y_{i_0,\ldots,i_d}.$$

For each $x \in V$, we denote by $x^\perp$ the subspace of V perpendicular to x with respect to b. So

$$x^\perp = \{y \in V \mid\mid b(x,y) = 0\}.$$

Then

$$D(p) = \{[z] \in \mathbf{PG}(W) \mid\mid B(z, \zeta(y)) = 0 \textit{ for all } y \in x^\perp\}. \tag{1.2}$$

We call the arcs $\mathcal{D}$ defined by Construction 1.3.5 *Veronesean dual arcs*. Below, we give two examples of our general construction.

Example 1.3.8 *Starting with $\mathbf{PG}(2,q)$, the mapping $\zeta : \mathbf{PG}(2,q) \to \mathbf{PG}(5,q)$ with*

$$\zeta([x_0, x_1, x_2]) = [x_0^2, x_1^2, x_2^2, x_0x_1, x_0x_2, x_1x_2]$$

defines the quadric Veronesean $\mathcal{V}_2^4$.

If $p = [a, b, c]$, the planes $D(p)$ defined above have the representation

$$D(p) = \{[ax_0, bx_1, cx_2, ax_1 + bx_0, ax_2 + cx_0, bx_2 + cx_1] \mid\mid x_0, x_1, x_2 \in \mathbb{F}_q\}\ .$$

These planes form a strongly regular generalized dual arc of $q^2 + q + 1$ planes of type $(5, 2, 0)$.

Example 1.3.9 *The map* $\zeta : \mathbf{PG}(2,q) \to \mathbf{PG}(9,q)$ *with*

$$\zeta([x_0,x_1,x_2]) = [x_0^3, x_1^3, x_2^3, x_0^2x_1, x_0^2x_2, x_1^2x_0, x_1^2x_2, x_2^2x_0, x_2^2x_1, x_0x_1x_2]$$

defines a cubic Veronesean. Construction 1.3.5 associates to each of the q^2+q+1 *points of* $\mathbf{PG}(2,q)$ *a* 5*-dimensional space in* $\mathbf{PG}(9,q)$*. Each two of these* 5*-spaces intersect in a plane. Each three* 5*-spaces share a common point and each four* 5*-spaces have an empty intersection.*

Three of the q^2+q+1 5-spaces are:

$$\begin{aligned}
\pi_0 &:= D([1,0,0]) = \{[e_0,0,0,e_1,e_2,e_3,0,e_4,0,e_5] \mid\mid e_i \in \mathbb{F}_q\},\\
\pi_1 &:= D([0,1,0]) = \{[0,e_0,0,e_1,0,e_2,e_3,0,e_4,e_5] \mid\mid e_i \in \mathbb{F}_q\},\\
\pi_2 &:= D([0,0,1]) = \{[0,0,e_0,0,e_1,0,e_2,e_3,e_4,e_5] \mid\mid e_i \in \mathbb{F}_q\}.
\end{aligned}$$

The intersections of π_i with the other q^2+q 5-spaces are planes, $i=0,1,2$. These planes are part of the generalized dual arc described in Example 1.3.8.

For π_0, the corresponding Veronesean has the following form

$$\mathcal{V}_0 := [x_0^2, 0, 0, x_0x_1, x_0x_2, x_1^2, 0, x_2^2, 0, x_1x_2].$$

To this Veronesean $\mathcal{V}_0$ Construction 1.3.5 associates q^2+q+1 planes; where q^2+q of these planes are intersections of π_0 with the other 5-spaces. The extra plane has the form

$$E_0 := \{[e_0,0,0,e_1,e_2,0,0,0,0,0] \mid\mid e_0,e_1,e_2 \in \mathbb{F}_q\} .$$

Similarly, we see in π_1 the Veronesean

$$\mathcal{V}_1 := [0, x_1^2, 0, x_0^2, 0, x_0x_1, x_1x_2, 0, x_2^2, x_0x_2]$$

and the extra plane

$$E_1 := \{[0,e_0,0,0,0,e_1,e_2,0,0,0] \mid\mid e_0,e_1,e_2 \in \mathbb{F}_q\},$$

and in π_2, we have the Veronesean

$$\mathcal{V}_2 := [0, 0, x_2^2, 0, x_0^2, 0, x_1^2, x_0x_2, x_1x_2, x_0x_1]$$

and the extra plane

$$E_2 := \{[0,0,e_0,0,0,0,0,e_1,e_2,0] \mid\mid e_0,e_1,e_2 \in \mathbb{F}_q\} .$$

Also to construct secret sharing schemes the previous constructions are very well-suited as we will show in Chapter 2. Actually, we don't apply generalized dual arcs directly. But the dual of these structures, which we call *generalized arcs.*

Definition 1.3.10 *A* generalized arc $\mathcal{A}$ *of degree* d *with dimensions* $n_1 < n_2 < \cdots < n_{d+1}$ *of* $\mathbf{PG}(n,q)$ *is a set of* n_1*-dimensional subspaces of* $\mathbf{PG}(n,q)$ *such that:*

1. *each* j *of these subspaces generate a subspace of dimension* n_j, $1 \leq j \leq d+1$,

2. *each* $d+2$ *of these subspaces span* $\mathbf{PG}(n,q)$.

We call $(n, n_1, \ldots, n_{d+1})$ *the* type *of the generalized arc.*

If in addition the common intersection of all n_{j+1}*-dimensional subspaces spanned by* $j+1$ *elements of the arc containing a given* n_j*-dimensional subspace* π *spanned by* j *elements of the arc is equal to* π*, we call the arc* regular.

Theorem 1.3.11 *The dual of a generalized arc of type* $(n, n_1, \ldots, n_{d+1})$ *is a generalized dual arc of type* $(n, n-1-n_1, \ldots, n-1-n_{d+1})$ *and vice versa.*

Furthermore, the dual arc is regular if and only if the arc is regular.

Proof Dualising in $\mathbf{PG}(n,q)$ maps every k-dimensional subspace onto an $(n-1-k)$-dimensional subspace. Dualising exchanges the concepts "span" and "intersection". □

Dual to Construction 1.3.5, we have the following construction of generalized arcs.

Construction 1.3.12 *As in Construction 1.3.5, let* $\mathbf{PG}(V)$ *be an* n*-dimensional space with basis* e_i $(0 \leq i \leq n)$.

Let $\mathbf{PG}(W)$ *be a* $\left(\binom{n+d+1}{d+1} - 1\right)$*-dimensional space with basis* $e_{i_0,\ldots,i_d}$ $(0 \leq i_0 \leq i_1 \leq \cdots \leq i_d \leq n)$.

We define $\zeta : \mathbf{PG}(V) \rightarrow \mathbf{PG}(W)$ *by*

$$\zeta : [\sum_{i=0}^{n} x_i e_i] \mapsto [\sum_{0 \leq i_0 \leq \cdots \leq i_d \leq n]} x_{i_0} \cdot \ldots \cdot x_{i_d} e_{i_0,\ldots,i_d}] \ .$$

With b *and* B *respectively, we denote the standard scalar product of* V *and* W*, i.e.,*

$$b(\sum_{i=0}^{n} x_i e_i, \sum_{i=0}^{n} y_i e_i) = \sum_{i=0}^{n} x_i y_i,$$

and

$$B(\sum_{0 \leq i_0 \leq \cdots \leq i_d \leq n} x_{i_0,\ldots,i_d} e_{i_0,\ldots,i_d}, \sum_{0 \leq i_0 \leq \cdots \leq i_d \leq n} y_{i_0,\ldots,i_d} e_{i_0,\ldots,i_d}) = \sum_{0 \leq i_0 \leq \cdots \leq i_d \leq n} x_{i_0,\ldots,i_d} y_{i_0,\ldots,i_d}.$$

For each $x \in V$, we denote by $x^\perp$ the subspace of V perpendicular to x with respect to b. So

$$x^\perp = \{y \in V \mid\mid b(x,y) = 0\}.$$

For each point $p = [x]$ of $\mathbf{PG}(V)$, we define a subspace $A(p)$ of $\mathbf{PG}(W)$ by

$$A(p) = \left\langle \zeta(y) \mid\mid y \in x^\perp \right\rangle. \tag{1.3}$$

Theorem 1.3.13 *The set $\mathcal{A} = \{A(p) \mid\mid p \in \mathbf{PG}(n,q)\}$, defined in Construction 1.3.12, is a generalized arc of type $n_i = \binom{n+d+1}{d+1} - \binom{n+d+1-i}{d+1-i} - 1$, $i = 1, \ldots, d+1$.*

The generalized dual arc described in Construction 1.3.5 is the dual of that arc.

Proof By definition (check equation (1.2)) we have $D(p) = A(p)^\perp$ with respect to the bilinear form B. Since B is a non-degenerate form, this means that $D(p)$ is dual to $A(p)$. Thus we may apply Theorem 1.3.11, which together with Theorem 1.3.6 shows that $\mathcal{A}$ is indeed a generalized arc. □

Remark 1.3.14 *The elements $A(p)$ are exactly the $\mathcal{V}_{n-1}$-subspaces defined above. Hence the set $\mathcal{D}$ of Construction 1.3.5 is the dual of the set of $\mathcal{V}_{n-1}$-subspaces.*

1.4 Blocking sets

A *blocking set B* in $\Pi = \mathbf{PG}(2,q)$ is a set of points of Π which meets every line. A line is an example of a blocking set, but a blocking set containing a line is called *trivial.*

A blocking set is called *minimal* if for every $p \in B$, the point set $B \setminus \{p\}$ is not a blocking set. It is easy to prove the following useful lemma.

Lemma 1.4.1 *A blocking set B is minimal if and only if for every point p of B, there is some line L such that $B \cap L = \{p\}$.*

A blocking set containing k points is called a *blocking k-set.* The following theorem gives an upper and a lower bound on the size of a non-trivial minimal blocking set. First we need two definitions.

Definition 1.4.2 *A* unital *of $\mathbf{PG}(2,q^2)$ is a set of q^3+1 points in $\mathbf{PG}(2,q^2)$ intersecting every line of $\mathbf{PG}(2,q^2)$ in either 1 or $q+1$ points.*

Definition 1.4.3 *Consider* $\Pi := \mathbf{PG}(n, q^2)$*. Let* $\mathcal{B} = (\mathcal{P}, \mathcal{L}, \mathbf{I})$ *be a geometry isomorphic to* $\mathbf{PG}(n, q)$*, whose point set* $\mathcal{P}$ *is a subset of the point set of* Π*, whose line set is a subset of the line set of* Π *and whose incidence is inherited from* Π*. Then the geometry* $\mathcal{B}$ *is called a* Baer subgeometry *of* Π*.*

Theorem 1.4.4 *Let* B *be a non-trivial minimal blocking set in* $\mathbf{PG}(2, q)$*. Then*

(i) $|B| \geq q + \sqrt{q} + 1$ *with equality if and only if* q *is a square and* B *is a Baer subplane [8].*

(ii) $|B| \leq q\sqrt{q} + 1$ *with equality if and only if* q *is a square and* B *is a unital [10].*

Next, let us consider multiple blocking sets.

Definition 1.4.5 *An* s-fold blocking set *in* $\mathbf{PG}(2, q)$ *is a set of points of* $\mathbf{PG}(2, q)$ *that intersects every line in at least* s *points. It is called* minimal *if no proper subset is an* s*-fold blocking set.*

A 1-fold blocking set is a blocking set. The following theorem shows that if $s > 1$, then in order to find s-fold blocking sets of small cardinality, one must look for sets not containing a line.

Theorem 1.4.6 *Let* B *be an* s*-fold blocking set of* $\mathbf{PG}(2, q), s > 1$*.*

(i) *If* B *contains a line, then* $|B| \geq sq + q - s + 2$ *[9].*

(ii) *If* B *does not contain a line, then* $|B| \geq sq + \sqrt{sq} + 1$ *[2] .*

For small s, this theorem can be improved, and if s is small and q is a square the smallest minimal s-fold blocking sets are classified [3]. Finally we introduce blocking sets in higher dimensional spaces.

Definition 1.4.7 *A* blocking set with respect to t-spaces *in* $\mathbf{PG}(n, q)$ *is a set* B *of points such that every* t*-dimensional subspace of* $\mathbf{PG}(n, q)$ *meets* B *in at least one point.*

The following result of Bose and Burton gives a nice characterization of the smallest ones [7].

Theorem 1.4.8 *If* B *is a blocking set with respect to* t*-spaces in* $\mathbf{PG}(n, q)$ *then* $|B| \geq |\mathbf{PG}(n - t, q)|$ *and equality holds if and only if* B *is an* $(n - t)$*-dimensional subspace.*

1.5 Arcs and caps in $\mathbf{PG}(n,q)$

1.5.1 Arcs and caps in projective spaces of small dimension

We begin with the classical definition of arcs in $\mathbf{PG}(2,q)$.

Definition 1.5.1 *A* k-arc *of* $\mathbf{PG}(2,q)$ *is a set of* k *points, no three collinear. Let* $m(2,q)$ *denote the maximal size of a* k*-arc in* $\mathbf{PG}(2,q)$*.*

We state the Bose result on the maximum size of a k-arc in $\mathbf{PG}(2,q)$ [6].

Theorem 1.5.2 *If* q *is odd, then* $m(2,q) = q+1$*. If* q *is even, then* $m(2,q) = q+2$*.*

Definition 1.5.3 *A* k-cap *in* $\mathbf{PG}(n,q)$ *is a set of* k *points in* $\mathbf{PG}(n,q)$*, no three of which are collinear.*

The size of a k-cap in $\mathbf{PG}(3,q)$ is bounded. For q even in [6] and for q odd in [43].

Theorem 1.5.4 *If* K *is a* k*-cap of* $\mathbf{PG}(3,q)$*, then* $k \leq q^2+1$ *for* $q>2$*, and* $k \leq 8$ *for* $q=2$*.*

Definition 1.5.5 *A* (q^2+1)*-cap of* $\mathbf{PG}(3,q)$*,* $q>2$*, is called an* ovoid*; an* ovoid of $\mathbf{PG}(3,2)$ *is a set of 5 points of* $\mathbf{PG}(3,2)$ *no four of which are coplanar. A* $(q+1)$*-arc of* $\mathbf{PG}(2,q)$ *is called an oval.*

Lemma 1.5.6 *Consider a set* K *of points in* $\mathbf{PG}(4,q)$*. Suppose all planes intersect* K *in* 1*,* $q+1$ *or* $2q+1$ *points. If* K *is a cap in* $\mathbf{PG}(4,q)$*, then* $|K| \leq q^3+1$*.*

Proof Consider a line L intersecting K in 2 points and consider all planes through L in $\mathbf{PG}(4,q)$. These planes cannot intersect K in $2q+1$ points, by Theorem 1.5.2. Hence, K contains at most

$$(q^2+q+1)(q-1)+2 = q^3+1$$

points. □

1.5.2 Arcs and caps in higher dimensional projective spaces

Next, we give the general definition of arcs in $\mathbf{PG}(n, q)$. These objects are of importance since they have applications in coding theory. In Chapter 4 we will use properties of these arcs.

Definition 1.5.7 *A* $(k; r, s; n, q)$-set $\mathcal{K}$ *is defined to be a set of* k *points in* $\mathbf{PG}(n, q)$ *with at most* r *points in any* s*-space and such that* $\mathcal{K}$ *is not contained in a proper subspace. Furthermore, the set* $\mathcal{K}$ *is* complete *if it is not contained in a* $(k + 1; r, s; n, q)$*-set. In particular, a* $(k; n, n - 1; n, q)$*-set is a* k*-set not contained in a hyperplane with at most* n *points in any hyperplane of* $\mathbf{PG}(n, q)$ *and is also called a* k-arc.

An important question is to find the maximum value $m(r, s; n, q)$ of k for a k-arc in $\mathbf{PG}(n, q)$. We will consider only the maximum value for a k-arc here and we denote it by $m(n, q)$. The theorem which we state below is certainly not the best one known, but it is sufficient for the results obtained in this thesis.

Theorem 1.5.8 *In* $\mathbf{PG}(3, q), q > 3$, $m(3, q) = q + 1$. *In* $\mathbf{PG}(4, q), q \geq 5$,

$$m(4, q) = q + 1.$$

For $q \geq 5, n \geq 5$,

$$m(n, q) \leq q + n - 3.$$

If $q \leq n$*, then* $m(n, q) = n + 2$.

Chapter 2

Message authentication codes and secret sharing schemes

In this chapter we discuss two important applications of the geometrical objects which are considered in this work, *authentication codes* and *secret sharing schemes*.

Firstly, authentication codes are discussed. They serve to authenticate for example the sender of a message. They are used in situations where a malicious intruder could send fake information or in situations where sender and receiver don't trust each other, for instance on the stock market.

The second part of the chapter discusses secret sharing schemes. These are designed to distribute a secret among a group of people such that only a limited number of subsets of this group can reconstruct the secret. They are used in environments where you don't want a single person to have all knowledge about some secret. At the end of this chapter we briefly describe a secret sharing scheme coming from a linear code. Here, the concept of a minimal codeword is introduced, linking this chapter to the next one, where minimal codewords in the binary Reed-Muller code will be discussed.

The results of this chapter are based on parts of the articles [45], [44], [35], [36] and [46].

2.1 Authentication codes

Authentication codes were introduced by Simmons in [53]. A good survey of the current status can be found in [42]. We start by explaining what authentication codes with and without arbitration are and mention some important properties of them. We illustrate these concepts by showing some easy known schemes. Next we show how generalized dual arcs can serve as a tool to construct authentication codes. Finally, we will briefly discuss some other geometric authentication schemes and how the schemes we constructed perform in comparison with them with regard to the properties described in the beginning of this chapter.

2.1.1 What is authentication?

Authentication is very important in information security, for instance when Alice and Bob try to exchange messages. It provides protection against malicious persons trying to change messages or to impersonate the sender of these messages. There are two main models:

- one where Alice and Bob trust each other, called *A-codes*;
- one where they do not, called *A^2-codes*.

In the latter case, an *arbiter* is needed.

We denote the set of all source states (messages) by $\mathcal{S}$, the set of keys by $\mathcal{K}$, the set of encoding rules by $\mathcal{E}$ and the set of all possible encoded messages (tags) by $\mathcal{M}$. The authentication scheme is denoted as $\mathcal{A} = (\mathcal{S}, \mathcal{M}, \mathcal{E})$ and the set of messages corresponding with an encoding rule by $\mathcal{M}(e)$.

In the A-model, sender Alice and receiver Bob agree upon a secret private key k. With each key, a unique encoding rule e is associated, which is a mapping from $\mathcal{S}$ to $\mathcal{M}$. Alice selects a source state s and encodes s into an encoded message m using the encoding rule e corresponding with the chosen key k. Upon receiving m, Bob checks whether it lies in the image of e. If it does, then the message is accepted as authentic. Bob can recover the possible source states as the preimage of the message m under e. If this preimage is always unique, then we say the code is *Cartesian*. So once the encoded message is observed, one can retrack the corresponding source state. Whence there is no secrecy involved here.

An opponent can try to construct a message lying in $e(\mathcal{S})$ after observing r valid messages. The probability of success of such a spoofing attack will be denoted by P_r.

In the A^2-model, we assume that Alice and Bob do not trust each other. In this case, they do not agree upon an encoding rule. Instead, a trusted person, the *arbiter*, is also involved in the scheme. Now Alice has a set of encoding rules $\mathcal{E}_T$, and Bob a set of decoding rules $\mathcal{E}_R$. If Alice and Bob want to communicate, Bob chooses a decoding rule $f \in \mathcal{E}_R$ and sends it to the arbiter. For every given f and given source state s, there is a set of valid messages $\mathcal{M}(s, f)$. On receipt of f, the arbiter selects one message $m(s, f)$ out of $\mathcal{M}(s, f)$, hereby forming an encoding rule $e \in \mathcal{E}_T$ which maps a source state s to the chosen message $m(s, f)$. The arbiter sends this encoding rule e secretly to Alice. In this case, the encoding rule e is valid for the decoding rule f. When Bob receives a message, he checks whether it is in some subset $\mathcal{M}(s, f)$. If so, he accepts it as a valid one and he can retrieve the corresponding source state. If there is a dispute between Alice and Bob about a message m, the arbiter checks if m is valid for the encoding rule given to the transmitter.

Below, we define the attack probabilities for both the A-model and the A^2-model more formally. We start with the A-model. As in [42], we will use the "worst case definition". Denote a set of r observed messages as $m^r = (m_1, \cdots, m_r)$ and the set of all sets of r observed messages as $\mathcal{M}_r$. Let $P(m^r)$ be the probability that one has observed m^r after r messages. Furthermore, let $P(m|m^r)$ be the probability that the message m is valid given that m^r has been observed. Then we define the *attack probability* P_{O_r} of the opponent as follows.

$$P_{O_r} = \sum_{m^r \in \mathcal{M}_r} P(m^r) \mathrm{max}_{m \in \mathcal{M}} P(m|m^r).$$

If we assume a uniform probability distribution for the messages, then we get

$$P_{O_r} = \mathrm{max}_{m \in \mathcal{M}} P(m|m^r).$$

Introduce the following notation:

$$\mathcal{E}(m^r) = \{e \in \mathcal{E} \parallel m_i \in e(\mathcal{S}), 1 \leq i \leq r\}.$$

Denote by m'^r the set of $r+1$ messages m^r and m'. Then

$$P_{O_r} = \frac{|\mathcal{E}(m^r)|}{|\mathcal{E}(m'^r)|}.$$

In the A^2-model, three types of attacks have to be considered. The first one is the spoofing attack by the opponent such as in the A-model. The other two attacks are the spoofing attack T by Alice, sending a message and then claiming not to have sent it, and the spoofing attack by Bob, claiming to have received a message from Alice while this is not the case. One denotes the corresponding probabilities by P_{O_r}, P_{R_r} and P_T respectively.

The opponent's *attack probability* P_{O_r} is defined as in the A-model.

Let $P(f)$ denote the probability of a decoding rule f, and let $P(m|f, m^r)$ denote the probability of the event that the message m could be valid for the encoding rule used by the transmitter, given the decoding rule f and the first r messages $m^r = (m_1, \ldots, m_r)$. The *spoofing attack probability* of the receiver is then defined as

$$P_{R_r} = \sum_{f \in \mathcal{E}_R} P(f) \sum_{m^r \in \mathcal{M}^r} P(m^r|f)\max_{m \in \mathcal{M}} P(m|f, m^r).$$

Let $P(e)$ denote the probability of an encoding rule e, and let $P(m'|e)$ denote the probability of the event that the message $m' \in \mathcal{M}'(e)$ is acceptable for the receiver, given the encoding rule e. The *spoofing attack probability* of the transmitter is then defined as

$$P_T = \sum_{e \in \mathcal{E}_T} P(e)\max_{m' \in \mathcal{M}'(e)} P(m'|e).$$

If we assume a uniform probability distribution on the messages, the formulas reduce in the same way as for the A-codes.

2.1.2 Previously known results

Combinatorial bounds. If we denote $|\mathcal{S}| = k$, $|\mathcal{M}| = v$, and by $\overline{\mathcal{M}^r}$ the set of r-tuples of elements of $\mathcal{M}$ and if we have observed r messages, then we have the following theorem [42, Proposition 3.3, pp. 36].

Theorem 2.1.1 *We have*

$$P_{O_r} \geq \frac{k-r}{v-r}.$$

Equality holds if and only if

$$P(m|m^r) = \frac{k-r}{v-r}$$

is satisfied for any $m^r = (m_1, \ldots, m_r) \in \overline{\mathcal{M}^r}$ *and any* $m \in \mathcal{M}$ *with* $m \neq m_i, 1 \leq i \leq r$.

Naturally, the number of encoding and decoding rules is lower bounded if one wants to construct good schemes.

For authentication without arbitration, we have the following result [42, Corollary 3.1, pp. 21].

Theorem 2.1.2 *If an authentication code has attack probabilities* $P_{O_r} = 1/n_r$ *(*$0 \leq r \leq l$*) for the opponent then* $|\mathcal{E}| \geq n_0 \cdot \cdots \cdot n_l$.

If equality holds, the authentication code is called *perfect*.

We have the following lower bounds on the number of encoding and decoding rules for a scheme with arbitration [42, Proposition 4.5, pp. 47].

Theorem 2.1.3

$$|\mathcal{E}_R| \geq (P_{O_0}P_{O_1}\cdots P_{O_{t-1}}P_T)^{-1},$$

$$|\mathcal{E}_T| \geq (P_{O_0}P_{O_1}\cdots P_{O_{t-1}}P_{R_0}P_{R_1}\cdots P_{R_{t-1}})^{-1}.$$

If equality holds in both inequalities above, then we call the arbitration scheme *t-fold perfect*.

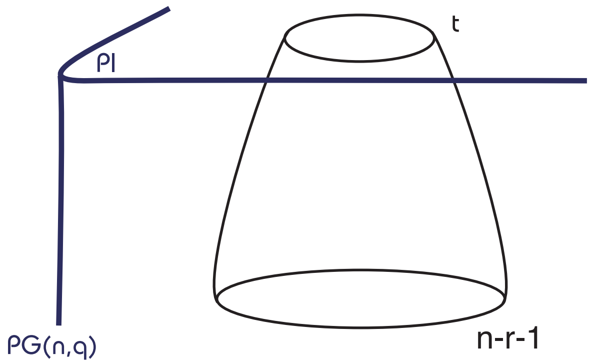
2.1.3 Examples of authentication schemes

All sorts of mathematics can be used to construct message authentication codes. Here we will focus primarily on schemes based on finite geometry. Most of the time, only the ideas behind the scheme are described, and not the actual calculations. For the schemes we proposed ourselves, more detail is provided.

Schemes without arbitration

The first scheme is a generalization of the first MAC scheme by Gilbert-MacWilliams-Sloane [24]. This scheme nicely illustrates the concept of authentication.

Fix an r-dimensional subspace Π_r in $\mathbf{PG}(n,q)$ where $1 \leq r \leq n-1$. All t-dimensional subspaces, $0 \leq t < r$, contained in Π_r are regarded as source states (messages). All $(n-r-1)$-dimensional subspaces which are skew from Π_r are regarded as keys. All $(n-r+t)$-dimensional spaces which intersect Π_r in a t-dimensional space are regarded as encoded messages (tags). A source state s together with a key k is encoded into the tag m, which is the space spanned by s and k.



If Eve wants to cheat, she has to produce a space which contains the space spanned by the key completely. She can do this by guessing the key. If she chooses a source state s, then all $(n-r-1)$-spaces inside the space generated by s and k are good guesses. After having seen one (source state, tag) pair, Eve knows the key lies in the tag space, so her chances to cheat will increase. We assume she can pick any source state she likes if she wants to cheat, except for the ones already used (so we exclude a so-called *replay attack*). Clearly the chance for her to achieve her goal will be the greatest if her chosen source state has a $(t-1)$-dimensional intersection space with the source state she has seen, since then the chance that the key is contained in her tag space is the greatest. If one performs the actual calculations, this yields that this scheme defines a Cartesian authentication scheme with $P_0 = q^{-(n-r)(r-t)}$, and $P_1 = q^{-(n-r)}$.

Now we show how to use generalized dual arcs to construct perfect MAC's.

Theorem 2.1.4 *Let Π be a hyperplane of $\mathbf{PG}(n+1,q)$ and let $\mathcal{D}$ be a generalized dual arc of degree d in Π of type $(n, n_1, \ldots, n_{d+1})$.*

The elements of $\mathcal{D}$ are the messages and the points of $\mathbf{PG}(n+1,q)$ not in Π are the keys. The authentication tag that belongs to a message and a key is the generated (n_1+1)-dimensional subspace.

This defines a perfect MAC of order $r = d+1$ with attack probabilities

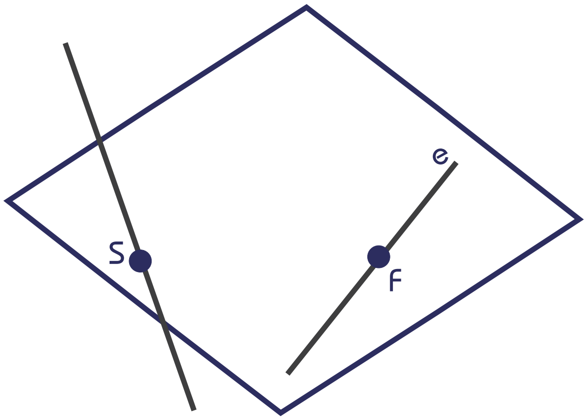
$$P_i = q^{n_{i+1}-n_i}.$$

Proof After i message tag pairs $(m_1,t_1),\ldots,(m_i,t_i)$ have been sent, the attacker knows that the key must lie in the (n_i+1)-dimensional space $\pi = t_1 \cap \cdots \cap t_i$. This space contains q^{n_i+1} different keys. A message m_{i+1} intersects $m_1 \cap \cdots \cap m_i$ in an n_{i+1}-dimensional space π'. Two keys K and $\bar{K}$ generate the same authentication tag if and only if K and $\bar{K}$ generate together with π' the same $(n_{i+1}+1)$-dimensional space. Thus the keys form groups of size $q^{n_{i+1}+1}$ and keys from the same group give the same authentication tag.

The attacker has to guess the correct group. The probability to guess the correct group is $P_i = q^{n_{i+1}+1}/q^{n_i+1}$. □

Arbitration schemes

The scheme below is due to Johansson [33]. Take a fixed line L in $\mathbf{PG}(3,q)$. The points on L are regarded as the source states. The decoding rules are the points not on L, and the encoding rules are the lines not intersecting L. The messages are planes spanned by a source state and an encoding rule. When Alice and Bob want to communicate, Bob chooses a decoding rule F and hands it to the arbiter. The arbiter chooses an encoding rule e which contains F and hands e to Alice. If Alice wants to transmit a message, she chooses a source state S and sends S and the plane $\langle S, e\rangle$ to Bob. In case of a dispute, the arbiter checks if the encoding rule he gave to Alice is contained in the transmitted plane. If this is the case, he decides Alice has sent the message, otherwise he decides it was someone else. This defines a 2-fold perfect Cartesian code with $P_0 = P_1 = \frac{1}{q}$.



Next we show how generalized dual arcs can be used to construct a MAC with arbitration.

Consider the space Π_n spanned by a generalized dual arc of type $(n = n_0, n_1, \ldots, n_{l+1})$ and embed Π_n in an $(n+2)$-dimensional space Π_{n+2}. The source states are the n_1-dimensional spaces which are the elements of the generalized dual arc, the decoding rules are the points in $\Pi_{n+2} \backslash \Pi_n$, the encoding rules are the lines in Π_{n+2} which are skew to Π_n, and the encoded messages are the $(n_1 + 2)$-dimensional spaces generated by a source state and an encoding rule. We assume that Alice and Bob do not trust each other. When Alice and Bob want to communicate, Bob chooses a point p in $\Pi_{n+2} \backslash \Pi_n$ as decoding rule and sends it to a trusted arbiter. The arbiter picks one of the lines L through p skew to Π_n as encoding rule and sends it to Alice. When receiving an $(n_1 + 2)$-dimensional space Π_{n_1+2}, Bob checks if $p \in \Pi_{n_1+2}$. If this is the case then he accepts the message, else he does not.

The goal for an opponent Eve is thus to produce a pair (Π_{n_1}, Π_{n_1+2}) such that $p \in \Pi_{n_1+2}$.

If there is a dispute between Alice and Bob about a valid message, then the arbiter checks if the encoding rule which he handed to Alice is contained in Π_{n_1+2}. If this is the case, then he decides that Alice has sent the message, else that she has not.

If Alice wants to fool Bob, she has to produce an $(n_1 + 2)$-dimensional space containing p but not L. If Bob wants to fool Alice, he has to produce an $(n_1 + 2)$-dimensional space which contains the line L.

The number of encoding rules for the transmitter is the number of lines skew to Π_n, this is equal to $|\mathcal{E}_T| = q^{2n_0+2}$. The number of decoding rules is the number of points in $\Pi_{n+2}\backslash\Pi_n$, this is $|\mathcal{E}_R| = (q+1)q^{n_0+1}$.

If an opponent wants to cheat, he has to produce an (n_1+2)-space containing the point p. His chance to do so after having seen i pairs is $P_{O_i} = q^{n_i - n_{i-1}}$.

If Alice wants to fool Bob, she has to guess which point p on L is Bob's decoding rule. Hence, she has a chance $P_T = \frac{1}{q+1}$.

If Bob wants to fool Alice, he has to produce an (n_1+2)-space containing L. After seeing i pairs, this chance is equal to $q^{n_i - n_{i-1}}$.

Comparing with the lower bounds above, this scheme is perfect.

Schemes from generalized quadrangles (GQs)

The first scheme is due to De Soete [16].

Let p be a fixed point of a GQ of order (s,t). The $t+1$ lines of the GQ through p are the source states, the points not collinear with p are the keys, and the points collinear with, but different from p are the messages. If Alice wants to send a message to Bob, she chooses one of the lines L of the GQ through p. If the key is the point k, then by (GQ3) there is a unique point r on L collinear with k. Alice sends the pair (L,r) to Bob. When receiving a (line, point)-pair, Bob checks if the point r is collinear with k. If and only if this is the case, he decides Alice has sent the message.

Theorem 2.1.5 *The De Soete scheme yields a Cartesian authentication code with*

$$|\mathcal{S}| = t+1,\ |\mathcal{M}| = (t+1)s,\ |\mathcal{E}| = ts^2.$$

Furthermore, $P_0 = P_1 = \frac{1}{s}$.

The two schemes below are joint work with K. Thas [46].

Suppose $\mathcal{S}$ is a GQ of order (s,t). Suppose $\mathcal{S}'$ is a subGQ of $\mathcal{S}$ of order $(s,t/s)$; then an easy counting exercise shows that each line of $\mathcal{S}$ meets $\mathcal{S}'$ in either 1 or $s+1$ points.

Let x be a point of $\mathcal{S}\setminus\mathcal{S}'$; then the $t+1$ points of $\mathcal{S}'$ which are collinear with x (and which respectively correspond to the lines incident with x by the previous property) are two by two non-collinear; since $t+1 = s\cdot t/s+1$, this means that these points form an *ovoid*, $\mathcal{O}_x$, of $\mathcal{S}'$. An ovoid of a GQ is a point set meeting each line precisely once. This ovoid is *subtended* by x.

Now suppose $\{\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_r\}$ is a set of $r > 0$ distinct subGQs of order $(s,t/s)$ of the GQ $\mathcal{S}$ of order (s,t), where $s \neq 1 \neq t$. Let Σ be the number of points in

$$\bigcup_{i=1}^{r} \mathcal{S}_i,$$

so that the number of points outside this union is

$$(s+1)(st+1) - \Sigma.$$

The $\mathcal{S}_j$'s are the source states. The keys are the points of $\mathcal{S} \setminus \bigcup_{i=1}^{r} \mathcal{S}_i$, and the messages are the ovoids in the GQs $\mathcal{S}_j$ which are subtended by a point outside their union.

Let k be the maximal number of points outside of $\bigcup_{i=1}^{r} \mathcal{S}_i$ that subtend the same ovoid of some $\mathcal{S}_j$. Then

$$P_0 = \frac{|\mathcal{E}(m)|}{|\mathcal{E}|} = \frac{k}{(s+1)(st+1) - \Sigma}.$$

By [41, 1.4.1], we have

$$k \leq \frac{s^2}{t} + 1$$

so that

$$P_0 \leq \frac{s^2/t + 1}{(s+1)(st+1) - \Sigma}.$$

We want to focus on two particular situations that appear to yield satisfactory results.

Example 2.1.6 *Let $t = s^2$ so that $t/s = s$. Then*

$$P_0 \leq \frac{2}{(s+1)(s^3+1) - \Sigma}.$$

Suppose now that in $\mathcal{S}$ we have the following situation: Γ is an $(s+1) \times (s+1)$-grid (that is, a subGQ of order $(s,1)$), and all the $\mathcal{S}_j$'s contain Γ. Then it follows easily that Γ is precisely the pairwise intersection of any two distinct $\mathcal{S}_j$'s. Moreover, if z is a point outside the subGQ union, and $\mathcal{S}_g$ and $\mathcal{S}_h$ are two elements of $\{\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_r\}$, then z obviously subtends different ovoids in $\mathcal{S}_g$ and $\mathcal{S}_h$.

Whence

$$P_0 \leq \frac{2}{(s+1)(s^3+1)-(s+1)^2-r(s^3-s)} = \frac{2}{(s+1)(s^2-s)(s+1-r)}.$$

Note that we can choose the subGQs in such a way that the inequality becomes strict.

Example 2.1.7 *Let $t = s$, so that $t/s = 1$ and*

$$P_0 \leq \frac{s+1}{(s+1)(s^2+1)-\Sigma}.$$

Also, let Γ be two distinct lines, and let all the $\mathcal{S}_j$'s contain Γ. It follows (again) that Γ is precisely the pairwise intersection of any two distinct $\mathcal{S}_j$'s. If z is a point outside of the union, and $\mathcal{S}_g$ and $\mathcal{S}_h$ are two elements of $\{\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_r\}$, then z subtends different ovoids in $\mathcal{S}_g$ and $\mathcal{S}_h$.

Whence

$$P_0 \leq \frac{s+1}{s(s^2+(1-r)s-1)}.$$

Remark 2.1.8 The schemes described above are *Cartesian*. Furthermore, the scheme is *perfect* if every ovoid is subtended by the same number of points outside $\cup\mathcal{S}_i$. Examples of this situation are given below.

We first describe all known generalized quadrangles of order (s, s^2) (for some natural number s) that have at least one subGQ of order s.

First, we recall the description of some classical examples of GQs.

Consider a non-singular quadric Q of Witt index 2, that is, of projective index 1, in $\mathbf{PG}(n, q)$, $n \in \{4, 5\}$. The points and lines of the quadric form a generalized quadrangle which is denoted by $Q(n, q)$ and has order (q, q^{n-3}). Next, let H be a non-singular Hermitian variety in $\mathbf{PG}(3, q^2)$. The points and lines of H form a generalized quadrangle $H(3, q^2)$, which has order (q^2, q).

Note that the variety H has the following canonical form:

$$X_0^{q+1} + X_1^{q+1} + X_2^{q+1} + X_3^{q+1} = 0.$$

A *flock* of the quadratic cone in $\mathbf{PG}(3,q)$, the 3-dimensional projective space over the finite field $\mathbb{F}_q$, is a partition of the cone without its vertex into q disjoint irreducible conics. The planes generated by the conics are the *flock planes*. Independently, Thas [62] and Walker [74] proved that one can associate a translation plane to a flock. Let $\mathcal{F}$ be a semifield flock [64][§4.5] of the quadratic cone in $\mathbf{PG}(3,q)$, q any prime power. This kind of flocks arise from a construction by Casse, Thas and Wild [13], and the associated translation plane is a semifield plane in this case, hence the name semifield flock. Then a GQ $\mathcal{S}(\mathcal{F})$ of order (q^2,q) can be constructed from $\mathcal{F}$ which has the property that its dual $\mathcal{S}(\mathcal{F})^D$ has a point (∞) such that there exists an elementary abelian automorphism group of $\mathcal{S}(\mathcal{F})^D$ that fixes (∞) linewise while acting sharply transitively on the points not collinear with (∞). This property has the advantage that from $\mathcal{S}(\mathcal{F})^D$ one can construct another GQ, the "translation dual" [64][§3.10], of the same order, which has an automorphism group with similar properties as the original one.

Consider the following sequence:

$$\mathcal{S}(\mathcal{F}) \xrightarrow{D} \mathcal{S}(\mathcal{F})^D \xrightarrow{*} (\mathcal{S}(\mathcal{F})^D)^* \xrightarrow{D} [(\mathcal{S}(\mathcal{F})^D)^*]^D.$$

(Here, the operation "$*$" means that we take the translation dual.) Then $(\mathcal{S}(\mathcal{F})^D)^*$ is a GQ of order (q,q^2) which has $Q(4,q)$-subGQs, with the following features.

Classical/Even case. If $\mathcal{F}$ is classical ("linear" — the flock planes share a line), then we have

$$\mathbf{H}(3,q^2) \cong \mathcal{S}(\mathcal{F}) \xrightarrow{D} Q(5,q) \cong \mathcal{S}(\mathcal{F})^D \xrightarrow{*} Q(5,q) \cong (\mathcal{S}(\mathcal{F})^D)^* \xrightarrow{D}$$

$$\mathbf{H}(3,q^2) \cong [(\mathcal{S}(\mathcal{F})^D)^*]^D.$$

In $Q(5,q)$, any $Q(4,q)$-subGQ has the property that each subtended ovoid is subtended by *precisely* two distinct points (see, for instance, [69]). For q even, we are necessarily in the classical case.

Nonclassical case. Then q is odd. We distinguish between two subcases.

- Kantor-Knuth. If $\mathcal{F}$ is a nonlinear Kantor-Knuth flock [68], then $(\mathcal{S}(\mathcal{F})^D)^* \cong \mathcal{S}(\mathcal{F})^D$, and the latter contains two classes of $Q(4,q)$-subGQs of order q, the union of which has size $q^3 + q^2$. In one class, each subtended ovoid is subtended by two distinct points, in the other class this is not the case.

- Not Kantor-Knuth. A result by K. Thas [70] states that no $Q(4, q)$-subGQ in $(\mathcal{S}(\mathcal{F})^D)^*$ can be doubly subtended. As in the Kantor-Knuth case, each such example contains $q^3 + q^2$ subGQs of $Q(4, q)$ type.

As for the specific scheme described in Example 2.1.7, we now introduce a class of generalized quadrangles that contains all known GQs of order s (for some integer s) which have $(s + 1) \times (s + 1)$-grids.

Suppose $H = \mathbf{PG}(3n - 1, q)$ is the finite projective $(3n - 1)$-space over $\mathbb{F}_q$, and let H be embedded in a $\mathbf{PG}(3n, q)$, say H'. Now consider a set $\mathcal{O} = \mathcal{O}(n, n, q)$ of $q^n + 1$ distinguished $(n - 1)$-dimensional subspaces of H, denoted $\mathbf{PG}(n - 1, q)^{(i)}$, so that (i) every three generate H; (ii) for every $i = 0, 1, \ldots, q^n$, there is a subspace $\mathbf{PG}(2n - 1, q)^{(i)}$ of H of dimension $2n - 1$, which contains $\mathbf{PG}(n - 1, q)^{(i)}$ and which is disjoint from any $\mathbf{PG}(n - 1, q)^{(j)}$ if $j \neq i$.

Then $\mathcal{O}$ is called a *pseudo-oval* or an $[n - 1]$-*oval* of $\mathbf{PG}(3n - 1, q)$. (Note that a [0]-oval of $\mathbf{PG}(2, q)$ is an *oval* of $\mathbf{PG}(2, q)$.)

From any such $\mathcal{O} = \mathcal{O}(n, n, q)$ there arises a GQ $\mathbf{T}(n, n, q) = \mathbf{T}(\mathcal{O})$, as follows.

- The Points are of three types.
  - (1) A symbol (∞).
  - (2) The subspaces $\mathbf{PG}(2n, q)$ of H' which intersect H in a $\mathbf{PG}(2n - 1, q)^{(i)}$.
  - (3) The points of $H' \setminus H$.
- The Lines are of two types.
  - (a) The elements of $\mathcal{O}(n, n, q)$.
  - (b) The subspaces $\mathbf{PG}(n, q)$ of $\mathbf{PG}(3n, q)$ which intersect H in an element of $\mathcal{O}$.
- Incidence is defined as follows: the point (∞) is incident with all the lines of Type (a) and with no other lines; a point of Type (2) is incident with the unique line of Type (a) contained in it and with all the lines of Type (b) containing it (as subspaces); finally, a point of Type (3) is incident with the lines of Type (b) that contain it.

Define

$$\mathcal{C}^+ = \{\mathbf{T}(\mathcal{O}) \parallel \quad \mathcal{O} \text{ is a pseudo-oval in even characteristic}\} \cup$$

$$\{\mathbf{T}(\mathcal{O})^D \parallel \quad \mathcal{O} \text{ is a pseudo-oval in even characteristic}\},$$

and

$$\mathcal{C}^- = \{\mathbf{T}(\mathcal{O}) \parallel \quad \mathcal{O} \text{ is a pseudo-oval in odd characteristic}\}.$$

Then every element of $\mathcal{C}^+ \cup \mathcal{C}^-$ is a GQ of order s for some integer s which has an $(s+1) \times (s+1)$-grid, and each known GQ with that property belongs to $\mathcal{C}^+ \cup \mathcal{C}^-$.

Authentication with arbitration: H-schemes

Consider the following situation. $\{\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_r\}$ is a set of distinct $Q(4,q)$-subGQs in a $Q(5,q)$ (which, as above, can be chosen in a suitable position), and let those subGQs be source states. Let x be a point of $Q(5,q)$ outside the union of the subGQs, which is chosen by Bob. For such a point x and for each source state $\mathcal{S}_j$, let $\mathcal{O}_x$ be the ovoid of $\mathcal{S}_j$ which is subtended by x. The arbiter chooses a point c_j of $\mathcal{S}_j$ on $\mathcal{O}_x$.

We can now make a scheme with arbitration as follows. For the system we choose a list $\mathbf{H}$ of subgroups of $\mathrm{Aut}(Q(5,q))$, being $\mathcal{O}^-(6,q) \rtimes \mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_p)$ (q is a power of the prime p). Bob chooses a fixed subgroup H in $\mathbf{H}$. Bob hands H and his chosen point x to the arbiter. The subgroup H has different orbits on $Q(5,q)$. The arbiter hands c_j and the H-orbit of c_j, denoted by c_j^H, as encoding rule to Alice for a given source state $\mathcal{S}_j$. If Alice transmits a message to Bob, then she picks the source state $\mathcal{S}_j$ and sends the triple $(\mathcal{S}_j, c_j, c_j^H)$ to Bob.

When receiving a triple (a,b,c), Bob accepts it as valid if b is on the ovoid of a and c is the H-orbit of b.

In case of a dispute concerning a triple (a,b,c), the arbiter checks if b is the point he handed to Alice for the subGQ a and if c is the orbit under H of b. If this is the case, then he decides Alice sent the message, otherwise that she has not.

If Bob wants to cheat, he has to make a guess about the point c_j.

If Alice wants to cheat, she has to make sure she gets the correct orbit. It is almost impossible for Alice to guess H from the orbits she sees, except possibly by exhaustive search through all subgroups of $\mathrm{Aut}(Q(5,q))$ if there are only very few groups producing an orbit she observes. But the arbiter can avoid this by choosing the appropriate points.

An opponent has to guess both c_j and the group H; an even harder task.

We do not make calculations in detail, but once one has chosen the list of allowed subgroups one can adapt the scheme to one's own needs.

This scheme depends largely on the list $\mathbf{H}$ of subgroups we allow. By choosing them appropriately, one can control the length of the orbits.

Remark 2.1.9 (i) Similar schemes can be built from other incidence geometries, such as the embedding of Hermitian quadrangles $\mathbf{H}(3, q^2) \subset \mathbf{H}(4, q^2)$.

(ii) We always assume that the points outside of the union of subGQs are chosen with equal probability. One could define a natural probability

$$P : \mathcal{S} \setminus \cup_i \mathcal{S}_i \mapsto]0, 1[,$$

on this set by comparing, for a pre-chosen subgroup G of $\mathrm{Aut}(\mathcal{S})_{\cup_i \mathcal{S}_i}$, the size of the G-orbit $G(x)$ that contains x, to $|\mathcal{S} \setminus \cup_i \mathcal{S}_i|$.

2.1.4 Link with designs and various schemes

In this subsection we will describe some other geometries which can be used to construct MAC's. This is not intended to be a complete overview, but is based on the author's personal taste and meant to give the readers some feeling which geometric ideas can be used if they want to construct a MAC themselves.

The link with designs

In the several examples we gave, one could see that for a given source state, there are a number of keys which produce the same encoded message. Using the language of design theory, we call such a group of keys a *block*. Especially if we have a perfect scheme, these blocks have a nice structure. We make this link more precise below. We follow [42]. First of all, we give some definitions coming from design theory.

Definition 2.1.10 *Let v , b , k , λ, t be positive integers with $t \leq k$. A* partially balanced t-design (PBD) *$t - (v, b, k; \lambda, 0)$ is a pair $(\mathcal{N}, \mathcal{F})$, where $\mathcal{N}$ is a set of v points and $\mathcal{F}$ is a family of b subsets of $\mathcal{N}$, each of cardinality k (called* blocks*) such that any t-subset of $\mathcal{N}$ either occurs together in exactly λ blocks or does not occur in any block.*

Definition 2.1.11 *If a partially balanced t-design $t-(v,b,k;\lambda_t,0)$ is a partially balanced r-design $r-(v,b,k;\lambda_r,0)$ for $1 \leq r < t$ as well, then it is called a* strong partially balanced t-design **(SPBD)** *and is denoted by $t-(v,b,k;\lambda_1,\cdots,\lambda_t,0)$.*

We will assume that any point of $\mathcal{M}$ appears in at least one block $\mathcal{M}(e)$, otherwise the point can be dismissed from $\mathcal{M}$. The following theorem links perfect authentication schemes without arbitration with **(SPBD)**'s.

Theorem 2.1.12 *An authentication scheme $\mathcal{A} = (\mathcal{S},\mathcal{M},\mathcal{E})$ with probabilities P_S and P_E is t-fold perfect if and only if the pair $(\mathcal{M},\{\mathcal{M}(e) \mid\mid e \in \mathcal{S}\})$ is a* **(SPBD)** *$t-(v,b,k;\lambda_1,\cdots,\lambda_t,0)$ with $\lambda_t = 1$, p_E is uniform, and $p_{S^r}, 1 \leq r \leq t$, are message uniform (p_{S^T} is always message uniform when $\lambda_t = 1$). Here*

$$v = |\mathcal{M}|,\ b = |\mathcal{E}|,\ k = |\mathcal{S}|,$$

$$\lambda_r = (P_r P_{r+1} \cdots P_{t-1})^{-1}, 1 \leq r \leq t-1.$$

As a lot of geometries are examples of designs, this explains why several geometries are well-suited to describe perfect authentication codes.

Rational normal curves, unitary and symplectic spaces

Consider the following set of points in $\mathbf{PG}(n,q)$, $2 \leq n \leq q-2$:

$$\{(1,\alpha,\cdots,\alpha^n) \mid\mid \alpha \in \mathbb{F}_q\} \cup \{(0,0,\cdots,0,1)\}.$$

The image of this point set under any projective transformation is called a *normal rational curve.* These normal rational curves can be used to construct a family of non-cartesian perfect A-codes, where source states are points on a fixed normal rational curve and the encoding rules are determined by projective transformations between various rational normal curves. A system based on symplectic spaces can be found in [75] and a system based on unitary spaces in [21]. More details can be found in [42].

2.2 Secret sharing schemes

2.2.1 Introduction

One of the applications where finite geometry turned out to be very useful are secret sharing schemes. A good reference for secret sharing schemes is [57] and a nice overview of the geometric aspects of secret sharing schemes is given in [32]. We give a short introduction on the subject.

Definition 2.2.1 *A* secret sharing scheme *is a method of distributing a secret amongst a set of participants by giving each participant a* share *in such a way that only specified subsets of participants, called* authorised sets *(defined by the* access structure Γ*) can reconstruct the secret from a pooling of their shares.*

Secret sharing schemes are used in situations where it is not desirable to give one single person all information about a secret, for example to decide to fire nuclear weapons, or for codes of bank accounts of large organisations. In such cases, it is better to distribute the secret among several people, thereby reducing the chances of any malicious activity.

The access structure of a secret sharing scheme says which subsets of participants are allowed to reconstruct the secret, these are the *authorised sets*. All the other subsets of participants are called *unauthorised*. Thus a secret sharing scheme has the two following important properties.

(i) *Privacy*: Unauthorised subsets of participants are not able to determine the secret.

(ii) *Recoverability*: Authorised subsets of participants should be able to determine the secret by combining their shares.

A secret sharing scheme is called *perfect* if unauthorised sets do not retrieve any information about the secret via their shares.

Most secret sharing schemes are assumed to have a *monotone access structure*, meaning that if a subset of participants A can reconstruct the secret, then the participants of any superset of A can also reconstruct the secret. The set of subsets of participants which are allowed to reconstruct the secret is denoted by Γ. The *dealer* of the secret sharing scheme is a fully trusted party, who is responsible for the setup of the system, meaning that he generates the shares and the secret, and he hands each participant his or her shares. The *combiner* is the person who pools the shares of a given subset of participants, and tries to reconstruct the secret.

Let $\mathcal{P}$ be the set of n participants of the secret sharing scheme. Furthermore, let k be an integer such that $1 \leq k \leq n$. The access structure is such that any group of at least k persons is allowed to reconstruct the secret. So $\Gamma = \{A \subset \mathcal{P} \mid\mid |A| \geq k\}$ is an access structure on $\mathcal{P}$, known as the (k, n)-*threshold access structure on* $\mathcal{P}$.

A famous example of a threshold scheme was given by Shamir in [52]. This threshold scheme is defined over $\mathbb{Z}_p$. To each participant P_i, one associates a unique non-zero x_i, which is not secret. If the secret is s, the dealer randomly chooses a polynomial $f(x)$ of degree at most $k-1$ over $\mathbb{Z}_p$ such that $f(0) = s$. The dealer then secretly gives $f(x_i)$ to participant P_i. The Shamir threshold scheme has perfect privacy since knowledge of $k-1$ shares does not leak any information about the secret s. Furthermore, any k participants can reconstruct the secret.

2.2.2 A geometric secret sharing scheme

Now we will investigate applications of generalized arcs in secret sharing schemes.

Before we describe the construction of a secret sharing scheme from a generalized arc in general, we give two examples that use the dual arc with parameters $(9, 5, 2, 0)$ we have seen in Example 1.3.9.

Example 2.2.2 *The dual of the dual arc with parameters* $(9, 5, 2, 0)$ *is an arc consisting of* $q^2 + q + 1$ 3*-spaces in* $\mathbf{PG}(9, q)$ *with the following properties:*

1. *Each two* 3*-spaces generate a* 6*-space.*

2. *Each three* 3*-spaces generate an* 8*-space.*

3. *Each four* 3*-spaces generate* $\mathbf{PG}(9, q)$*.*

Now take the space $\mathbf{PG}(10, q)$*. Choose any hyperplane as the secret. In that hyperplane, choose the above configuration of* q^2+q+1 *3-spaces as shares.*

If the attacker does not have a share, he has a probability of $\frac{q-1}{q^{11}-1}$ *to guess the secret* 9*-space.*

If the attacker knows only one share, he has to guess a 9-space through the known 3*-space so he has a probability of* $\frac{q-1}{q^7-1}$ *to guess the secret.*

Similarly, an attacker that knows 2 *or* 3 *shares has a probability of* $\frac{q-1}{q^4-1}$ *or* $\frac{q-1}{q^2-1} = \frac{1}{q+1}$ *to guess the share.*

Any 4 *shares reconstruct the secret.*

Example 2.2.3 *As in the previous example, we choose a hyperplane* Π *in* $\mathbf{PG}(10, q)$ *and an arc consisting of* q^2+q+1 3*-spaces with the same properties as above. One of these 3-spaces* π *will be the secret. The other* 3*-spaces are the shares.*

Furthermore, we choose a 4*-space* Π_4 *through* π *not contained in* Π *and make it public. If an attacker wants to find the secret space, he has to reconstruct* Π *and then the secret space is the intersection* $\Pi \cap \Pi_4$*. A short calculation shows that an attacker who knows* i $(i \leq 4)$ *shares has a probability of* $\frac{q-1}{q^{5-i}-1}$ *to guess the secret.*

Another way to vary the attack probabilities is the following. Remember that the $q^2 + q + 1$ 5*-spaces of the dual arc are of the form* $D(p)$ *where* p *is a point of a* 2*-dimensional space* $\mathbf{PG}(2, q)$*. The* $q + 1$ 5*-spaces that correspond* *to the $q+1$ points of a line lie in a common 8-space. In the dual setting, this means that the $q+1$ 3-spaces intersect in a common point.*

So if we fix one 3-space π, it has $q+1$ different intersection points with the other q^2+q 3-spaces. These $q+1$ points form the well-known arc of the points $p_a = [1, a, a^2, a^3]$ ($a \in \mathbb{F}_q$) and $p_\infty = [0, 0, 0, 1]$. Choose a plane in π which contains no such intersection point. This is possible, since $\mathbb{F}_q[x]$ contains an irreducible polynomial of degree 3.

Now we choose as the secret a 3-space through this plane, not contained in Π. An attacker who knows i ($i < 4$) shares has probabilities $p_0 = p_1 = \frac{1}{q^3+q^2+q+1}$, $p_2 = \frac{1}{q^2+q+1}$ and $p_3 = \frac{1}{q+1}$ to guess the secret. Thus the new scheme leaks no information if only one share is known.

By choosing the correct subspace of π, we can also construct schemes that have no information leak for 2 or 3 shares. Then we must choose a line or a point inside π and take a plane or line respectively as the secret.

Now we give two theorems which use generalized arcs to construct secret sharing schemes.

Theorem 2.2.4 *In $\mathbf{PG}(n+1, q)$ choose an n-dimensional subspace Π as secret. In Π choose a generalized arc $\mathcal{A}$ of degree $k-2$ with n' elements and of type $(n, d_1, \ldots, d_{k-1})$. The elements of $\mathcal{A}$ are the shares.*

This describes a k-out-of-n' secret sharing scheme with the attack probabilities

$$P_i = \frac{q-1}{q^{n+1-d_i}-1}$$

for $0 \leq i < k$ (formally we set $d_0 = -1$).

Proof Every k shares span Π, since $\mathcal{A}$ is a generalized arc of degree $k-2$.

Less than k participants can take their shares $\pi_1, \ldots, \pi_i$ and compute the d_i-dimensional space $\langle \pi_1, \ldots, \pi_i \rangle$. They know that Π must contain that space. But for every n-dimensional space Π' containing $\langle \pi_1, \ldots, \pi_i \rangle$, there exists an arc which has $\pi_1, \ldots, \pi_i$ as elements. Thus the best attack is to guess an n-dimensional space through $\langle \pi_1, \ldots, \pi_i \rangle$. The number of such spaces is $\frac{q^{n+1-d_i}-1}{q-1}$. □

Theorem 2.2.5 *In $\mathbf{PG}(n+1, q)$, choose a (d_1+1)-dimensional subspace π' and make it public. In π', choose a d_1-dimensional subspace π as the secret. Choose any hyperplane Π of $\mathbf{PG}(n+1, q)$ that contains π but not π'. Let $\mathcal{A}$ be a generalized dual arc of Π of degree $k-2$ with $n+1$ elements and of type $(n, d_1, \ldots, d_{k-1})$. The subspace π should be an element of $\mathcal{A}$. The n elements of $\mathcal{A}$, different from π, are the shares.*

This describes a k-out-of-n secret sharing scheme with the attack probabilities

$$P_i = \frac{q-1}{q^{d_{i+1}-d_i+1}-1}$$

for $0 \leq i < k-1$ (formally we set $d_0 = -1$ and $d_k = n$).

Proof Every k shares span Π, since $\mathcal{A}$ is a generalized arc of degree $k-2$. Thus k participants can compute $\Pi \cap \pi'$ which is the secret π.

Less than k participants can take their shares $\pi_1, \ldots, \pi_i$ and compute the d_i-dimensional space $\langle \pi_1, \ldots, \pi_i \rangle$. Since the secret π is also an element of the arc $\mathcal{A}$, we find that $\langle \pi_1, \ldots, \pi_i, \pi \rangle$ has dimension d_{i+1}. This means that

$$\dim(\langle \pi_1, \ldots, \pi_i \rangle \cap \pi) = d_i + d_1 - d_{i+1} \ .$$

Since by construction $\pi' \cap \Pi = \pi$ we also have

$$\dim(\langle \pi_1, \ldots, \pi_i \rangle \cap \pi') = d_i + d_1 - d_{i+1} \ .$$

The i participants know that π is a d_1-dimensional subspace of π' containing the $-d_{i+1}+d_i+d_1$ dimensional subspace $\langle \pi_1, \ldots, \pi_i \rangle \cap \pi'$. But for every d_1-dimensional subspace $\bar{\pi}$, there exists a generalized arc containing $\pi_1, \ldots, \pi_i$ and $\bar{\pi}$. So the i participants have no further information and must guess a d_1-dimensional subspace of π'. The probability for guessing this correctly is

$$P_i = \frac{q-1}{q^{d_1+1-(d_i+d_1-d_{i+1})}} \ .$$

□

2.2.3 Minimal codewords and secret sharing

Minimal codewords were introduced by Massey [40] for cryptographical purposes. They are used in particular secret sharing schemes, to model the access structures. Here we describe Massey's scheme. In the next chapter, we will study minimal codewords in the particular case of Reed-Muller codes.

Definition 2.2.6 *The* support *of a codeword c, denoted by $supp(c)$, is the set of positions in which the non-zero digits appear.*

Definition 2.2.7 *Let C be a q-ary linear code. A non-zero codeword $c \in C$ is called* minimal *if its leftmost non-zero component is a 1 and if it has a support that does not contain the support of any other non-zero codeword with leftmost component 1 as a proper subset. The support of a minimal codeword is called* minimal *with respect to C.*

Now we explain how one can construct a secret sharing scheme based on a linear $[n, k]$-code where the first digit in every codeword is not always 0. The secret is chosen as the first digit of a codeword. The digits in $k - 1$ chosen positions, selected so that together with the first position they form an *information set*, meaning they uniquely determine the full codeword, are selected uniformly at random over $\mathbb{F}_q$ and the full codeword then computed; and the $s = n - 1$ shares are all the codeword digits after the first.

In [40], the following is proved.

Proposition 2.2.8 *The access structure of the secret sharing scheme corresponding to the linear q-ary $[n, k]$-code C is specified by those minimal codewords in the dual code $C^{\perp}$ whose first component is a 1 in the manner that the set of shares specified by each such minimal codeword in the dual code is the set of shares corresponding to those locations after the first where this minimal codeword is non-zero.*

Chapter 3

Minimal codewords

Minimal codewords were introduced by Massey [40] for cryptographical purposes. They are used in particular secret sharing schemes to model the access structures. We study minimal codewords of weight smaller than $3 \cdot 2^{m-r}$ in the binary Reed-Muller codes $\mathrm{RM}(r, m)$ and translate our problem into a geometrical one, using a classification result of Kasami, Tokura, and Azumi [34] on Boolean functions. In this geometrical setting, we calculate numbers of non-minimal codewords. So we obtain the number of minimal codewords in the cases where we have information about the weight distribution of the code $\mathrm{RM}(r, m)$.

The presented results, based on the paper [48], improve previous results obtained theoretically by Borissov, Manev, and Nikova [5], and computer aided results of Borissov and Manev [4].

3.1 Introduction

First we give some definitions and theorems required for a good statement of the problem. We will associate geometrical objects to the codewords. This will allow us to translate the problem into an equivalent geometrical problem.

Definition 3.1.1 *For any m and r, $0 \leq r \leq m$,* the binary r-th order Reed-Muller code $\mathrm{RM}(r, m)$ *is defined to be the set of all binary vectors f of length $n = 2^m$ associated with Boolean polynomials $f(x_1, x_2, ..., x_m)$ of degree at most r.*

Definition 3.1.2 *If $f(x_1, ..., x_m)$ is a Boolean function, then $T(f)$ is the collection of vectors $X = (x_1, ..., x_m)$ such that $f(X) = 1$.*

Definition 3.1.3 *The* support *of a codeword $c \in \mathrm{RM}(r, m)$, denoted by supp(c), is the set of positions in which the non-zero digits appear.*

Definition 3.1.4 *Let C be a q-ary linear code. A non-zero codeword $c \in C$ is called* minimal *if its leftmost non-zero component is a 1 and if it has a support that does not contain the support of any other non-zero codeword with leftmost component 1 as a proper subset. The support of a minimal codeword $c \in C$ is called* minimal *with respect to C.*

The following properties can be found in [1]; we will use the second one later on.

Lemma 3.1.5 *Let C be a binary linear $[n, k, d]$-code.*

(i) *Every support of a codeword of weight $\leq 2d - 1$ is minimal with respect to C.*

(ii) *The codeword c is a non-minimal codeword in C if and only if there is a pair of non-zero codewords c_1, c_2, with disjoint supports contained in the support of c, such that $c = c_1 + c_2$.*

(iii) *If c is a minimal codeword in C, then $wt(c) \leq n - k + 1$.*

So a naturally arising question is what happens for weights in between the above bounds. The smallest non-trivial case is $wt(c) = 2d$. This was solved by Borissov, Manev, and Nikova for RM(r, m) [5], by interpreting the non-minimal codewords of weight $2d$ geometrically as a union of two disjoint affine spaces $\mathbf{AG}(m - r, 2)$. To state their result, we first need some notations.

Definition 3.1.6 *The quantity known as q-*ary Gaussian coefficient *is defined by:* $\begin{bmatrix} m \\ i \end{bmatrix} = \prod_{j=0}^{i-1} \frac{q^m - q^j}{q^i - q^j}$, $\begin{bmatrix} m \\ 0 \end{bmatrix} = 1$, *for $i = 1, 2, \ldots, m$.*

Furthermore, we use the following notations:

$$A_{r,m} = 2^{r-1} \begin{bmatrix} m \\ m - r + 1 \end{bmatrix}.$$

$$B_{r,m} = \frac{2^{r+1} - 4}{4} \begin{pmatrix} 2^{r+1} \\ 3 \end{pmatrix} \begin{bmatrix} m \\ m - r - 1 \end{bmatrix}.$$

$$S_{r,m} = (2^{m-r+1} - 1)A_{r,m} + 3B_{r,m}.$$

$$E_{r,m} = \sum_{k=\max\{0, m-2r\}}^{m-r} 2^{(m-r-k)(m-r-k+1)} \begin{bmatrix} m - r \\ k \end{bmatrix} \begin{bmatrix} r \\ m - r - k \end{bmatrix}.$$

$$P_{r,m} = 2^{r-1} \begin{bmatrix} m \\ m - r \end{bmatrix} (2^r \begin{bmatrix} m \\ m - r \end{bmatrix} - E_{r,m}).$$

Now we can state their main theorem.

Theorem 3.1.7 *The number of non-minimal codewords of weight* $2d = 2^{m-r+1}$ *in* $\mathrm{RM}(r,m)$ *is* $A_{r,m} + B_{r,m} + P_{r,m} - S_{r,m}$.

We translate the problem for larger values $wt(c)$ into a geometrical one, making use of the following result of Kasami, Tokura, and Azumi [34].

Theorem 3.1.8 *Let* $f(x_1,...,x_m)$ *be a Boolean function of degree at most* r, *where* $r \geq 2$, *such that* $|T(f)| < 2^{m-r+1}$. *Then* f *can be transformed by an affine transformation into either*

$$f = x_1 \cdots x_{r-2}(x_{r-1}x_r + \cdots + x_{r+2\mu-3}x_{r+2\mu-2}),\ 2 \leq 2\mu \leq m-r+2,\ \textit{or}$$

$$f = x_1 \cdots x_{r-\mu}(x_{r-\mu+1} \cdots x_r + x_{r+1} \cdots x_{r+\mu}),\ 3 \leq \mu \leq r, \mu \leq m-r.$$

We call codewords of the forms above *codewords of first and second type* respectively. It is not hard to determine the weight of these codewords. As is well-known, the smallest weight vectors in $\mathrm{RM}(r,m)$ are the ones of weight 2^{m-r} which can be interpreted as the incidence vectors of $(m-r)$-dimensional affine spaces, see [39].

We need the following lemma which can be found in [39].

Lemma 3.1.9 *The number of values* $(x_1,...,x_{2h})$ *for which*

$$\sum_{i=1}^{h} x_{2i-1}x_{2i} = 0$$

is equal to $2^{2h-1} + 2^{h-1}$.

Lemma 3.1.10 *The weight of codewords of first type is equal to*

$$2^{m-r-2\mu+2}(2^{2\mu-1} - 2^{\mu-1}) = 2^{m-r-\mu+1}(2^{\mu} - 1).$$

The weight of codewords of second type is equal to

$$2^{m-\mu-r+1}(2^{\mu} - 1).$$

These weight functions are both increasing in μ, *so the smallest weights are found for the smallest values of* μ.

Proof For the codewords of first type, we use the lemma above, where we must have

$$x_{r-1}x_r + \cdots + x_{r+2\mu-3}x_{r+2\mu-2} = 1.$$

We also have to put the first $r-2$ coordinates equal to 1, so only $m-(r+2\mu-2)$ coordinates can be chosen freely.

Hence, the weight of the codewords of first type is

$$2^{m-r-2\mu+2}(2^{2\mu-1}-2^{\mu-1}).$$

For those of second type, we note that if

$$x_{r-\mu+1}\cdots x_r + x_{r+1}\cdots x_{r+\mu} = 1,$$

then not all coordinates $x_{r-\mu+1},...,x_{r+\mu}$ can be one. If $(x_{r-\mu+1},...,x_r) \neq (1,...,1)$, which happens $2^\mu-1$ times, then necessarily $(x_{r+1},...,x_{r+\mu}) = (1,...,1)$. The same reasoning works with $(x_{r+1},...,x_{r+\mu})$; hence we obtain $2(2^\mu-1)$ solutions. We can still choose $m-r-\mu$ coordinates freely, so the weight of a codeword of second type becomes $2^{m-\mu-r+1}(2^\mu-1)$. □

The second smallest weight of the code $\mathrm{RM}(r,m)$ is $3\cdot\frac{2^{m-r}}{2}$. We will count the number of non-minimal codewords $c = c_1 + c_2$ of weight smaller than $3\cdot 2^{m-r}$. This implies that either c_1 or c_2 can be interpreted as an affine $(m-r)$-dimensional space.

We can regard vectors $(x_1,...,x_m)$ as points of the affine space $\mathbf{AG}(m,2)$. So by adding an extra variable X_0, we can consider the problem in the projective space $\mathbf{PG}(m,2)$; this means we set $x_i = \frac{X_i}{X_0}$ and hence we are working in a projective space where $X_0 = 0$ denotes the space at infinity. For $\mu = 1$, the set $T(f)$ of a codeword of first type is defined by the equations

$$X_1 = X_0, \ldots,\ X_0 = X_r,$$

so represents an $(m-r)$-dimensional space. So let $\mu > 1$. The first object then can be considered as the incidence vector of the geometrical object defined by the following equations:

$$X_1 = X_0,\ ...,\ X_{r-2} = X_0,\ X_0^2 = X_{r-1}X_r + \cdots + X_{r+2\mu-3}X_{r+2\mu-2}.$$

The first $r-2$ equations all describe hyperplanes, so their intersection is a $\mathbf{PG}(m-r+2,2)$. The remaining equation is the standard equation of a non-singular parabolic quadric in 2μ dimensions. If we look at the intersection with infinity, we get

$$X_0 = 0,$$

$$X_{r-1}X_r + \cdots + X_{r+2\mu-3}X_{r+2\mu-2} = 0.$$

This is the standard equation of a non-singular hyperbolic quadric in $2\mu-1$ dimensions. Furthermore we see that the coordinates $X_{r+2\mu-1},...,\ X_m$ can be chosen freely, so in the $\mathbf{PG}(m-r+2,2)$ defined by $X_1 = X_0,\ldots,X_{r-2} = X_0$, this codeword defines a cone Ψ with as vertex a $\mathbf{PG}(m-r+1-2\mu,2)$

at infinity, and base a 2μ-dimensional parabolic quadric $Q(2\mu, q)$ having a $(2\mu - 1)$-dimensional hyperbolic quadric at infinity. We must also keep in mind that the codeword defines the affine part of this cone Ψ.

The object of second type is easily seen to define all affine points lying inside the union of two $(m - r)$-dimensional affine spaces α and β, but not in the $(m - r - \mu)$-dimensional affine intersection space $\alpha \cap \beta$; we will call this kind of object a *symmetric difference.*

A codeword c of $\mathrm{RM}(r, m)$ is non-minimal if and only if $c = c_1 + c_2$, where c_1 and c_2 are non-zero codewords having disjoint supports. Since we are interested in counting the number of non-minimal codewords of weight less than $3 \cdot 2^{m-r}$, we take c_1 to be a non-zero codeword of smallest weight, namely 2^{m-r}, and c_2 to be a codeword of first or second type with small μ. We don't take weight 2^{m-r} for both codewords since this case has already been solved by Borissov, Manev, and Nikova [5]; their result is stated here in Theorem 3.1.7. So a non-minimal codeword corresponds to a pair (c_1, c_2) of geometric objects having no affine intersection points, where c_1 is an $(m - r)$-dimensional space, and where c_2 is a quadric or a symmetric difference. This geometrical problem will be solved more generally over $\mathbb{F}_q$ instead of over $\mathbb{F}_2$.

3.2 The geometrical setting

In this section, we describe the different geometrical situations that can occur, which we will treat in the following sections. First of all, we distinguish between two cases according to the choice of the second codeword c_2. We will first only describe the situations, to give an overview of the possibilities. The goal is to clarify the sections that follow, in which the actual calculations will take place.

3.2.1 The second codeword c_2 is a quadric Ψ

Let Π be the $(m-r+2)$-dimensional projective space containing the quadric Ψ and let α be the projective completion of the $(m - r)$-dimensional affine space corresponding to the codeword c_1 of smallest weight. The intersection of Π with the space at infinity is denoted by Π_∞. Note that Ψ has an $(m-r-2\mu+1)$-dimensional vertex Γ at infinity. Denote the 2μ-dimensional parabolic quadric base of the cone Ψ by B, and the intersection of B with Π_∞ by B_∞.

First we describe the different situations in $\mathbf{AG}(m, q)$ which occur if we want to count the pairs (Ψ, α) having no affine points in common, where Ψ is the quadric and where α is a projective space $\mathbf{PG}(m - r, q)$ not lying at infinity. Note that in the case $q = 2$, the affine part of α defines the codeword c_1 and that the affine part of Ψ defines the codeword c_2.

Case 1) The spaces α and Π have no points in common. So α certainly does not have affine points in common with Ψ.

Case 2) The spaces α and Π intersect in an x-dimensional space, $x \geq 0$, lying completely in Π_∞. All these spaces α have no affine points in common with Ψ. To find the number of such spaces, we take a fixed x-dimensional space Π_x lying in Π_∞ and we count how many $(m-r)$-dimensional affine spaces have a projective completion that intersects Π exactly in Π_x.

Case 3) The spaces α and Π intersect in a l-dimensional space Π_l, $l \geq 0$, not lying completely in Π_∞. If $l = 0$, we count how many $(m-r)$-dimensional affine spaces have a projective completion that intersects Π exactly in an affine point not lying on Ψ.

So assume that $l > 0$. Denote the $(l-1)$-dimensional intersection space $\Pi_l \cap \Pi_\infty$ by Π_{l-1}. Suppose that α has an s-dimensional space Π_s in common with the vertex Γ of Ψ. Consider a complementary space Π_{l-s-2} of Π_s in Π_{l-1}. Take in Π a complementary space Π_b of dimension 2μ of the vertex Γ that contains Π_{l-s-2}, and assume that B is contained in Π_b. The intersection of Π_l with the quadric Ψ is a quadric in Π_l having a certain vertex $\Pi_{l'}$ of dimension $l' \geq -1$, and a non-singular base $Q_{l-l'-1}$ in a space of dimension $l-l'-1$. The space $\Pi_{l'}$ can only have points at infinity in common with the quadric Ψ, since c_1 and c_2 share no affine points. So $Q_{l-l'-1}$ does not span a space of dimension $l-l'-1$. So $Q_{l-l'-1}$ is either a space of dimension $l-l'-2$ or $l-l'-3$. Hence, the intersection of the projective completion of α with B_∞ must be a subspace Π_k, $k \geq -1$.

Consider the $(s+k+1)$-dimensional space Π_{s+k+1} generated by Π_s and Π_k. We claim that Π_{s+k+1} is either equal to Π_{l-1}, so a hyperplane of Π_l, or a hyperplane of Π_{l-1}, so a hyperplane in the hyperplane at infinity of Π_l.

Indeed, project Π_l from Π_{s+k+1} onto a complementary space of Π_{s+k+1} in Π_l. After projecting we get a $(l-(s+k+1)-1)$-dimensional space. This space is not allowed to contain points of the quadric Ψ. Every quadric lying in a space of dimension at least 2 contains points. So we have $l \leq s+k+3$. Hence, our claim is proved.

We summarize these results in the following lemma.

Lemma 3.2.1 *Let α be an $(m-r)$-dimensional affine space in $\mathbf{AG}(m,q)$ having a non-empty intersection with the $(m-r+2)$-dimensional affine space Π containing the quadric Ψ. Assume that $\alpha \cap \Pi$ is skew to Ψ, then $\alpha \cap \Pi_\infty$ is either contained in $\Psi \cap \Pi_\infty$ or $\alpha \cap \Pi_\infty \cap \Psi$ is a hyperplane of $\alpha \cap \Pi_\infty$.*

Terminology. *For the rest of this chapter, we refer to these two cases as the cases "hyperplane" and "hyperplane in the hyperplane".*

We always start from an intersection at infinity. This intersection must be the space at infinity of an affine space having no points in common with the cone Ψ. To obtain such affine spaces, we need to consider external lines to the quadric Ψ through a point p. We have to consider several cases according to whether or not p lies on or off the quadric Ψ, in Π_∞ or not, ... The number of such lines in each case is calculated in several lemmas in further sections before the actual counting arguments take place. If some space Π'_∞ is the space at infinity of some affine space Π' of dimension l, we will say that the affine space Π' *extends* Π'_∞. We now use the notations s and k of above.

a) If $k = -1$, then we have two possibilities. If Π_{l-1} lies entirely in the vertex space Γ of the quadric Ψ, we extend this intersection to an l-dimensional affine space skew to Ψ. If Π_{l-1} intersects Π_b in an external point of the quadric Ψ (and then $s = l-2$), we again extend the $(l-1)$-dimensional space Π_{l-1} to an affine l-dimensional space having no affine points in common with Ψ.

b) If $k \geq 0$ and if we are in the case "hyperplane", we extend the $(s+k+1 = l-1)$-dimensional space to an $(s+k+2 = l)$-dimensional affine space, such that we don't get affine intersection points with Ψ.

c) If $k \geq 0$ and if we are in the case "hyperplane in the hyperplane", we extend the $(s+k+1 = l-2)$-dimensional space contained in $\Psi \cap \Pi_\infty$ to an $(s+k+2 = l-1)$-dimensional space at infinity without adding intersection points with the cone Ψ. Then we extend this $(s+k+2 = l-1)$-dimensional space at infinity to an $(s+k+3 = l)$-dimensional space not lying completely at infinity, such that we do not get affine intersection points with Ψ.

After this is done, we describe which situations we might have double counted. To see in which situations this occurs, we assume that we can write a given non-minimal codeword c in two ways as a pair of non-zero codewords with disjoint supports, so we assume that

$$c = c_1 + c_2 = c_3 + c_4.$$

The codewords c_1 and c_3 are both assumed to be of minimal weight. They correspond to $(m-r)$-dimensional affine spaces in $\mathbf{AG}(m,q)$. These intersect in a t-dimensional affine space. This intersection dimension t puts severe restrictions on the intersection possibilities, see Section 3.7. First we prove that the projective completion of the $(m-r)$-dimensional affine space c_3 must contain the whole vertex Γ of the quadric c_2, so Ψ, in order to have an interchange. Then we will consider this situation and perform a case by case study. In very few cases, an actual interchange and hence a double counting will occur, see Section 3.8.

3.2.2 The second codeword c_2 is a symmetric difference

Denote by β and γ the two $(m-r)$-dimensional projective spaces forming the symmetric difference c_2, and let α be the $(m-r)$-dimensional projective space corresponding to the codeword c_1. We start from a given symmetric difference and we count how many $(m-r)$-dimensional affine spaces have no affine intersection points with it.

Case 1) The space α has no intersection points with β nor γ. Then it certainly has no affine intersection points with any of these two spaces.

Case 2) The only intersection points of α with β and γ lie in $\beta \cap \gamma$. So the intersection is a k-dimensional space lying in $\beta \cap \gamma$.

Case 3) There are intersection points of α with β or γ not lying in $\beta \cap \gamma$. Then all intersection points of α with $\beta \cup \gamma$ have to lie at infinity, otherwise we get affine intersection points not lying in $\beta \cap \gamma$.

The cases 2) and 3) are solved in a very similar way using projections. We start from given intersection spaces $\alpha \cap \beta$ and $\alpha \cap \gamma$. So we have a starting configuration. We count how many times each starting configuration can occur. Then we gradually extend this starting configuration until we have an $(m-r)$-dimensional affine space α. In each step, we project on a complementary space of the space we have already constructed. Then we can count how many extensions are possible at this given step. This yields an inductive formula, from which we can calculate the required number of $(m-r)$-dimensional affine spaces having no affine intersection points with the given symmetric difference.

3.3 Counting the number of objects

In this section, we determine how many basic objects of each type, namely quadrics and symmetric differences, there are. From now on, we work more generally over $\mathbb{F}_q$ instead of $\mathbb{F}_2$. Hence, we will no longer use the term codeword, since only for $q = 2$, the geometric objects correspond to codewords.

However, we will still use sentences like "the projective space defined by c_1", and such sentences will be used to indicate that we are talking about the generalization over $\mathbb{F}_q$ of the geometric object in $\mathbb{F}_2$ that corresponds to the codeword c_1.

Denote the number of m-dimensional spaces $\mathbf{PG}(m,q)$ lying inside an n-dimensional space $\mathbf{PG}(n,q)$ by $\phi(m;n,q)$, the number of non-singular hyperbolic quadrics $Q^+(2\mu-1,q)$ inside a $(2\mu-1)$-dimensional space $\mathbf{PG}(2\mu-1,q)$ by $O(Q^+(2\mu-1,q))$, and the number of non-singular parabolic quadrics $Q(2\mu,q)$ inside a 2μ-dimensional space $\mathbf{PG}(2\mu,q)$ by $O(Q(2\mu,q))$.

These numbers can be found in [28].

We now determine how many quadrics Ψ there are, where Ψ is a cone having an $(m-r-2\mu+1)$-dimensional vertex Γ at infinity and having as base a non-singular 2μ-dimensional parabolic quadric $Q(2\mu,q)$. This quadric Ψ lies in an $(m-r+2)$-dimensional subspace Π of $\mathbf{AG}(m,q)$. To calculate this number, we first fix the $(m-r+1)$-dimensional space at infinity Π_∞ of Π. This can be done in the following number of ways:

$$F_1 = \phi(m-r+1; m-1, q).$$

Once we have fixed this space Π_∞, we must look for the number of $\mathbf{PG}(m-r+2,q)$ through Π_∞, but not contained in the space at infinity of $\mathbf{AG}(m,q)$. This is $F_2 = q^{r-2}$.

Inside the space at infinity Π_∞, we must choose the vertex Γ of dimension $m-r-2\mu+1$ of the quadric Ψ. The number of choices equals

$$F_3 = \phi(m-r+1-2\mu; m-r+1, q).$$

Consider a complementary space Π_b of the $(m-r-2\mu+1)$-dimensional vertex space Γ inside $\Pi = \mathbf{PG}(m-r+2,q)$, this is a 2μ-dimensional space; take the space Π_b as the space spanned by the base of the quadric Ψ. This space Π_b intersects Π_∞ in a $(2\mu-1)$-dimensional space. Inside this last space, we have $F_4 = O(Q^+(2\mu-1,q))$ different ways to choose the base $Q^+(2\mu-1,q)$ at infinity. Finally, we need the number F_5 of non-singular parabolic quadrics $Q(2\mu,q)$ through a fixed $Q^+(2\mu-1,q)$ lying inside the selected 2μ-dimensional space Π_b. This number can be found by double counting. First we notice that

$$H = |Q^+(2\mu-1,q) \text{ in } \mathbf{PG}(2\mu,q)| = \phi(2\mu-1; 2\mu, q)F_4.$$

Furthermore,

$$|O(Q(2\mu,q))||Q^+(2\mu-1,q) \text{ on a given } Q(2\mu,q)| = HF_5.$$

The total number of quadrics Ψ is the product $F = F_1F_2F_3F_4F_5$.

Since for $q=2$, the weight distribution for codewords of $\mathrm{RM}(r,m)$ of weight less than $2.5d = \frac{5}{2}2^{m-r}$ is known [34], we also have the number of symmetric difference objects in this case, but not in general. Note that a symmetric difference $(\alpha\cup\beta)\backslash(\alpha\cap\beta)$ is defined by two affine $(m-r)$-dimensional spaces α and β, intersecting in an affine $(m-r-\mu)$-dimensional space, with $3 \leq \mu \leq m-r, \mu \leq r$. We count them as follows. Take an $(m-r-\mu)$-dimensional affine space inside $\mathbf{AG}(m,q)$. For this space, we have the following number of choices

$$F_1(m,r,\mu,q) = \frac{q^m(q^m-1)(q^m-q)\cdots(q^m-q^{m-r-\mu-1})}{q^{m-r-\mu}(q^{m-r-\mu}-1)(q^{m-r-\mu}-q)\cdots(q^{m-r-\mu}-q^{m-r-\mu-1})}.$$

The number of $\mathbf{PG}(m-r,q)$ through such an $(m-r-\mu)$-dimensional affine space is $\phi(r-1;\mu-1+r,q)$. This is exactly the number of choices for the first $\mathbf{AG}(m-r,q)$ through this given $(m-r-\mu)$-dimensional affine space. The number of choices for the second $\mathbf{AG}(m-r,q)$ is the number of $(m-r)$-dimensional affine spaces inside $\mathbf{AG}(m,q)$ that intersect a given $(m-r)$-dimensional affine space of $\mathbf{AG}(m,q)$ in a given $(m-r-\mu)$-dimensional affine space. This is equal to

$$F_2(m,r,\mu,q) = \frac{(q^m - q^{m-r})(q^m - q^{m-r+1})\cdots(q^m - q^{(m-r)+(\mu-1)})}{(q^{m-r} - q^{m-r-\mu})(q^{m-r} - q^{m-r-\mu+1})\cdots(q^{m-r} - q^{m-r-1})}.$$

We will have counted all the pairs constituting the symmetric differences twice, hence we find

$$\frac{\phi(r-1;\mu-1+r,q)F_1(m,r,\mu,q)F_2(m,r,\mu,q)}{2}$$

symmetric difference objects, consisting of two affine $(m-r)$-dimensional spaces intersecting in an affine $(m-r-\mu)$-dimensional space.

3.4 Counting affine spaces skew to the quadric Ψ

Suppose that we have fixed a quadric Ψ in $\mathbf{AG}(m,q)$, where Ψ is a cone having an $(m-r-2\mu+1)$-dimensional vertex Γ at infinity and having as base a non-singular 2μ-dimensional parabolic quadric $Q(2\mu,q)$, and we wish to determine how many $(m-r)$-dimensional affine spaces $\mathbf{AG}(m-r,q)$ are skew to the affine part of the quadric Ψ. If the projective completion α of $\mathbf{AG}(m-r,q)$ has no points in common with the $(m-r+2)$-dimensional projective space Π spanned by the quadric Ψ, then $\mathbf{AG}(m-r,q)$ is certainly skew to the affine part of Ψ, so suppose that α has intersection points with Π.

We distinguish between several cases for the intersections at infinity of α and Ψ, and then for each case, we count the number of affinely skew extensions. In order to achieve this, we need the following two lemmas.

Lemma 3.4.1 *Consider in $\mathbf{PG}(2\mu,q)$ a parabolic quadric $Q(2\mu,q)$, intersecting a particular hyperplane, playing the role of hyperplane at infinity, in a hyperbolic quadric $Q^+(2\mu-1,q)$.*

For q even, a point p at infinity of $\mathbf{PG}(2\mu,q)$, not lying on $Q^+(2\mu-1,q)$, lies in $\mathbf{PG}(2\mu,q)$ on

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

affine external lines to $Q(2\mu,q)$.

Proof Since p lies at infinity, it is not equal to the nucleus n of $Q(2\mu, q)$. The tangent lines through p all lie in a hyperplane through the line $\langle p, n\rangle$. So this is a tangent hyperplane $T_r(Q(2\mu, q))$ at some $r \in Q(2\mu, q)$. All $\frac{q^{2\mu-1}-1}{q-1}$ lines through p inside this hyperplane are tangent lines to $Q(2\mu, q)$. There are $q^{2\mu-2}$ affine ones among them. The quadric $Q(2\mu, q)$ has

$$|Q(2\mu, q)| - |Q^+(2\mu-1, q)| = \frac{q^{2\mu}-1}{q-1} - \frac{(q^\mu-1)(q^{\mu-1}+1)}{q-1} = q^{2\mu-1} - q^{\mu-1}$$

affine points. So there are

$$\frac{q^{2\mu-1} - q^{\mu-1} - q^{2\mu-2}}{2}$$

affine bisecants through p. There are $q^{2\mu-1}$ affine lines through p. So the number of affine external lines through p equals

$$q^{2\mu-1} - q^{2\mu-2} - \frac{q^{2\mu-1} - q^{\mu-1} - q^{2\mu-2}}{2}.$$

□

For q odd, there are two types of points of $\mathbf{PG}(2\mu, q)$ at infinity lying off the hyperbolic quadric $Q^+(2\mu-1, q)$, call a representant of each of them p^+ and p^-. For p^+, the associated hyperplane with respect to the polarity defined by $Q(2\mu, q)$ intersects $Q(2\mu, q)$ in a hyperbolic quadric $Q^+(2\mu-1, q)$, and for p^-, the associated hyperplane with respect to the polarity intersects $Q(2\mu, q)$ in an elliptic quadric $Q^-(2\mu-1, q)$.

Lemma 3.4.2 *For q odd, through p^+, there pass $\frac{(q-1)q^{2\mu-2}}{2}$ affine external lines of $Q(2\mu, q)$ lying in $\mathbf{PG}(2\mu, q)$, and through p^-, there pass $\frac{(q-1)q^{2\mu-2}}{2} + q^{\mu-1}$ affine external lines of $Q(2\mu, q)$ lying in $\mathbf{PG}(2\mu, q)$. Furthermore, the number of points p^+ equals the number of points p^-, and is equal to $\frac{q^{\mu-1}(q^\mu-1)}{2}$.*

Proof Let α be the number of affine external lines to $Q(2\mu, q)$ inside $\mathbf{PG}(2\mu, q)$ through a point p at infinity not belonging to the quadric at infinity $Q^+(2\mu-1, q)$, let β be the number of affine tangents through p, and let γ be the number of affine bisecants through p. Then we immediately obtain the following equality

$$\alpha + \beta + \gamma = q^{2\mu-1}$$

for the total number of affine lines through p, and the equation

$$\beta + 2\gamma = q^{2\mu-1} - q^{\mu-1},$$

counting the number of affine points of the quadric $Q(2\mu, q)$ in $\mathbf{PG}(2\mu, q)$.

This yields $\alpha = \frac{q^{2\mu-1}+q^{\mu-1}-\beta}{2}$, so if we can calculate the number β, we have the desired numbers. For a point p^+, there are

$$|Q^+(2\mu-1, q)| - |Q(2\mu-2, q)| = q^{2\mu-2} + q^{\mu-1}$$

affine tangents through it inside $\mathbf{PG}(2\mu, q)$. For a point p^-, there are

$$|Q^-(2\mu-1, q)| - |Q(2\mu-2, q)| = q^{2\mu-2} - q^{\mu-1}$$

affine tangents through it inside $\mathbf{PG}(2\mu, q)$.

The subgroup $G(Q(2\mu, q))$ of $\mathbf{PGL}(2\mu+1, q)$ fixing $Q(2\mu, q)$ has two orbits on the set of external points of the quadric $Q(2\mu, q)$, see [28]. The intersections of these orbits with respect to $Q(2\mu, q)$ with the space at infinity $\mathbf{PG}(2\mu-1, q)$ yield the two orbits of the group $G(Q^+(2\mu-1, q))$, the subgroup of $\mathbf{PGL}(2\mu, q)$ fixing $Q^+(2\mu-1, q)$, on the points of $\mathbf{PG}(2\mu-1, q)$ not on $Q^+(2\mu-1, q)$, see [63]; hence the number of points p^+ equals the number of points p^-. Since the total number of points of $\mathbf{PG}(2\mu-1, q)$ lying off the quadric $Q^+(2\mu-1, q)$ at infinity in $\mathbf{PG}(2\mu-1, q)$ is equal to $|\mathbf{PG}(2\mu-1, q)| - |Q^+(2\mu-1, q)|$, both the numbers of points p^+ and p^- are equal to $q^{\mu-1}\frac{q^{\mu}-1}{2}$. □

The projective quadric Ψ spans an $(m-r+2)$-dimensional projective space Π over $\mathbb{F}_q$, intersecting at infinity in Π_∞. Let α be an affine $(m-r)$-dimensional space skew to the affine part of Ψ.

We look at a given intersection $\Pi_\infty \cap \alpha$ at infinity and determine how many suitable affine spaces extending it we can find, skew to the affine quadric Ψ. To improve transparency, we treat the cases separately in several little lemmas. In the proofs, we need the number of affine external lines to the quadric $Q(2\mu, q)$ through a point p lying at infinity; these numbers were calculated above. Albeith that these numbers differ for different situations, we denote this number by N. Furthermore, we always denote the quadric by Ψ, the $(m-r-2\mu+1)$-dimensional vertex at infinity of Ψ by Γ, the 2μ-dimensional base of Ψ by $Q(2\mu, q)$, the space spanned by $Q(2\mu, q)$ by Π_b, and the intersection of $Q(2\mu, q)$ with Π_∞ by $Q^+(2\mu-1, q)$.

Lemma 3.4.3 *Through an $(s+k+1)$-dimensional space Π_{s+k+1} at infinity, completely lying on Ψ, that intersects the vertex Γ in an s-dimensional space Π_s, there pass*

$$H(s,k) = \frac{q^{m-r+2-2\mu}(q^{2\mu-2k-2} - q^{2\mu-2k-3} + q^{\mu-k-2})}{q^{s+1}}$$

affine $(s+k+2)$-dimensional spaces of Π skew to the affine part of the quadric Ψ.

Proof Consider a complementary space of Π_s in Π_{s+k+1}, say Π_k, and consider a complementary $(2\mu-1)$-dimensional space $\Pi_\infty \cap \Pi_b$ to the vertex space Γ in Π_∞ that contains Π_k.

We take Π_b as the space spanned by the base $Q(2\mu, q)$ of the quadric Ψ. Since $\Pi_{s+k+1} \subset \Psi$, the space Π_k lies entirely on the quadric $Q^+(2\mu-1, q)$ at infinity of the base $Q(2\mu, q)$ of Ψ.

The number of affine 2μ-dimensional spaces passing through the $(2\mu-1)$-dimensional space $\langle Q^+(2\mu-1, q)\rangle$, and lying inside Π, is $q^{m-r+2-2\mu}$.

Every affine $(s+k+2)$-dimensional space contains $\frac{q^{s+k+2}}{q^{k+1}} = q^{s+1}$ affine $(k+1)$-dimensional spaces through a k-dimensional space Π_k at infinity.

Every skew $(k+s+2)$-dimensional affine space through Π_{s+k+1} will have an intersection with Π_b that lies in $\Pi_k^\perp$, the polar space of Π_k with respect to $Q(2\mu, q)$. This space $\Pi_k^\perp$ intersects $Q(2\mu, q)$ in a cone with vertex the k-dimensional space Π_k and base a parabolic quadric $Q(2\mu-2k-2, q)$. In order to have an affinely skew space, we have to take an affine external point inside the $(2\mu-2k-2)$-dimensional space spanned by the parabolic quadric $Q(2\mu-2k-2, q)$. There are

$$q^{2\mu-2k-2} - q^{2\mu-2k-3} + q^{\mu-k-2}$$

such points. So taking multiple countings into account, we find

$$\frac{q^{m-r+2-2\mu}(q^{2\mu-2k-2} - q^{2\mu-2k-3} + q^{\mu-k-2})}{q^{s+1}}$$

$(s+k+2)$-dimensional affine spaces through Π_{s+k+1} inside Π skew to the affine part of the quadric Ψ. □

Lemma 3.4.4 *Through an $(s+k+1)$-dimensional space Π_{s+k+1} at infinity, lying completely on Ψ, that intersects the vertex Γ of Ψ in an s-dimensional space Π_s, there are in Π*

$$HIH(s,k) = \frac{q^{2m-2r-3\mu-2s-k}(q^{\mu-k-1}-1)((q-1)q^{2\mu-2k-4} + q^{\mu-k-2})}{2}$$

affine $(s+k+3)$-dimensional spaces Π_{s+k+3} skew to the affine part of the quadric Ψ, intersecting Π_∞ in an $(s+k+2)$-dimensional space only intersecting Ψ in Π_{s+k+1}.

Proof Let $\Pi_r = \Pi_{s+k+1}$ be the space we start from at infinity. The polar space of Π_r with respect to the quadric at infinity $\Gamma Q^+(2\mu-1, q)$, denoted by $T_{\Pi_r}(\Gamma Q^+(2\mu-1, q))$, is equal to

$$\Gamma T_{\Pi_k}(Q^+(2\mu-1, q)) = \langle \mathbf{PG}(m-r-2\mu+1, q), T_{\Pi_k}(Q^+(2\mu-1, q))\rangle.$$

Here T_{Π_r} means the intersection of all tangent spaces $T_p, p \in \Pi_r$, with respect to $\Gamma Q^+(2\mu - 1, q)$. In order to extend Π_r at infinity without changing the intersection space with Ψ, we have to choose a point in $T_{\Pi_r}(\Gamma Q^+(2\mu - 1, q))$ not lying on Ψ. So we get the following number of choices for the extension point.

$$C = |\mathbf{PG}(m - r - k, q)| - |\langle\langle\Gamma, \Pi_k\rangle, Q^+(2\mu - 2k - 3, q)\rangle|.$$

A calculation yields $C = q^{m-r-k} - q^{m-r-\mu+1}$. In $T_{\Pi_{s+k+1}}(\Gamma Q^+(2\mu - 1, q))$ we see a cone with vertex the space $\langle\Gamma, \Pi_k\rangle$ and base a non-singular hyperbolic quadric $Q^+(2\mu-2k-3, q)$. Every $(s+k+2)$-dimensional space through Π_{s+k+1} in $T_{\Pi_{s+k+1}}$ is contained in Ψ, or only intersects Ψ in Π_{s+k+1}; so contains q^{s+k+2} points not in Ψ. So to know the number of $(s + k + 2)$-dimensional spaces through Π_{s+k+1} in $T_{\Pi_{s+k+1}}$ only sharing Π_{s+k+1} with Ψ, we divide C by q^{s+k+2} to get

$$q^{m-r-s-2k-2} - q^{m-r-\mu-s-k-1}$$

such $(s + k + 2)$-dimensional spaces $\langle\Pi_s, \Pi_{k+1}\rangle$.

Once we have fixed such a space Π_{k+1}, we count in how many ways this space can be extended in $\mathbf{PG}(2\mu, q)$ to a $(k + 2)$-dimensional affine space Π_{k+2} skew to the affine part of $Q(2\mu, q)$. We have the inclusion $\Pi_{k+2} \subset \Pi_k^\perp$, where the polarity is taken with respect to the parabolic quadric $Q(2\mu, q)$. The intersection $\Pi_k^\perp \cap Q(2\mu, q)$ is a cone with as vertex Π_k and as base a non-singular parabolic quadric $Q(2\mu - 2k - 2, q)$. The required number is the number N of affine external lines of $Q(2\mu-2k-2, q)$ through the intersection p of Π_{k+1} and $\langle Q(2\mu - 2k - 2, q)\rangle$. Note that, for q odd, the number of affine external lines through a point p depends on the type of the point p (Lemma 3.4.2), but since the number of points p^+ equals the number of points p^-, the total number of spaces Π_{k+2} defined by all spaces Π_{k+1} is the total number of points p times the average of the numbers of affine external lines through p, see Lemma 3.4.2. Hence for all q, we find

$$\frac{q^{m-r+2-2\mu}}{q^{s+1}}(q^{m-r-s-2k-2} - q^{m-r-\mu-s-k-1})(\frac{(q-1)q^{2\mu-2k-4}}{2} + \frac{q^{\mu-k-2}}{2}),$$

and after simplification

$$\frac{q^{2m-2r-3\mu-2s-k}(q^{\mu-k-1} - 1)((q-1)q^{2\mu-2k-4} + q^{\mu-k-2})}{2}$$

affine $(s + k + 3)$-dimensional spaces through Π_{s+k+1} lying inside Π and skew to the affine part of Ψ, intersecting Ψ at infinity in Π_{s+k+1}, and intersecting the $(m-r+1)$-dimensional space at infinity Π_∞ of the $(m-r+2)$-dimensional affine space Π containing Ψ in an $(s + k + 2)$-dimensional space. □

We now determine how many times we can start from a given $(s+k+1)$-dimensional space lying completely on the quadric $\Gamma Q^+(2\mu-1,q)$ at infinity and intersecting the vertex Γ of the quadric Ψ in an s-dimensional space. Denote the number of c-dimensional projective spaces lying inside an a-dimensional projective space Π_a that are skew to a given b-dimensional projective space of Π_a by $Skew(a,b,c)$.

Lemma 3.4.5 *The number $Skew(a,b,c)$ is equal to*

$$\prod_{k=-1}^{c-1} \frac{q^{a-k}-q^{b+1}}{q^{k+2}-1}.$$

Proof We start by choosing a point inside the a-dimensional space Π_a not lying in the b-dimensional space Π_b. The number of such points is equal to

$$\frac{q^{a+1}-q^{b+1}}{q-1}.$$

Suppose that we have already constructed all k-dimensional spaces Π_k in Π_a skew to Π_b. Consider a space complementary to some Π_k inside Π_a; this is an $(a-k-1)$-dimensional space Π_{a-k-1}. Since Π_b has nothing in common with Π_k, the projection Π_b^* of Π_b from Π_k onto Π_{a-k-1} is a b-dimensional space. So the number of choices to extend Π_k to a $(k+1)$-dimensional space having no points in common with Π_b is the number of points in Π_{a-k-1} not lying in Π_b^*. This number is equal to

$$\frac{q^{a-k}-q^{b+1}}{q-1}.$$

Doing this for all spaces Π_k, we will have obtained each $(k+1)$-dimensional space of Π_a skew to Π_b several times, namely the number of k-dimensional spaces lying in a $(k+1)$-dimensional space, that is,

$$\frac{q^{k+2}-1}{q-1}.$$

Hence, extending to a c-dimensional space skew to the given space Π_b yields the above formula. □

In the lemma below, the following numerical notation is used:

$$[r,s]_+ = (q^r+1)(q^{r+1}+1)\cdots(q^s+1) \text{ if } s \geq r.$$

$$[r,s]_- = (q^r-1)(q^{r+1}-1)\cdots(q^s-1) \text{ if } s \geq r.$$

If $s<r$, then $[r,s]_+ = [r,s]_- = 1$.

Lemma 3.4.6 *The number of $(s+k+1)$-dimensional spaces Π_{s+k+1} at infinity lying on the quadric $\Gamma Q^+(2\mu-1,q)$ and intersecting the vertex Γ in some s-dimensional space Π_s is equal to*

$$S(s,k) = \phi(s;v,q)q^{(k+1)(v-s)}\frac{[\mu-1-k,\mu-1]_+[\mu-k,\mu]_-}{[1,k+1]_-}$$

with $v = m-r-2\mu+1$.

Proof The number of choices for the s-dimensional spaces in the vertex Γ is $\phi(s;v,q)$ with $v = m-r+1-2\mu$. Once we have fixed the s-dimensional intersection space Π_s with the vertex Γ, we have to determine how many $(s+k+1)$-dimensional spaces lie completely on the quadric $\Gamma Q^+(2\mu-1,q) = \Psi \cap \Pi_\infty$ at infinity, that intersect the vertex space Γ exactly in Π_s. Suppose that we have a k-dimensional space Π_k on $\Psi \cap \Pi_\infty$ skew to the vertex space Γ. If we project this space from the vertex Γ on $\langle Q^+(2\mu-1,q)\rangle$, we get a k-dimensional space Π'_k lying on the hyperbolic quadric $Q^+(2\mu-1,q)$.

The number of k-dimensional spaces lying on a hyperbolic quadric $Q^+(2\mu-1,q)$ is equal to

$$N(k;2\mu-1,q) = \frac{[\mu-1-k,\mu-1]_+[\mu-k,\mu]_-}{[1,k+1]_-},$$

see [28].

The same space Π'_k is the projection of all k-dimensional spaces skew to the vertex space Γ inside the $(v+k+1)$-dimensional space spanned by the vertex Γ and Π'_k. The number of them is equal to

$$Skew(v+k+1,v,k) = q^{(k+1)(v+1)}.$$

We have counted the number of $(s+k+1)$-dimensional spaces intersecting the vertex space Γ exactly in the s-dimensional space Π_s several times; namely as many times as the number of k-dimensional spaces lying in an $(s+k+1)$-dimensional space and skew to a given s-dimensional space. This is $Skew(s+k+1,s,k) = q^{(s+1)(k+1)}$. Hence we finally find

$$\phi(s;m-r+1-2\mu,q)q^{(k+1)(v-s)}\frac{[\mu-1-k,\mu-1]_+[\mu-k,\mu]_-}{[1,k+1]_-}.$$

□

So we know for each possible intersection Π_{s+k+1} at infinity, lying on Ψ and intersecting the vertex Γ of Ψ in an s-dimensional space and the base $Q^+(2\mu-1,q)$ in a k-dimensional space, which we will call a *starting configuration* from now on, in how many ways we can extend this intersection to an affine space Π_{s+k+2} or Π_{s+k+3} lying in $\Pi = \mathbf{PG}(m-r+2,q)$ and skew to the affine part of Ψ, intersecting Π_∞ in this given starting configuration Π_{s+k+1} for Π_{s+k+2} or intersecting Π_∞ in an $(s+k+2)$-dimensional space only sharing Π_{s+k+1} with Ψ for Π_{s+k+3}.

The remaining problem consists of determining the number of ways these spaces $\Pi_{x'}$, $x' \geq 0$, $x' = s+k+2$ or $x' = s+k+3$, can be extended to $(m-r)$-dimensional affine spaces in the space $\mathbf{AG}(m,q)$, that intersect the affine part $\mathbf{AG}(m-r+2,q)$ of Π exactly in the space $\Pi_{x'}$, and determining the number of spaces $\mathbf{AG}(m-r,q)$ that are affinely completely skew to the $\mathbf{AG}(m-r+2,q)$. The number of ways to extend $\Pi_{x'}$ to an $(m-r)$-dimensional space intersecting $\mathbf{AG}(m-r+2,q)$ in $\Pi_{x'}$ is

$$Ext_Q(x') = \frac{(q^m - q^{m-r+2})\cdots(q^m - q^{(m-r+2)+m-r-x'-1})}{(q^{m-r} - q^{x'})\cdots(q^{m-r} - q^{m-r-1})}.$$

Lemma 3.4.7 *The number P of $\mathbf{AG}(m-r,q)$ skew to a given space $\mathbf{AG}(m-r+2,q)$ in $\mathbf{AG}(m,q)$ is equal to*

$$P = \sum_{x=-1}^{m-r-1} \phi(x; m-r+1, q) T(x),$$

where $T(x)$ is equal to $Skew(m-x-1, m-r+1-x, m-r-x-1)$-$Skew(m-x-2, m-r-x, m-r-x-1)$.

Proof The projective completion of every such space $\mathbf{AG}(m-r,q)$ intersects the projective completion $\mathbf{PG}(m-r+2,q)$ of the given space $\mathbf{AG}(m-r+2,q)$ at infinity in an x-dimensional space Π_x, $x \geq -1$. Project from Π_x on a complementary space Π_{m-x-1} of Π_x in the space $\mathbf{PG}(m,q)$. The number of ways to extend Π_x to an $(m-r)$-dimensional projective space such that the intersection with $\mathbf{PG}(m-r+2,q)$ remains Π_x is then equal to $Skew(m-x-1, m-r+1-x, m-r-x-1)$. However we must exclude the ones lying completely in the space at infinity Π_∞. We can count them in a similar way by projecting from Π_x onto a complementary space of Π_x in Π_∞. It follows that the number of ways to extend Π_x to an $(m-r)$-dimensional space having exactly Π_x in common with $\mathbf{PG}(m-r+2,q)$ and not lying completely at infinity is equal to

$$Skew(m-x-1, m-r+1-x, m-r-x-1) - Skew(m-x-2, m-r-x, m-r-x-1).$$

The number of x-dimensional spaces lying in an $(m-r+1)$-dimensional space is equal to $\phi(x; m-r+1, q)$. Hence, the result follows. □

Since we have determined for all dimensions x how many affine spaces $\mathbf{AG}(m-r,q)$ intersect $\mathbf{AG}(m-r+2,q)$ in a given x-dimensional affine space, $x \geq 0$, and since we know the number of $\mathbf{AG}(m-r,q)$ skew to $\mathbf{AG}(m-r+2,q)$, the number of affine $(m-r)$-dimensional subspaces of $\mathbf{AG}(m,q)$ skew to the affine part of Ψ can be counted.

Theorem 3.4.8 *The number of affine $(m-r)$-dimensional subspaces of $\mathbf{AG}(m,q)$ skew to the affine part of a given cone $\Psi = \Gamma Q(2\mu,q)$, where Γ is the $(m-r-2\mu+1)$-dimensional vertex at infinity of Ψ, is equal to*

$$P + \sum_{(s,k)\in R(s,k)} S(s,k)(H(s,k)Ext_Q(s+k+2) + HIH(s,k)Ext_Q(s+k+3)),$$

where

$$R(s,k) = \{(s,k)| -1 \leq s \leq m-r+1-2\mu,\ -1 \leq k \leq \mu-1\},$$

and where P is defined in Lemma 3.4.7.

Proof First of all, by Lemma 3.4.7, we have P distinct $(m-r)$-dimensional affine spaces that have no affine points in common with $\Pi = \mathbf{AG}(m-r+2,q)$. By Lemma 3.4.6, the number of $(s+k+1)$-dimensional spaces at infinity Π_{s+k+1} lying on the quadric $\Gamma Q^+(2\mu-1,q)$ and intersecting the vertex Γ in some s-dimensional space Π_s is equal to $S(s,k)$. We recall Lemma 3.4.3. Through an $(s+k+1)$-dimensional space Π_{s+k+1} at infinity that intersects the vertex Γ in an s-dimensional space Π_s, and supposing that we are in the case hyperplane, there pass $H(s,k)$ affine $(s+k+2)$-dimensional spaces in Π skew to the affine part of the quadric Ψ. Another case is treated in Lemma 3.4.4. Through an $(s+k+1)$-dimensional space Π_{s+k+1} at infinity that intersects the vertex Γ in an s-dimensional space Π_s, and supposing that we are in the case hyperplane in the hyperplane, there are $HIH(s,k)$ affine $(s+k+3)$-dimensional affine spaces in Π skew to the affine part of the quadric Ψ.

So suppose that we already have such an $(s+k+2)$- or $(s+k+3)$-dimensional affine space in Π. A given space Π_x, $x \geq 0$, can be extended to $(m-r)$-dimensional affine spaces in the space $\mathbf{AG}(m,q)$, that intersect the affine part $\mathbf{AG}(m-r+2,q)$ of Π exactly in the space Π_x, in $Ext_Q(x)$ ways. □

3.5 Counting affine spaces skew to a symmetric difference

We are going to count the number of $(m-r)$-dimensional affine spaces $\mathbf{AG}(m-r,q)$ having no affine points in common with a fixed symmetric difference. We repeat that a symmetric difference is equal to $(\alpha\cup\beta)\setminus(\alpha\cap\beta)$, with α and β two affine $(m-r)$-dimensional spaces, intersecting in an $(m-r-\mu)$-dimensional affine space, where $3 \leq \mu \leq r, \mu \leq m-r$ (Theorem 3.1.8).

We look at the projective completion Π_{m-r} of such an $(m-r)$-dimensional affine space. Denote the $(m-r)$-dimensional projective spaces forming the symmetric difference by α and β.

Since Π_{m-r} is allowed to contain affine points lying in $\alpha \cap \beta$, we have to distinguish between two cases.

1) The $(m-r)$-dimensional space Π_{m-r} has affine points in common with $\alpha \cap \beta$.

Suppose that Π_{m-r} has a k-dimensional projective intersection space Π_k, $\Pi_k \not\subset \Pi_\infty$, in common with $\alpha \cap \beta$, which is a space of dimension $m-r-\mu$. There are

$$N(k) = \frac{q^{m-r-\mu}(q^{m-r-\mu}-1)\cdots(q^{m-r-\mu}-q^{k-1})}{q^k(q^k-1)\cdots(q^k-q^{k-1})}$$

choices for such a space Π_k.

Suppose that we have fixed such a k-dimensional intersection space Π_k. We are going to extend it to an $(m-r)$-dimensional affine space without adding any point of $\alpha\cup\beta$ to it. We do this inductively on the dimension and we work in the projective space $\mathbf{PG}(m,q)$. Such an $(m-r)$-dimensional space has a t-dimensional intersection space with the space generated by α and β, further denoted by $\langle\alpha,\beta\rangle$.

We start from a given k-dimensional intersection space Π_k and we first construct the t-dimensional intersection spaces $\Pi_{k,t}$ with $\langle\alpha,\beta\rangle$ that intersect $\alpha\cup\beta$ exactly in $\Pi_k \subset \alpha\cap\beta$.

Suppose that we have already constructed all a-dimensional affine spaces in $\langle\alpha,\beta\rangle$ through Π_k that have exactly Π_k in common with $\alpha\cup\beta$. Let γ be an a-dimensional space through Π_k, having only Π_k in common with $\alpha\cup\beta$. We project from γ onto a complementary space of γ in the m-dimensional projective space $\mathbf{PG}(m,q)$; this complementary space γ^* has dimension $m-a-1$. Denote the projections on γ^* of α, β, and $\langle\alpha,\beta\rangle$ from γ by α^*, β^*, and $\langle\alpha,\beta\rangle^*$ respectively. These spaces have dimension $m-r-k-1$, $m-r-k-1$, and $m-r+\mu-a-1$ respectively, and $\alpha^*\cap\beta^*$ has dimension $m-r-\mu-2k+a-1$. So in order to have an extension of γ to an $(a+1)$-dimensional space lying in $\langle\alpha,\beta\rangle$, such that the intersection space with $\alpha\cup\beta$ remains Π_k, we must choose points in $\langle\alpha,\beta\rangle^*$, but outside of $\alpha^*\cup\beta^*$. In this way, we get

$$Q(a,k) = \frac{q^{m-r+\mu-a}-1}{q-1} - 2\frac{q^{m-r-k}-1}{q-1} + \frac{q^{m-r-\mu-2k+a}-1}{q-1}$$

choices for an extension of this a-dimensional space γ to an $(a+1)$-dimensional space in $\langle \alpha, \beta \rangle$, intersecting $\alpha \cup \beta$ in Π_k.

Denote the number of a-dimensional affine spaces in $\langle \alpha, \beta \rangle$ that intersect $\alpha \cup \beta$ exactly in $\Pi_k \subset \alpha \cap \beta$ by $\psi(a, k)$. Then we have $\psi(k, k) = 1$, namely the k-dimensional space Π_k itself. If we have a given a-dimensional space in $\langle \alpha, \beta \rangle$ intersecting $\alpha \cup \beta$ exactly in Π_k, then we have $Q(a, k)$ extensions to an $(a+1)$-dimensional affine space lying in $\langle \alpha, \beta \rangle$ and intersecting $\alpha \cup \beta$ exactly in Π_k. In this $(a+1)$-dimensional space, there are $\phi(a-k-1; a-k, q) = \phi(0; a-k, q)$ a-dimensional spaces through Π_k. Hence, we get the following induction formula

$$\psi(a+1, k) = \frac{Q(a, k)\psi(a, k)}{\phi(0; a-k, q)}.$$

The number of t-dimensional affine spaces lying in $\langle \alpha, \beta \rangle$ that intersect $\alpha \cup \beta$ exactly in a given affine space Π_k of dimension k contained in $\alpha \cap \beta$ is thus equal to $\psi(t, k)$, and the number of t-dimensional affine spaces that intersect $\alpha \cup \beta$ exactly in some k-dimensional space lying in $\alpha \cap \beta$, but not in Π_∞, is equal to $N(k)\psi(t, k)$.

Next we are going to count in how many ways we can extend a given t-dimensional space Π_t lying in $\langle \alpha, \beta \rangle$, which intersects $\alpha \cup \beta$ in a given k-dimensional affine space Π_k lying in $\alpha \cap \beta$, with Π_k not lying completely in Π_∞, to an $(m-r)$-dimensional affine space without changing the intersection with $\langle \alpha, \beta \rangle$. Suppose that we have already constructed all a-dimensional spaces through Π_t that have exactly Π_k in common with $\alpha \cup \beta$ and that have exactly Π_t in common with $\langle \alpha, \beta \rangle$. Let γ be an a-dimensional affine space through Π_t, having only Π_t in common with $\langle \alpha, \beta \rangle$. We project from γ onto a complementary space of γ in the m-dimensional projective space $\mathbf{PG}(m, q)$; this complementary space γ^* has dimension $m - a - 1$. Denote the projection on γ^* of $\langle \alpha, \beta \rangle$ from γ by $\langle \alpha, \beta \rangle^*$. This space has dimension $m - r + \mu - t - 1$. So in order to have an extension of γ to an $(a+1)$-dimensional space, such that the intersection space with $\langle \alpha, \beta \rangle$ remains Π_t, we must choose points in γ^* outside of $\langle \alpha, \beta \rangle^*$. In this way, we get

$$R(a, k, t) = \frac{q^{m-a} - 1}{q - 1} - \frac{q^{m-r+\mu-t} - 1}{q - 1}$$

choices for an extension.

Denote the number of a-dimensional affine spaces γ that intersect $\langle \alpha, \beta \rangle$ exactly in Π_t, and $\alpha \cap \beta$ exactly in a k-dimensional space, $k \geq 0$, not lying at infinity, by $\rho(a, k, t)$. Then we have $\rho(t, k, t) = 1$, namely the t-dimensional space Π_t itself. If we have a given a-dimensional affine space intersecting $\langle \alpha, \beta \rangle$ exactly in Π_t, then we have $R(a, k, t)$ extensions to an $(a+1)$-dimensional affine space intersecting $\langle \alpha, \beta \rangle$ exactly in Π_t. In this $(a+1)$-dimensional space, there are $\phi(a-t-1; a-t, q) = \phi(0; a-t, q)$ a-dimensional spaces through Π_t. Hence, we get the following induction formula

$$\rho(a+1, k, t) = \frac{R(a, k, t)\rho(a, k, t)}{\phi(0; a-t, q)}.$$

The number of $(m-r)$-dimensional affine spaces intersecting $\langle \alpha, \beta \rangle$ in a given t-dimensional affine space Π_t, where $\Pi_t \cap \alpha \cap \beta = \Pi_k$, $k \geq 0$, is thus equal to $\rho(m-r, k, t)$.

In order to find the total number of such $(m-r)$-dimensional spaces, we must sum over all possible dimensions k and t, which yields the following theorem.

Theorem 3.5.1 *The number of $(m-r)$-dimensional affine spaces in $\mathbf{AG}(m, q)$ having no affine points in common with a fixed symmetric difference formed by two affine $(m-r)$-dimensional spaces α and β, but having at least one affine intersection point with the $(m-r-\mu)$-dimensional space $\alpha \cap \beta$, is equal to*

$$\sum_{k=0}^{m-r-\mu} \sum_{t=k}^{m-r} N(k)\psi(t, k)\rho(m-r, k, t).$$

2) Now suppose that all intersection points of Π_{m-r} and $\alpha \cup \beta$ lie at infinity.

We start from such an intersection at infinity. Denote the intersections of α and β with the space at infinity by α_∞ and β_∞ respectively. These are $(m-r-1)$-dimensional spaces intersecting in an $(m-r-\mu-1)$-dimensional space.

Suppose that the affine space Π_{m-r} intersects α_∞ in a k-dimensional space Π_k, β_∞ in an l-dimensional space Π_l, and $\alpha_\infty \cap \beta_\infty$ in an u-dimensional space Π_u. If these intersection spaces are given, we call this a (k, l, u)*-starting configuration.*

We denote the number of a-dimensional spaces contained in Π_∞, and intersecting α_∞, β_∞, $\alpha_\infty \cap \beta_\infty$, and $\langle \alpha_\infty, \beta_\infty \rangle$ in a k-dimensional, l-dimensional, u-dimensional, and f-dimensional space, respectively, by $\psi(a, k, l, u, f)$.

The number of u-dimensional spaces inside an $(m-r-\mu-1)$-dimensional space is equal to $\phi(u; m-r-\mu-1, q)$. Suppose that we have fixed an u-dimensional space Π_u inside $\alpha_\infty \cap \beta_\infty$. We count in how many ways we can extend Π_u to a k-dimensional space Π_k in α_∞ that intersects $\alpha_\infty \cap \beta_\infty$ exactly in Π_u. Project the $(m-1)$-dimensional space at infinity $\tilde{\Pi}_\infty$ of $\mathbf{AG}(m, q)$ from Π_u onto an $(m-u-2)$-dimensional complementary space of Π_u in $\tilde{\Pi}_\infty$. Then α_∞ and $\alpha_\infty \cap \beta_\infty$ are projected onto an $(m-r-u-2)$-dimensional space $\Pi_{m-r-u-2}$ and an $(m-r-\mu-u-2)$-dimensional space $\Pi_{m-r-\mu-u-2}$ respectively. We must choose a $(k-u-1)$-dimensional space inside $\Pi_{m-r-u-2}$ skew to $\Pi_{m-r-\mu-u-2}$. Hence, by Lemma 3.4.5, we have $Skew(m-r-u-2, m-r-\mu-u-2, k-u-1)$ choices. Hence,

$$E_1(k,u) = \prod_{a=u}^{k-1} \frac{(q^{m-r-a-1} - q^{m-r-\mu-u-1})}{q^{a-u+1}-1}.$$

In a similar way, the number of l-dimensional spaces inside β_∞ that intersect $\alpha_\infty \cap \beta_\infty$ exactly in a given u-dimensional space is equal to

$$E_2(l,u) = \prod_{a=u}^{l-1} \frac{(q^{m-r-a-1} - q^{m-r-\mu-u-1})}{q^{a-u+1}-1}.$$

The number $S(k,l,u)$ of (k,l,u)-starting configurations is equal to

$$\psi(k+l-u, k, l, u, k+l-u) = \phi(u; m-r-\mu-1, q)E_1(k,u)E_2(l,u).$$

So suppose that we now have a certain (k,l,u)-starting configuration and we look at the $(k+l-u)$-dimensional space Π_{k+l-u} generated by the spaces of this configuration.

Similarly to the previous case, we will inductively extend this space in $\tilde{\Pi}_\infty$ to larger spaces without changing the intersection spaces with α and β. We will do this in two steps: first we extend this space to an f-dimensional space Π_f lying completely in $\langle \alpha_\infty, \beta_\infty \rangle$, then we extend Π_f to an $(m-r-1)$-dimensional space in $\tilde{\Pi}_\infty$ without changing the intersection space Π_f with $\langle \alpha_\infty, \beta_\infty \rangle$.

Denote by $\lambda(k,l,u,s)$ the number of s-dimensional spaces lying completely in $\langle \alpha_\infty, \beta_\infty \rangle$ which intersect α_∞, β_∞, and $\alpha_\infty \cap \beta_\infty$ in a given k-, l-, and u-dimensional space respectively. Suppose that we have already constructed an s-dimensional space Π_s in $\langle \alpha_\infty, \beta_\infty \rangle$ with the correct intersection dimensions with α_∞, β_∞, and $\alpha_\infty \cap \beta_\infty$.

We project onto a complementary space of Π_s in the $(m-r+\mu-1)$-dimensional space $\langle \alpha_\infty, \beta_\infty \rangle$; this is a space Π_s^* of dimension $m-r+\mu-s-2$. The projection of α_∞ from Π_s onto Π_s^* is an $(m-r-k-2)$-dimensional space α_∞^*. Similarly, β_∞ is projected on an $(m-r-2-l)$-dimensional space β_∞^*, and $\alpha_\infty^* \cap \beta_\infty^*$ is a space of dimension

$$(m-r-k-2)+(m-r-l-2)-(m-r+\mu-s-2) = m-r-k-l-\mu+s-2.$$

We want to extend Π_s in $\langle \alpha_\infty, \beta_\infty \rangle$ without changing the intersections with α_∞ or β_∞.

Hence, we have to choose a point in Π_s^* not belonging to the projected spaces α_∞^* or β_∞^*, so we find the following number $Ext_S(k,l,u,s)$ of extension points

$$\frac{q^{m-r+\mu-s-1}-1}{q-1}-\frac{q^{m-r-k-1}-1}{q-1}-\frac{q^{m-r-l-1}-1}{q-1}+\frac{q^{m-r-k-l-\mu+s-1}-1}{q-1}.$$

An $(s+1)$-dimensional space contains $\phi(0; s-(k+l-u), q)$ s-dimensional spaces containing a given $(k+l-u)$-dimensional space.

So we can calculate $\lambda(k,l,u,s)$ by induction, with $\lambda(k,l,u,k+l-u)=1$, by the induction formula

$$\lambda(k,l,u,s+1)=\frac{\lambda(k,l,u,s)Ext_S(k,l,u,s)}{\phi(0; s-(k+l-u), q)}.$$

We call an f-dimensional space constructed in this way a (k,l,u,f)*-space.*

Next suppose that we have a given (k,l,u,f)-space Π_f. We project again from Π_f onto a complementary space Π_f^* of Π_f; this time complementary to Π_f in $\tilde{\Pi}_\infty$. So suppose that we already have constructed all a-dimensional spaces at infinity, which intersect α_∞, β_∞, $\alpha_\infty\cap\beta_\infty$, and $\langle\alpha_\infty,\beta_\infty\rangle$ in a given k-, l-, u-, and f-dimensional space respectively. Consider one of these spaces Π_a. We want to extend Π_a without changing the intersections with α_∞, β_∞, and $\langle\alpha_\infty,\beta_\infty\rangle$.

Hence, we have to choose a point in Π_a^* not belonging to the projected space $\langle\alpha_\infty,\beta_\infty\rangle^*$. Here $\langle\alpha_\infty,\beta_\infty\rangle$ is an $(m-r+\mu-1)$-dimensional space, hence $\langle\alpha_\infty,\beta_\infty\rangle^*$ has dimension $m-r+\mu-f-2$. So we find the following number of extension points

$$Q(a,k,l,u,f)=\frac{q^{m-1-a}-1}{q-1}-\frac{q^{m-r+\mu-f-1}-1}{q-1}.$$

In an $(a+1)$-dimensional space, there are

$$\phi(a-f-1; (a+1)-f-1, q)$$

a-dimensional spaces containing a given f-dimensional space. Hence, we have as starting formula $\psi(f,k,l,u,f)=\lambda(k,l,u,f)$ and the following induction formula,

$$\psi(a+1,k,l,u,f)=\frac{\psi(a,k,l,u,f)Q(a,k,l,u,f)}{\phi(a-f-1; a-f, q)}.$$

Suppose that we have an $(m-r-1)$-dimensional space Δ lying at infinity, which is the extension of a (k,l,u,f)-space. We still have to extend Δ to an $(m-r)$-dimensional space, not lying at infinity. We project from Δ onto a complementary space Δ^* of Δ in $\mathbf{PG}(m,q)$; the space Δ^* has dimension $m-(m-r-1)-1=r$. The spaces α and β, respectively, are projected onto spaces α^* and β^*, of dimension $m-r-k-1$ and $m-r-l-1$. The space $\alpha^* \cap \beta^*$ has dimension $(m-r-k-1)+(m-r-l-1)-(m-r+\mu-f-1) = m-r-k-l-\mu+f-1$.

Since we have to choose affine points not lying in $\alpha^* \cup \beta^*$, we find the following number of extension points:

$$E(k,l,u,f) = q^r - q^{m-r-1-k} - q^{m-r-1-l} + q^{m-r-k-l-\mu+f-1}.$$

The total number of affine $(m-r)$-dimensional spaces intersecting a given symmetric difference only at infinity is found by summing over all possible (k,l,u)-starting configurations and the corresponding (k,l,u,f)-spaces. We collect the restrictions on k, l, u, and f by introducing the following set:

$$\begin{aligned} Res(k,l,u,f) = \{(k,l,u,f) | -1 \le k,\ l \le m-r-1;\ -1 \le u \le m-r-\mu-1; \\ \max(k-\mu, l-\mu, -1) \le u \le k,l;\ k+l-u \le f \le m-r-1\}. \end{aligned}$$

With the above introduced notations, we get the following theorem.

Theorem 3.5.2 *The number of $(m-r)$-dimensional affine spaces having no affine points in common with fixed $(m-r)$-dimensional affine spaces α and β, which intersect in an affine $(m-r-\mu)$-dimensional space and together form a symmetric difference is equal to*

$$\sum_{(k,l,u,f)\in Res(k,l,u,f)} S(k,l,u)\psi(m-r-1,k,l,u,f)E(k,l,u,f).$$

Proof We have $S(k,l,u)$ possibilities to obtain a (k,l,u)-starting configuration Π_{k+l-u}. We have $\lambda(k,l,u,f)$ ways to extend a given (k,l,u)-starting configuration to an f-dimensional space Π_f contained in $\langle \alpha_\infty, \beta_\infty \rangle$ which intersects $\alpha_\infty \cup \beta_\infty$ in the given (k,l,u)-starting configuration. A given space Π_f can be extended at infinity to an $(m-r-1)$-dimensional space Π_{m-r-1} intersecting $\langle \alpha_\infty, \beta_\infty \rangle$ in Π_f in $\psi(m-r-1,k,l,u,f)$ ways. A given space Π_{m-r-1} can be extended to an affine space Π_{m-r} having no affine points in common with $\alpha \cup \beta$ in $E(k,l,u,f)$ ways. □

The previous two theorems together yield the following theorem.

Theorem 3.5.3 *The number of $(m-r)$-dimensional affine spaces having no affine points in common with a fixed symmetric difference, formed by two $(m-r)$-dimensional affine spaces α and β which intersect in an affine $(m-r-\mu)$-dimensional space, is equal to $N_a + N_{ea}$, where*

$$N_a = \sum_{k=0}^{m-r-\mu} \sum_{t=k}^{m-r} N(k)\psi(t,k)\rho(m-r,k,t),$$

$$N_{ea} = \sum_{(k,l,u,f)\in Res(k,l,u,f)} S(k,l,u)\psi(m-r-1,k,l,u,f)E(k,l,u,f).$$

3.6 Interchange with the symmetric difference

We want to obtain the number of minimal codewords in the coding-theoretical setting corresponding with the case $q = 2$. In the geometrical translation of the problem, we count the number of non-minimal codewords; geometrically they correspond to two geometrical objects of $\mathbf{AG}(m, q)$ which have no affine points in common. The non-minimal codeword then corresponds to the union of the affine point sets of the two objects. It might happen however that a given affine point set corresponding to a non-minimal codeword can be split in several ways into two disjoint affine point sets forming the correct geometrical objects. Then we have counted these objects more than once. In which cases this happens, is investigated in this section and in the one that follows.

Suppose that $c_1 \cup c_2 = c_3 \cup c_4$ considered as affine point sets, where c_1 and c_3 are two $(m-r)$-dimensional affine spaces and where c_2 is a symmetric difference, formed by two $(m-r)$-dimensional spaces α and β. There are two possibilities for $c_1 \cap c_3$. Either it is an empty intersection or $c_1 \cap c_3$ is a t-dimensional space, hence $|c_1 \cap c_3| = q^t$ for a certain t, with $0 \leq t \leq m-r$.

If $t = m-r$, then c_1 and c_3 are equal. This means that c_2 and c_4 are equal when considered as affine point sets. Hence, c_4 also has to be a symmetric difference. Suppose that c_4 is formed by two $(m-r)$-dimensional spaces γ and δ. We may assume that none of them is equal to α or β. One of γ and δ, say γ, has to cover at least $\frac{q^{m-r}-q^{m-r-\mu}}{2} > q^{m-r-2}$ points of the symmetric difference belonging to α. Hence, γ intersects α in an $(m-r-1)$-dimensional space. Furthermore, even if δ covers q^{m-r-1} points of β, there are still $(q-1)q^{m-r-1} - q^{m-r-\mu}$ points of β left to be covered by γ. Since $\mu \geq 3$, this means that also γ intersects β in an $(m-r-1)$-dimensional space. Since α and β intersect in an $(m-r-\mu)$-dimensional space, this yields a contradiction with the dimension theorem, because then $\dim\langle\alpha,\beta\rangle \leq m-r+2$, while $\dim\langle\alpha,\beta\rangle \geq m-r+3$.

So from here on, we will suppose that $t < m-r$.

1) First suppose that $c_1 \cap c_3$ is empty. This means that c_3 is completely contained in c_2 and that $q = 2$, since $c_3 = (c_3 \cap \alpha) \cup (c_3 \cap \beta)$; so c_3 is the union of two $(m-r-1)$-dimensional spaces. So c_3 needs to have $(m-r-1)$-dimensional spaces in common with α and β, and these spaces should intersect each other in an $(m-r-2)$-dimensional space at infinity. But $\alpha \cap \beta$ intersects infinity only in an $(m-r-\mu-1)$-dimensional space, $\mu \geq 3$, so this case is impossible.

2) Next suppose that c_1 and c_3 have a non-empty intersection, so suppose that $|c_1 \cap c_3| = q^t$, $0 \leq t < m-r$. Then we have

$$|c_2 \cap c_3| = q^{m-r} - q^t = q^t(q^{m-r-t} - 1).$$

Denote the dimensions of the intersections of c_3 with α, β, and $\alpha \cap \beta$, by k, l, and u respectively. We consider several cases, and we determine in which cases a possible interchange can occur. We always assume that $k \geq l$ without loss of generality. The symmetric situation is taken into account when we make the actual calculations in Theorem 3.6.1. We first treat the different cases. Our arguments will also show that in case of an interchange $c_1 + c_2 = c_3 + c_4$, there is never a swap from a sum $c_1 + c_2$ consisting of an $(m-r)$-dimensional space $c_1 = \mathbf{AG}(m-r, q)$ and a symmetric difference c_2 to a sum $c_3 + c_4$ consisting of an $(m-r)$-dimensional space $c_3 = \mathbf{AG}(m-r, q)$ and a quadric c_4.

Case 1: $k \geq l = u \geq 0$. Then there are $q^k - q^u$ points contained in $c_2 \cap c_3$. Comparing this number with the previous expression, we find the equation

$$q^t(q^{m-r-t} - 1) = q^u(q^{k-u} - 1).$$

After comparing both sides and their respective powers of q, we find $t = u$ and $m - r - t = k - u$, so $k = m - r$. Hence, c_3 is equal to α. So $l = m - r - \mu = u$. What has happened is the following: c_1 contains $\alpha \cap \beta$; when considering $c_1 + c_2$, this makes $c_3 = \alpha$ possible. For a given pair (c_1, c_2) satisfying the conditions above, there will be one other pair corresponding to $c_3 = \alpha$ which also yields the same affine point set. Considering also the symmetric configuration with $c_3 = \beta$, this type of configuration will be counted three times. The number of such configurations follows from the proof of Theorem 3.5.1 and the number of symmetric difference objects which is $A = \frac{\phi(r-1;\mu-1+r,q)F_1(m,r,\mu,q)F_2(m,r,\mu,q)}{2}$ by Section 3.3, and using the same notations as before this number is equal to

$$\sum_{t=m-r-\mu}^{m-r} \psi(t, m-r-\mu)\rho(m-r, m-r-\mu, t)A,$$

where we have substituted $k = m - r - \mu$ and replaced $N(k = m - r - \mu)$ by 1 in the sum stated in Theorem 3.5.1; see the beginning of Section 3.5 for the definition of $N(k)$.

Case 2: $k \geq l > u \geq 0$. This time we get

$$q^t(q^{m-r-t} - 1) = q^k + q^l - 2q^u = q^u(q^{k-u} + q^{l-u} - 2).$$

If $q \neq 2$, then comparing the powers of q yields $t = u$ and the equation

$$q^{m-r-t} - 1 = q^{k-u} + q^{l-u} - 2.$$

A calculation modulo q yields a contradiction for this equation.

If $q = 2$, we have the equation

$$2^t(2^{m-r-t} - 1) = 2^{u+1}(2^{k-u-1} + 2^{l-u-1} - 1).$$

a) If $l = u + 1$, we get
$$2^k = 2^t(2^{m-r-t} - 1).$$

Hence, $k = t$ and $m - r - t = 1$, so $k = t = m - r - 1$. This means that $c_1 \cap c_3$ is a hyperplane and that $c_2 \cap c_3$ has to be the parallel hyperplane of it in c_3. The space $c_3 \cap \alpha$ is an $(m - r - 1)$-dimensional space, the space $c_3 \cap c_1$ is also an $(m - r - 1)$-dimensional space, and these two spaces intersect in a u-dimensional space, where $u \leq m - r - \mu$. For c_3 shares an $0 \leq u \leq (m - r - \mu)$-dimensional space with $\alpha \cap \beta$, so c_3 shares a point with $\alpha \cap \beta$; this point must lie in $c_3 \cap c_1$. So they span at least a space of dimension $(m - r - 1) + (m - r - 1) - (m - r - \mu) = m - r + \mu - 2$. This yields a contradiction since $\mu \geq 3$ and $\dim c_3 = m - r$.

b) If $l > u + 1$, then we get $t = u + 1$ and the equation
$$2^{k-(u+1)} + 2^{l-(u+1)} = 2^{m-r-t}.$$

Hence, we get $k = l$ and so the equation $2^{k-u} = 2^{m-r-t}$. This implies $k - u = m - r - t = m - r - (u + 1)$, hence $k = m - r - 1$. But then c_3 has dimension $k + l - u \geq m - r - 1 + l - u > m - r$, which yields a contradiction.

Case 3: $k \geq l \geq 0$, $u = -1$, where $u = -1$ denotes that c_3 has no affine points in common with $\alpha \cap \beta$. We find
$$q^t(q^{m-r-t} - 1) = q^l(q^{k-l} + 1).$$

For $q = 2$ and $k = l$, we find $t = l + 1$ and $t = m - r - 1$. So $c_1 \cap c_3$ is an $(m-r-1)$-dimensional space, and $\alpha \cap c_3$ and $\beta \cap c_3$ are $(m-r-2)$-dimensional spaces. This $(m - r - 1)$-dimensional and these two $(m - r - 2)$-dimensional spaces must be parallel since their union must be c_3, so they all pass through the same $(m - r - 3)$-dimensional space at infinity; but then in particular $\dim(\alpha_\infty \cap \beta_\infty) \geq m - r - 3$, but this is impossible since $\dim(\alpha_\infty \cap \beta_\infty) = m - r - \mu - 1 \leq m - r - 4$, since $\mu \geq 3$.

In the other cases, comparing powers of q yields $t = l$, and the remaining equation is
$$q^{m-r-l} - 2 = q^{k-l}.$$

If $q > 3$, this yields a contradiction. If $q = 2$, we get $k = m-r-1$, $l = m-r-2$, so these spaces should intersect at least in an $(m - r - 3)$-dimensional space at infinity, but the space at infinity $\alpha_\infty \cap \beta_\infty$ only has dimension $m-r-\mu-1$, $\mu \geq 3$. This yields a contradiction. If $q = 3$, then we obtain $k = l = m - r - 1$, but this contradicts the fact that $\alpha_\infty \cap \beta_\infty$ is only an $(m - r - \mu - 1)$-dimensional space.

Case 4: $k \geq 0$, $u = -1$, and $l = -1$. Then the equation becomes
$$q^t(q^{m-r-t} - 1) = q^k.$$

Comparing the prime factors of both sides yields $q^{m-r-t}-1=1$ and $k=t$, hence $q=2$ and $k=m-r-1$. Since $l=-1$, c_3 intersects α_∞ exactly in an $(m-r-2)$-dimensional space Π_{m-r-2}. Furthermore, the space Π_{m-r-2} has to contain the $(m-r-\mu-1)$-dimensional space $\alpha_\infty \cap \beta_\infty$ completely since the $(m-r-1)$-dimensional space $c_2 \cap c_3$ through Π_{m-r-2} has no affine points in common with $\alpha \cap \beta$. The intersection $c_1 \cap c_3$ has to be the parallel $(m-r-1)$-dimensional space to $c_3 \cap c_2$ in c_3. Moreover, since $l=-1$, c_3 intersects $\alpha_\infty \cup \beta_\infty$ exactly in an $(m-r-2)$-dimensional space Π_{m-r-2} through $\alpha_\infty \cap \beta_\infty$ or c_3 intersects $\alpha_\infty \cup \beta_\infty$ in an $(m-r-2)$-dimensional space Π_{m-r-2} completely lying in α_∞ and passing through $\alpha_\infty \cap \beta_\infty$ and in an $(m-r-\mu)$-dimensional space $\Pi_{m-r-\mu}$ completely lying in β_∞ and passing through $\alpha_\infty \cap \beta_\infty$.

The number of $(m-r-2)$-dimensional spaces completely containing an $(m-r-\mu-1)$-dimensional space inside an $(m-r-1)$-dimensional space is equal to $2^\mu - 1$.

Hence, in this Case 4, for a given symmetric difference c_2, the spaces c_1 for which there are interchange possibilities are the following.

(1) Assume that the space c_1 intersects α_∞ in an $(m-r-2)$-dimensional space lying completely in α_∞, and containing $\alpha_\infty \cap \beta_\infty$. Suppose that we have such a c_1 together with the fixed c_2. We may select one of the two $(m-r-1)$-dimensional spaces Π_{m-r-1} through Π_{m-r-2} inside c_1. The space Π_{m-r-1} together with the unique $(m-r-1)$-dimensional space in α through Π_{m-r-2} and skew to β forms the space c_3 which is then used for interchange. So in this case we have two interchange possibilities w.r.t. the original c_1 and c_2.

We calculate the number of such spaces c_1. We start with an $(m-r-2)$-dimensional space Π_{m-r-2} which is completely contained in α_∞ and which contains the $(m-r-\mu-1)$-dimensional space $\alpha_\infty \cap \beta_\infty$ completely. So we have $2^\mu - 1$ such starting possibilities for the intersection $c_1 \cap \alpha_\infty$, where $c_1 \cap \alpha \cap \Pi_\infty$ has dimension $m-r-2$.

We calculate in how many ways we can extend Π_{m-r-2} completely contained in α_∞ to an $(m-r)$-dimensional affine space having exactly Π_{m-r-2} in common with $\alpha_\infty \cup \beta_\infty$, or Π_{m-r-2} with α_∞ and $\Pi_{m-r-\mu}$ with β_∞. We proceed in two steps. First, we extend Π_{m-r-2} to an $(m-r-1)$-dimensional space at infinity.

We project from Π_{m-r-2} onto an r-dimensional space Π_r which is complementary to Π_{m-r-2} in $\tilde{\Pi}_\infty$, the space at infinity of $\mathbf{AG}(m,q)$. Then α_∞ is projected onto a point α^*, β_∞ is projected onto a $(\mu-1)$-dimensional space β^*, and $\langle \alpha_\infty, \beta_\infty \rangle$ is projected onto a μ-dimensional space. Hence, $\alpha^* \cap \beta^*$ has dimension -1. We can either select:

(a) a point contained in $\langle \alpha^*, \beta^* \rangle$, but not in $\alpha^* \cup \beta^*$. We have $2^{\mu+1}-$

$1-(2^\mu-1)-1=2^\mu-1$ choices for the extension point in Π_r to get into this situation.

(b) a point contained in β^*. We have $2^\mu-1$ possibilities for this extension point to get into this situation.

(c) a point outside of $\langle\alpha^*,\beta^*\rangle$. We have $2^{r+1}-1-(2^{\mu+1}-1)=2^{r+1}-2^{\mu+1}$ choices for the extension point in Π_r to get into this situation.

Next, we count the number of affine extension possibilities in all cases (a), (b), and (c) above.

(a) We still have to extend the $(m-r-1)$-dimensional space Π_{m-r-1} to an affine $(m-r)$-dimensional space. We project from Π_{m-r-1} onto an r-dimensional space Π_r complementary to Π_{m-r-1} in the m-dimensional space $\mathbf{PG}(m,q)$. Then α is projected onto a line α^*, β onto an $m-r-(m-r-\mu-1)-1=\mu$-dimensional space β^*, and $\langle\alpha^*,\beta^*\rangle$ has dimension $m-r+\mu-(m-r-1)-1=\mu$, so $\alpha^*\subset\beta^*$. We have to select an affine point not contained in $\alpha^*\cup\beta^*$. Hence, we have 2^r-2^μ choices for our extension point. This gives in total $(2^\mu-1)(2^\mu-1)(2^r-2^\mu)$ such affine $(m-r)$-dimensional spaces c_1, all giving two interchange possibilities.

(b) We still have to extend the $(m-r-1)$-dimensional space Π_{m-r-1} to an affine $(m-r)$-dimensional space. We project from Π_{m-r-1} onto an r-dimensional space Π_r complementary to Π_{m-r-1} in the m-dimensional space $\mathbf{PG}(m,q)$. Then α is projected onto a line α^*, β onto an $m-r-(m-r-\mu)-1=(\mu-1)$-dimensional space β^*, and $\langle\alpha^*,\beta^*\rangle$ has dimension $m-r+\mu-(m-r-1)-1=\mu$, so $\dim(\alpha^*\cap\beta^*)=0$, i.e., it is equal to a point. This intersection point of α^* and β^* must correspond to the affine extension of Π_{m-r-1} by an affine point of $\alpha\cap\beta$. So we have $2^r-2^{\mu-1}-2+1=2^r-2^{\mu-1}-1$ affine choices for our extension point. This gives in total $(2^\mu-1)(2^\mu-1)(2^r-2^{\mu-1}-1)$ such affine $(m-r)$-dimensional spaces c_1, all giving two interchange possibilities.

(c) We still have to extend the $(m-r-1)$-dimensional space Π_{m-r-1} to an affine $(m-r)$-dimensional space. We project from Π_{m-r-1} onto an r-dimensional space Π_r complementary to Π_{m-r-1} in $\mathbf{PG}(m,q)$. Then α is projected onto a line α^*, β onto a μ-dimensional space β^*, and $\langle\alpha^*,\beta^*\rangle$ has dimension $m-r+\mu-(m-r-2)-1=\mu+1$. Hence, $\alpha^*\cap\beta^*$ is an affine point. The number of affine points not contained in $\alpha^*\cup\beta^*$ is equal to $2^r-2-2^\mu+1=2^r-2^\mu-1$. This gives in total $(2^\mu-1)(2^{r+1}-2^{\mu+1})(2^r-2^\mu-1)$ such affine $(m-r)$-dimensional spaces c_1; all giving two interchange possibilities.

(2) Assume that the space c_1 intersects $\alpha_\infty\cup\beta_\infty$ in the $(m-r-1)$-dimensional space α_∞. For each of the $2^\mu-1$ $(m-r-2)$-dimensional spaces contained in α_∞ containing completely the $(m-r-\mu-1)$-dimensional space $\alpha_\infty\cap\beta_\infty$, we have the interchange possibilities as described in (1), hence we

have $2 \cdot (2^{\mu} - 1)$ possibilities for an interchange in this case. We calculate the number of such spaces c_1. We start with α_∞. The number of ways to extend α_∞ to an affine $(m-r)$-dimensional space c_1 is calculated as follows. We project from α_∞ onto an r-dimensional space complementary to α_∞ in $\mathbf{PG}(m,q)$. Then α is projected onto a point α^*, β onto a μ-dimensional space β^*, and $\langle \alpha, \beta \rangle$ onto an $m-r+\mu-(m-r-1)-1=\mu$-dimensional space. We have to select an affine point not contained in $\alpha^* \cup \beta^* = \beta^*$. Hence, we have $2^r - 2^{\mu}$ choices for an extension. So for a given c_2, we find $2^r - 2^{\mu}$ such spaces c_1. This gives $2 \cdot (2^{\mu}-1)+1$ times the same sum $c_1 + c_2$ for a given choice for c_2.

This concludes the discussion of the four cases, where we assumed that $k \geq l$. For the actual calculations in Theorem 3.6.1, the symmetric situation $l \geq k$ is of course also considered.

If $q \neq 2$, then case 1 is the only case which occurs. If $q = 2$, then both case 1 and case 4 can occur. We show the following. After having made an interchange of type case 4, one cannot get a configuration where an interchange of type case 1 is possible. For it is clear in both cases that the $(m-r-\mu)$-dimensional affine intersection space $\alpha \cap \beta$ of the two $(m-r)$-dimensional affine spaces α and β forming the symmetric difference c_4 has to be the same as the one of the symmetric difference c_2. Since in case 1, c_3 contains this intersection space and in case 4, c_3 does not contain this intersection space, we cannot have switched.

We also notice that if $c_1 + c_2 = c_3 + c_4$, for c_1 and c_3 affine $(m-r)$-dimensional spaces and c_2 a symmetric difference, then also c_4 is a symmetric difference.

The above results now yield the following theorem.

Theorem 3.6.1 *Denote the number of symmetric differences consisting of two affine $(m-r)$-dimensional spaces intersecting in an affine $(m-r-\mu)$-dimensional space*

$$\frac{\phi(r-1; \mu-1+r, q) F_1(m,r,\mu,q) F_2(m,r,\mu,q)}{2}$$

by A. Then there are

$$\sum_{t=m-r-\mu}^{m-r} \psi(t, m-r-\mu) \rho(m-r, m-r-\mu, t) A$$

pairs (c_1, c_2), where c_1 is an affine $(m-r)$-dimensional space and where c_2 is a symmetric difference, which can be partitioned into blocks of three pairs, such that the three pairs of a given block determine the same affine union.

Furthermore, if $q = 2$, there are an extra

$$2\cdot(2^{\mu}-1)((2^{\mu}-1)(2^{r}-2^{\mu})+(2^{\mu}-1)(2^{r}-2^{\mu-1}-1)+(2^{r+1}-2^{\mu+1})(2^{r}-2^{\mu}-1))A$$

pairs (c_1, c_2), where c_1 is an affine $(m-r)$-dimensional space and where c_2 is a symmetric difference, which can be partitioned into blocks of three pairs, such that the three pairs of a given block determine the same affine union.

Finally, if $q = 2$, there are

$$2\cdot(2^{r}-2^{\mu})A$$

pairs (c_1, c_2), where c_1 is an affine $(m-r)$-dimensional space and where c_2 is a symmetric difference, which can be partitioned into blocks of $2\cdot(2^{\mu}-1)+1$ *pairs, such that the* $2\cdot(2^{\mu}-1)+1$ *pairs of a given block determine the same affine union.*

Proof The interchanges only occur in cases 1 and 4. In case 1, the interchange occurs for all q. We obtain always blocks of three pairs (c_1, c_2) determining the same affine union.

In case 4, which only can occur for $q = 2$, we get blocks of three pairs (c_1, c_2) determining the same affine union (case (1)), and blocks of $2\cdot(2^{\mu}-1)+1$ pairs determining the same affine union (case (2)).

In the arguments above, we always assumed $k \geq l$; now we also have to include the possibility $l \geq k$; this explains the leftmost factor 2 in the two final formulas in the statement of this theorem. For the first formula $\sum_{t=m-r-\mu}^{m-r}\psi(t, m-r-\mu)\rho(m-r, m-r-\mu, t)A$, the factor 2 is not necessary since c_1 passes through $\alpha\cap\beta$, so c_1 has the same status w.r.t. α and β. □

3.7 Interchange with quadrics

Suppose that $c_1 \cup c_2 = c_3 \cup c_4$ as affine point sets, where c_1 and c_3 are $(m-r)$-dimensional affine spaces and where c_2 is a cone. Recall that $c_1 \cap c_2 = \emptyset$ and $c_3 \cap c_4 = \emptyset$, if they are considered as affine point sets. From the previous section, it follows that if this interchange effectively occurs, also c_4 is a quadric.

1) First suppose that $c_1 \cap c_3 = \emptyset$. Then all affine points of c_3 lie on c_2. But c_3 is a space of dimension $m-r$ while the largest spaces lying completely on c_2 are of dimension

$$\mu - 1 + m - r + 1 - 2\mu + 1 = m - r - \mu + 1.$$

This yields a contradiction since $\mu > 1$.

2) Next suppose that $c_1 \cap c_3$ is a t-dimensional affine space. If $t = m-r$, then $c_1 = c_3$. Hence, c_2 and c_4 are equal if considered as affine point sets. If

c_4 is a cone, then $c_2 = c_4$ because the cone is completely determined by its affine point set. So suppose that c_4 is a symmetric difference. This yields a contradiction, since the quadrics determine an $(m-r+2)$-dimensional space and the symmetric differences an $(m-r+\mu)$-dimensional space, where $\mu \geq 3$.

Hence, we may suppose that $0 \leq t < m-r$, so $|c_1 \cap c_3| = q^t$ and $|c_2 \cap c_3| = q^{m-r} - q^t$.

Suppose that c_3 intersects the projective completion Π of the $(m-r+2)$-dimensional affine space spanned by the cone $c_2 = \Gamma Q(2\mu, q)$ in an l-dimensional space Π_l. Furthermore, suppose that c_3 shares a k-dimensional space Π_k with the vertex Γ of the cone $c_2 = \Gamma Q(2\mu, q)$. Consider a space complementary to the space Π_k in Π_l; this is an $(l-k-1)$-dimensional space Π_{l-k-1} chosen in such a way that $c_2 \cap \Pi_{l-k-1}$ is maximal. Suppose that c_3 intersects $c_2 \cap \Pi_{l-k-1}$ in z affine points. This means that $|c_2 \cap c_3| = zq^{k+1}$. Take a space Π_b complementary to the vertex space of c_2 in Π and containing Π_{l-k-1}. We will call this space the *base space*.

Comparing the two equations above for the number of affine intersection points of c_2 and c_3, and rewriting them, yields the following equation,

$$q^{m-r-t} = 1 + zq^{k+1-t}.$$

Since $m - r > t$, we have $zq^{k+1-t} \geq 1$. We introduce the variables x and y by putting $t = m-r-x$ and $k = t-y = m-r-(x+y)$. Since k is at most the dimension of the vertex Γ of $c_2 = \Gamma Q(2\mu, q)$, we have

$$m - r - (x+y) \leq m - r + 1 - 2\mu, \text{ so } x + y \geq 2\mu - 1.$$

We want to prove that in case of interchange, c_3 has to contain the vertex Γ of $c_2 = \Gamma Q(2\mu, q)$; this means $x + y = 2\mu - 1$.

The base space Π_b contains $q^{\mu-1}(q^\mu - 1)$ affine points of the quadric Ψ, so z can be at most this number. Combining this with $zq^{k+1-t} \geq 1$ yields:

$$q^{\mu-y}(q^\mu - 1) \geq 1.$$

Hence, we find that $q^{y-\mu} < q^\mu$, and since y is an integer, we have

$$y \leq 2\mu - 1.$$

Next suppose that $x + y = 2\mu - 1 + \psi$, with $\psi > 1$. Then using previous expressions, we find

$$z = q^{m-r-k-1} - q^{t-k-1} = q^{x+y-1} - q^{y-1} = q^{2\mu-1+\psi-1} - q^{y-1}.$$

So bringing into account that this number is at most the number $q^{2\mu-1} - q^{\mu-1}$ of base points of the quadric Ψ, yields the inequality

$$q^{2\mu-1+\psi-1} - q^{y-1} \leq q^{\mu-1}(q^\mu - 1).$$

After dividing both sides by $q^{\mu-1}$ and rearranging terms, we find

$$q^{\mu}(q^{\psi-1}-1) \leq q^{y-\mu}-1.$$

Since $\psi > 1$, we have

$$q^{\mu} \leq q^{\mu}(q^{\psi-1}-1) \leq q^{y-\mu}-1 \leq q^{y-\mu}.$$

It follows that $q^{\mu} \leq q^{y-\mu}$, which contradicts $y \leq 2\mu-1$.

So we are left with two possibilities. Either $x+y=2\mu-1$ or $x+y=2\mu$. We want to eliminate the latter possibility.

So suppose that $x+y=2\mu$. The same technique as above, but now with $\psi=1$, yields that $y \geq \mu$. We introduce an other variable s by setting $y=\mu+s$. Since we also proved that $y \leq 2\mu-1$, the variable s satisfies $0 \leq s \leq \mu-1$. We have

$$z = q^{\mu-1}(q^{\mu}-q^{s}).$$

If $s=0$, then $x=y=\mu$, hence $z=q^{2\mu-1}-q^{\mu-1}$ equals the number of affine points in the base $Q(2\mu,q)$ belonging to the quadric Ψ. In this case, the dimension theorem yields that the dimension of c_3 is at least $k+2\mu+1 = m-r-2\mu+2\mu+1 = m-r+1$, a contradiction.

If $1 \leq s < \mu-1$, we find $z > q^{2\mu-2}$, so c_3 intersects the space Π_b spanned by the base of Ψ either in a $(2\mu-1)$-dimensional affine space or in a 2μ-dimensional affine space. The latter is impossible by the dimension argument as shown above for $s=0$.

We will treat the case $s=\mu-1$ in detail first.

If $s=\mu-1$, then $z=q^{2\mu-2}(q-1)$. If $q \neq 2$, then $z > |\mathbf{AG}(2\mu-2,q)|$, so c_3 intersects the space Π_b in a $(2\mu-1)$-dimensional space; by the dimension argument already used above, $c_3 \cap \Pi_b$ cannot be 2μ-dimensional. So assume that $q=2$, hence $z=2^{2\mu-2}$. Either $\Pi_b \cap c_3$ is $(2\mu-1)$-dimensional or $(2\mu-2)$-dimensional.

(a) If $q=2$, $s=\mu-1$, and $\Pi_b \cap c_3$ is $(2\mu-2)$-dimensional, then $|\Pi_b \cap c_3| = z = 2^{2\mu-2}$, so $\Pi_b \cap c_3$ is contained in the affine part of the non-singular parabolic quadric $Q(2\mu,2)$. An affine quadric in $(2\mu-2)$-dimensional affine space coincides with the space if and only if it consists of two parallel affine $(2\mu-3)$-dimensional spaces. As a generator of $Q(2\mu,2)$ has dimension $\mu-1$, it follows that $2\mu-3 \leq \mu-1$, so $\mu \leq 2$. If $\mu=2$, then we would get two parallel affine lines. But then their intersection point at infinity would lie on 4 lines of $Q(4,2)$, since $Q(4,2) \cap \Pi_\infty = Q^+(3,2)$, a contradiction.

(b) Suppose that $q=2$, $s=\mu-1$, and $\Pi_b \cap c_3$ is a $(2\mu-1)$-dimensional space. The points of $\Pi_b \cap c_3$, not contained in $c_2 \cap \Pi_b$, have to be covered by c_1. As $z=2^{2\mu-2}$, $c_1 \cap c_3$ intersects Π_b in a $(2\mu-2)$-dimensional affine space $\Pi_{2\mu-2}$.

Since c_1 and c_2 have no affine points in common, $c_2 \cap c_3 \cap \Pi_b$ has to be the affine space in $\Pi_b \cap c_3$ parallel to the space $\Pi_{2\mu-2}$. We can proceed now as in case (a).

We return to the case $1 \leq s < \mu - 1$, and the case $q > 2$ and $s = \mu - 1$.

So we may now suppose that c_3 intersects Π_b in a $(2\mu - 1)$-dimensional space $\Pi_{2\mu-1}$. We will look at the possibilities of intersection of c_3 and the quadric Ψ inside Π_b, and comparing the number of intersection points with z will yield contradictions.

So c_3 intersects the quadric $Q(2\mu, q)$ of Π_b in a quadric Q of $\Pi_{2\mu-1}$.

1) In a non-singular hyperbolic quadric $Q = Q^+(2\mu - 1, q)$, which intersects Π_∞ in a non-singular parabolic quadric $Q(2\mu - 2, q)$.

Then we have $q^{\mu-1}(q^{\mu-1} + 1)$ affine points. Comparing with z yields the following equation

$$z = q^{\mu-1}(q^\mu - q^s) = q^{\mu-1}(q^{\mu-1} + 1),$$

which yields

$$q^s + 1 = q^{\mu-1}(q - 1).$$

Hence, since $\mu \geq 2$, $s = 0$, a case which we already proved to be impossible.

2) In a non-singular hyperbolic quadric $Q = Q^+(2\mu - 1, q)$, which intersects Π_∞ in a cone with vertex a point and as base a non-singular hyperbolic quadric $Q^+(2\mu-3, q)$. Then we have $q^{2\mu-2}$ affine points. The equation becomes

$$z = q^{\mu-1}(q^\mu - q^s) = q^{2\mu-2},$$

and after simplification

$$q^s = q^{\mu-1}(q - 1).$$

Hence, we find $q = 2$, $s = \mu - 1$, this is case (b) mentioned above.

3) In a non-singular elliptic quadric $Q = Q^-(2\mu - 1, q)$, which intersects Π_∞ in a non-singular parabolic quadric $Q(2\mu - 2, q)$.

Then we have $q^{\mu-1}(q^{\mu-1} - 1)$ affine points. We have the equation

$$z = q^{\mu-1}(q^\mu - q^s) = q^{\mu-1}(q^{\mu-1} - 1),$$

leading to

$$q^s - 1 = q^{\mu-1}(q - 1).$$

This yields a contradiction for all s, since $\mu \geq 2$.

4) In a cone Q with vertex a point r and base a non-singular parabolic quadric $Q(2\mu - 2, q)$. If the point r does not lie at infinity, we may choose the base of this cone to lie at infinity. Then we find $q^{2\mu-2}$ affine points, which reduces to cases 2) and (b) mentioned above.

If the point r lies at infinity, we look at the number of points in the intersection of the tangent hyperplane $\Pi_{2\mu-1} = T_r(Q(2\mu,q))$ of $Q(2\mu,q)$ at this point r with the quadric $Q^+(2\mu-1,q)$ of $Q(2\mu,q)$ in the space at infinity; denote this number by x'. The number of affine points is the total number of points lying on the cone inside $\Pi_{2\mu-1}$ minus x'.

Necessarily, $T_r(Q(2\mu,q)) \cap Q(2\mu,q) \cap \Pi_\infty = rQ^+(2\mu-3,q)$. We find $q^{\mu-1}(q^{\mu-1}-1)$ affine points which yields a contradiction, as in case 3).

3.8 Vertex

In the previous section, we have shown that in order to have a possible interchange with quadrics, c_3 must contain the whole vertex Γ of the quadric Ψ. In this section, we will show, that even if this is the case, only in a few exceptional cases there is an actual interchange possible. We keep using the notations of the previous section. So here we have $x+y=2\mu-1$. Set $y=\mu+s$, hence z becomes $q^{\mu-2}(q^\mu - q^{s+1})$. This implies that $s \geq -(\mu-1)$, otherwise z is not an integer. Since $x>0$ and $x+y=2\mu-1$, we also have $s \leq \mu-2$. In contrast to the previous section, the parameter s can also take on negative values here. In particular, $s=-1$ will turn up if $\mu=2$. So from here on, we only consider values s such that $-(\mu-1) \leq s \leq \mu-2$.

For $-(\mu-1) \leq s \leq \mu-3$ and for $s=\mu-2$, $q>2$, we find $z>q^{2\mu-3}$, so c_3 intersects the space Π_b spanned by the base of Ψ at least in a $(2\mu-2)$-dimensional space $\Pi_{2\mu-2}$. This intersection dimension cannot be larger than $2\mu-2$, otherwise the dimension theorem yields a contradiction since c_3 also contains the $(m-r-2\mu+1)$-dimensional vertex Γ of Ψ.

We treat the case $q=2$, $s=\mu-2$, separately first. Note that in this case $x=1$, so $t=m-r-1$.

(a) If $\Pi_b \cap c_3$ is a $(2\mu-3)$-dimensional affine space, then $|\Pi_b \cap c_3| = z$, so $\Pi_b \cap c_3$ is contained in the non-singular parabolic quadric $Q(2\mu,2)$. An affine quadric in $(2\mu-3)$-dimensional affine space coincides with the space if and only if it consists of two parallel affine $(2\mu-4)$-dimensional spaces or if its projective completion is completely contained in the quadric. As a generator of $Q(2\mu,2)$ has dimension $\mu-1$, it follows that $2\mu-4 \leq \mu-1$, so $\mu \leq 3$. Consider the case $\mu=3$. The planes through a line L lying completely on $Q(6,2)$ have to lie in the tangent space at L to $Q(6,2)$. This tangent space intersects $Q(6,2)$ in a cone with vertex the line L and base a conic $Q(2,2)$. Hence, the number of such planes is equal to 3. By a similar reasoning for the tangent space at L to $Q^+(5,2)$, we find that two of them lie on the hyperbolic quadric $Q^+(5,2)$ of $Q(6,2)$ at infinity. So there are no two parallel affine planes through L lying on $Q(6,2)$. Hence, for $\mu=3$, there is no interchange possible in this case.

Furthermore, if $s = \mu - 2$, then $y = 2\mu - 2$, $x = 1$, and hence $t = m - r - x = m - r - 1$. If $\mu = 2$, then $z = 2$ for $q = 2$. The case $\mu = 2$ will be treated separately afterwards in Section 3.9.

(b) Suppose that $\Pi_b \cap c_3$ is a $(2\mu - 2)$-dimensional affine space, with $z = 2^{2\mu-3}$. The points of $\Pi_b \cap c_3$ not contained in $c_2 \cap \Pi_b$ have to be covered by c_1. So $c_1 \cap c_3$ intersects Π_b in a $(2\mu - 3)$-dimensional space $\Pi_{2\mu-3}$. Since c_1 and c_2 have no affine points in common, $c_2 \cap c_3 \cap \Pi_b$ has to be the affine space in $\Pi_b \cap c_3$ parallel to $\Pi_{2\mu-3}$. We can proceed now as in case (a). Here the comparison with the generator size yields $2\mu - 3 \leq \mu - 1$, so $\mu \leq 2$. As above, if $\mu = 2$, then $z = 2$, and this case $\mu = 2$ will be treated in Section 3.9.

From now on, we will assume that we are not in the case $q = 2$, $s = \mu - 2$. As in the previous Section 3.7 concerning interchange with quadrics, we check all possibilities for the intersection of c_3 with the space Π_b and we will be able to exclude almost all possibilities by simple comparison with the number z of intersection points.

Remark 3.8.1 *Sometimes there will be possibilities for $\mu = 2$ and $\mu = 3$, but we don't treat them in full detail here, since we will treat these cases separately later on in Sections 3.9 and 3.10.*

So c_3 intersects the non-singular base quadric $Q(2\mu, q)$ of Ψ in a quadric Q of $\Pi_{2\mu-2}$.

1) The projective completion of c_3 intersects $Q(2\mu, q)$ in a non-singular parabolic quadric $Q = Q(2\mu - 2, q)$.

Case A: At infinity, $c_3 \cap c_2 \cap \Pi_b$ is a hyperbolic quadric $Q^+(2\mu - 3, q)$.

We find $q^{\mu-2}(q^{\mu-1} - 1)$ affine points. Comparing with the expression for z yields the equation

$$z = q^{\mu-2}(q^{\mu} - q^{s+1}) = q^{\mu-2}(q^{\mu-1} - 1),$$

reducing to

$$q^{s+1} - 1 = q^{\mu-1}(q - 1).$$

Comparing the powers of q yields a contradiction for all s if $\mu \geq 2$.

Case B: At infinity, $c_3 \cap c_2 \cap \Pi_b$ is an elliptic quadric $Q^-(2\mu - 3, q)$.

We find $q^{\mu-2}(q^{\mu-1} + 1)$ affine points, which leads to the following equation

$$z = q^{\mu-2}(q^{\mu} - q^{s+1}) = q^{\mu-2}(q^{\mu-1} + 1),$$

and hence

$$q^{s+1} + 1 = q^{\mu-1}(q - 1).$$

The comparison of the powers of q again yields a contradiction if $\mu > 2$. If $\mu = 2$, then $q = 2$, $s = -1$, is a possibility and so as above $t = m - r - x = m - r - 2$ as $x + y = 2\mu - 1 = 3$, $y = \mu + s = 1$, and $z = 3$.

Case C: At infinity, $c_3 \cap c_2 \cap \Pi_b$ is a cone with vertex a point r and base a non-singular parabolic quadric $Q(2\mu - 4, q)$; we denote this cone by $rQ(2\mu - 4, q)$.

We find $q^{2\mu-3}$ affine points, which yields the equation

$$z = q^{\mu-2}(q^{\mu} - q^{s+1}) = q^{2\mu-3},$$

which becomes

$$q^{s+1} = q^{\mu-1}(q - 1).$$

Hence, $q = 2$ and $s = \mu - 2$, Case (b) which we described above.

2) The projective completion of c_3 intersects $Q(2\mu, q)$ in a cone with vertex a point r and base a non-singular hyperbolic quadric $Q^+(2\mu - 3, q)$. Denote this cone by $rQ^+(2\mu - 3, q)$.

Case A: The vertex r does not lie at infinity.

In this case we can select the base to lie at infinity, so the number of affine points is

$$1 + (q - 1)|Q^+(2\mu - 3, q)| = q^{\mu-2}(q^{\mu-1} + q - 1).$$

Comparing with z leads to the following equation

$$z = q^{\mu-2}(q^{\mu} - q^{s+1}) = q^{\mu-2}(q^{\mu-1} + q - 1),$$

thus

$$q^{\mu-1}(q - 1) = q(q^s + 1) - 1.$$

Since an even number can never be equal to an odd number, this yields a contradiction for all q.

Case B: The vertex r lies at infinity.

First possibility: at infinity $c_2 \cap c_3 \cap \Pi_b$ is a cone $rQ(2\mu - 4, q)$. The number of affine points is equal to

$$q(|Q^+(2\mu - 3, q)| - |Q(2\mu - 4, q)|) = q^{\mu-1}(q^{\mu-2} + 1).$$

We obtain the following equation

$$z = q^{\mu-2}(q^{\mu} - q^{s+1}) = q^{\mu-1}(q^{\mu-2} + 1),$$

and hence

$$q^{\mu-2} + 1 = q^{\mu-1} - q^s,$$

so

$$q^s + 1 = q^{\mu-2}(q-1).$$

This yields a contradiction unless $\mu = 2$, $q = 3$, $s = 0$, or $\mu = 3$, $q = 2$, $s = 0$. In both cases, we have $s = 0$, so if $\mu = 2$, $q = 3$, then $y = 2$, $x = 1$, $t = m - r - x = m - r - 1$, $z = 6$, and if $\mu = 3$, $q = 2$, then $y = 3$, $x = 2$, $t = m - r - 2$, $z = 12$.

Second possibility: at infinity $c_2 \cap c_3 \cap \Pi_b$ is a cone $rsQ^+(2\mu - 5, q)$, so a cone with vertex a line rs and base a non-singular hyperbolic quadric $Q^+(2\mu - 5, q)$. We find $q^{2\mu-3}$ affine points, a case which we already treated above.

3) The projective completion of c_3 intersects $Q(2\mu, q)$ in a cone with vertex a point r and base a non-singular elliptic quadric $Q^-(2\mu-3, q)$. Denote this cone by $rQ^-(2\mu - 3, q)$.

Case A: The vertex r does not lie at infinity.

In this case we can select the base to lie at infinity, so the number of affine points is

$$1 + (q-1)|Q^-(2\mu - 3, q)| = q^{\mu-2}(q^{\mu-1} - q + 1).$$

We obtain the following equation

$$z = q^{\mu-2}(q^\mu - q^{s+1}) = q^{\mu-2}(q^{\mu-1} - q + 1),$$

so

$$q^{\mu-1}(q-1) = q(q^s - 1) + 1.$$

Since an even number is never equal to an odd number, this yields a contradiction for all q.

Case B: The vertex r lies at infinity.

First possibility: at infinity $rQ^-(2\mu-3, q)$ intersects in an $rQ(2\mu-4, q)$. The number of affine points is equal to

$$q(|Q^-(2\mu - 3, q)| - |Q(2\mu - 4, q)|) = q^{\mu-1}(q^{\mu-2} - 1).$$

The equation becomes

$$z = q^{\mu-2}(q^\mu - q^{s+1}) = q^{\mu-1}(q^{\mu-2} - 1),$$

$$q^{\mu-2}(q-1) = q^s - 1.$$

We find $\mu = 2, s = 1$, but then $s = \mu - 1$ which was impossible.

Second possibility: at infinity $rQ^-(2\mu-3, q)$ intersects in an $rsQ^-(2\mu - 5, q)$, so a cone with vertex a line rs and base a non-singular elliptic quadric

$Q^-(2\mu - 5, q)$. We find again $q^{2\mu-3}$ affine points, reducing to Case (c) of 1) above.

4) The projective completion of c_3 intersects $Q(2\mu, q)$ in a cone with as vertex a line L and as base a non-singular parabolic quadric $Q(2\mu - 4, q)$.

Case A: The line L does not lie completely at infinity.

Hence we can select the base to lie at infinity. We find again $q^{2\mu-3}$ affine points, reducing to Case (c) of 1) above.

Case B: The line L lies completely at infinity.

We distinguish between the following three cases.

(1) If the non-singular parabolic quadric $Q(2\mu-4, q)$ intersects infinity in a non-singular hyperbolic quadric $Q^+(2\mu - 5, q)$, then we have $q^{\mu-1}(q^{\mu-2} - 1)$ affine points. We already treated this case in 3) Case B.

(2) If $Q(2\mu - 4, q)$ intersects infinity in a non-singular elliptic quadric $Q^-(2\mu-5, q)$, then we have $q^{\mu-1}(q^{\mu-2}+1)$ affine points, and also this case was already treated in 2) Case B.

(3) If $Q(2\mu - 4, q)$ intersects infinity in a cone with vertex a point p and base a non-singular quadric $Q(2\mu - 6, q)$, then we have $q^{2\mu-3}$ affine points, reducing to Case (C) of 1) above.

The results of the preceding section, together with those of this section, now lead to the following theorem.

Theorem 3.8.2 *If $\mu > 3$, then an interchange with a quadric Ψ is impossible. For $\mu = 2$ and $\mu = 3$, an interchange can only occur if the vertex of Ψ is contained in c_3. If interchange is possible for $\mu = 2$, we have $q = 2$, $t = m-r-2$, $z = 3$, or $q = 3$, $t = m-r-1$, $z = 6$, or $q = 2$, $t = m-r-1$, $z = 2$. If interchange is possible for $\mu = 3$, then we have $q = 2$, $t = m-r-2$, $z = 12$.*

Proof Going through all the cases on the previous pages shows that 1) Case B yields the possibility $\mu = 2$, $q = 2$, $t = m - r - 2$, $z = 3$, 2) Case B yields the possibilities $\mu = 2$, $q = 3$, $t = m - r - 1$, $z = 6$, and $\mu = 3$, $q = 2$, $t = m-r-2$, $z = 12$. The last possibility comes from (a) in the beginning of this section and yields the possibility $\mu = 2$, $q = 2$, $t = m - r - 1$, $z = 2$. □

3.9 The case $\mu = 2$

We have already shown that in this case the vertex of Ψ has to be contained in $c_3 \cap c_2$ in case of an interchange. By Theorem 3.8.2, $c_1 \cap c_3$ has dimension $m - r - 2$ or dimension $m - r - 1$. Even in these cases, only for $q = 2$ and $q = 3$, there were only a few possibilities that could occur.

3.9.1 $q = 2$

The base of Ψ is a non-singular parabolic quadric $Q(4, 2)$ and the vertex Γ is of dimension $k = m - r - 3$.

(a) If the dimension of $c_1 \cap c_3$ is $m-r-2$, we have $z = 3$ by Theorem 3.8.2; this implies that c_3 intersects Π_b at least in a plane. Since c_3 also contains the whole $(m - r - 3)$-dimensional vertex Γ of Ψ, the intersection $\pi = c_3 \cap \Pi_b$ is a plane. Three of the four affine points of π belong to $c_3 \cap c_2$. The fourth affine point p of π belongs to $c_1 \cap c_3$. Since c_3 contains the vertex Γ of Ψ, all affine points in the space spanned by the vertex Γ and p have to be contained in $c_1 \cap c_3$. Hence, the projective completion of c_1 also has to contain Γ.

So starting from a given pair (c_1, c_2), in order to have an interchange, c_1 has to contain at least one point of Π_b, which is the space spanned by the base of c_2, and c_1 also has to contain the vertex Γ of c_2. The intersection $c_2 \cap \Pi_b$ contains 6 affine points, and let I be the set formed by these 6 affine points.

By the previous paragraph, we have to find a plane π lying in Π_b which contains exactly three points of I. The space spanned by π and the vertex space Γ of Ψ can then serve as the space c_3.

Consider a point r in $c_1 \cap \Pi_b$ and a point $s \in I$. The line L spanned by r and s intersects infinity in a point p'. Through p', there passes exactly one line that contains two points belonging to L, regardless if $p' \in Q^+(3, 2)$ or not; call this line L'. Hence, $\langle L, L' \rangle$ is the plane π we were looking for.

Since I contains 6 points, we find 6 planes for a given point r in $c_1 \cap \Pi_b$. However, we will have counted all these planes three times. So we find only 2 such different affine planes through r. Hence, depending on the number of affine points contained in $c_1 \cap \Pi_b$, namely 0, 1, 2, or 4, we get 0, 2, 4, or 8 possibilities for an interchange in this way. Note that by Theorem 3.1.8, $(c_1 \cup c_2) \backslash c_3$ corresponds to a quadric of the suitable type, since we are in the case $q = 2$ and $\mu = 2$.

(b) If the dimension of $c_1 \cap c_3$ is $m - r - 1$, we have $z = 2$ by Theorem 3.8.2. Since c_3 has to contain the $(m - r - 3)$-dimensional vertex Γ of Ψ and the dimension of $c_1 \cap c_3$ is $m - r - 1$, it follows that the vertex space Γ of Ψ is completely contained in the projective completion of c_1.

Suppose now that we are given a pair (c_1, c_2). If we want to have an interchange, then c_3 has to contain one affine bisecant L of c_2 in Π_b, which intersects Π_∞ in a point r. The space $c_1 \cap c_3$ is an $(m - r - 1)$-dimensional space which intersects Π_∞ in the $(m-r-2)$-dimensional space spanned by the $(m-r-3)$-dimensional vertex $\Gamma = \Pi_{m-r-3}$ and r. The intersection $c_2 \cap c_3$ has to be the parallel $(m-r-1)$-dimensional affine space through $\langle \Gamma, r \rangle = \langle \Pi_{m-r-3}, r \rangle$ in c_3. Hence, the projective completion of c_1 has to contain the point r.

As the projective completion of L intersects Π_∞ in a point r belonging to

c_1, then the space Π' spanned by the vertex space Γ and the plane formed by L and a line L', which is parallel to l and belongs to c_1, can serve as c_3. The number of affine lines through the point r at infinity in the $(m-r)$-dimensional space c_1 is 2^{m-r-1}. As stated above, with each line L', there corresponds a space Π'. However, each space Π' is obtained for 2^{m-r-2} different lines through r, hence we have $\frac{2^{m-r-1}}{2^{m-r-2}} = 2$ interchange possibilities.

We look at the situation for a point p' belonging to $c_1 \cap \Pi_b \cap \Pi_\infty$. As already remarked above, regardless if $p' \in Q^+(3,2)$ or not, there is exactly one line L' through p' that contains 2 points of L. So for each such point p', we have two possibilities for interchange. Note that as above, because of $q = 2$, $\mu = 2$, and Theorem 3.1.8, the points in the set $(c_1 \cup c_2) \backslash c_3$ form a quadric with $(m-r-3)$-dimensional vertex and base $Q(4,2)$, so that we really have an interchange.

So starting from a given pair (c_1, c_2), we look for the number of points contained in $c_1 \cap \Pi_b \cap \Pi_\infty$.

If c_1 has 4 affine points in Π_b, then it intersects $\Pi_b \cap \Pi_\infty$ in a line, so then we find 6 interchanges of this type.

If c_1 has 2 affine points in Π_b, then it intersects $\Pi_b \cap \Pi_\infty$ in a point, so two interchanges of this type.

If c_1 has 1 affine point in Π_b, then it does not intersect $\Pi_b \cap \Pi_\infty$, so no interchanges of this type.

If c_1 has no affine points in Π_b, then either $c_1 \cap \Pi_b \cap \Pi_\infty$ is empty or c_1 intersects $\Pi_b \cap \Pi_\infty$ in a point or a line. We have $0, 2$, or 6 interchanges in the respective cases.

To summarize, we have the following result. If we have a given quadric c_2, then in order to have an interchange, c_1 always has to contain the vertex Γ of c_2 completely. Furthermore, we distinguish between the following four cases.

(1) If c_1 has all its affine points outside of Π_b, we have counted the sum $c_1 + c_2$ precisely $1 + 6 = 7, 1 + 2 = 3$, or 1 times if the number of points belonging to $c_1 \cap \Pi_b \cap \Pi_\infty$ is $3, 1$, or 0 respectively.

(2) If c_1 has one affine point in Π_b, we obtain the sum $c_1 + c_2$ precisely $1 + 2 = 3$ times.

(3) If two affine points are in Π_b, we obtain the sum $c_1 + c_2$ precisely $1 + 2 + 4 = 7$ times.

(4) If all affine points are in Π_b, we obtain the sum $c_1 + c_2$ precisely $1 + 6 + 8 = 15$ times.

Note that for cases (2), (3), and (4), we also have included the interchanges discussed in case (a).

Remark 3.9.1 *The pairs (c_1, c_2) and (c_3, c_4) play the same role with respect to interchange, since each role has its specific number of interchanges. So we cannot jump from one case to another.*

Since we now have determined in which cases there is an actual interchange and how many times we have counted the same affine point set in these cases, the only thing left to do is to count how many times these cases effectively occur. This can be done exactly in the same way as done in Section 3.4 concerning the skew space-quadric pairs, but now only considering the specific starting situations where interchange can occur. Let c_2 be a fixed quadric and let Π_{m-r+2} be the space spanned by the point set of c_2.

(α) Assume that the $(m-r)$-dimensional space c_1 has all its affine points outside of Π_b. Note that in Case (a) above, there is no interchange here, so we can assume that we are in Case (b), which means that c_1 shares at least an $(m-r-2)$-dimensional space with $\Pi_{m-r+2} \cap \Pi_\infty$. We distinguish between two cases.

(α.1) The intersection $c_1 \cap \Pi_{m-r+2} \cap \Pi_\infty$ is $(m-r-2)$-dimensional. So $c_1 \cap \Pi_b \cap \Pi_\infty$ is a point r. We have 15 choices for the point r in the space $\Pi_b \cap \Pi_\infty$. The number of affine $(m-r)$-dimensional spaces intersecting Π_{m-r+2} exactly in the space spanned by the vertex Γ and the point r is found by projecting from the $(m-r-2)$-dimensional space $\langle \Gamma, r\rangle = c_1 \cap \Pi_{m-r+2} \cap \Pi_\infty$ onto a complementary $(r+1)$-dimensional space Π_{r+1} in $\mathbf{AG}(m, 2)$. We have to choose an affine line in Π_{r+1} skew to the 3-dimensional complementary space of $\mathbf{AG}(m-r+2, 2)$, which also does not lie at infinity. This means that there are $Skew(r+1, 3, 1) - Skew(r, 2, 1) = 2^6(2^{r-2}-1)(2^{r-3}-1)$ such lines. Hence, this case occurs

$$15 \cdot 2^6(2^{r-2}-1)(2^{r-3}-1)$$

times. These are all counted 3 times.

(α.2) The intersection $c_1 \cap \Pi_{m-r+2} \cap \Pi_\infty$ is $(m-r-1)$-dimensional. So $c_1 \cap \Pi_b \cap \Pi_\infty$ is a line L. We have $\frac{15\cdot 14}{3\cdot 2} = 35$ choices for the line L in the space $\Pi_b \cap \Pi_\infty$. The number of affine $(m-r)$-dimensional spaces intersecting Π_{m-r+2} exactly in the space spanned by the vertex Γ of Ψ and the line L is equal to $(2^m - 2^{m-r+2})/2^{m-r} = 2^r - 2^2$. Hence, this case occurs $35 \cdot (2^r - 2^2)$ times and they are all counted 7 times.

(β) Assume that the space c_1 has one affine point p in Π_b, so $c_1 \cap \Pi_{m-r+2} \cap \Pi_\infty$ is $(m-r-3)$-dimensional and equals the vertex Γ of Ψ. We have $16-6 = 10$ choices for this affine point p in Π_b. For each space spanned by such a point p and the vertex Γ, we have $Ext_Q(m-r-2)$ extensions, see Section 3.4. So we have

$$10 \cdot \frac{2^8(2^{r-2}-1)(2^{r-3}-1)}{3}$$

such spaces. These pairs are all counted 3 times.

(γ) Assume that the space c_1 has a line in common with Π_b, and $c_1 \cap \Pi_{m-r+2} \cap \Pi_\infty$ is $(m-r-2)$-dimensional. There are 10 affine points in Π_b not lying on c_2, so they determine $\frac{10 \cdot 9}{2} = 45$ choices for the line $L = c_1 \cap \Pi_b$. For each space spanned by such a line L and the vertex Γ, we have $Ext_Q(m-r-1)$ extensions. So we get

$$45 \cdot 2^3 \cdot (2^{r-2} - 1)$$

such spaces. These pairs are all counted 7 times.

(δ) Assume that the space c_1 lies completely in Π_{m-r+2}. For each point p lying in $\Pi_b \cap \Pi_\infty$, there is exactly one line in Π_b through p which intersects the quadric Ψ in 2 affine points. So three lines in Π_b through p not lying completely at infinity have no points in common with c_2. Hence, there are exactly three planes through p which have no affine points in common with c_2. We have counted all these planes three times. So we find 15 such spaces in total. These pairs are all counted 15 times.

The above arguments yield the following theorem concerning pairs (c_1, c_2) which are counted several times, where c_2 is a quadric $\Gamma Q(4,2)$ with Γ an $(m-r-3)$-dimensional space and with c_1 an affine $(m-r)$-dimensional space.

Theorem 3.9.2 *Denote the number of quadrics c_2, where c_2 is a quadric $\Gamma Q(4,2)$, with Γ an $(m-r-3)$-dimensional space at infinity, which we calculated in Section 3.3, by the same notation F. Let c_1 be an affine $(m-r)$-dimensional space skew to c_2. Then there are*

$$(15 \cdot 2^6(2^{r-2} - 1)(2^{r-3} - 1) + 10 \cdot \frac{2^8(2^{r-2} - 1)(2^{r-3} - 1)}{3})F$$

pairs (c_1, c_2) which are counted 3 times. The following number of pairs (c_1, c_2) are counted 7 times

$$(35 \cdot (2^r - 2^2) + 45 \cdot 2^3 \cdot (2^{r-2} - 1))F.$$

Finally, $15F$ pairs (c_1, c_2) are counted 15 times.

3.9.2 $q = 3$

In this case of possible interchange of Theorem 3.8.2, the base of the quadric Ψ is a non-singular parabolic quadric $Q(4,3)$ and the vertex Γ at infinity has dimension $k = m - r - 3$. The only possibility for interchange is Case 2) B of Section 3.8. The intersection space $\Pi_b \cap c_3$ is a plane π in this case. The intersection $\Pi_b \cap c_2 \cap c_3$ consists of two lines L and L' which intersect in a point

r lying on the non-singular hyperbolic quadric $Q^+(3,3)$ of $Q(4,3)$ at infinity since this intersection should contain $z = 6$ affine points. So in the base of the quadric c_2, we have 6 affine points contained in $c_3 \cap c_2$. The third parallel affine line through r in π belongs to $c_1 \cap \Pi_b$.

In the case $q = 3$, we cannot apply Theorem 3.1.8 directly, so we still have to check that the affine point set formed by the affine points belonging to $(c_1 \cup c_2)\backslash c_3$ forms a singular quadric c_4 with base a parabolic quadric $Q'(4,3)$.

Since $c_1 \cap c_3 \cap \Pi_b$ is a line and $t = m-r-1$, it follows that the vertex space Γ of Ψ is completely contained in the projective completion of c_1. All points in $(c_1 \cup c_2)\backslash c_3$ have to be covered by c_4. Consider a point s in $\Pi_b \cap ((c_1 \cup c_2)\backslash c_3)$. Let p be an arbitrary point in the vertex Γ of c_2. The three affine points on the line sp have to be covered by the quadric c_4, but then the whole line sp, so in particular p, has to belong to c_4.

This implies that c_4 contains the $(m-r-3)$-dimensional vertex space Γ of c_2. As the point p belongs to at least 18 lines of c_4, namely the lines connecting p with the $24 - 6 = 18$ affine points of c_2 in Π_b not covered by c_3, p is necessarily a singular point of c_4. These 18 affine points of $Q(4,3)$ span the 4-dimensional space $\Pi_b = \Pi_4$ of $Q(4,3)$, since the only possibility in 3 dimensions would be 2 parallel affine planes, but there are no planes lying on $Q(4,3)$. Since p lies on a line of c_4 to all these 18 points, necessarily p is singular for c_4. So all points of Γ are singular points for c_4.

There cannot be other singular points, since then c_4 is no longer a quadric of the required form, that is, a cone with an $(m-r-3)$-dimensional vertex at infinity and with base a 4-dimensional parabolic quadric $Q'(4,3)$. Hence, the vertex of c_4 is equal to the vertex Γ of c_2.

The quadric c_4 has to contain 18 of the 24 affine base points of the non-singular parabolic quadric $Q = Q(4,3)$, which is the base of c_2. These 18 affine points of Q in $c_4 \cap \Pi_b$ span the 4-dimensional space Π_b completely. Since we already know that the vertex space of c_4 has no points in common with Π_b, we can choose the base $Q' = Q'(4,3)$ of c_4 to lie in Π_b.

Suppose that we have an interchange so that we can write the affine point set formed by c_1 and c_2 also as an affine point set formed by an $(m-r)$-dimensional affine space c_3 and a quadric c_4.

The 18 affine points of $Q\backslash(L \cup L')$ must lie on Q'. Through r, there pass two lines L_1 and L_2 lying completely on the non-singular hyperbolic quadric $Q^+(3,3)$ of Q at infinity.

Every point of $(L_1 \cup L_2) \setminus \{r\}$ lies on two affine lines containing 3 points of the base $Q' = Q'(4,3)$ of c_4. So these points of $(L_1 \cup L_2)\backslash\{r\}$ also lie on the projective completion of c_4. But then L_1 and L_2 contain 3 points of c_4, so also $r \in c_4$.

The plane spanned by the lines L_1 and L_2 lies in 4 solids of $\mathbf{PG}(4,3)$.

One of them is $T_r(Q(4,3))$ containing L, L', L_1, and L_2. One of them is $\mathbf{PG}(3,3)_\infty = \mathbf{PG}(4,3) \cap \Pi_\infty$; the other 2 solids contain skew lines of $Q(4,3)$; so intersect $Q(4,3)$ in two distinct non-singular hyperbolic quadrics $Q^+(3,3)$. So it should be the case that the bases $Q(4,3)$ and $Q'(4,3)$ of c_2 and c_4 are two parabolic quadrics $Q(4,3)$ and $Q'(4,3)$ in the pencil of quadrics of $\mathbf{PG}(4,3)$ defined by these two hyperbolic quadrics $Q^+(3,3)$.

We study the pencil of quadrics in $\mathbf{PG}(4,3)$ containing the 25 points of $Q \cap Q'$. The number of points of $\mathbf{PG}(4,3)$ is 121, the number of points contained in a non-singular parabolic quadric $Q(4,3)$ is 40, the number of points contained in two intersecting hyperplanes is 67, and the number of points contained in a cone with vertex a point and base a non-singular hyperbolic quadric $Q^+(3,3)$ is equal to 49. The pencil of quadrics defined by the two 3-dimensional hyperbolic quadrics $Q^+(3,3)$ intersecting in the two lines L_1 and L_2 certainly contains the base $Q(4,3)$ of c_2 in Π_b and the union of the two solids containing the two hyperbolic quadrics $Q^+(3,3)$. Since Q and Q' have 25 points in common, there are still $121 - 25 - 15 - 42 = 24 + 15$ points remaining in $\mathbf{PG}(4,3)$. The only possibility is that they belong to one other 4-dimensional parabolic quadric and to one cone with vertex a point and base a 3-dimensional hyperbolic quadric. So this shows that this pencil of quadrics defined by the bases Q and Q' of c_2 and c_4 effectively occurs.

We look at the pencil of quadrics in $T_r(Q)$ induced by the pencil of quadrics defined by Q and Q'. Then Q intersects $T_r(Q)$ in a cone with vertex r and base a conic. We coordinatize this cone with vertex the point r and base a conic as follows. The point r has coordinates $(0,0,0,1)$, the base plane has equation $X_3 = 0$, and the conic in the base has equation $X_1^2 = X_0X_2$. We furthermore choose the lines L_1 and L_2 to have the equations $X_1 = 0$, $X_2 = 0$ and $X_0 = 0$, $X_1 = 0$ respectively. The two 3-dimensional hyperbolic quadrics in $Q \cap Q'$ which determine the pencil of quadrics containing Q and Q' intersect in the lines L_1 and L_2. So the two corresponding hyperplanes containing them, whose union is one of the quadrics in the pencil of quadrics defined by Q and Q', both intersect $T_r(Q)$ in the plane $\langle L_1, L_2 \rangle$. So this plane $\langle L_1, L_2 \rangle$, counted with multiplicity two, is one of the quadrics in the pencil of quadrics induced in $T_r(Q)$. Here, the plane $\langle L_1, L_2 \rangle$ has equation $X_1 = 0$, thus the pencil of quadrics induced in $T_r(Q)$ is defined by $X_1^2 - X_0X_2 = 0$ and $X_1^2 = 0$.

We also find the union of the two planes $X_0 = 0$ and $X_2 = 0$ in the pencil, and the cone $X_1^2 + X_0X_2 = 0$ with vertex r and base $X_1^2 + X_0X_2 = X_3 = 0$. The base $X_1^2 + X_0X_2 = X_3 = 0$ contains the points $(1,0,0,0)$, $(0,0,1,0)$, $(1,-1,-1,0)$, $(1,1,-1,0)$. The two cones share the lines L_1 and L_2. Take the two other lines of the first cone with equation $X_1^2 = X_0X_2$. These lines intersect the base in the points $P_1 = (1,1,1,0)$ and $P_2 = (1,-1,1,0)$. We are interested in the third point on the line

$\langle(1,1,1,0),\ (1,-1,1,0)\rangle$ different from the intersection point with $X_1 = X_3 = 0$. This is the point $(0,1,0,0)$. Since this point is collinear with the points $(1,-1,-1,0)$ and $(1,1,-1,0)$ of the cone $X_1^2 + X_0X_2 = 0$, the interchange can occur. Furthermore, the reasoning above shows that for a given cone c_2 and a given point $r \in c_2 \cap \Pi_\infty$, there is exactly one c_1 which gives exactly one interchange. Namely, c_1 is the $(m-r)$-dimensional affine space defined by Γ and the plane defined by the two affine lines of $Q(4,3)$ through r. This yields the following counting. In Theorem 3.4.8, we proved the following theorem on the number of affine $(m-r)$-dimensional subspaces of $\mathbf{AG}(m,3)$ skew to the affine part of a given cone $\Psi = \Gamma Q(4,3)$.

Theorem 3.9.3 *The number of affine $(m-r)$-dimensional subspaces of $\mathbf{AG}(m,3)$ skew to the affine part of a given cone $\Psi = \Gamma Q(4,3)$, with an $(m-r-3)$-dimensional vertex Γ at infinity and base $Q(4,3)$, is equal to*

$$A_1 = P + \sum_{(s,k)\in R(s,k)} S(s,k)(H(s,k)Ext_Q(s+k+2) + HIH(s,k)Ext_Q(s+k+3)),$$

where

$$R(s,k) = \{(s,k) | -1 \leq s \leq m-r-3,\ -1 \leq k \leq 1\},$$

and where P is defined in Lemma 3.4.7.

Hence, the number of distinct unions $c_1 \cup c_2$ for the case $q = 3, \mu = 2$, is equal to

$$F \cdot (A_1 - 16) + \frac{16F}{2} = F \cdot (A_1 - 8).$$

Proof There are F choices for the quadric c_2, see Section 3.3. For a given quadric c_2, there are 16 pairs doubly counted, corresponding to the 16 points at infinity of the base $Q(4,3)$ of c_2. □

3.10 The case $\mu = 3$

In this case $q = 2$, the vertex Γ has dimension $m-r-5$ and the base of the quadric Ψ is a non-singular parabolic quadric $Q(6,2)$ which intersects the space Π_∞ at infinity in a non-singular hyperbolic quadric $Q^+(5,2)$.

By Theorem 3.8.2, the intersection space $c_1 \cap c_3$ has dimension $t = m - r - 2$. Note that if we can find an $(m-r)$-dimensional affine space c_3 lying on $c_1 \cup c_2$, then by Theorem 3.1.8, the affine point set $(c_1 \cup c_2)\backslash c_3$ forms a quadric or a symmetric difference. Since in Section 3.6, we never got a quadric for c_4 after interchange, we know that we will not get a symmetric difference for c_4 here. Hence, the points in the set $(c_1 \cup c_2)\backslash c_3$ form a quadric of the same type, that is, $c_4 = (c_1 \cup c_2) \setminus c_3$ is a cone with an $(m-r-5)$-dimensional vertex and a 6-dimensional parabolic quadric $Q(6,2)$ as base.

The interchange which can occur is Case 2) B of Section 3.8. By Theorem 3.8.2, in this case, we have $q = 2$, $t = m - r - 2$, and $z = 12$.

Moreover, by Case 2) B of Section 3.8, the projective completion of the space c_3 intersects the projective completion of $\Pi_b \cap c_2$ in a cone with vertex a point r lying in Π_∞ and base a non-singular hyperbolic quadric $Q^+(3,2)$ which intersects Π_∞ in a cone with vertex r and base a conic $C = Q(2,2)$. This cone has to lie entirely in the tangent space to $Q(6,2)$ at r, which is a cone with vertex the point r and as base a non-singular parabolic quadric $Q(4,2)$ which intersects Π_∞ in a non-singular hyperbolic quadric $Q^+(3,2)$. But then there pass two non-singular hyperbolic quadrics $Q^+(3,2)$ through the conic C inside the non-singular parabolic quadric $Q(4,2)$, a contradiction. Hence, this case is impossible.

3.11 Summary and conclusion

In this chapter, the goal was the calculation of the number of non-minimal codewords in a binary Reed-Muller code RM(r,m) of weight smaller than $3 \cdot 2^{m-r}$; thereby extending the results of Borissov, Manev, and Nikova, who calculated the number of non-minimal codewords in RM(r,m) of weight $2 \cdot 2^{m-r}$ (Theorem 3.1.7). We transformed the original problem into a geometrical one concerning affine point sets, and studied this geometrical problem for general q. In the geometrical setting for $q = 2$, we are in fact calculating the number of non-minimal codewords. If the weight distribution of the Reed-Muller code is known, we can also calculate the number of minimal codewords.

We summarize our results for the numbers of pairs (c_1, c_2), with c_1 and c_2 point sets of $\mathbf{AG}(m,q)$ having empty intersection, where c_1 is an $(m-r)$-dimensional space and where c_2 is either a quadric (particular cone) or a symmetric difference. In this summary, we use the same notations as before, but we will not recall their meaning here. Additionally, some new shorthand notations will be used here, to be able to write down the formulas in a concise way.

In Section 3.3, we calculated the number F of quadrics $\Gamma Q(2\mu, q)$ and the number S of symmetric differences defined by two affine $(m-r)$-dimensional spaces intersecting in an $(m-r-\mu)$-dimensional affine space. If we denote

$$\frac{F_1F_2F_3}{\phi(2\mu-1;2\mu,q)} = \frac{q^{r-2}\phi(m-r+1;m-1,q)\phi(m-r+1-2\mu;m-r+1,q)}{\phi(2\mu-1;2\mu,q)}$$

by F_h, then we get

$$F = F_h|O(Q(2\mu,q))||Q^+(2\mu-1,q) \text{ on a given } Q(2\mu,q)|$$

$$S = \frac{\phi(r-1;\mu-1+r,q)F_1(m,r,\mu,q)F_2(m,r,\mu,q)}{2}.$$

In Theorem 3.4.8, we proved the following theorem on the number of affine $(m-r)$-dimensional subspaces of $\mathbf{AG}(m,q)$ skew to the affine part of a given cone Ψ.

Theorem 3.11.1 *The number of affine $(m-r)$-dimensional subspaces of $\mathbf{AG}(m,q)$ skew to the affine part of a given cone $\Psi = \Gamma Q(2\mu,q)$, where Γ is an $(m-r-2\mu+1)$-dimensional vertex at infinity, is equal to*

$$A_1 = P + \sum_{(s,k)\in R(s,k)} S(s,k)(H(s,k)Ext_Q(s+k+2) + HIH(s,k)Ext_Q(s+k+3)),$$

where

$$R(s,k) = \{(s,k)| -1 \leq s \leq m-r+1-2\mu,\ -1 \leq k \leq \mu-1\},$$

and where P is defined in Lemma 3.4.7.

In Theorem 3.5.3, we calculated the number of affine $(m-r)$-dimensional spaces having no affine points in common with a fixed symmetric difference. We obtained the following result.

Theorem 3.11.2 *The number of $(m-r)$-dimensional affine spaces having no affine points in common with a fixed symmetric difference, formed by two $(m-r)$-dimensional affine spaces α and β which intersect in an affine $(m-r-\mu)$-dimensional space, is equal to $A_2 = N_a + N_{ea}$, where*

$$N_a = \sum_{k=0}^{m-r-\mu}\sum_{t=k}^{m-r} N(k)\psi(t,k)\rho(m-r,k,t),$$

$$N_{ea} = \sum_{(k,l,u,f)\in Res(k,l,u,f)} S(k,l,u)\psi(m-r-1,k,l,u,f)E(k,l,u,f).$$

In Sections 3.6 to 3.10, we studied the problem of affine point sets $c_1 \cup c_2$ which might have been counted several times.

Concerning the possible multiple countings of an affine point set which can be written as $c_1 \cup c_2$, where c_1 is an $(m-r)$-dimensional affine space and where c_2 is a symmetric difference, we obtained the following theorem at the end of Section 3.6.

Theorem 3.11.3 *Denote the number of symmetric differences consisting of two affine $(m-r)$-dimensional spaces intersecting in an affine $(m-r-\mu)$-dimensional space*

$$\frac{\phi(r-1;\mu-1+r,q)F_1(m,r,\mu,q)F_2(m,r,\mu,q)}{2}$$

by A. Then there are

$$A_3 = \sum_{t=m-r-\mu}^{m-r} \psi(t,m-r-\mu)\rho(m-r,m-r-\mu,t)A$$

pairs (c_1,c_2), where c_1 is an affine $(m-r)$-dimensional space and where c_2 is a symmetric difference, which can be partitioned into blocks of three pairs, such that the three pairs of a given block determine the same affine union.

Furthermore, if $q=2$, there are an extra

$$A_4 = 2\cdot(2^\mu-1)((2^\mu-1)(2^r-2^\mu)+(2^\mu-1)(2^r-2^{\mu-1}-1)+(2^{r+1}-2^{\mu+1})(2^r-2^\mu-1))A$$

pairs (c_1,c_2), where c_1 is an affine $(m-r)$-dimensional space and where c_2 is a symmetric difference, which can be partitioned into blocks of three pairs, such that the three pairs of a given block determine the same affine union.

Finally, if $q=2$, there are

$$A_5 = 2\cdot(2^r-2^\mu)A$$

pairs (c_1,c_2), where c_1 is an affine $(m-r)$-dimensional space and where c_2 is a symmetric difference, which can be partitioned into blocks of $2\cdot(2^\mu-1)+1$ pairs, such that the $2\cdot(2^\mu-1)+1$ pairs of a given block determine the same affine union.

For the possible multiple countings of pairs where c_2 is a quadric, Sections 3.7 and 3.8 yielded the following Theorem 3.8.2.

Theorem 3.11.4 *If $\mu>3$, then an interchange with a quadric Ψ is impossible. For $\mu=2$ and $\mu=3$, an interchange can only occur if the vertex of Ψ is contained in c_3. If interchange is possible for $\mu=2$, we have $q=2$, $t=m-r-2$, $z=3$, or $q=3$, $t=m-r-1$, $z=6$, or $q=2$, $t=m-r-1$, $z=2$. If interchange is possible for $\mu=3$, then we have $q=2$, $t=m-r-2$, $z=12$.*

In Sections 3.9 and 3.10, the analysis of the remaining cases showed that there were only two cases where an interchange was possible.

If $\mu=2$ and $q=2$, an interchange is possible, and in this case we obtained the following result.

Theorem 3.11.5 *If $\mu = 2$, $q = 2$, there are*

$$A_6 = 15 \cdot 2^6(2^{r-2}-1)(2^{r-3}-1) + 10\frac{2^8(2^{r-2}-1)(2^{r-3}-1)}{3})F$$

pairs (c_1, c_2) which are counted 3 times. The following number of pairs (c_1, c_2) are counted 7 times

$$A_7 = (35 \cdot (2^r - 2^2) + 45 \cdot 2^3(2^{r-2}-1))F.$$

Finally, $A_8 = 15F$ pairs (c_1, c_2) are counted 15 times.

If $\mu = 2$ and $q = 3$, we counted $(A_1 - 8)F$ different pairs (Theorem 3.9.3).

This eventually leads to our Main Theorem, where for $q = 2$, the obtained numbers are the numbers of non-minimal codewords of weight $2^{m-r} + 2^{m-r-\mu+1}(2^\mu - 1) = 3 \cdot 2^{m-r} - 2^{m-r-\mu+1}$ in the Reed-Muller code $\mathrm{RM}(r, m)$ we started from. In the Theorem below, we impose $\mu \geq 2$, since the case $\mu = 1$ reduces to the results of Borissov, Manev and Nikova, see Theorem 3.1.7.

Theorem 3.11.6 *The number of affine point sets formed by two disjoint affine point sets c_1 and c_2, where c_1 is the point set of an $(m-r)$-dimensional affine space and where c_2 is the point set of either a quadric $\Gamma Q(2\mu, q)$, $4 \leq 2\mu \leq m-r+2$, with an $(m-r-2\mu+1)$-dimensional vertex Γ at infinity, or a symmetric difference defined by two affine $(m-r)$-dimensional spaces intersecting in an affine $(m-r-\mu)$-dimensional space, $3 \leq \mu \leq r$, $\mu \leq m-r$, is equal to A_1F if $q > 3$, $\mu = 2$.*

It is $A_1F + A_2S - A_3 + \frac{A_3}{3}$ if $q > 2$, $\mu > 2$.

If $q = 2, \mu > 2$, we get

$$A_1F + A_2S - (A_3 + A_4 + A_5) + \frac{A_3}{3} + \frac{A_4}{3} + \frac{A_5}{2(2^\mu - 1) + 1}.$$

If $q = 2, \mu = 2$, we obtain

$$(A_1F + A_2S - \sum_{i=3}^{8} A_i) + \frac{A_3}{3} + \frac{A_4}{3} + \frac{A_5}{2(2^\mu-1)+1} + \frac{A_6}{3} + \frac{A_7}{7} + \frac{A_8}{15}.$$

Finally, if $q = 3, \mu = 2$, we obtain

$$(A_1 - 8)F.$$

Proof For $q > 3, \mu = 2$, we only need to consider the case c_2 is a quadric, and there are no double countings. So there are A_1F distinct unions $c_1 \cup c_2$ since there are F possibilities for c_2 and A_1 for c_1 (Theorem 3.11.1). In the next case, we first count the total number $A_1F + A_2S$ of pairs (c_1, c_2), where either: (1) c_1 is an affine $(m-r)$-dimensional space and c_2 is a quadric $\Gamma Q(2\mu, q)$ which are disjoint, or (2) c_1 is an affine $(m-r)$-dimensional space and c_2 is a symmetric difference which are disjoint. Note that there are S possibilities for the symmetric difference and A_2 possibilities for c_1, given a fixed symmetric difference c_2 (Theorem 3.11.2). We then subtract all pairs (c_1, c_2) which lead to unions $c_1 \cup c_2$ which are counted multiple times. Then we add each such union $c_1 \cup c_2$ once back to the sum, leading finally to the correct number of distinct unions $c_1 \cup c_2$. □

Chapter 4

Characterizations of the generalized Veronesean

In [65], a characterization of the finite quadric Veronesean $\mathcal{V}_n^{2^n}$ by means of properties of the set of its $\mathcal{V}_{n-1}$-spaces is proved. These $\mathcal{V}_{n-1}$-spaces form a regular generalized dual arc. In [35] and [36], we prove an extension result for regular generalized dual arcs, which is then used inductively to provide a similar characterization of the finite generalized Veronesean.

In the second part of this chapter, we characterize the finite Veronesean variety by means of intersection properties. For the smallest Veronesean, the conic, this was already done in the odd case by Segre, in his celebrated characterization of conics: "every set of $q + 1$ points in $\mathbf{PG}(2, q)$, q odd, no three of which are collinear, is a conic" [51]. This was in fact the starting point of this kind of results. For the Veronese surface of all conics in $\mathbf{PG}(2, q)$, this was already done by Ferri [22], Hirschfeld and Thas [28], and Thas and Van Maldeghem [66]. These results of the second part of this chapter can be found in [50].

4.1 A characterization result of the generalized Veronesean

4.1.1 Known results

In 1947, Bose studied ovals in [6]. In that paper, he proved that a cap in $\mathbf{PG}(2, q)$ has at most $q + 1$ points if q is odd and at most $q + 2$ points if q is even. If these bounds are attained we call the cap an oval and a hyperoval respectively.

Special cases of generalized dual arcs have a long history. A generalized dual arc of degree 0 is just a (partial) spread of $\mathbf{PG}(n, q)$. The generalized dual arc of degree $n-1$ in $\mathbf{PG}(n, q)$ of type $(n, n-1, \ldots, 1, 0)$ is just the dual of an ordinary arc of points in $\mathbf{PG}(n, q)$. Generalized dual arcs of degree 1 with $n_2 = 0$ are known as n_1-dimensional dual arcs. It is known that the dimension n of the ambient space $\mathbf{PG}(n, q)$ of an n_1-dimensional dual arc satisfies $2n_1 \leq n \leq \frac{1}{2}n_1(n_1+3)$ (see [73]).

Definition 4.1.1 *A family $\mathcal{A}$ of $\frac{q^{l+1}-1}{q-1}+1$ l-dimensional subspaces of $\mathbf{PG}(n, q)$ with $n \geq 2$ is called an l-dimensional dual hyperoval if it satisfies the following three axioms:*

- *every two elements of $\mathcal{A}$ intersect in a point,*
- *every three elements of $\mathcal{A}$ have no point in their intersection,*
- *all members of $\mathcal{A}$ span the whole space $\mathbf{PG}(n, q)$.*

The n_1-dimensional dual arc in $\mathbf{PG}(\frac{1}{2}n_1(n_1+3), q)$, defined by Construction 1.3.5, was first described in [73].

We need the following theorem about this Veronesean dual arc.

Theorem 4.1.2 *For q odd, the Veronesean dual arc is maximal, with respect to the property of being a Veronesean dual arc, while for q even, the Veronesean dual arc can be extended by an n_1-dimensional space to an n_1-dimensional dual hyperoval. The extension element is called the* nucleus*.*

Proof In every arc element $\Omega = D((x_0, \ldots, x_{n_1}))$, there is only one point not covered by a second arc element. This point is

$$\zeta((x_0, \ldots, x_{n_1})) = (x_0^2, \ldots, x_{n_1}^2, 2x_0x_1, \ldots, 2x_{n_1-1}x_{n_1}),$$

where ζ is the Veronesean map.

For odd q, these points $\zeta((x_0, \ldots, x_{n_1}))$ span $\mathbf{PG}(\frac{1}{2}n_1(n_1+3), q)$, i.e. the Veronesean dual arc is not extendable. For q even, they form an n_1-dimensional space which extends the Veronesean dual arc. This space is called the nucleus. □

The set $\mathcal{F}$ of q^2+q+1 planes in $\mathbf{PG}(5, q)$ from Example 1.3.8 has the following properties:

(P1) Each two of these planes intersect in a point.

(P2) Each three of these planes have an empty intersection.

Definition 4.1.3 *The tangent space of $\mathcal{V}_n^{2^n}$ at $p \in \mathcal{V}_n^{2^n}$ is the union of the tangent lines at p of the conics on $\mathcal{V}_n^{2^n}$ containing p (for $q = 2$ one considers the conics which are the images of the lines of $\mathbf{PG}(n, 2)$).*

If q is odd, then $D(p)$ is the tangent plane to $\mathcal{V}_2^4$ at p.

In 1958, Tallini [60] (see also [28]) showed that every set of $q^2 + q + 1$ planes in $\mathbf{PG}(5, q)$, q odd, for which (P1) and (P2) hold, must be isomorphic to the set $\mathcal{F}$ of Example 1.3.8, so isomorphic to the set of all tangent planes of $\mathcal{V}_2^4$.

Furthermore, tangent planes are related to conic planes, see Theorem 25.1.18 of [28].

Theorem 4.1.4 *If q is odd, then $\mathbf{PG}(5, q)$ admits a polarity which maps the set of all conic planes of $\mathcal{V}_2^4$ onto the set of all tangent planes of $\mathcal{V}_2^4$.*

This allows to state a dual version of Tallini's result.

Theorem 4.1.5 *If $\mathcal{L}$ is a set of $q^2 + q + 1$ planes of $\mathbf{PG}(5, q)$, q odd, with the following properties*

(i) *Any two distinct elements of $\mathcal{L}$ have exactly one point in common.*

(ii) *Any three distinct elements of $\mathcal{L}$ generate $\mathbf{PG}(5, q)$.*

(iii) *There is no point belonging to all elements of $\mathcal{L}$.*

Then $\mathcal{L}$ is the set of all conic planes of a Veronesean $\mathcal{V}_2^4$.

This result was generalized to higher dimensions and to q even in [65]. They obtained the following characterization of the finite quadric Veronesean $\mathcal{V}_n^{2^n}$.

Theorem 4.1.6 *([65]) Let $\mathcal{F}$ be a set of $\frac{q^{n+1}-1}{q-1}$ subspaces of dimension $\frac{(n-1)(n+2)}{2}$ in $\mathbf{PG}(N = \frac{n(n+3)}{2}, q)$, $n \geq 2$, with the following properties:*

(VS1) Each two members of $\mathcal{F}$ generate a hyperplane of $\mathbf{PG}(N, q)$.

(VS2) Each three elements of $\mathcal{F}$ generate $\mathbf{PG}(N, q)$.

(VS3) No point is contained in every member of $\mathcal{F}$.

(VS4) The intersection of any non-empty collection of members of $\mathcal{F}$ is a subspace of dimension $N_i = \frac{i(i+3)}{2}$ for some $i \in \{-1, 0, 1, \cdots, n-1\}$.

(VS5) There exist 3 members Ω_1, Ω_2, Ω_3 of $\mathcal{F}$ with $\Omega_1 \cap \Omega_2 = \Omega_2 \cap \Omega_3 = \Omega_3 \cap \Omega_1$.

Then either $\mathcal{F}$ is the set of $\mathcal{V}_{n-1}$-subspaces of a quadric Veronesean $\mathcal{V}_n^{2^n}$ in $\mathbf{PG}(N, q)$ *or q is even, there are two members $\Omega_1, \Omega_2 \in \mathcal{F}$ with the property that no other member of $\mathcal{F}$ contains $\Omega_1 \cap \Omega_2$, and there is a unique subspace Ω of dimension $\frac{(n-1)(n+2)}{2}$ such that $\mathcal{F} \cup \{\Omega\}$ is the set of $\mathcal{V}_{n-1}$-subspaces together with the nucleus subspace of a quadric Veronesean $\mathcal{V}_n^{2^n}$. In particular, if $n = 2$, then the statement holds under the weaker hypothesis of $\mathcal{F}$ satisfying* (**VS1**)*,* (**VS2**)*,* (**VS3**) *and* (**VS5**)*.*

For $n = 2$ one can classify all examples that do not satisfy (**VS5**) by a result of [15], and the only possibilities occur for $q = 2$ and $q = 4$. This classification remains open for $n \geq 3$, although an infinite class of examples is known for $q = 2$, see [65].

We work in the dual setting. Recall from Remark 1.3.14 that the Veronesean dual arc is the dual of the set of $\mathcal{V}_{n-1}$-subspaces. The dual formulation of the above theorem reads as follows. We will prove an extension of this dual version.

Theorem 4.1.7 *Let $\mathcal{F}$ be a set of $\frac{q^{n+1}-1}{q-1}$ n-dimensional spaces in* $\mathbf{PG}(\frac{n(n+3)}{2}, q)$ *with the following properties:*

(VS1) Each two elements of $\mathcal{F}$ intersect in a point.

(VS2) Each three elements of $\mathcal{F}$ are skew.

(VS3) The elements of $\mathcal{F}$ span $\mathbf{PG}(\frac{n(n+3)}{2}, q)$*.*

(VS4) Any proper subspace of $\mathbf{PG}(\frac{n(n+3)}{2}, q)$ *that is spanned by a collection of elements of $\mathcal{F}$ is a subspace of dimension $\frac{i(2n-i+3)}{2}-1$, for some $i \in \{0, \ldots, n\}$.*

(VS5) If q is even, at least one space spanned by two elements of $\mathcal{F}$ contains more than two elements of $\mathcal{F}$.

Then either $\mathcal{F}$ is the Veronesean dual arc defined by Construction 1.3.5 or q is even, there are two members $\Omega_1, \Omega_2 \in \mathcal{F}$ such that the $2n$-dimensional space $\langle \Omega_1, \Omega_2 \rangle$ only contains 2 elements of $\mathcal{F}$ and there is a unique subspace Ω of dimension n such that $\{\Omega\} \cup \mathcal{F}$ is the Veronesean dual arc defined by Construction 1.3.5 together with the nucleus subspace of a quadric Veronesean $\mathcal{V}_n^{2^n}$. In particular, if $n = 2$, then the statement holds under the weaker hypotheses of $\mathcal{F}$ satisfying $(VS1)$, $(VS2)$, $(VS3)$ and $(VS5)$.

4.1.2 Algebraic characterisation of dual arcs

Let $\mathcal{F}$ be a strongly regular generalized dual arc of size $\frac{q^{n+1}-1}{q-1}-\delta$ of type $(n_0,\dots,n_{d+1})$, where $n_i=\binom{n+d+1-i}{n}-1$.

Definition 4.1.8 *If any proper subspace spanned by a collection of elements of $\mathcal{F}$ has dimension $\binom{n+d+1}{d+1}-\binom{n+d+1-i}{d+1}-1$ for some $i\in\{0,\dots,n\}$ then $\mathcal{F}$ has* property (P)*.*

We will prove the following theorem.

Theorem 4.1.9 *Assume that $d+\delta\le\frac{q-5}{2}$ for q odd and $d+\delta\le\frac{q-6}{2}$ for q even.*

Let $\mathcal{F}$ be a strongly regular generalized dual arc of size $\frac{q^{n+1}-1}{q-1}-\delta$ of type $(n_0,\dots,n_{d+1})$, where $n_i=\binom{n+d+1-i}{n}-1$. having property (P).

If q is even, then we require in addition that there are two elements $\Omega_0,\Omega_1\in\mathcal{F}$, such that $\langle\Omega_0,\Omega_1\rangle$ contains at least three elements of $\mathcal{F}$.

Then $\mathcal{F}$ is extendable to a strongly regular generalized dual arc of size $\frac{q^{n+1}-1}{q-1}$.

If q is even and $d=1$, then the dual arc is even extendable to a dual arc of size $\frac{q^{n+1}-1}{q-1}+1$.

In any case, the dual arc is a subset of the maximal dual arc described by Construction 1.3.5 or of the Veronesean dual arc plus the nucleus subspace in the case $d=1$, q even.

Property (P) seems somewhat artificial, but we can prove that for $q\ge n$, property (P) is satisfied by every strongly regular generalized dual arc (Lemma 4.1.35).

The arc of Construction 1.3.5 satisfies property (P). Since the generalized dual arc of Construction 1.3.5 has the group $\mathbf{PGL}(n+1,q)$ as automorphism group, it is sufficient to determine the dimension of $\langle D(e_0),D(e_1),\dots,D(e_{i-1})\rangle$. The arc element $D(e_j)$ is spanned by all points of the form $p_{jx\dots x}$. Thus the span of $D(e_0),D(e_1),\dots,D(e_{i-1})$ contains all points which have either 0, 1, …, or $i-1$ as an index. There are $\binom{n+d+1}{d+1}$ different points and $\binom{n+d+1-i}{d+1}$ only contain indices from i to d.

The proof of this theorem consists of two parts, which will be covered by the next two sections. At this point, we just give an overview.

In the case $d=1$, we prove that for $\delta>0$, δ small, a dual arc of type (n_0,n_1,n_2) of size $\frac{q^{n+1}-1}{q-1}-\delta$ is not maximal. The proof techniques are similar to the techniques used in [28] to give an algebraic characterisation of a dual arc of size $\frac{q^{n+1}-1}{q-1}$. The main difference is that the deficiency δ makes simple counting arguments impossible, so we have to use more difficult structural arguments.

For $d > 1$, we use induction on d. The idea of this part is the following. In Construction 1.3.5, we have $n + 1$ special arc elements of the form $D((0, \ldots, 0, 1, 0, \ldots, 0))$. In each of these arc elements, the other arc elements induce a degree $d - 1$ dual arc of size $\frac{q^{n+1}-1}{q-1} - 1$. Thus each arc element $D((0, \ldots, 0, 1, 0, \ldots, 0))$ contains an extension space. Now we look at the dual arc induced in the extension space and find again an extension space inside and so on.

The indices of a point $p_{e_0,\ldots,e_d}$ describe in which arc elements in which extension spaces this point lies. For example, $e_0 = i$ means that $p_{e_0,\ldots,e_d}$ lies in $D((0, \ldots, 0, 1, 0, \ldots, 0))$ where the 1 stands at the i-th position, and $e_0 = e_1 = i$ means that in addition the point lies in the extension space of $D((0, \ldots, 0, 1, 0, \ldots, 0))$.

The idea of the proof is to take $n + 1$ elements of the dual arc that span $\mathbf{PG}(n_0, q)$. These elements will be the elements of the form $D((0, \ldots, 0, 1, 0, \ldots, 0))$. Define the basis points $p_{e_0,\ldots,e_d}$ as the intersection of the appropriate extension spaces. Then use the known algebraic characterisation for dual arcs of degree $d - 1$ to find the generalized Veronesean surface.

4.1.3 The case $d = 1$

For $d = 1$, the main theorem reads as follows.

Theorem 4.1.10 *Assume that $\delta \leq \frac{q-7}{2}$ for q odd and $\delta \leq \frac{q-8}{2}$ for q even, and let $\mathcal{F}$ be a set of $\frac{q^{n+1}-1}{q-1} - \delta$ different n-dimensional spaces in $\mathbf{PG}(\frac{n(n+3)}{2}, q)$ with the following properties:*

(1) each two elements of $\mathcal{F}$ intersect in a point,

(2) each three elements of $\mathcal{F}$ are skew,

(3) the elements of $\mathcal{F}$ span $\mathbf{PG}(\frac{n(n+3)}{2}, q)$,

(4) any proper subspace of $\mathbf{PG}(\frac{n(n+3)}{2}, q)$ that is spanned by a collection of elements of $\mathcal{F}$ is a subspace of dimension $\frac{i(2n-i+3)}{2} - 1$, for some $i \in \{0, \ldots, n\}$,

(5) if q is even, at least one space spanned by two elements of $\mathcal{F}$ contains more than two elements of $\mathcal{F}$.

Then $\mathcal{F}$ is extendable to a strongly regular generalized dual arc of size $\frac{q^{n+1}-1}{q-1}$. (In the case q even, this dual arc of size $\frac{q^{n+1}-1}{q-1}$ is even extendable to a dual hyperoval.)

The idea of the proof is in the same spirit as the proof of Theorem 4.1.6, so the proofs of some results describing the general structure will look very similar as the ones used for that result. The main work lies in the lemmata which actually deal with the deficiency itself, where we have to reconstruct the missing elements.

Definition 4.1.11 *A* contact point *is a point belonging to exactly one element of $\mathcal{F}$.*

Property (4) seems very technical. Our next lemma shows that for large q, property (4) is no restriction. This motivates property (4).

Lemma 4.1.12 *Let $q \geq n$, then any configuration $\mathcal{F}$ which satisfies the properties (1)-(3) also satisfies property (4).*

Proof Assume that the claim of the lemma is wrong, i.e. there exists a sequence $\pi_0, \ldots, \pi_k$ of elements in $\mathcal{F}$ with the property:

- $\Pi_j = \langle \pi_0, \ldots, \pi_j \rangle$, for $j \leq k$,
- $\dim \Pi_j = \frac{(j+1)(2n-j+2)}{2} - 1$, for $j < k$,
- $\frac{k(2n-k+3)}{2} - 1 < \dim \Pi_k < \frac{(k+1)(2n-k+2)}{2} - 1$.

By induction, we will construct a sequence $\pi_{k+1}, \ldots, \pi_{n+1}$ of members of $\mathcal{F}$ with the properties:

(I) the subspace defined recursively by $\Pi_i = \langle \Pi_{i-1}, \pi_i \rangle$ has at least an i-dimensional subspace in common with π_{i+1},

(II) the space π_{i+1} is not contained in Π_i.

For $i = n$, these two conditions yield a contradiction, because the elements of $\mathcal{F}$ have dimension n. This proves the lemma.

Now we construct π_{j+1} from the sequence $\pi_0, \ldots, \pi_j$. Note that $\dim \Pi_j$ is bounded by

$$\dim \Pi_k + (n-k) + \cdots + (n-(j-1)) \leq \\ \frac{(k+1)(2n-k+2)}{2} - 2 + \frac{(j-k)(2n-k-j+1)}{2} \leq \frac{n(n+3)}{2} - 1 \ .$$

Thus Π_j is not the whole space. By property (3), we know that there exists a space $\bar{\pi}_{j+1}$ of $\mathcal{F}$ not in Π_j. There are at least $q^n - 1 - \delta$ elements of $\mathcal{F}$ meeting $\bar{\pi}_{j+1}$ in a point outside of Π_j. Thus there are at least $q^n - \delta$ elements of $\mathcal{F}$ not in Π_j. Since π_{i+1} has at most an $(n-1)$-dimensional space in common with Π_i $(i < k)$, we conclude that at most $\frac{q^n-1}{q-1}$ elements of $\mathcal{F}$ intersect π_{i+1} in a point of Π_i. Thus for at most $j\frac{q^n-1}{q-1}$ elements of $\mathcal{F}$, there exists an $i < j$ such that this element intersects π_{i+1} in a point of Π_i. Because $k \leq n \leq q$,

$$q^n - \delta - k\frac{q^n-1}{q-1} > 0,$$

implying that there is an element π_{j+1} of $\mathcal{F}$ with the property that π_{j+1} is not in Π_j and $\pi_{j+1} \cap \pi_{i+1} \notin \Pi_i$. Especially, we have dim $\langle \pi_{j+1} \cap \pi_{i+1} \mid\mid -1 \leq i < j \rangle = j$, i.e. $\pi_{j+1} \cap \Pi_j$ is at least a j-dimensional space.

Thus, by induction, we have found the members of $\mathcal{F}$ with the properties (I) and (II), which proves the lemma. □

Property (4) allows us to compute the dimensions of many objects related to $\mathcal{F}$. An important special case is the following result.

Remark 4.1.13 *Let Π be a $2n$-dimensional space spanned by two elements of $\mathcal{F}$. Then an element of $\mathcal{F}$ either lies inside Π or intersects Π in a line.*

The next lemma gives us an upper bound on the number of elements of $\mathcal{F}$ contained in a space having one of the dimensions mentioned in property (4).

Lemma 4.1.14 *Every $\left(\frac{i(2n-i+3)}{2} - 1\right)$-dimensional space contains at most $\frac{q^i-1}{q-1}$ elements of $\mathcal{F}$.*

Proof Let Π be an $\left(\frac{i(2n-i+3)}{2} - 1\right)$-dimensional space spanned by i elements $\pi_1, \ldots, \pi_i$ of $\mathcal{F}$.

An element of $\mathcal{F}$, not contained in Π, intersects Π in an $(i-1)$-dimensional space Π_i (this is part of property (4)). Each element of $\mathcal{F}$, contained in Π, must share a point with Π_i. Furthermore, no two elements of $\mathcal{F}$ in Π intersect Π_i in the same point, so Π contains at most $\frac{q^i-1}{q-1}$ elements of $\mathcal{F}$. □

To understand the goal of the next lemma, consider the dual arc obtained by Construction 1.3.5. In this example, every element of $\mathcal{F}$ corresponds to a point of a projective space $\mathbf{PG}(n,q)$. The $2n$-dimensional spaces spanned by two elements of $\mathcal{F}$ correspond to the lines of $\mathbf{PG}(n,q)$. Thus if a dual arc with $\frac{q^{n+1}-1}{q-1} - \delta$ elements is a subset of this example, then the following is true:

Every $2n$-dimensional space spanned by two elements of $\mathcal{F}$ contains at least $q+1-\delta$ elements of $\mathcal{F}$.

Lemma 4.1.15 is the first step in that direction.

Lemma 4.1.15 *Every $2n$-dimensional space contains 0, 1, 2 or at least $q-\delta$ ($\delta \leq (q-7)/2$ for q odd and $\delta \leq (q-8)/2$ for q even) elements of $\mathcal{F}$.*

If q is odd, no $2n$-dimensional space contains exactly 2 elements of $\mathcal{F}$.

Proof Let Π be a $2n$-dimensional space which contains k elements of $\mathcal{F}$, where $2 \leq k < q-\delta$.

Let π' be any element of $\mathcal{F}$ not contained in Π. This element π' intersects Π in a line L' by the remark after Lemma 4.1.12. At least $q-\delta$ points of L' must be covered by a second element of $\mathcal{F}$. Since $q-\delta-k>0$, there must be a second element π'' of $\mathcal{F}$, not contained in Π, which intersects L'. Let $\pi'' \cap \Pi = L''$.

The lines L' and L'' span a plane π. Since every one of the k elements of $\mathcal{F}$ in Π must intersect π' and π'', these k elements intersect π' and π'' in a point on L', respectively on L'', different from $L' \cap L''$. Hence, they intersect π in lines.

Assume that π''' is another element of $\mathcal{F}$, not contained in Π, that intersects Π in L'''. We prove that if L''' has a point in common with L', then it has also a point in common with L''.

Suppose that L''' intersects L'. If L''' does not intersect L'', then every element of $\mathcal{F}$ contained in Π must share a line with the plane spanned by L' and L'', and has a point in common with L'''. Thus these elements share a plane with the 3-dimensional space spanned by L', L'' and L'''. Especially, two of these elements intersect each other in a line, a contradiction.

This proves that the elements of $\mathcal{F}$, not contained in Π, can be partitioned into *groups*. The elements from one group intersect each other in Π, and elements from different groups intersect each other outside of Π. Each group defines a plane inside Π and the k elements of $\mathcal{F}$ contained in Π must intersect such a plane in lines.

Let π_1 and π_2 be two planes inside Π defined by such groups. We distinguish several cases for the intersection $\pi_1 \cap \pi_2$.

(1) The planes π_1 and π_2 cannot be skew to each other. Otherwise, they would span a 5-dimensional space Ω. Now every element of $\mathcal{F}$ in Π shares a line with π_1 and π_2, so shares at least a 3-dimensional space with Ω, but then the elements of $\mathcal{F}$ in Π intersect each other in at least a line, which is false.

(2) If π_1 and π_2 intersect in a line, then at most one element of $\mathcal{F}$ contained in Π contains the line $\pi_1 \cap \pi_2$. So at least $k-1$ elements of $\mathcal{F}$ contained

in Π must share a plane with the 3-dimensional space spanned by π_1 and π_2. Thus each two of these elements must share a line, a contradiction for $k > 2$. We now eliminate the case $k = 2$, where one of the two elements of $\mathcal{F}$ in Π, for instance π, passes through the line $\text{Ł} = \pi_1 \cap \pi_2$.

For $k = 2$, all groups have size at least $q - \delta - 1$. For, consider a first element π' of $\mathcal{F}$ not in Π, then consider the line $\text{Ł}' = \pi' \cap \Pi$. This line has at most $\delta + 1$ contact points, so it is intersected in a point by at least $q - 2 - \delta$ elements of $\mathcal{F}$, not lying in Π. This shows that a group of elements of $\mathcal{F}$, not lying in Π, has at least size $q - \delta - 1$.

But now consider the line $\text{Ł} = \pi_1 \cap \pi_2$, lying in an element π of $\mathcal{F}$ in Π, and in the two planes π_1 and π_2 containing at least $q - \delta - 1$ lines lying in elements of $\mathcal{F}$, not contained in Π. Since no point of Ł lies in three elements of $\mathcal{F}$, and every point of Ł already lies in the element π of $\mathcal{F}$, we must have $q + 1 \geq 2(q - \delta - 1) + 1$, where the $+1$ arises from the second element of $\mathcal{F}$ in Π. This implies $q \leq 2\delta + 2$, a contradiction.

(3) Thus π_1 and π_2 intersect in a point s. But then the only possibility for an element of $\mathcal{F}$ contained in Π to intersect π_1 and π_2 in lines is that s is a point of that element. Thus all elements of $\mathcal{F}$ contained in Π contain s. Since every three elements of $\mathcal{F}$ are skew, this means that $k = 2$.

Assume now that we are in the case $k = 2$ and q is odd. Since there are $\frac{q^{n+1}-1}{q-1} - 2 - \delta$ elements of $\mathcal{F}$ not contained in Π, and since for odd q a dual arc of lines in $\mathbf{PG}(2, q)$ contains at most $q + 1$ elements, each group can contain at most $q - 1$ elements, so there are at least

$$\frac{1}{q-1}\left(\frac{q^{n+1}-1}{q-1} - 2 - \delta\right) > \frac{q^n - 1}{q-1}$$

different groups.

Each group defines a plane through s which intersects an element of $\mathcal{F}$ contained in Π in a line. Since an n-dimensional space only contains $\frac{q^n-1}{q-1}$ different lines through s, there must exist two groups which define planes π_1 and π_2 intersecting in a line. But this is impossible as we already proved.

So the case $k = 2$ is only possible for q even. □

Even if we could not exclude the case $k = 2$ for q even, we have proven in step (3) the following characterisation:

Corollary 4.1.16 *Let q be even and let $\langle \pi, \pi' \rangle$ be a $2n$-space that contains only π and π' as elements of $\mathcal{F}$. Then the elements of $\mathcal{F} \backslash \{\pi, \pi'\}$ intersect $\langle \pi, \pi' \rangle$ in groups of pairwise intersecting lines. Furthermore, there can be at most $\frac{q^n-1}{q-1}$ such groups.*

We call a $2n$-dimensional space *big* if it contains at least $q-\delta$ elements of $\mathcal{F}$. The next lemma associates with each big $2n$-dimensional space Π a plane $\bar{\pi}$ which will be very important in the remaining part of this section.

Lemma 4.1.17 *Let Π be a $2n$-dimensional space containing $q+1-\delta_i \geq q-\delta$ elements of $\mathcal{F}$. Then Π contains a plane $\bar{\pi}$ which intersects the $q+1-\delta_i$ elements of $\mathcal{F}$ in Π in lines. The elements of $\mathcal{F}$, not in Π, intersect Π in a line. These lines either lie in $\bar{\pi}$, or they are skew to $\bar{\pi}$ and then contain δ_i contact points. Moreover, those latter lines skew to $\bar{\pi}$ which are the intersection of Π with an element of $\mathcal{F}$ not lying in Π are pairwise disjoint.*

Proof Assume that two elements $\tilde{\pi}_1$ and $\tilde{\pi}_2$ of $\mathcal{F}$, not in Π, intersect Π in two intersecting lines $Ł_1$ and $Ł_2$. Let $\bar{\pi}$ be the plane spanned by $Ł_1$ and $Ł_2$.

We are not in the case which is assumed in the beginning of the proof of Lemma 4.1.15. However, the same kind of arguments as the ones used in the proof of Lemma 4.1.15 show that

1. Every line in Π that intersects $\bar{\pi}$ and that comes from an element of $\mathcal{F}$ not in Π must lie in $\bar{\pi}$.

2. Every element of $\mathcal{F}$ in Π must intersect $\bar{\pi}$ in a line.

3. The lines in Π that come from an element of $\mathcal{F}$ not in Π and that do not lie in $\bar{\pi}$ must be pairwise disjoint.

Property 3 is proven in the following way. Otherwise we have two planes $\bar{\pi}_1$ and $\bar{\pi}_2$ corresponding with two different groups of lines as in the proof of Lemma 4.1.15. We have shown in the proof of Lemma 4.1.15 that $\bar{\pi}_1$ and $\bar{\pi}_2$ must intersect in a point s which lies on every element of $\mathcal{F}$ in Π. But this implies that Π has only 2 elements of $\mathcal{F}$ which is not the case.

So, from now on, we may assume that all the elements of $\mathcal{F}$, not in Π, intersect Π in pairwise disjoint lines. Now we construct the plane $\bar{\pi}$.

Let π_1, π_2 and π_3 be three elements of $\mathcal{F}$ in Π. Let $s_{12} = \pi_1 \cap \pi_2$, $s_{13} = \pi_1 \cap \pi_3$ and $s_{23} = \pi_2 \cap \pi_3$.

The points s_{12}, s_{13}, s_{23} generate a plane $\bar{\pi}$, since otherwise, π_1, π_2, π_3 share a line. Assume that an element of $\mathcal{F}$, not in Π, intersects Π in a line $Ł$ that meets $\bar{\pi}$. We claim that $Ł$ must lie in $\bar{\pi}$. Suppose the contrary. Without loss of generality, we may assume that $Ł \cap \bar{\pi} \notin \pi_1 \cup \pi_2$. But then π_1 and π_2 share a plane with the 3-dimensional space $\langle \bar{\pi}, Ł \rangle$, i.e. they share a line, a contradiction.

At most one line in Π that comes from an element of $\mathcal{F}$ not in Π lies in $\bar{\pi}$, since these lines are pairwise disjoint. Since every element of $\mathcal{F}$ has only

$\delta+1$ contact points, this proves that at least $q-\delta-1$ points of $s_{12}s_{13}$ lie in an element of $\mathcal{F}$ in Π, different from π_1.

Assume that there exists an element π of $\mathcal{F}$ in Π which intersects π_1 in a point s not on $s_{12}s_{13}$. The above arguments show that $s_{12}s_{13}$, ss_{12} and ss_{13} must contain at least $3(q-\delta-1)-3 > q+1$ points in π_1 which lie on two elements of $\mathcal{F}$ inside Π, a contradiction with Lemma 4.1.14.

Thus every element π of $\mathcal{F}$ in Π meets $s_{12}s_{13}$, $s_{12}s_{23}$ and $s_{13}s_{23}$, i.e. it has a line in common with $\bar{\pi}$. □

The next series of lemmas deal with the case q even and $k=2$. Let us again have a look at the example that comes from Construction 1.3.5. In this example, every $2n$-dimensional space containing at least one element of $\mathcal{F}$ contains either 1 or $q+1$ elements of $\mathcal{F}$. If q is even, we can extend the dual arc of size $\frac{q^{n+1}-1}{q-1}$ by one element π. This element π has the special property that for all other elements $\pi' \in \mathcal{F}$, the $2n$-space $\langle \pi, \pi' \rangle$ contains no other element of $\mathcal{F}$, see [65]. We call this element the *nucleus* of $\mathcal{F}$.

We will prove in Lemma 4.1.20 that this property holds for every regular generalized dual arc for q even.

Lemma 4.1.18 *Let q be even and let $\pi, \pi' \in \mathcal{F}$ be such that the $2n$-dimensional space $\langle \pi, \pi' \rangle$ contains no other element of $\mathcal{F}$. Let $s = \pi \cap \pi'$.*

Let Π be a big $2n$-dimensional space containing π and let $\bar{\pi}$ be the plane inside Π described by Lemma 4.1.17. Then $s \in \bar{\pi}$.

Proof Let $\Pi = \langle \pi, \pi'' \rangle$, $\pi'' \in \mathcal{F} \backslash \{\pi, \pi'\}$. Let $\bar{\pi}' = \langle s = \pi \cap \pi', \pi'' \cap \pi, \pi'' \cap \pi' \rangle$. As we have already seen in Corollary 4.1.16, this gives us a group of intersecting lines in this plane. But Lemma 4.1.17 states that the only plane in Π which contains a group of intersecting lines is $\bar{\pi}$, i.e. $\bar{\pi} = \bar{\pi}'$. □.

Lemma 4.1.19 *Let q be even. For each $\pi \in \mathcal{F}$ either all $2n$-dimensional spaces $\langle \pi, \pi' \rangle$ with $\pi \neq \pi' \in \mathcal{F}$ contain exactly two elements of $\mathcal{F}$, or there exists at most one element $\pi \neq \pi' \in \mathcal{F}$ such that $\langle \pi, \pi' \rangle$ contains exactly two elements of $\mathcal{F}$.*

Proof Assume that π lies in a big $2n$-dimensional space Π, and let $\bar{\pi}$ be the plane described by Lemma 4.1.17 and let Ł be the line $\bar{\pi} \cap \pi$. By Lemma 4.1.18, we know that an element π' of $\mathcal{F}$ for which $\langle \pi, \pi' \rangle$ contains no other element of $\mathcal{F}$ must intersect π in a point of Ł.

Since Ł has only $q+1$ points and $|\mathcal{F}| = \frac{q^{n+1}-1}{q-1} - \delta$, this means that π must lie in more than one big $2n$-space Π'. But then we have a second line $Ł' = \bar{\pi}' \cap \pi$ and every element π' of $\mathcal{F}$ for which $\langle \pi, \pi' \rangle$ contains no other element of $\mathcal{F}$ must intersect π in a point of $Ł \cap Ł'$. (Ł and Ł' are different, since Ł must meet the $q-\delta$ elements of $\mathcal{F}$ in Π, Ł$'$ must meet the $q-\delta$ elements of $\mathcal{F}$ in Π' and $2q-2\delta-2 > q+1$, see also step (2) of Lemma 4.1.15.) This proves the lemma. □

Lemma 4.1.20 *Let q be even and assume that there exists a $2n$-dimensional space Π which contains exactly two elements of $\mathcal{F}$. Then there exists one element $\pi \in \mathcal{F}$ such that for every $\pi \neq \pi' \in \mathcal{F}$, the $2n$-space $\langle \pi, \pi' \rangle$ contains exactly two elements of $\mathcal{F}$.*

Proof Let $\Pi = \langle \pi, \pi' \rangle$. Assume that both elements π and π' lie in a big $2n$-dimensional space. Then all other elements of $\mathcal{F}$ generate with π and π', respectively, a big $2n$-dimensional space (Lemma 4.1.19). Let π'' be such an element and $\Pi_0 = \langle \pi, \pi'' \rangle$ with the special plane $\bar{\pi}_0$ and $\Pi_1 = \langle \pi', \pi'' \rangle$ with the special plane $\bar{\pi}_1$. By the proof of Lemma 4.1.18, we know that $\bar{\pi}_0 = \langle \pi \cap \pi', \pi \cap \pi'', \pi' \cap \pi'' \rangle = \bar{\pi}_1$.

But this is a contradiction since this plane cannot contain $2(q-\delta)-1 > q+2$ different lines coming from elements of $\mathcal{F}$ in Π_0 and Π_1. Thus either π or π' does not lie in big $2n$-dimensional spaces. They cannot both lie only in $2n$-spaces which contain 2 elements of $\mathcal{F}$ or else by condition (5) of Theorem 4.1.10 which we assume to be valid for $\mathcal{F}$, we find a $\pi'' \in \mathcal{F} \backslash \{\pi, \pi'\}$ lying in at least one big $2n$-space and in two $2n$-spaces with only two elements of $\mathcal{F}$, a contradiction with Lemma 4.1.19. □

If q is even and the special element π from Lemma 4.1.20 exists, we simply remove it from $\mathcal{F}$. This increases the deficiency by 1.

Remark 4.1.21 *Thus from now on, we assume that a $2n$-space cannot contain 2 elements of $\mathcal{F}$ and that $\delta \leq (q-6)/2$ when q is even and $\delta \leq (q-7)/2$ when q is odd.*

Our next goal is a stronger version of Lemma 4.1.17 which states that an element of $\mathcal{F}$, not in a big $2n$-space Π, must be skew to the plane $\bar{\pi}$. We will reach this goal with Lemma 4.1.28.

Lemma 4.1.22 *Let Π_1, Π_2 and Π_3 be distinct $2n$-dimensional spaces containing at least $q-\delta$ elements of $\mathcal{F}$.*

Then $\dim(\Pi_1 \cap \Pi_2 \cap \Pi_3) \leq n$.

Proof By property (4), we know that $\dim(\Pi_1 \cap \Pi_2) \leq n+1$.

Assume that $\Pi_1 \cap \Pi_2 \cap \Pi_3$ is an $(n+1)$-dimensional space Π. Since two elements of $\mathcal{F}$ span a $2n$-dimensional space, the space Π contains at most one element of $\mathcal{F}$ and the other elements of $\mathcal{F}$ in Π_i intersect Π in a line.

Let Ł be such a line in Π that comes from an element of $\mathcal{F}$ in Π_1. The elements in Π_2 and Π_3 intersect Ł in a point. Since $2(q-\delta-1) > q+1$, some point of Ł lies on an element of $\mathcal{F}$ in Π_1, Π_2 and Π_3. A contradiction since each point lies on at most 2 elements of $\mathcal{F}$. □

In the case of Construction 1.3.5, we know that the big $2n$-dimensional spaces correspond to the lines of an n-dimensional projective space $\mathbf{PG}(n,q)$. Thus in that case, every element of $\mathcal{F}$ lies in exactly $\frac{q^n-1}{q-1}$ big $2n$-spaces. Now we can prove this for a regular generalized dual arc.

Lemma 4.1.23 *Let $\pi \in \mathcal{F}$. Consider all $2n$-dimensional spaces through π containing at least $q-\delta$ elements of $\mathcal{F}$. Then the planes $\bar{\pi}$ of these $2n$-spaces intersect π in different lines through a common point.*

Moreover, there are exactly $\frac{q^n-1}{q-1}$ different big $2n$-spaces through π.

Proof Let Π and Π' be two different $2n$-spaces through π, and let $\bar{\pi}$ and $\bar{\pi}'$ be the corresponding planes defined by Lemma 4.1.17. By Lemma 4.1.17, we know that $\pi \cap \bar{\pi}$ and $\pi \cap \bar{\pi}'$ are lines. These lines must be different since otherwise $\pi \cap \bar{\pi} = \pi \cap \bar{\pi}'$ would contain at least $2(q-\delta-1) > q+1$ points lying on π and on another element of $\mathcal{F}$.

By the proof of Lemma 4.1.17, we know that at most $\delta+2$ elements of $\mathcal{F}$ not in Π' intersect Π' in lines contained in $\bar{\pi}'$. The other elements intersect Π' in pairwise skew lines. Thus Π contains at least $q-2\delta-3 \geq 3$ elements of $\mathcal{F}$ that intersect Π' in pairwise skew lines; we call this set of lines $\mathcal{L}_1$. By symmetry, we know that Π' contains at least $q-2\delta-3 \geq 3$ elements of $\mathcal{F}$ that intersect Π in pairwise skew lines; we call this set of lines $\mathcal{L}_2$.

Each line in $\mathcal{L}_1$ must intersect each line of $\mathcal{L}_2$, in the intersection point of the corresponding elements of $\mathcal{F}$. Thus $\mathcal{L}_1$ and $\mathcal{L}_2$ are the lines of two opposite reguli of a hyperbolic quadric $Q^+(3,q)$.

By Lemma 4.1.17, we know that every element of $\mathcal{F}$ in Π has a line in common with $\bar{\pi}$. Thus the line $\pi \cap \bar{\pi}$ intersects all lines of $\mathcal{L}_1$, i.e. it lies in the regulus defined by $\mathcal{L}_2$. By symmetry, $\pi \cap \bar{\pi}'$ lies in the regulus defined by $\mathcal{L}_1$. Thus $\pi \cap \bar{\pi}$ and $\pi \cap \bar{\pi}'$ intersect. In addition we see that every element of Π different from π must lie in the regulus defined by $\mathcal{L}_1$, i.e. all elements of Π intersect Π' in pairwise skew lines not in $\bar{\pi}'$. Thus the first case in Lemma 4.1.17 cannot occur. Especially the intersection point of $\pi \cap \bar{\pi}$ and $\pi \cap \bar{\pi}'$ must be a contact point, since it can lie only in elements of $\mathcal{F}$ that lie in the intersection $\Pi \cap \Pi'$.

This proves that either the lines of the form $\pi \cap \bar{\pi}$ share a common point or they lie in a common plane since they pairwise share a point. But the lines of the form $\pi \cap \bar{\pi}$ must additionally cover all non-contact points in π and intersect only in contact points. Thus the lines of the form $\pi \cap \bar{\pi}$ share a common contact point and there are at most $\frac{q^n-1}{q-1}$ lines of the form $\pi \cap \bar{\pi}$. That there are at least that many such lines follows from the fact that each big $2n$-space contains at most $q+1$ elements of $\mathcal{F}$ and hence π is contained in at least $(\frac{q^{n+1}-1}{q-1} - \delta - 1)/q > \frac{q^n-1}{q-1} - 1$ big $2n$-spaces. □

Remark 4.1.24 *We note that in this proof, we encounter the strongest condition on δ, namely $q - 2\delta - 3 \geq 3$; equivalently, $\delta \leq (q-6)/2$ for $d = 1$.*

An important consequence of Lemma 4.1.23 is the following result.

Corollary 4.1.25 *Let $\Pi_1, \ldots, \Pi_{\frac{q^n-1}{q-1}}$ be the big $2n$-spaces containing a given element π of $\mathcal{F}$. Let the space Π_i contain $q+1-\delta_i$ elements of $\mathcal{F}$. Then $\sum_{i=1}^{\frac{q^n-1}{q-1}} \delta_i = \delta$.*

Especially, most big $2n$-dimensional spaces through π contain $q+1$ elements of $\mathcal{F}$. Moreover, each $2n$-space contains at least $q+1-\delta$ elements of $\mathcal{F}$.

Proof We already know that every $2n$-space containing more than two elements of $\mathcal{F}$, contains $q+1-\delta_i \geq q-\delta$ elements of $\mathcal{F}$ (Lemma 4.1.15).

Since $\sum_{i=1}^{\frac{q^n-1}{q-1}} \delta_i = \delta$, necessarily $\delta_i \leq \delta$, so we can conclude that every $2n$-space containing more than two elements of $\mathcal{F}$, contains $q+1-\delta_i \geq q+1-\delta$ elements of $\mathcal{F}$. □

The next lemma allows us to reduce the case of an $(\frac{n(n+3)}{2}, n, 0)$-arc to the case of a $(5, 2, 0)$-arc.

Lemma 4.1.26 *Let $\hat{\Pi}$ be a $(3n-1)$-space spanned by three elements of $\mathcal{F}$. Let $\hat{\mathcal{F}}$ be the set of elements of $\mathcal{F}$ in $\hat{\Pi}$.*

For every π in $\hat{\mathcal{F}}$, define

$$\hat{\pi} := \left\langle \pi \cap \pi' \mid\mid \pi \neq \pi' \in \hat{\mathcal{F}} \right\rangle .$$

For every π in $\hat{\mathcal{F}}$, the space $\hat{\pi}$ is a plane and these planes form a dual arc in 5 dimensions.

Proof For each element π in $\hat{\mathcal{F}}$, we define a linear space $\mathcal{L}$ with the following properties:

(i) The points of the linear space are the points $\pi \cap \pi'$, with $\pi \neq \pi' \in \hat{\mathcal{F}}$.

(ii) The lines of the linear space are the lines of π through two points of the form $\pi \cap \pi'$ and $\pi \cap \pi''$ ($\pi' \neq \pi, \pi'' \neq \pi \in \hat{\mathcal{F}}$).

If π is not contained in the $2n$-dimensional space Π spanned by π' and π'', then it intersects Π in a line containing $\pi \cap \pi'$ and $\pi \cap \pi''$; in fact, this line contains at least $q - \delta$ elements of the form $\pi \cap \pi'''$, with $\pi''' \neq \pi \in \hat{\mathcal{F}}$ (Lemma 4.1.15).

If π is contained in the $2n$-space Π, then $\pi \cap \pi'$ and $\pi \cap \pi''$ lie on the intersection line of π with the plane $\bar{\pi}$ of Π (Lemma 4.1.17) which contains at least $q - \delta - 1$ intersection points of π with other planes of $\hat{\mathcal{F}}$.

The number of points in $\mathcal{L}$ is at least $3(q - \delta - 1) - 3$ (Lemma 4.1.15) and at most $q^2 + q + 1$ (Lemma 4.1.14).

If p_0, p_1 and p_2 are three non-collinear points of the linear space, then p_0p_1 contains at least $q-\delta-1$ intersection points of two elements of $\mathcal{F}$ and thus there are at least $q-\delta-1$ lines through p_2 and therefore at least $(q-\delta-1)(q-\delta-2)+1$ intersection points in the plane $\langle p_0, p_1, p_2 \rangle$.

By the same arguments, four points p_0, p_1, p_2 and p_3 of the linear space $\mathcal{L}$ that do not lie in a plane would imply that the linear space $\mathcal{L}$ contains at least $(q - \delta - 2)((q - \delta - 1)(q - \delta - 2) + 1) + 1$ points. But this is not possible since the number of points in $\mathcal{L}$ is bounded by $q^2 + q + 1$.

Thus $\hat{\pi} := \left\langle \pi \cap \pi' \mid\mid \pi \neq \pi' \in \hat{\mathcal{F}} \right\rangle$ is a plane.

It remains to be proven that the planes $\hat{\pi}$ span a 5-space. Their span has at most dimension 5 as we know from [73]. Assume that they only span a 4-space. Then the three elements of $\mathcal{F}$ that span $\hat{\Pi}$ would have a plane in common with this 4-dimensional space. This would imply that $\hat{\Pi}$ has at most dimension $4 + 3(n - 2) = 3n - 2$, but this is false. □

Corollary 4.1.27 *Every big $2n$-space lies in exactly $\frac{q^{n-1}-1}{q-1}$ different $(3n-1)$-spaces spanned by three elements of $\mathcal{F}$.*

Proof Every big $2n$-space Π through π corresponds to a line $\bar{\pi} \cap \pi$ and all these lines go through a common point s. A $(3n - 1)$-space defined by three elements of $\mathcal{F}$ through π corresponds to the lines in one plane through s inside π by Lemma 4.1.26. Thus the $(3n - 1)$-spaces defined by three elements of $\mathcal{F}$ through Π correspond to planes inside π through $\bar{\pi} \cap \pi$. There are exactly $\frac{q^{n-1}-1}{q-1}$ such planes. □

Now we are able to improve the result of Lemma 4.1.17.

Lemma 4.1.28 *With the notations of Lemma 4.1.17, the following result holds: no element of $\mathcal{F}$ not in Π intersects $\bar{\pi}$.*

Proof We know from the preceding lemma that $\bar{\pi}$ shares a line with every element π of $\mathcal{F}$ in Π, passing through a fixed contact point of π. Assume that $\bar{\pi}$ contains an extra line from an element π' of $\mathcal{F}$ not contained in Π. Let $\{r\} = \pi \cap \pi' \cap \bar{\pi}$.

The elements π and π' define a big $2n$-dimensional space Π', and Π' contains a plane $\bar{\pi}'$. The intersection $\bar{\pi}' \cap \pi$ is a line which contains r and the fixed contact point. Thus $\pi \cap \bar{\pi}' = \pi \cap \bar{\pi}$, a contradiction.

Thus $\bar{\pi}$ contains no line that comes from an element of $\mathcal{F}$ not in Π. Elements of $\mathcal{F}$ inside Π intersect $\bar{\pi}$ in a dual arc of $q+1-\delta_i$ lines. □

Remark 4.1.29 *If $\bar{\pi}$ contains lines of contact points, these lines extend the dual arc of $q+1-\delta_i$ lines induced by the elements of $\mathcal{F}$ in Π. For $\delta_i = 1$ and q odd, we find one line of contact points, and for $\delta_i = 1$ and q even, we find two lines of contact points.*

Now we are reaching our final goal to prove that $\mathcal{F}$ is not maximal. As a first step, we prove that the planes $\bar{\pi}$ contain lines of contact points.

Lemma 4.1.30 *Let Π_1 and Π_2 be two big $2n$-spaces with the property that $\langle \Pi_1, \Pi_2 \rangle$ is a $(3n-1)$-dimensional space. Assume that Π_1 and Π_2 share no element of $\mathcal{F}$. Let $\bar{\pi}_1$ and $\bar{\pi}_2$ be the planes in Π_1 and Π_2 which exist by Lemmas 4.1.17 and 4.1.28. Then $\bar{\pi}_1 \cap \Pi_2$ is a line of contact points.*

Proof First of all, it is impossible that the plane $\bar{\pi}_1$ is contained in Π_2. For assume the contrary. We obtain a contradiction in the following way. Every element π of $\mathcal{F}$ in Π_1 intersects Π_2 in a line. If $\bar{\pi}_1$ lies completely in Π_2, then the intersection line Ł $= \Pi_2 \cap \pi$ equals the line $\bar{\pi}_1 \cap \pi$. This line contains at least $q - \delta_1$ points lying in two elements of $\mathcal{F}$ in Π_1. But the $q+1-\delta_2$ elements of $\mathcal{F}$ in Π_2 must intersect π in a point. So at least $q+1-\delta_2$ points of Ł still lie in an element of $\mathcal{F}$ in Π_2. Then there are points of Ł lying in three elements of $\mathcal{F}$. This is false.

Note that the plane $\bar{\pi}_1$ lies in the 5-space $\hat{\Pi}_1 \subseteq \Pi_1$ spanned by the planes $\hat{\pi}$ defined in Lemma 4.1.26. Then Π_2 cannot contain $\hat{\Pi}_1$, since otherwise every element of $\hat{\mathcal{F}}$ would intersect Π_2 at least in a plane, contradicting the remark after Lemma 4.1.12. Thus $\Pi_2 \cap \hat{\Pi}_1$ is a 4-dimensional space, spanned by two planes $\hat{\pi}$ and $\hat{\pi}'$ corresponding to elements π and π' of $\mathcal{F}$ in Π_2. The plane $\bar{\pi}_1$ lies in the 5-dimensional space $\hat{\Pi}_1$ and thus it intersects the 4-dimensional space $\Pi_2 \cap \hat{\Pi}_1$, and therefore Π_2, in at least a line.

Consider again the intersection line Ł $= \Pi_2 \cap \pi$ of an element π of $\mathcal{F}$ in Π_1 with Π_2. This line contains $q+1-\delta_2$ points lying on an element of $\mathcal{F}$ in Π_2 and δ_2 contact points (Lemma 4.1.17 and Lemma 4.1.28). So the points of Ł do not lie in an other element of $\mathcal{F}$ in Π_1.

Now Ł and $\pi \cap \bar{\pi}_1$ intersect in a point, since both lines lie in the plane $\hat{\pi}$ defined by Lemma 4.1.26. This point must be a contact point, for else, it lies in a second plane of $\mathcal{F}$ in Π_1, but this was excluded in the preceding paragraph.

So π shares a contact point with Π_2, which also lies on the intersection line of Π_2 with $\bar{\pi}_1$.

This proves that the line $\bar{\pi}_1 \cap \Pi_2$ intersects the dual arc in $\bar{\pi}_1$, consisting of lines of the form $\bar{\pi}_1 \cap \pi$, where π is an element of $\mathcal{F}$ in Π_1, only in contact points, i.e. $\bar{\pi}_1 \cap \Pi_2$ only contains points covered by at most one element of $\mathcal{F}$.

This proves the theorem. □

Lemma 4.1.31 *Let Π_1 and Π_2 be two big $2n$-dimensional spaces with the property that $\langle \Pi_1, \Pi_2 \rangle$ is a $(3n-1)$-space. Assume that Π_1 and Π_2 share no element of $\mathcal{F}$ and let $q+1-\delta_1$ be the number of elements of $\mathcal{F}$ in Π_1 and let $q+1-\delta_2$ be the number of elements of $\mathcal{F}$ in Π_2.*

Let $\bar{\pi}_1$ and $\bar{\pi}_2$ be the planes in Π_1 and Π_2 which exist by Lemma 4.1.17.

Then the lines $\mathcal{L}_1 = \{\bar{\pi}_2 \cap \Pi_1\} \cup \{\pi_1 \cap \Pi_2 \mid\mid \pi_1 \in \mathcal{F}, \pi_1 \subset \Pi_1\}$ and $\mathcal{L}_2 = \{\bar{\pi}_1 \cap \Pi_2\} \cup \{\pi_2 \cap \Pi_1 \mid\mid \pi_2 \in \mathcal{F}, \pi_2 \subset \Pi_2\}$ are lines of two opposite reguli of a hyperbolic quadric $Q^+(3,q)$.

Especially this implies that $\delta_1 > 0$ and $\delta_2 > 0$ since a regulus has only $q+1$ lines, and that $\bar{\pi}_2 \cap \Pi_1$ and $\bar{\pi}_1 \cap \Pi_2$ are concurrent.

Proof By Lemma 4.1.28, we know that the elements of $\mathcal{F}$ in Π_1 intersect Π_2 in pairwise skew lines. Thus $\mathcal{L}'_1 = \{\pi_1 \cap \Pi_2 \mid\mid \pi_1 \in \mathcal{F}, \pi_1 \subset \Pi_1\}$ and $\mathcal{L}'_2 = \{\pi_2 \cap \Pi_1 \mid\mid \pi_2 \in \mathcal{F}, \pi_2 \subset \Pi_2\}$ are sets of pairwise skew lines. Since $\pi_1 \cap \pi_2 \subset \Pi_1 \cap \Pi_2$, every line of $\mathcal{L}'_1$ intersects every line of $\mathcal{L}'_2$.

Since both sets contain more than 2 lines, it follows that the lines of $\mathcal{L}'_1$ and $\mathcal{L}'_2$ are lines of opposite reguli.

Now consider the line $\bar{\pi}_2 \cap \Pi_1$, which exists by Lemma 4.1.30. By Lemma 4.1.28, the plane $\bar{\pi}_2$ is skew to all elements of $\mathcal{F}$ in Π_1. Thus $\bar{\pi}_2 \cap \Pi_1$ is different from all lines in $\mathcal{L}'_1$. But every element π_2 of $\mathcal{F}$, contained in Π_2, has a line in common with $\bar{\pi}_2$. Thus $\bar{\pi}_2 \cap \Pi_1$ intersects all lines of $\mathcal{L}'_2$. This proves that $\mathcal{L}_1 = \{\bar{\pi}_2 \cap \Pi_1\} \cup \mathcal{L}'_1$ are the lines of a regulus. By symmetry, the same is true for $\mathcal{L}_2$. □

Recall that the final goal is to prove that $\mathcal{F}$ is given by Construction 1.3.5. Thus every element of $\mathcal{F}$ should correspond to a point of $\mathbf{PG}(n,q)$. Since $\mathcal{F}$ has only $\frac{q^{n+1}-1}{q-1} - \delta$ elements, δ points of $\mathbf{PG}(n,q)$ are not used in Construction 1.3.5. The next lemma will identify these *holes*.

Consider the linear space $\mathcal{L}$ with the elements of $\mathcal{F}$ as points and the $2n$-spaces generated by two elements of $\mathcal{F}$ as lines. This is a linear space with $\frac{q^{n+1}-1}{q-1} - \delta$ points.

As planes of $\mathcal{L}$, we define the $(3n-1)$-dimensional spaces generated by three elements of $\mathcal{F}$.

Lemma 4.1.32 *Every plane of $\mathcal{L}$ is a projective plane of order q with possibly some holes.*

Proof Let P be a $(3n-1)$-dimensional space generated by three elements of $\mathcal{F}$.

Let $\Pi \subset P$ be a $2n$-dimensional space that contains $q+1$ elements of $\mathcal{F}$. This $2n$-space Π exists since there are $q+1$ different big $2n$-dimensional spaces through an element π of $\mathcal{F}$ in P and at most δ of them contain less than $q+1$ elements of $\mathcal{F}$ (Corollary 4.1.25). Let Π' be an other big $2n$-dimensional space in P. By Lemma 4.1.31, we know that Π and Π' share an element of $\mathcal{F}$.

Let Π_1 and Π_2 be two big $2n$-dimensional spaces in P. Let π be an element of $\mathcal{F}$ in Π_1, but not in Π_2. Since Π_2 contains at least $q+1-\delta$ elements of $\mathcal{F}$, there must be at least $q+1-\delta$ big $2n$-dimensional spaces in P through π.

At most δ of the $\frac{q^n-1}{q-1}$ different big $2n$-dimensional spaces through π contain less than $q+1$ elements of $\mathcal{F}$ (Corollary 4.1.25). Each of the at least $q+1-\delta$ elements of Π_2 spans together with π a big $2n$-dimensional space in P. Thus there are at least $q+1-2\delta \geq 2$ big $2n$-spaces in P through π which contain exactly $q+1$ elements of $\mathcal{F}$. We denote these $2n$-dimensional spaces by Π_1 and Π_2.

By the same arguments we find an additional $2n$-dimensional space Π_3 which contains $q+1$ elements of $\mathcal{F}$, and which intersects Π_1 and Π_2 in different elements of $\mathcal{F}$.

Thus that plane P of $\mathcal{L}$ contains a triangle Π_1, Π_2, Π_3, and each side of the triangle contains $q+1$ points of $\mathcal{L}$. Every other big $2n$-dimensional space in P intersects Π_1, Π_2 and Π_3 in elements of $\mathcal{F}$ (Lemma 4.1.31), thus a direct counting argument shows us that P contains $(q-1)^2+3(q-1)+3 = q^2+q+1$ lines of $\mathcal{L}$, where $(q-1)^2$ is the number of lines intersecting the side of the triangle in different points, $3(q-1)$ is the number of lines through a vertex different from the sides and 3 is the number of sides of the triangle. The number of elements of $\mathcal{F}$ in P is at most q^2+q+1 (by Lemma 4.1.14) and at least $q^2+q+1-\delta$ (by Corollary 4.1.25).

Now consider any line Ł of P with $q+1-x$ points ($x \geq 1$). Then $q(q+1-x)$ lines intersect Ł and thus there are xq lines skew to Ł. Every point not on Ł lies on x lines that do not intersect Ł. Thus there must exist a point not on Ł that lies on a line Ł$'$ disjoint to Ł with at least $\frac{(q^2+q+1-\delta-(q+1-x))x}{qx} > q-1$ points. By Lemma 4.1.31, Ł$'$ has q points.

As we have seen above, there are q lines of P skew to Ł$'$ and every point not on Ł$'$ lies on such a line. We may extend $\mathcal{L}$ by a point that lies on Ł$'$ and all lines skew to Ł$'$. Extending $\mathcal{L}$ stepwise by at most δ points, we obtain a $2-(q^2+q+1, q+1, 1)$ design, i.e. a projective plane of order q. □

Lemma 4.1.33 *Let $\mathcal{F}$ be a dual arc that satisfies the assumptions of Theorem 4.1.10. Let $\delta > 0$, then $\mathcal{F}$ is not maximal.*

Proof Since $\delta > 0$, we find a big $2n$-space which contains less than $q+1$ elements of $\mathcal{F}$ (Corollary 4.1.25). Every $(3n-1)$-dimensional space spanned by three elements of $\mathcal{F}$ through such a $2n$-space contains less than q^2+q+1 elements of $\mathcal{F}$. Let P be such a $(3n-1)$-space.

Select a $2n$-space Π in P that contains exactly q elements of $\mathcal{F}$. Such a space exists, because by Lemma 4.1.32, the linear space $\mathcal{L}$ is a projective plane with at most δ holes and such linear spaces contain lines with exactly q points.

Consider the $(3n-1)$-spaces through Π generated by three elements of $\mathcal{F}$. By Lemma 4.1.32, these $(3n-1)$-spaces define projective planes with holes. We will call a big $2n$-space Π' parallel to Π if it "goes through" the unique hole of Π in the corresponding projective plane defined by Lemma 4.1.32.

The $2n$-spaces parallel to Π partition the set $\mathcal{F}$. By Corollary 4.1.27, we know that every big $2n$-space lies in $\frac{q^{n-1}-1}{q-1}$ different $(3n-1)$-spaces spanned by three elements of $\mathcal{F}$. Thus there are exactly

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

$2n$-spaces parallel to Π, including Π itself.

Consider two big $2n$-spaces Π_1 and Π_2 parallel to Π. If $\Pi_2 \not\subset \langle \Pi, \Pi_1 \rangle$, then $\langle \Pi, \Pi_1, \Pi_2 \rangle$ is a $(4n-3)$-dimensional space (Property (4)). Since $2n < \dim \langle \Pi_1, \Pi_2 \rangle < \dim \langle \Pi, \Pi_1, \Pi_2 \rangle = 4n-3$, Property (4) implies that $\dim \langle \Pi_1, \Pi_2 \rangle = 3n-1$. Thus any two elements in the parallel class satisfy the conditions of Lemma 4.1.30 and Lemma 4.1.31, i.e. they lie in a $(3n-1)$-space.

Let q be odd. Choose any $2n$-space Π' parallel to Π which contains exactly q elements of $\mathcal{F}$. By a direct counting argument we find that at least $\frac{q^n-1}{q-1} - (\delta-1)$ of the $\frac{q^n-1}{q-1}$ elements in the parallel class have this property. Then by Lemma 4.1.28, the plane $\bar{\pi}'$ of Π' contains exactly one line of contact points. By Lemma 4.1.30, these lines must lie in the common intersection Ω of all $2n$-spaces parallel to Π. Thus Ω contains $\frac{q^n-1}{q-1} - (\delta-1)$ lines of contact points that share a common point s (Lemma 4.1.31). This proves that Ω is an n-dimensional space; it cannot be bigger by Lemma 4.1.22. Now look at any big $2n$-space Π'' parallel to Π containing $q+1-\delta_i$ elements of $\mathcal{F}$. By Lemma 4.1.30 and Lemma 4.1.31, the plane $\bar{\pi}''$ must share a line through s with every other $2n$-space parallel to Π. This line must lie in Ω since otherwise $\bar{\pi}''$ would need different lines for each $2n$-space. Thus Ω contains $\frac{q^n-1}{q-1}$ lines of contact points through s, i.e., it only contains contact points and we can extend $\mathcal{F}$ by Ω.

For q even, the situation is more complicated. We have always two lines of contact points and we must choose the correct one. Let Π_1 be a $2n$-space which contains exactly q elements of $\mathcal{F}$. By Lemma 4.1.30, the plane $\bar{\pi}_1$ of Π_1 must share a line of contact points with each $2n$-space parallel to Π_1. By the pigeon hole principle there are at least $\frac{1}{2}(\frac{q^n-1}{q-1}-\delta)$ different $2n$-spaces parallel to Π_1, which contain q elements of $\mathcal{F}$ and which intersect $\bar{\pi}_1$ in the same line $Ł_1$ of contact points.

Let Π_2 and Π_3 be two such spaces. Choose Π_2 and Π_3 such that $\dim(\Pi_1 \cap \Pi_2 \cap \Pi_3) = n$. For $n=2$, this is always the case since the intersection of three 4-spaces in a 5-space is at least a plane, and since Lemma 4.1.22 states that $\dim(\Pi_1 \cap \Pi_2 \cap \Pi_3) \leq 2$. For $n>2$, we can choose Π_2 and Π_3 such that $\dim \langle \Pi_1, \Pi_2, \Pi_3 \rangle = 4n-3$ and then we obtain $\dim(\Pi_1 \cap \Pi_2 \cap \Pi_3) = n$ by the dimension formula.

Let $Ł_2$ be the line $\bar{\pi}_2 \cap \Pi_1$. Consider the hyperbolic quadric with the two reguli $\mathcal{L}_1 = \{\bar{\pi}_2 \cap \Pi_1\} \cup \{\pi_1 \cap \Pi_2 \mid\mid \pi_1 \in \mathcal{F}, \pi_1 \subset \Pi_1\}$ and $\mathcal{L}_2 = \{\bar{\pi}_1 \cap \Pi_2\} \cup \{\pi_2 \cap \Pi_1 \mid\mid \pi_2 \in \mathcal{F}, \pi_2 \subset \Pi_2\}$ (see Lemma 4.1.31).

Then Π_3 contains the line $Ł_1 = \bar{\pi}_1 \cap \Pi_2$ of this hyperbolic quadric since Π_1 shares the same line of $\bar{\pi}_1$ with Π_2 and Π_3. Hence, Π_3 must contain a second line of this hyperbolic quadric. We prove this as follows. We know that $\dim(\Pi_1 \cap \Pi_2) = n+1$ and that $\dim(\Pi_1 \cap \Pi_2 \cap \Pi_3) = n$. The hyperbolic quadric $\mathcal{L}_1 \cup \mathcal{L}_2$ cannot lie in $\Pi_1 \cap \Pi_2 \cap \Pi_3$, or else every space $\pi_1 \in \mathcal{F}$ of Π_1 shares the same line with Π_2 and Π_3. Then some points of this line necessarily lie on three elements of $\mathcal{F}$ (false). So $\Pi_1 \cap \Pi_2 \cap \Pi_3$ intersects the solid containing the hyperbolic quadric $\mathcal{L}_1 \cup \mathcal{L}_2$ in a plane. This plane contains already one line $Ł_1$ of this hyperbolic quadric $\mathcal{L}_1 \cup \mathcal{L}_2$, so it contains a second line of $\mathcal{L}_1 \cup \mathcal{L}_2$.

But for each $\pi_1 \in \Pi_1$, we find that the line $\pi_1 \cap \Pi_2$ cannot lie in Π_3 since otherwise $\pi_1 \cap \Pi_2$ would meet q elements of $\mathcal{F}$ in Π_2 and q elements of $\mathcal{F}$ in Π_3, a contradiction. Thus $Ł_2 = \bar{\pi}_2 \cap \Pi_1$ must be the second line of the hyperbolic quadric in Π_3.

By symmetry, we also find that $\bar{\pi}_3$ intersects Π_1 and Π_2 in the same line.

Applying this argument for all the $\frac{1}{2}(\frac{q^n-1}{q-1}-\delta)+1$ different parallel spaces found in the first step, we obtain a space Ω in the common intersection which contains $\frac{1}{2}(\frac{q^n-1}{q-1}-\delta)+1$ different lines of contact points. This proves that Ω must have dimension n and we can copy the final steps of the case q odd to prove that Ω contains only contact points. □

Applying Lemma 4.1.33 precisely δ times, we find that $\mathcal{F}$ can be extended to a dual arc $\mathcal{F}'$ of size $\frac{q^{n+1}-1}{q-1}$. Even in the case q even, no $2n$-dimensional space contains exactly 2 elements of $\mathcal{F}'$. By Theorem 4.1.6, this implies that $\mathcal{F}'$ is the dual arc given by Construction 1.3.5. As we know from Theorem 4.1.2, in the case q even this dual arc can be extended by one extra element.

4.1.4 The case $d \geq 2$

Now we want to prove Theorem 4.1.9 for $d \geq 2$.

We start with a lemma concerning strongly regularity in the induced arcs.

Lemma 4.1.34 *If $\mathcal{F}$ is strongly regular, then $\mathcal{F}_\Omega = \{\Omega \cap \Omega' || \Omega' \in \mathcal{F} \setminus \{\Omega\}\}$ is strongly regular.*

Proof Let $\Omega_1, \ldots, \Omega_k, \Omega'_1, \ldots, \Omega'_{k'}$ be elements of $\mathcal{F}$. Then $\Omega_1 \cap \Omega, \ldots, \Omega_k \cap \Omega$ and $\Omega'_1 \cap \Omega, \ldots, \Omega'_{k'} \cap \Omega$ are elements of $\mathcal{F}_\Omega$. Since $\mathcal{F}$ is strongly regular, we have:

$$\begin{aligned}
\langle \Omega_1 \cap \Omega, \ldots, \Omega_k \cap \Omega \rangle \cap \bigcap_{i=1}^{k'} (\Omega'_i \cap \Omega) &= \langle \Omega_1, \ldots, \Omega_k \rangle \cap \Omega \cap \bigcap_{i=1}^{k'} (\Omega'_i \cap \Omega) \\
&= \langle \Omega_1, \ldots, \Omega_k \rangle \cap \Omega \cap \bigcap_{i=1}^{k'} \Omega'_i \\
&= \left\langle \Omega_1 \cap \Omega \cap \bigcap_{i=1}^{k'} \Omega'_i, \ldots, \Omega_k \cap \Omega \cap \bigcap_{i=1}^{k'} \Omega'_i \right\rangle \\
&= \left\langle (\Omega_1 \cap \Omega) \cap \bigcap_{i=1}^{k'} (\Omega'_i \cap \Omega), \ldots, (\Omega_k \cap \Omega) \cap \bigcap_{i=1}^{k'} (\Omega'_i \cap \Omega) \right\rangle .
\end{aligned}$$

That means that $\mathcal{F}_\Omega$ is strongly regular. □

Next we prove a lemma that shows that property (P) of Theorem 4.1.9 is no restriction if $q \geq n$.

Lemma 4.1.35 *Let $\mathcal{F}$ be a strongly regular generalized dual arc with $q \geq n$. Then $\mathcal{F}$ satisfies property (P).*

Proof We prove this by induction on the degree d. For $d = 1$, this statement is Lemma 4.1.12. Assume from now on that $d \geq 2$. We prove by induction on k that if we have elements $\Omega_1, \ldots, \Omega_k$ such that $\Omega_{i+1} \not\subset \langle \Omega_1, \ldots, \Omega_i \rangle$, then $\langle \Omega_1, \ldots, \Omega_k \rangle$ has dimension

$$\binom{n+d+1}{d+1} - \binom{n+d+1-k}{d+1} - 1.$$

For $k = 1$, there is nothing to prove. Assume now that $k > 1$. Since we assume that $\mathcal{F}$ is strongly regular, we have

$$\langle \Omega_1, \ldots, \Omega_{k-1} \rangle \cap \Omega_k = \langle \Omega_1 \cap \Omega_k, \ldots, \Omega_{k-1} \cap \Omega_k \rangle \ .$$

This is a span of elements of the degree $(d-1)$ strongly regular generalized dual arc

$$\mathcal{F}_{\Omega_k} = \{\Omega \cap \Omega_k | \Omega \in \mathcal{F} \backslash \{\Omega_k\}\},$$

and by induction, we know that

$$\dim \langle \Omega_1 \cap \Omega_k, \ldots, \Omega_{k-1} \cap \Omega_k \rangle = \binom{n+d}{d} - \binom{n+d-(k-1)}{d} - 1.$$

We also know by induction that

$$\dim \langle \Omega_1, \ldots, \Omega_{k-1} \rangle = \binom{n+d+1}{d+1} - \binom{n+d+2-k}{d+1} - 1.$$

Thus by the dimension formula

$$\dim \langle \Omega_1, \ldots, \Omega_k \rangle = \binom{n+d+1}{d+1} - \binom{n+d+1-k}{d+1} - 1.$$

□

We will prove Theorem 4.1.9 by induction on d. In Section 4.1.3, we handled the case $d = 1$. Now let $d \geq 2$. First we have to show that we can apply the induction hypothesis.

Fix an element Ω of $\mathcal{F}$. Consider the intersections $\Omega \cap \Omega_i$ with the other dual arc elements Ω_i of $\mathcal{F}$. By the definition of a generalized dual arc, $\mathcal{F}_\Omega = \{\Omega \cap \Omega_i \mid\mid \Omega_i \in \mathcal{F} \backslash \{\Omega\}\}$ is a generalized dual arc of degree $d - 1$.

The next series of lemmas will prove that $\mathcal{F}_\Omega$ satisfies all conditions of Theorem 4.1.9.

Lemma 4.1.36 *If $\mathcal{F}$ is strongly regular and satisfies property (P), then $\mathcal{F}_\Omega$ satisfies property (P).*

Proof We have to show that

$$\dim \langle \Omega_1 \cap \Omega, \ldots, \Omega_k \cap \Omega \rangle = \binom{n+d}{d} - \binom{n+d-i}{d} - 1,$$

for some i.

We distinguish between the following two cases.

Case 1: $\Omega \subseteq \langle \Omega_1, \ldots, \Omega_k \rangle$.

In this case, $\Omega = \langle \Omega_1 \cap \Omega, \ldots, \Omega_k \cap \Omega \rangle$, since $\mathcal{F}$ is strongly regular.

Case 2: $\Omega \not\subseteq \langle \Omega_1, \ldots, \Omega_k \rangle$.

By property (P), we know that

$$\dim \langle \Omega_1, \ldots, \Omega_k \rangle = \binom{n+d+1}{d+1} - \binom{n+d+1-i}{d+1} - 1,$$

for some i and

$$\dim \langle \Omega_1, \ldots, \Omega_k, \Omega \rangle = \binom{n+d+1}{d+1} - \binom{n+d+1-i-1}{d+1} - 1.$$

By the dimension formula, we have

$$\begin{aligned}
\dim \langle \Omega_1 \cap \Omega, \ldots, \Omega_k \cap \Omega \rangle &= \dim \langle \Omega_1, \ldots, \Omega_k \rangle \cap \Omega \\
&= \dim \Omega + \dim \langle \Omega_1, \ldots, \Omega_k \rangle - \dim \langle \Omega_1, \ldots, \Omega_k, \Omega \rangle \\
&= \left(\binom{n+d}{d} - 1 \right) + \left(\binom{n+d+1}{d+1} - \binom{n+d+1-i}{d+1} - 1 \right) \\
&\quad - \left(\binom{n+d+1}{d+1} - \binom{n+d+1-(i+1)}{d+1} - 1 \right) \\
&= \binom{n+d}{d} - \binom{n+d-i}{d} - 1.
\end{aligned}$$

Thus $\mathcal{F}_\Omega$ satisfies property (P). □

Lemma 4.1.37 *Let q be even and suppose that $\mathcal{F}$ is a strongly regular generalized dual arc, which satisfies property (P) and which has three elements $\Omega'_1, \Omega'_2, \Omega'_3$, with $\Omega'_3 \subset \langle \Omega'_1, \Omega'_2 \rangle$.*

Then $\mathcal{F}_\Omega$ has three elements $\Omega_1 \cap \Omega, \Omega_2 \cap \Omega, \Omega_3 \cap \Omega$, with $\Omega_3 \cap \Omega \subset \langle \Omega_1 \cap \Omega, \Omega_2 \cap \Omega \rangle$.

Proof We distinguish between the following two cases.

Case 1: Ω'_1, Ω'_2 and Ω'_3 are all different from Ω.

Since $\mathcal{F}$ is strongly regular, we find

$$\langle \Omega \cap \Omega'_1, \Omega \cap \Omega'_2, \Omega \cap \Omega'_3 \rangle = \langle \Omega'_1, \Omega'_2, \Omega'_3 \rangle \cap \Omega = \langle \Omega'_1, \Omega'_2 \rangle \cap \Omega = \langle \Omega \cap \Omega'_1, \Omega \cap \Omega'_2 \rangle \ .$$

Case 2: $\Omega = \Omega'_1$.

Choose $\Omega_1, \dots, \Omega_{d-1}$ different from $\Omega'_1, \Omega'_2, \Omega'_3$. Let $\Pi = \Omega_1 \cap \cdots \cap \Omega_{d-1}$, then

$$\mathcal{F}_\Pi = \{\Pi \cap \Omega' | \Omega' \in \mathcal{F} \backslash \{\Omega_1, \dots, \Omega_{d-1}\}\}$$

is a dual arc of degree one. Since $\mathcal{F}$ is strongly regular, we find $\Pi \cap \Omega'_3 \subset \langle \Pi \cap \Omega'_1, \Pi \cap \Omega'_2 \rangle$. Thus the dual arc in Π satisfies the assumptions of Section 4.1.3; i.e. it is a Veronesean. Especially, we have $\Omega''_1, \Omega''_2, \Omega''_3$ different from $\Omega = \Omega'_1$, with $\Pi \cap \Omega''_3 \subset \langle \Pi \cap \Omega''_1, \Pi \cap \Omega''_2 \rangle$. By property (P), we conclude that either

$$\dim\langle \Omega''_1, \Omega''_2, \Omega''_3 \rangle = \binom{n+d+1}{d+1} - \binom{n+d-1}{d+1} - 1,$$

or

$$\dim\langle \Omega''_1, \Omega''_2, \Omega''_3 \rangle = \binom{n+d+1}{d+1} - \binom{n+d-2}{d+1} - 1.$$

But $\dim(\Omega''_3 \cap \langle \Omega''_1, \Omega''_2 \rangle) \geq \dim(\Omega''_3 \cap \Pi \cap \langle \Omega''_1 \cap \Pi, \Omega''_2 \cap \Pi \rangle) = \dim(\Omega''_3 \cap \Pi) = n$. By the dimension formula we find that

$$\begin{aligned}\dim\langle \Omega''_1, \Omega''_2, \Omega''_3 \rangle &= \dim\langle \Omega''_1, \Omega''_2 \rangle + \dim \Omega''_3 - \dim(\langle \Omega''_1, \Omega''_2 \rangle \cap \Omega''_3) \\ &\leq \left(2\binom{n+d}{d} - \binom{n+d-1}{d-1} - 1\right) + \left(\binom{n+d}{d} - 1\right) - n \\ &< \binom{n+d+1}{d+1} - \binom{n+d-2}{d+1} - 1.\end{aligned}$$

Hence, we find that $\dim\langle \Omega''_1, \Omega''_2, \Omega''_3 \rangle = \dim\langle \Omega''_1, \Omega''_2 \rangle$. Since Ω is different from all of $\Omega''_1, \Omega''_2, \Omega''_3$, we are back in case 1. □

Now we know that we can apply induction; thus the dual arc $\mathcal{F}_\Omega$ induced in Ω satisfies the assumptions of Theorem 4.1.9.

We need an analog to Lemma 4.1.14.

Lemma 4.1.38 *Let $\mathcal{F}$ be a strongly regular generalized dual arc, that satisfies property (P). Then $\langle \Omega_0, \dots, \Omega_k \rangle$ contains at most $\frac{q^{k+1}-1}{q-1}$ elements of $\mathcal{F}$.*

Proof Choose elements $\Omega'_1, \ldots, \Omega'_{d-1} \in \mathcal{F}$, different from $\Omega_0, \ldots, \Omega_k$. Let $\Pi = \Omega'_1 \cap \cdots \cap \Omega'_{d-1}$. Investigate the dual arc $\mathcal{F}_\Pi$ of degree one in Π defined by

$$\mathcal{F}_\Pi = \{\Omega \cap \Pi \mid\mid \Omega \in \mathcal{F} \backslash \{\Omega'_1, \ldots, \Omega'_{d-1}\}\}.$$

By the induction hypothesis applied to Theorem 4.1.9, the dual arc $\mathcal{F}_{\Omega'_1}$ in Ω'_1 is Veronesean, and hence the "subarc" $\mathcal{F}_\Pi$ is Veronesean.

Since $\mathcal{F}$ is strongly regular, we have

$$\Pi \cap \langle \Omega_0, \ldots, \Omega_k \rangle = \langle \Omega_0 \cap \Pi, \ldots, \Omega_k \cap \Pi \rangle \ .$$

By Lemma 4.1.14, we know that $\langle \Omega_0 \cap \Pi, \ldots, \Omega_k \cap \Pi \rangle$ contains at most $\frac{q^{k+1}-1}{q-1}$ elements $\Omega \cap \Pi$ of $\mathcal{F}_\Pi$.

But $\Omega \subset \langle \Omega_0, \ldots, \Omega_k \rangle$ implies that $\Omega \cap \Pi \subset \langle \Omega_0 \cap \Pi, \ldots, \Omega_k \cap \Pi \rangle$, thus there are at most $\frac{q^{k+1}-1}{q-1}$ elements $\Omega \in \mathcal{F}$ that lie in $\langle \Omega_0, \ldots, \Omega_k \rangle$. □

For q even, $d = 2$, we must exclude the case that $\Omega \cap \Omega'$ is the nucleus in the dual arc $\mathcal{F}_\Omega$ induced in Ω. We do this as follows. Suppose that $\Omega' \cap \Omega''$ is not the nucleus in $\mathcal{F}_{\Omega''}$. Then there exist two other arc elements Ω_1, Ω_2 with $\dim \langle \Omega' \cap \Omega'', \Omega_1 \cap \Omega'', \Omega_2 \cap \Omega'' \rangle = 2n$. Since the dual arc is strongly regular, $\dim \langle \Omega', \Omega_1, \Omega_2 \rangle = \binom{n+3}{3} - \binom{n+1}{3} - 1$, and hence $\dim \langle \Omega' \cap \Omega, \Omega_1 \cap \Omega, \Omega_2 \cap \Omega \rangle = 2n$, a contradiction to the assumption that $\Omega \cap \Omega'$ is the nucleus of $\mathcal{F}_\Omega$.

Hence, the only possibility is that $\Omega' \cap \Omega$ is the nucleus in $\mathcal{F}_\Omega$, for all $\Omega \neq \Omega'$. In this case, we remove Ω' from the arc and we apply the remaining arguments to $\mathcal{F} \backslash \{\Omega'\}$.

Remark 4.1.39 *Note that in this case, none of the induced dual arcs contains a nucleus, so we have the extension result for q even with $d + \delta \leq \frac{q-6}{2}$.*

We will see at the end of the proof that an element $\Omega' \in \mathcal{F}$, with $\Omega' \cap \Omega$ being the nucleus in $\mathcal{F}_\Omega$ cannot exist.

For $q = 4^r$, we can prove this directly without using the strongly regular property.

Lemma 4.1.40 *Let $d = 2$, $q = 4^r$, and let $\mathcal{F} = \{\Omega_0, \ldots, \Omega_{\frac{q^{n+1}-1}{q-1} - \delta - 1}\}$ be a regular but not necessarily strongly regular generalized dual arc that satisfies the assumptions of Theorem 4.1.9.*

Then $\{\Omega_0 \cap \Omega_1, \ldots, \Omega_0 \cap \Omega_{\frac{q^{n+1}-1}{q-1} - \delta - 1}\}$ can be extended to a dual hyperoval $\mathcal{F}_0$ which is defined by a Veronesean. The nucleus of that dual hyperoval is not of the form $\Omega_0 \cap \Omega_i$, with $1 \leq i < \frac{q^{n+1}-1}{q-1} - \delta$.

Proof Assume that the nucleus of $\mathcal{F}_0$ has the form $\Omega_0 \cap \Omega_1$. We distinguish between two cases: Either $\Omega_0 \cap \Omega_1$ is also the nucleus of the hyperoval $\mathcal{F}_1$ in Ω_1 which contains the intersections $\Omega_1 \cap \Omega_i$ or not.

Case 1 : $\Omega_0 \cap \Omega_1$ is the nucleus of $\mathcal{F}_1$ in Ω_1.

In this case, we can choose coordinates $p^{(i)}_{i_0 i_1}$, $0 \leq i_0 \leq i_1 \leq n$, in Ω_i, $i = 0, 1$, such that the Veronesean defining $\mathcal{F}_i$ is in standard form. Since $\Omega_0 \cap \Omega_1$ is the nucleus of $\mathcal{F}_1$ and $\mathcal{F}_0$, we have $\Omega_0 \cap \Omega_1 = \left\langle p^{(j)}_{i_0 i_0} \mid\mid 0 \leq i_0 \leq n \right\rangle$, $j = 0, 1$. We can choose the coordinates in Ω_0 and Ω_1 in such a way that $p^{(0)}_{i_0 i_0} = p^{(1)}_{i_1 i_1}$.

We select the coordinates such that there exists a dual arc element $\Omega \in \mathcal{F}$ different from Ω_0 and Ω_1, which contains $p^{(0)}_{00} = p^{(1)}_{00}$.

Consider the at most q dual arc elements Ω', different from Ω and Ω_0, which contain a point of the form $xp^{(0)}_{00} + p^{(0)}_{01}$. Since we know that the dual arc in Ω_0 is described by a Veronesean in standard form, $xp^{(0)}_{00} + p^{(0)}_{01} \in \Omega'$ implies that

$$\Omega' \cap \Omega_0 = D_0((x, 1, 0, \ldots, 0)) = \left\langle xp^{(0)}_{0i} + p^{(0)}_{1i} \mid\mid i = 0, \ldots, n \right\rangle .$$

But this means that $\Omega' \cap \Omega_0 \cap \Omega_1 = xp^{(0)}_{00} + p^{(0)}_{11}$ since $\Omega_0 \cap \Omega_1$ is the nucleus of $\mathcal{F}_0$, and since the dual arc in Ω_1 is described by a Veronesean in standard form we determine

$$\Omega' \cap \Omega_1 = D_1((x, 1, 0, \ldots, 0)) = \left\langle xp^{(1)}_{0i} + p^{(1)}_{1i} \mid\mid i = 0, \ldots, n \right\rangle ,$$

especially $xp^{(1)}_{00} + p^{(1)}_{01} \in \Omega'$. (Note that we always identify p_{01} with p_{10}, see Construction 1.3.5.) Since $p^{(0)}_{00} = p^{(1)}_{00}$, this implies $p^{(0)}_{01} - p^{(1)}_{01} \in \Omega'$, i.e. we have found a point which lies in at least $q - \delta - 1$ dual arc elements. A contradiction, since $q - \delta - 1 > 2$. Remark that we have excluded case 1 for all $q = 2^r$, $r > 1$.

Case 2 : $\Omega_0 \cap \Omega_1$ is not the nucleus in Ω_1.

In this case, we can choose the coordinates as follows: $p^{(0)}_{ii} = p^{(1)}_{0i}$, for $i = 0, \ldots, n$, and

$$\Omega_0 \cap \Omega_1 = \left\langle p^{(0)}_{ii} \mid\mid i = 0, \ldots, n \right\rangle = \left\langle p^{(1)}_{0i} \mid\mid i = 0, \ldots, n \right\rangle \ .$$

Then the element $D_0((a_0, \ldots, a_n))$ of the Veronesean dual arc in Ω_0 shares a point with the element $D_1((a_0^2, \ldots, a_n^2))$ of the Veronesean dual arc in Ω_1. Thus these two n-spaces must lie in a common element Ω_i of the degree 2 dual arc.

Now look at the intersections of Ω_i with the plane $\pi = \left\langle p^{(0)}_{00} = p^{(1)}_{00}, p^{(0)}_{01}, p^{(1)}_{11} \right\rangle$. With the chosen coordinates, we have $\Omega_i \cap \Omega_0 = D_0((x, 1, 0, \ldots, 0))$ and

$\Omega_i \cap \Omega_1 = D_1((x^2, 1, 0, \ldots, 0))$ for some $x \in \mathbb{F}_q$. A straightforward calculation gives that $\Omega_i \cap \pi = \left\langle xp^{(0)}_{00} + p^{(0)}_{01}, x^4 p^{(1)}_{00} + p^{(1)}_{11} \right\rangle$.

The property that the Ω_i belong to a dual arc of degree 2 implies that no four of the lines $\Omega_i \cap \pi$ share a common point. But this is not true for $q = 4^d$, since $p^{(0)}_{01} + p^{(1)}_{11} \in \left\langle xp^{(0)}_{00} + p^{(0)}_{01}, x^4 p^{(1)}_{00} + p^{(1)}_{11} \right\rangle$, for $x \in \mathbb{F}_4$. □

Next we prove that for $d \geq 2$ the generalized dual arc defined by the Veronesean is maximal.

Theorem 4.1.41 *Let $d \geq 2$, then the strongly regular generalized dual arc $\mathcal{F}$ of degree d defined by Construction 1.3.5 is maximal.*

Proof Let $\{\Omega_1, \ldots, \Omega_{\frac{q^{n+1}-1}{q-1}}\}$ be the generalized dual arc defined by Construction 1.3.5.

Assume that the dual arc can be extended by an element Ω'. Then for each i, the elements $\Omega_i \cap \Omega_j$, $j \neq i$, form $\frac{q^{n+1}-1}{q-1} - 1$ elements of a Veronesean dual arc $\mathcal{F}_i$ of degree $d-1$ in Ω_i. For $d \neq 2$ or q odd, this dual arc has an unique extension element E_i and the extended dual arc is a Veronesean dual arc $\mathcal{F}_i$. For $d = 2$ and q even, there are two extension elements (one belongs to the Veronesean dual arc and the other is the nucleus of this Veronesean dual arc). By the arguments preceding Lemma 4.1.40, $\Omega' \cap \Omega$ is either always or never the nucleus in $\mathcal{F}_\Omega$.

Suppose that $d = 2$, q even, and that $\Omega' \cap \Omega$ is always the nucleus of the induced Veronesean dual arc $\mathcal{F}_\Omega$ in Ω. For $\Omega_x = \{\theta(x, x_1, x_2) \mid\mid x_1, x_2 \in \mathbf{PG}(n, q)\}$, we have $\Omega' \cap \Omega_x = \{\theta(x, y, y) \mid\mid y \in \mathbf{PG}(n, q)\}$. Thus Ω' contains all points of the form p_{ijj}, i.e. Ω' has at least rank $(n+1)^2$, a contradiction with the fact that arc elements should have rank $\binom{n+1}{2}$.

Now we may treat the case that $\Omega' \cap \Omega$ is never the nucleus of $\mathcal{F}_\Omega$. This includes also the case q odd or $d > 2$, in which cases the condition is trivial since the dual arc $\mathcal{F}_\Omega$ has no nucleus.

Then a straightforward calculation gives that the extension element E_i of the space $\Omega_i = \langle \theta(p_i, x_1, \ldots, x_d) \mid\mid x_1, \ldots, x_d \in \mathbf{PG}(n, q) \rangle$ is the space

$$E_i = \langle \theta(p_i, p_i, x_2, \ldots, x_d) \mid\mid x_2, \ldots, x_d \in \mathbf{PG}(n, q) \rangle \enspace .$$

Especially, if we set $p_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, we get $E_i = \langle p_{iii_2 \cdots i_d} \rangle$, where i denotes the position of the 1. This means that Ω' contains all points $p_{i_0 \cdots i_d}$, with at least two indices being the same. This proves that Ω' has at least dimension

$$\binom{n+d+1}{d+1} - 1 - \binom{n+1}{d+1} > \binom{n+d+1}{d+1} - 1 - \binom{n+d}{d+1} = \binom{n+d}{d} - 1,$$

in contradiction to the fact that Ω' extends the dual arc $\mathcal{F}$ and therefore has dimension $\binom{n+d}{d} - 1$. □

Now we may assume by induction that Theorem 4.1.9 is true for $d-1$. Let Ω_0 and Ω_1 be two elements of the dual arc. Let $\Pi_{01} = \Omega_0 \cap \Omega_1$. The $\frac{q^{n+1}-1}{q-1} - \delta - 2$ other elements of the dual arc intersect Π_{01} in a regular dual arc of type $(n_2, \ldots, n_d)$. By the induction hypothesis, this strongly regular dual arc can be extended to a dual arc $\mathcal{F}_{01}$ of size $\frac{q^{n+1}-1}{q-1}$. The intersections of Ω_0 with the other elements of the dual arc form a strongly regular dual arc of size $\frac{q^{n+1}-1}{q-1} - \delta - 1$. By the induction hypothesis, this dual arc can be extended to a dual arc $\mathcal{F}_0$ of size $\frac{q^{n+1}-1}{q-1}$ in Ω_0. The elements of $\mathcal{F}_0$ different from Π_{01} intersect Π_{01} in $\frac{q^{n+1}-1}{q-1} - 1$ elements of $\mathcal{F}_{01}$. Let $\hat{E}_0^{(1)}$ be the remaining element of $\mathcal{F}_{01}$.

By symmetry, the intersections of Ω_1 with the other dual arc elements define a dual arc $\mathcal{F}_1$ and a remaining element $\hat{E}_1^{(0)}$ of $\mathcal{F}_{01}$.

Lemma 4.1.42 *For any two spaces Ω_0 and Ω_1, we have $\hat{E}_0^{(1)} \neq \hat{E}_1^{(0)}$.*

Proof Assume the contrary.

Step 1: Coordinates in Π_{01}.

By the induction hypothesis, we know that $\mathcal{F}_{01}$ comes from a Veronesean $\mathcal{V}_{01}$ of degree $d-2$. Choose the coordinates $e^{(01)}_{i_0,\ldots,i_{d-2}}$ $(0 \le i_0 \le \cdots \le i_{d-2} \le n)$ in such a way that $\mathcal{V}_{01}$ is in standard form and

$$\hat{E}_0^{(1)} = \hat{E}_1^{(0)} = D_{01}((1,0,\ldots,0)) = \left\langle e^{(01)}_{0,i_1,\ldots,i_{d-2}} \mid\mid 0 \le i_1 \le \cdots \le i_{d-2} \le n \right\rangle$$

where D_{01} is the map from $\mathbf{PG}(n,q)$ to $\mathcal{V}_{01}$ described by Construction 1.

Step 2: Coordinates in Ω_0 and Ω_1.

In Ω_0, choose coordinates $e^{(0)}_{i_0,\ldots,i_{d-1}}$ in such a way that $\mathcal{F}_0$ comes from a Veronesean $\mathcal{V}_0$ in standard form. We may choose in addition the coordinates such that

$$\Pi_{01} = D_0((1,0,\ldots,0)) = \left\langle e^{(0)}_{0,i_1,\ldots,i_{d-1}} \mid\mid 0 \le i_1 \le \cdots \le i_{d-1} \le n \right\rangle$$

where D_0 is the map from $\mathbf{PG}(n,q)$ to $\mathcal{F}_0$, and in Π_{01}, we have

$$e^{(0)}_{0,i_1,\ldots,i_{d-1}} = e^{(01)}_{i_1,\ldots,i_{d-1}}.$$

Similarly, we obtain coordinates $e^{(1)}_{i_0,\ldots,i_{d-1}}$ in Ω_1 with $e^{(1)}_{0,i_1,\ldots,i_{d-1}} = e^{(01)}_{i_1,\ldots,i_{d-1}}$.

Step 3: Finding $q-\delta-2$ elements with a common intersection.

Now consider the elements $D_x = D_{01}((x, 1, 0, \ldots, 0))$ $(x \in \mathbb{F}_q)$ of $\mathcal{F}_{01}$. At least $q - \delta - 2$ of these elements are an intersection $\Omega_0 \cap \Omega_1 \cap \Omega_x$ of three elements of the dual arc.

Now Ω_x intersects Ω_0 in $D_0((x, 1, 0, \ldots, 0))$. Especially, Ω_x contains the point $xe^{(0)}_{0n\ldots n} + e^{(0)}_{1n\ldots n}$ in Ω_0. By symmetry, Ω_x contains the point $xe^{(1)}_{0n\ldots n} + e^{(1)}_{1n\ldots n}$ of Ω_1.

We have chosen the coordinates such that $e^{(0)}_{0n\ldots n} = e^{(01)}_{n\ldots n} = e^{(1)}_{0n\ldots n}$, thus Ω_x contains the point $e^{(0)}_{1n\ldots n} - e^{(1)}_{1n\ldots n}$. But now we have a point which lies in the intersection of at least $q - \delta - 2 > d + 1$ elements of the generalized dual arc of degree d. This is a contradiction. □

By Lemma 4.1.42, there exists an element $E^{(1)}_0$ of $\mathcal{F}_0$ which intersects Π_{01} in $\hat{E}^{(0)}_1$. We will call $E^{(1)}_0$ the extension element of Ω_0 with respect to Ω_1. If the dual arc is given by Construction 1.3.5, the extension element of Ω_0 is independent of Ω_1. We will now prove this for $d \geq 3$. We will see the case $d = 2$ as a consequence of Theorem 4.1.9. This will force us in Step 4 of the proof of Theorem 4.1.9 to include a special argument for $d = 2$.

Lemma 4.1.43 *Let $d \geq 3$ and let $\Omega_0, \Omega_1, \Omega_2 \in \mathcal{F}$. Then $E^{(1)}_0 = E^{(2)}_0$.*

Proof Let $\Pi_{012} = \Omega_0 \cap \Omega_1 \cap \Omega_2$. By induction, we know that the other $\frac{q^{n+1}-1}{q-1} - \delta - 3$ elements of $\mathcal{F}$ induce a generalized dual arc $\mathcal{F}_{012}$ in Π_{012} that comes from Construction 1.3.5. From the $\frac{q^{n+1}-1}{q-1}$ elements of $\mathcal{F}_{012}$ we obtain $\frac{q^{n+1}-1}{q-1} - 1$ as intersections of the form $\Pi_{012} \cap \pi$, with $\pi \in \mathcal{F}_{12}$ where $\mathcal{F}_{12}$ is the dual arc of size $\frac{q^{n+1}-1}{q-1}$ induced in $\Pi_{12} = \Omega_1 \cap \Omega_2$. Let E_{012} be the remaining element of $\mathcal{F}_{012}$.

By Lemma 4.1.42 (applied to the dual arc $\mathcal{F}_1$ in Ω_1 with the arc elements $\Omega_0 \cap \Omega_1$ and $\Omega_2 \cap \Omega_1$), we find that $E_{012} = E_{01} \cap \Pi_{012}$ for some element E_{01} of the dual arc $\mathcal{F}_{01}$ in $\Pi_{01} = \Omega_0 \cap \Omega_1$. By the choice of E_{012} we know that E_{01} cannot be of the form $\Pi_{01} \cap \pi$, with $\pi \in \mathcal{F}_1$ where $\mathcal{F}_1$ is the dual arc induced in Ω_1. Thus by Lemma 4.1.42, we get $E_{01} = \Pi_{01} \cap E^{(1)}_0$.

By symmetry, we define the arc element E_{02} in $\mathcal{F}_{02}$ with $E_{02} = \Pi_{02} \cap E^{(2)}_0$.

But $E_{012} = E_{01} \cap \Pi_{012} = E_{02} \cap \Pi_{012}$ and thus $E^{(1)}_0 \cap \Pi_{012} = E^{(2)}_0 \cap \Pi_{012}$. This is only possible if $E^{(1)}_0 = E^{(2)}_0$. □

We are now ready to prove the main theorem.

Proof of Theorem 4.1.9:

Step 1: Selection of $\Omega_0, \ldots, \Omega_n$.

We choose Ω_0 arbitrarily. In Ω_0, the other elements of the generalized dual arc induce a generalized dual arc of size $\frac{q^{n+1}-1}{q-1} - \delta - 1$. By the induction hypothesis, in Ω_0 we can extend this generalized dual arc to a generalized dual arc of size $\frac{q^{n+1}-1}{q-1}$. (Note that even in the case $d = 2$, q even, we can be sure not to have a nucleus, see the remarks before Lemma 4.1.40.) Let $\hat{E}_0, \ldots, \hat{E}_\delta$ be the extension elements.

By the pigeon hole principle, there exist at least $\left(\frac{q^{n+1}-1}{q-1} - \delta - 1\right)/(\delta + 1) > 2\frac{q^n-1}{q-1}$ elements $\Omega_i \in \mathcal{F}$ for which $E_0^{(i)}$ is the same extension element E_0. (Actually, we proved in Lemma 4.1.43 that for $d \geq 3$, all Ω_i induce the same extension element in Ω_0, and we will see later in this proof that this is also true for $d = 2$.) Let $\hat{\mathcal{F}}$ be the set of at least $\left(\frac{q^{n+1}-1}{q-1} - \delta - 1\right)/(\delta+1)$ elements in $\mathcal{F}$ which define the same extension element E_0 in Ω_0.

Now choose $\Omega_1 \in \hat{\mathcal{F}}$. If we have already chosen the elements $\Omega_0, \ldots, \Omega_i$ ($i < n$), we choose Ω_{i+1} in $\hat{\mathcal{F}}$ such that

1. $\Omega_{i+1} \not\subseteq \langle \Omega_0, \ldots, \Omega_i \rangle$ and
2. $\Omega_{i+1} \cap \Omega_0 \not\subseteq \langle E_0, \Omega_1 \cap \Omega_0, \ldots, \Omega_i \cap \Omega_0 \rangle$.

This is possible, because by Lemma 4.1.38, there are at most $2\frac{q^{i+1}-1}{q-1}$ elements in $\mathcal{F}$ which do not satisfy one of these two conditions.

By property (P), we find that $\dim \langle \Omega_0, \ldots, \Omega_i \rangle = \binom{n+d+1}{d+1} - \binom{n+d+1-i-1}{d+1} - 1$. In particular $\Omega_0, \ldots, \Omega_n$ span the whole space.

Step 2: Ω_i is spanned by $\Omega_i \cap \Omega_j$ and $E_i^{(0)}$.

In what follows, we denote the induced arc in Ω_i by $\mathcal{F}_i$, $\Pi_{ij} = \Omega_i \cap \Omega_j$ and the induced arc in Π_{ij} is $\mathcal{F}_{ij}$. By induction, the induced arc can be extended to a generalized dual arc given by Construction 1.3.5; we will call these generalized dual arcs Veronesean dual arcs.

The Veronesean dual arc $\mathcal{F}_0$ in Ω_0 defines in each arc element Ω_i a contact space. Let $\hat{E}_{0i}^{(0)}$ be the contact space in Π_{0i}. Then $\hat{E}_{0i}^{(0)}$ is an element of the induced Veronesean arc in Π_{0i}. By Lemma 4.1.42, $\hat{E}_{0i}^{(0)}$ is the intersection of the extension element $E_i^{(0)}$ of $\mathcal{F}_i$ in Ω_i with respect to Ω_0 and Π_{0i}.

Since the dual arc $\mathcal{F}_0$ is Veronesean and Ω_0 is spanned by the arc elements $E_0^{(i)} = E_0$, $\Pi_{0i} = \Omega_i \cap \Omega_0$ ($1 \leq i \leq n$), we find that the induced dual arc in Π_{0i} is spanned by the elements $\Omega_j \cap \Pi_{0i}$ ($1 \leq j \leq n$, $j \neq i$), $E_0 \cap \Pi_{0i}$ and $\hat{E}_{0i}^{(0)} = E_i^{(0)} \cap \Pi_{0i}$.

Since the induced arc in Ω_i is Veronesean and its element Π_{0i} is spanned by $\Omega_j \cap \Pi_{0i}$ ($1 \leq j \leq n$, $j \neq i$), $E_0 \cap \Pi_{0i}$ and $\hat{E}_{0i}^{(0)} = E_i^{(0)} \cap \Pi_{0i}$, we know that Ω_i is spanned by the corresponding arc elements $\Omega_j \cap \Omega_i$ ($1 \leq j \leq n$, $j \neq i$), $\Omega_0 \cap \Omega_i$ and $E_i^{(0)}$.

Step 3: Choosing a basis in Ω_i.

By induction, we know that in Ω_i we find a Veronesean dual arc. We want to choose a basis $p_{i_1,\ldots,i_d}^{(i)}$ in Ω_i such that $\Omega_i \cap \Omega_j = D_i((0, \ldots, 0, 1, 0, \ldots, 0))$

where the 1 stands on position j and $E_i^{(0)} = D_i((0,\ldots,0,1,0,\ldots,0))$ with the 1 at position i. This is possible since Ω_i is spanned by $\Omega_j \cap \Omega_i$ ($0 \leq j \leq n$, $j \neq i$) and $E_i^{(0)}$.

To fix the coordinates we must still choose the all one vector. To that end, let Ω' be an element of $\mathcal{F}$ such that $\Omega' \cap \Omega_0$ lies in general position with respect to $\Omega_i \cap \Omega_0$ ($1 \leq i \leq n$) and E_0. Then we can choose the coordinates in Ω_0 such that $\Omega' \cap \Omega_0 = D_0((1,\ldots,1))$. With this choice the Veronesean dual arc in Ω_0 is uniquely determined.

Since $\Omega' \cap \Omega_0$ lies in general position with respect to $\Omega_i \cap \Omega_0 = \Pi_{0i}$ ($1 \leq i \leq n$) and E_0, $\Omega' \cap \Pi_{0i}$ lies in general position with respect to $\Omega_j \cap \Pi_{0i}$ ($1 \leq i \leq n$, $j \neq i$), $E_0 \cap \Pi_{01}$, $E_i^{(0)} \cap \Pi_{0i}$. Thus $\Omega' \cap \Omega_i$ lies in general position with respect to $\Omega_j \cap \Omega_i$ ($0 \leq j \leq n$, $j \neq i$) and $E_i^{(0)}$ for all i.

We choose the coordinates in Ω_i such that $\Omega' \cap \Omega_i = D_i((1,\ldots,1))$. Now that the coordinates are fixed, we have no remaining degree of freedom.

By the choice of the coordinates we have for each $\Omega \in \mathcal{F}$ that $\Omega \cap \Omega_0 = D_0((a_0,\ldots,a_n))$ implies that $\Omega \cap \Omega_i = D_i((a_0,\ldots,a_n))$.

Step 4: Determining the basis of $\mathbf{PG}(\binom{n+d+1}{n} - 1, q)$.

Now we define a basis in $\mathbf{PG}(\binom{n+d+1}{n} - 1, q)$ by $p_{i_0,\ldots,i_d} = p^{(i_0)}_{i_1,\ldots,i_d}$.

It remains to be proven that for each permutation σ we have $p_{i_0,\ldots,i_d} = p_{i_{\sigma(0)},\ldots,i_{\sigma(d)}}$. If $\sigma(0) = 0$ this follows by induction.

We only have to prove that $p_{i_0,i_1,\ldots,i_d} = p_{i_1,i_0,i_2,\ldots,i_d}$. For $i_0 = 0$ or $i_1 = 0$, this is a direct consequence of Lemma 4.1.42, in fact

$$P^{(i_0)}_{i_1,\ldots,i_d} = P^{(i_1)}_{i_0,i_2,\ldots,i_d}$$

is just a symbolic reformulation of Lemma 4.1.42.

If $i_0 \neq 0$ and $i_1 \neq 0$, we must prove that $E^{(0)}_{i_0} = E^{(i_1)}_{i_0}$ and $E^{(0)}_{i_1} = E^{(i_0)}_{i_1}$ to apply Lemma 4.1.42.

For $d \geq 3$, we have done this in Lemma 4.1.43. For $d = 2$ we argue as follows.

Let Ω be an element of $\mathcal{F}$ with the following properties.

1. $\Omega \cap \Omega_0 \not\subseteq \langle \Omega_0 \cap \Omega_{i_0}, \Omega_0 \cap \Omega_{i_1} \rangle$.

2. $\Omega \cap \Omega_{i_0} \not\subseteq \langle \Omega_{i_0} \cap \Omega_0, \Omega_{i_0} \cap \Omega_{i_1} \rangle$.

3. $\Omega \cap \Omega_{i_1} \not\subseteq \langle \Omega_{i_1} \cap \Omega_0, \Omega_{i_1} \cap \Omega_{i_0} \rangle$.

There are at least $\frac{q^{n+1}-1}{q-1} - \delta - 3q$ elements Ω that satisfy these conditions.

Since we are considering an arc of degree two, we have $\dim(\Omega \cap \Omega_{i_0} \cap \Omega_{i_1}) = 0$.

Let $\Omega \cap \Omega_0 = D_0((a_0, \ldots, a_n))$ be the coordinate representation of $\Omega \cap \Omega_0$. Then $\Omega \cap \Omega_0 \cap \Omega_{i_0} = D_{0i_0}((a_0, \ldots, a_n))$ and hence $\Omega \cap \Omega_{i_0} = D_{i_0}((a_0, \ldots, a_n))$. Especially $\sum_{i=0}^n a_i p_{ii_1}^{(i_0)}$ is a point in Ω.

By symmetry, we also have $\sum_{i=0}^n a_i p_{ii_0}^{(i_1)} \in \Omega$, and since $\dim(\Omega \cap \Omega_{i_0} \cap \Omega_{i_1}) = 0$ we get

$$\sum_{i=0}^n a_i p_{ii_1}^{(i_0)} = \sum_{i=0}^n a_i p_{ii_0}^{(i_1)}.$$

This equation holds for at least $\frac{q^{n+1}-1}{q-1} - \delta - 3q$ different vectors $(a_0, \ldots, a_n)$. Thus $p_{ji_0}^{(i_1)} = p_{ji_1}^{(i_0)}$, i.e. the coordinates in Ω_{i_0} fit with the coordinates in Ω_{i_1}.

Now we have defined the points $p_{i_0,i_1,\ldots,i_d}$. By definition, each Ω_i is spanned by the points of the form $p_{i,i_1,\ldots,i_d}$, thus the points span the whole space, since $\Omega_0, \ldots, \Omega_n$ span the space $\mathbf{PG}(\binom{n+d+1}{n} - 1, q)$.

Step 5: Check the formulas.

Now take any element Ω of $\mathcal{F}$ different from $\Omega_0, \ldots, \Omega_n$. By Step 3 the induced dual arc in Ω_0 is in standard form. By Construction 1.3.5 this means that $\Omega^{(0)} = \Omega \cap \Omega_0$ has the form

$$\Omega^{(0)} = \left\langle \sum_{i_0=0}^n a_{i_0} p_{i_0 0 i_2 \ldots i_d} \mid\mid 0 \leq i_2, \ldots, i_d \leq n \right\rangle$$

for some $a_{i_0} \in \mathbb{F}_q$.

Now we can compute the intersection $\Omega^{(0,i)} = \Omega^{(0)} \cap \Omega_i = \Omega \cap \Omega_0 \cap \Omega_i$. By definition (Step 2), we have $\Omega_i = \langle p_{ii_1 \ldots i_d} \mid\mid 0 \leq i_1, \ldots, i_d \leq n \rangle$ and thus

$$\Omega^{(0,i)} = \left\langle \sum_{i_0=0}^n a_{i_0} p_{i_0 0 i i_3 \ldots i_d} \mid\mid 0 \leq i_3, \ldots, i_d \leq n \right\rangle .$$

(Note that in the special case $d = 2$, $\Omega^{(0,i)} = \sum_{i_0=0}^n a_{i_0} p_{i_0 0 i}$)

But by Step 3 we know that the Veronesean $\mathcal{V}_i$ in Ω_i is in standard form. Thus $\Omega^{(i)} = \Omega \cap \Omega_i$ must be the unique element of the Veronesean dual arc $\mathcal{F}_i$ which intersects Ω_0 in $\Omega^{(0,i)}$. This implies that

$$\Omega^{(i)} = \left\langle \sum_{i_0=0}^n a_{i_0} p_{i_0 i \; i_2 \ldots i_d} \mid\mid 0 \leq i_2, \ldots, i_d \leq n \right\rangle .$$

By Definition, we have $\Omega^{(i)} \subset \Omega$ for all i, thus

$$\begin{aligned}\left\langle \Omega^{(0)}, \ldots, \Omega^{(n)} \right\rangle &\subset \Omega \\ \left\langle \bigcup_{i=0}^{n} \{ \sum_{i_0=0}^{n} a_{i_0} p_{i_0 i i_2 \ldots i_d} \mid\mid 0 \leq i_2, \ldots, i_d \leq n \} \right\rangle &\subset \Omega \\ \left\langle \sum_{i_0=0}^{n} a_{i_0} p_{i_0 i_1 i_2 \ldots i_d} \mid\mid 0 \leq i_1, \ldots, i_d \leq n \right\rangle &\subset \Omega.\end{aligned}$$

But the space on the left hand side is exactly the space defined by Construction 1.3.5. Since $\dim \left\langle \Omega^{(0)}, \ldots, \Omega^{(n)} \right\rangle = \binom{n+d}{d} = \dim \Omega$ and $\left\langle \Omega^{(0)}, \ldots, \Omega^{(n)} \right\rangle \subseteq \Omega$ this proves that $\Omega = \left\langle \Omega^{(0)}, \ldots, \Omega^{(n)} \right\rangle$ as desired. □

4.1.5 Open problems

- We are not aware of any regular dual arc that is not strongly regular. Do such examples exist?

- For $d = 1$, we have examples of non-Veronesean dual arcs in which no $2n$-space contains more than two elements. Do such examples exist for $d > 1$?

- We proved property (P) for $q \geq n$. Do there exist counterexamples for property (P) for $q < n$?

4.2 Characterizations of the finite quadric Veroneseans by intersection numbers

In this section we provide two characterizations of the finite quadric Veronesean by intersection numbers. The second will be proved by reduction to the first one. Very small values of q are excluded. In some cases we found counterexamples, while in other cases we were not able to prove the statement.

For $n = 2$, Theorem 4.1.6 is a generalization of Theorem 25.2.14 of [28] to q even, and allows to generalize Theorem 25.3.14 of [28] to q even, and so there arises

Theorem 4.2.1 *([67]) If $\mathcal{K}$ is a set of k points of $\mathbf{PG}(5, q)$, $q \neq 2, 4$, which satisfies the following conditions*

(i) $|\Pi_4 \cap \mathcal{K}| = 1,\ q + 1,\ 2q + 1$ for every hyperplane Π_4 of $\mathbf{PG}(5, q)$ and there exists a hyperplane Π_4 for which $|\Pi_4 \cap \mathcal{K}| = 2q + 1$.

(ii) Any plane of $\mathbf{PG}(5,q)$ *with four points in* $\mathcal{K}$ *has at least* $q+1$ *points in* $\mathcal{K}$.

Then $\mathcal{K}$ *is the point set of a Veronesean* $\mathcal{V}_2^4$.

A theorem by Zanella [76] gives an upper bound for the intersection of k-dimensional subspaces with the quadric Veronese variety, so for the intersections $\Pi_k \cap \mathcal{V}_n$.

Theorem 4.2.2 *([76]) Consider the Veronese variety defined by the mapping*

$$\zeta : \mathbf{PG}(n,q) \to \mathbf{PG}(\frac{n(n+3)}{2}, q),$$

$$(x_0, x_1, \cdots, x_n) \to (x_0^2, x_1^2, \cdots, x_{n-1}x_n).$$

If k, a *are natural numbers such that* $k+1 \leq \frac{(a+3)(a+2)}{2}$*, then the intersections* $\Pi_k \cap \mathcal{V}_n$ *contain at most*

$$\frac{q^{a+1}-1}{q-1} + q^{k-\frac{(a+2)(a+1)}{2}}$$

points.

Applying this for small dimensions yields the upper bounds $q+1$, $q+2$, $2q+1$ and q^2+q+1 for $k=2$, $k=3$, $k=4$ and $k=5$ respectively.

A result of Thas and Van Maldeghem [66] characterizes Veronese varieties in terms of ovals.

Theorem 4.2.3 *Let* X *be a set of points in* $\Pi := \mathbf{PG}(M,q)$, $M > 2$*, spanning* Π*, and let* $\mathcal{P}$ *be a collection of planes such that for any* $\pi \in \mathcal{P}$*, the intersection* $X \cap \pi$ *is an oval in* π*. For* $\pi \in \mathcal{P}$ *and* $x \in X \cap \pi$*, we denote by* $T_x(\pi)$ *the tangent line to* $X \cap \pi$ *at* x *in* π*. We assume the following three properties.*

(U) Any two points $x, y \in X$ *lie in a unique member of* $\mathcal{P}$ *which we denote by* $[x,y]$.

(NE) If $\pi_1, \pi_2 \in \mathcal{P}$ *and* $\pi_1 \cap \pi_2$ *is non-empty then* $\pi_1 \cap \pi_2 \subset X$.

(TP) If $x \in X$ *and* $\pi \in \mathcal{P}$ *with* $x \notin \pi$*, then each of the lines* $T_x([x,y])$, $y \in X \cap \pi$*, is contained in a plane of* Π*, denoted by* $T(x,\pi)$.

Then there exists a natural number $n \geq 2$ *(called the index of* X*), a projective space* $\Pi' := \mathbf{PG}(\frac{n(n+3)}{2}, q)$ *containing* Π*, a subspace* R *of* Π' *skew to* Π*, and a quadric Veronesean* $\mathcal{V}_n$ *of index* n *in* Π'*, with* $R \cap \mathcal{V}_n = \emptyset$*, such that* X *is the (bijective) projection of* $\mathcal{V}_n$ *from* R *onto* Π*. The subspace* R *can be empty, in which case* X *is projectively equivalent to* $\mathcal{V}_n$.

4.2.1 First characterization

We want to use the following set of conditions to characterize the quadric Veronesean. Consider a set $\mathcal{K}$ of $\frac{q^{n+1}-1}{q-1}$ points spanning $\mathbf{PG}(\frac{n(n+3)}{2}, q)$, with $n \geq 2$, such that the following conditions are satisfied.

(P) If a plane intersects $\mathcal{K}$ in more than three points then it contains exactly $q+1$ points of $\mathcal{K}$. Furthermore, any two points p_1, p_2 of $\mathcal{K}$ are contained in a plane containing $q+1$ points of $\mathcal{K}$.

(S) If a 3-space Π_3 intersects $\mathcal{K}$ in more than 4 points then there are four points of $\mathcal{K}$ contained in a plane of Π_3. In particular, by (P), this implies that if $|\Pi_3 \cap \mathcal{K}| > 4$, then $|\Pi_3 \cap \mathcal{K}| \geq q+1$.

(V) If a 5-space Π_5 intersects $\mathcal{K}$ in more than $2q+2$ points then it intersects $\mathcal{K}$ in exactly q^2+q+1 points.

Definition 4.2.4 *Planes intersecting $\mathcal{K}$ in $q+1$ points and 5-spaces intersecting $\mathcal{K}$ in q^2+q+1 points will be called* big planes *and* big 5-spaces *respectively.*

Assume $q \geq 5$ in the following.

We will prove the following main theorem.

Theorem 4.2.5 *If $q \geq 5$, then the set $\mathcal{K}$ is the point set of the Veronese variety of all quadrics of $\mathbf{PG}(n, q)$.*

Remark 4.2.6 *A counterexample for $q = 2$, $n > 2$, to the previous theorem is given by removing one point of a Veronese variety and replacing it by a point in the projective space which corresponds with a matrix of maximal rank, using the correspondence of Theorem 1.3.4.*

A counterexample for $q = 3$, $n = 2$, is given by the point set formed by the points of an elliptic quadric $\mathcal{E}$ lying in a space $\Pi_3 \subset \mathbf{PG}(5, 3)$ and 3 points on a line $L \subset \mathbf{PG}(5, 3)$ which does not intersect Π_3.

First of all we have to prove that these conditions are well-chosen, meaning the object we want to characterize satisfies them.

Theorem 4.2.7 *The Conditions (P), (S) and (V) above hold for the Veronesean $\mathcal{V}_n^{2^n}$.*

Proof For Condition (P), we cannot use Lemma 25.3.1 of [28] directly, since we don't know a priori that every plane containing more than three points of $\mathcal{V}_n^{2^n}$ is contained in a 5-space intersecting $\mathcal{K}$ in a $\mathcal{V}_2^4$ but a slight adaptation of the argument works. Suppose that the plane π contains at least four distinct points q_1, q_2, q_3, q_4 of $\mathcal{V}_n^{2^n}$. By Corollary 1 of Theorem 25.1.9 of [28], the points q_i, q_j, with $i \neq j$, are contained in a unique conic of $\mathcal{V}_n^{2^n}$. Let C', in the plane π', be the conic defined by q_1 and q_2, and let C'', in the plane π'', be the conic defined by q_2 and q_3. Suppose that $C' \neq C''$. By Theorem 4.2.2 the conic planes π' and π'' generate a 4-space Π_4 such that $|\Pi_4 \cap \mathcal{K}| \leq 2q+1$. But besides the $2q+1$ points in $C' \cup C''$, the point q_4 would also be contained in this 4-space, a contradiction. Hence $|\pi \cap \mathcal{K}| \geq q+1$ and by Theorem 4.2.2, $|\pi \cap \mathcal{K}| = q+1$. Conditions (S) and (V) can be proved using a coordinatization and checking the different possibilities for the position of the inverse images of the points in $\mathbf{PG}(n,q)$. □

We prove some upper bounds on the number of points of $\mathcal{K}$ contained in low-dimensional spaces.

Lemma 4.2.8 *If $n > 2$, every 4-space contains at most $2q+2$ points of $\mathcal{K}$.*

Proof Let Π be a 4-space. By Condition (V), it follows directly that $|\Pi \cap \mathcal{K}| \leq q^2+q+1$ and clearly $|\Pi \cap \mathcal{K}| = q^2+q+1$ also yields a contradiction.

Suppose that $2q+2 < |\Pi \cap \mathcal{K}| < q^2+q+1$. Again by Condition (V), every 5-space through Π contains exactly q^2+q+1 points of $\mathcal{K}$. The number of 5-spaces through a fixed 4-space in $\mathbf{PG}(\frac{n(n+3)}{2}, q)$ is equal to $\frac{q^{\frac{n(n+3)}{2}-4}-1}{q-1}$. Hence, we get at least

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

points in $\mathcal{K}$, a contradiction for $n > 2$. □

Lemma 4.2.9 *Any line L meets $\mathcal{K}$ in at most 2 points. Hence, a plane π with $\pi \cap \mathcal{K}| = q+1$ intersects $\mathcal{K}$ in an oval.*

Proof First suppose that $|L \cap \mathcal{K}| = 3$. If $n > 2$, then consider 3 planes π_1, π_2, π_3 through L containing more than 3 points of $\mathcal{K}$ and hence by Condition (P) $q+1$ points of $\mathcal{K}$. Then $\dim\langle \pi_1, \pi_2, \pi_3 \rangle \leq 4$. For $q > 5$, this yields a contradiction by Lemma 4.2.8. If $q = 5$, then consider a 3-space Π_3 through L containing at least 9 points of $\mathcal{K}$ inside a big 5-space Π_5. But then considering all 4-spaces through Π_3 inside Π_5, by Lemma 4.2.8, we get at most $6 \cdot 3 + 9 = 27$ points in $\Pi_5 \cap \mathcal{K}$, a contradiction.

If $n = 2$ then we get the following equation for the number α of planes through L which contain exactly $q+1$ points of $\mathcal{K}$:

$$\alpha(q-2) + 3 = q^2 + q + 1.$$

This yields a contradiction if $q \geq 5$. Next, suppose that $|L \cap \mathcal{K}| = x$, with $3 < x < q+1$. Consider all planes through L. Then clearly, we get too many points for our set $\mathcal{K}$, a contradiction. Finally, if $|L \cap \mathcal{K}| = q+1$, we also get a contradiction as planes can contain at most $q+1$ points of $\mathcal{K}$. □

The previous lemma allows us for $n = 2$ to prove the same upper bound as in Lemma 4.2.8.

Lemma 4.2.10 *Every 4-space intersects $\mathcal{K}$ in at most $2q+2$ points. Hence, every 3-space contained in a big 5-space intersects $\mathcal{K}$ in at most $q+3$ points.*

Proof For $n > 2$ this is Lemma 4.2.8. Next let $n = 2$.

Suppose there exists a 3-space Π_3 which contains two planes π_1 and π_2 which intersect $\mathcal{K}$ in ovals $\mathcal{O}_1$ and $\mathcal{O}_2$ respectively which have two points p_1, p_2 of $\mathcal{K}$ in common. Consider two points r_1 and r_2, different from p_1 and p_2, which lie on $\mathcal{O}_1$ and $\mathcal{O}_2$ respectively. Then there are at most 4 planes through the line $\langle r_1, r_2 \rangle$ which are not $(q+1)$-planes, namely the planes containing either the point p_1 or p_2 or those which intersect π_i in a tangent line to $\mathcal{O}_i$ at r_i for $i = 1$ or $i = 2$.

Hence, we get at least

$$2 + (q-3)(q-1) + 4 = q^2 - 4q + 9$$

points in $\Pi_3 \cap \mathcal{K}$.

The bound above is already sufficient for the remainder of the proof if $q > 5$. But since we now know there is a point p in $\Pi_3 \cap \mathcal{K}$ not contained in $\mathcal{O}_1 \cup \mathcal{O}_2$ we can consider all planes through the line $\langle p, p_1 \rangle$ inside Π_3. In this case, we get at most three exceptions, namely the plane containing p_2 and those which intersect π_i in a tangent line to $\mathcal{O}_i$ at p_1. Hence we get at least

$$2 + 3 + (q-2)(q-1) = q^2 - 3q + 7$$

points in $\Pi_3 \cap \mathcal{K}$.

If one would carry out this argument a bit more carefully one can get up to $q^2 + 1$ points in $\Pi_3 \cap \mathcal{K}$, and hence this intersection is an ovoid. However this does not shorten the reasonings made in the remainder of this proof.

Hence if there are three such 3-spaces we distinguish the following cases.

Case (i): Any two of them only intersect in a line. Then the union of the 3-spaces contains at least $3(q^2 - 3q + 7) - 3 \cdot 2$ points of $\mathcal{K}$, a contradiction since $q \geq 5$.

Case (ii): There are two of them which intersect in a plane. Then we get a 4-space Π_4 containing at least $2(q^2 - 3q + 7) - (q+1) = 2q^2 - 7q + 13$ points of $\mathcal{K}$. Consider a point p in $\mathcal{K}$ not contained in Π_4. Through p and any point

r in $\Pi_4 \cap \mathcal{K}$ there passes an oval of $\mathcal{K}$ by Condition (P). If none of these ovals have two points of $\mathcal{K}$ in common, we get too many points, a contradiction. If two of these ovals have two points of $\mathcal{K}$ in common then the 3-space spanned by these two ovals contains at least $q^2 - 3q + 7$ points of $\mathcal{K}$. Hence, we get at least

$$2q^2 - 7q + 13 + q^2 - 3q + 7 - (q + 1)$$

points in $\mathcal{K}$, a contradiction since $q \geq 5$.

If there are exactly one or two such 3-spaces we consider a 4-space Π_4 containing such a 3-space Π_3 and a point p in $\mathcal{K}$ not contained in Π_4. Through p and each point r in $\Pi_4 \cap \mathcal{K}$ there passes an oval by Condition (P). For each such point r we choose exactly one such oval. If we have two ovals of $\mathcal{K}$ through p and a point r of $\mathcal{K}$ in Π_4, then these two ovals define a 3-space Π_3' containing at least $q^2 - 3q + 7$ points of $\mathcal{K}$, and then the line rp lies in at most $q + 1$ planes of the solid containing an oval of $\Pi_3' \cap \mathcal{K}$. If there are more than $q + 1$ ovals through p sharing two points of $\mathcal{K}$, then there would be another 3-space Π_3'' through p sharing at least $q^2 - 3q + 7$ points with $\mathcal{K}$. Now Π_3' and Π_3'' are different from the solid Π_3 in Π_4 sharing at least $q^2 - 3q + 7$ points of $\mathcal{K}$. But this contradicts the assumption that there are no three such solids. Hence we clearly get too many points in $\mathcal{K}$, a contradiction.

Now consider a 4-space Π_4 which intersects $\mathcal{K}$ in x points. Consider a point p of $\mathcal{K}$ not in Π_4. By Condition (P) through every 2 points of $\mathcal{K}$ there passes an oval of $\mathcal{K}$. Consider all ovals through p and a point r of $\Pi_4 \cap \mathcal{K}$. Any two of these ovals can intersect in at most one point. Since any oval through p intersects $\Pi_4 \cap \mathcal{K}$ in at most 2 points, we get at least $\frac{x}{2}$ ovals, which all contain $q - 2$ points in $\Pi_5 \cap \mathcal{K}$ different from p and the x points in $\Pi_4 \cap \mathcal{K}$. Hence we get the following equation,

$$\frac{x}{2}(q - 2) + x + 1 \leq q^2 + q + 1.$$

This yields $x \leq 2q + 2$.

Consider a 3-space Π_3 in a big 5-space Π_5 which intersects $\mathcal{K}$ in $q + 3 + y$ points. Since all 4-spaces through Π_3 inside Π_5 intersect $\mathcal{K}$ in at most $2q + 2$ points we get the following inequality

$$(q + 1)(q - 1 - y) + q + 3 + y \geq q^2 + q + 1.$$

This implies $y \leq 0$. □

Now we are able to lower the bound of Lemma 4.2.10.

Lemma 4.2.11 *(i) Every 4-space Π_4 intersecting $\mathcal{K}$ in more than $q + 1$ points contains a plane which intersects $\mathcal{K}$ in an oval.*

(ii) Every 4-space Π_4 contains at most $2q+1$ points of $\mathcal{K}$.

Proof (i) Suppose that $|\Pi_4 \cap \mathcal{K}| > q+1$. Since $q \geq 5$, by a result on arcs, namely Theorem 27.6.3 of [28], there are 5 points which are contained in a 3-space. By Condition (S), it follows that there are 4 of them which are contained in a plane π. Hence, by Lemma 4.2.9, π intersects $\mathcal{K}$ in an oval.

(ii) Suppose that $|\Pi_4 \cap \mathcal{K}| = 2q+2$. Consider a plane π in Π_4 intersecting $\mathcal{K}$ in an oval $\mathcal{O}$. Such a plane always exists by (i).

Consider 2 points a and b in $\Pi_4 \cap \mathcal{K}$, but not in π, such that $\langle a, b\rangle \cap \pi = \emptyset$. Note that this is always possible, since at most $q+3$ points of $\mathcal{K}$ are contained in a 3-space by Lemma 4.2.10.

Consider a third point c in $(\Pi_4 \cap \mathcal{K}) \setminus \pi$, and let p be the intersection point of π and $\pi' = \langle a,\ b,\ c\rangle$.

We distinguish the following cases.

Case (i): $p \in \mathcal{O}$.

Since π' contains at least 4 points of $\mathcal{K}$ it contains at least $q+1$ points of $\mathcal{K}$ by Condition (P). The planes π and π' both intersect $\mathcal{K}$ in an oval, $\mathcal{O}$ and $\mathcal{O}'$. Denote the remaining point in $\Pi_4 \cap \mathcal{K}$ by p'. Consider a plane π'' spanned by p' and two points a' and b' belonging to $\mathcal{O} \setminus \{p\}$. The planes π' and π'' intersect in a point r. If r belongs to $\mathcal{K}$ then π'' contains at least 4 and hence, by Condition (P), $q+1$ points of $\mathcal{K}$. If r does not belong to $\mathcal{K}$ we may assume it is not the nucleus of $\mathcal{O}'$, otherwise we can restart the reasoning with two other points of $\mathcal{O}$. Then the 3-space spanned by π'' and a bisecant to $\mathcal{O}'$ through r, but not through p, contains at least 5 and hence by Condition (S) at least $q+1$ points. Since $q \geq 5$, in both cases we get more than $2q+2$ points in $\Pi_4 \cap \mathcal{K}$, a contradiction by Lemma 4.2.10.

Case (ii): $p \notin \mathcal{O}$.

(ii.A) First of all, we assume that not all points in $\Pi_4 \cap \mathcal{K}$ are contained in $\pi \cup \pi'$. Since not all points in $\Pi_4 \cap \mathcal{K}$ are contained in $\pi \cup \pi'$, we may assume that p is not the nucleus of $\mathcal{O}$. Indeed, if p would be the nucleus of $\mathcal{O}$ we consider a point c' of $\Pi_4 \cap \mathcal{K}$ not in $\pi' \cup \pi$ and the plane $\pi'' = \langle a,\ b,\ c'\rangle$ which then intersects π in a point p', with p' not the nucleus of $\mathcal{O}$. So in that case we continue the reasonings with π'' instead of π'. Consider two secants of $\mathcal{O}$ through p, say L and L'. The 3-spaces $\langle \pi', L\rangle$ and $\langle \pi', L'\rangle$ both contain at least 5 points of $\mathcal{K}$, hence they both contain a plane intersecting $\mathcal{K}$ in an oval. These planes have to coincide, since also π intersects $\mathcal{K}$ in an oval, otherwise we get too many points in $\Pi_4 \cap \mathcal{K}$. Hence, the plane π' intersects $\mathcal{K}$ in an oval $\mathcal{O}'$. This yields a contradiction with the assumption at the beginning of this paragraph. Note that as a byproduct we proved that if a 4-space contains at least $q+5$ points of $\mathcal{K}$, it contains two planes which intersect $\mathcal{K}$ in an oval, hence $|\Pi_4 \cap \mathcal{K}| \geq 2q+1$. Indeed we only used 4 points a, b, c and c' in $\mathcal{K}$ but not in π to find the second oval $\mathcal{O}'$. Furthermore, these ovals can have at most one point in common, otherwise they only span a 3-space, but a 3-space inside Π_5 intersects $\mathcal{K}$ in at most $q+3$ points by Lemma 4.2.10.

(ii.B) Next, we may suppose that $\Pi_4 \cap \mathcal{K}$ is a union of two ovals $\mathcal{O}$ and $\mathcal{O}'$ contained in planes π and π' which intersect in a point p.

(ii.B.1) If p is the nucleus of neither $\mathcal{O}$ nor of $\mathcal{O}'$, then consider a secant T of $\mathcal{O}$ and a secant T' of $\mathcal{O}'$ through p. The plane spanned by T and T' contains 4 and hence $q+1$ points of $\mathcal{K}$, and so $|\Pi_4 \cap \mathcal{K}| > 2q+2$, a contradiction.

(ii.B.2) If p is the nucleus of $\mathcal{O}$, but not the nucleus of $\mathcal{O}'$, then consider a 5-space Π_5 containing Π_4 which intersects $\mathcal{K}$ in q^2+q+1 elements. Since p is not the nucleus of $\mathcal{O}'$, there is a secant L' of $\mathcal{O}'$ through p. Hence, by Lemma 4.2.10, the 3-space Π_3 spanned by $\mathcal{O}$ and L' contains exactly $q+3$ elements of $\mathcal{K}$. It follows that exactly one of the 4-spaces containing Π_3 in Π_5 intersects $\mathcal{K}$ in $2q+1$ points, while all the other 4-spaces through Π_3 in Π_5 contain $2q+2$ points of $\mathcal{K}$.

By the foregoing there is a 4-space $\Pi_4' \neq \Pi_4$ containing Π_3 inside Π_5 which intersects $\mathcal{K}$ in $2q+2$ elements on two ovals $\mathcal{O}$ and $\mathcal{O}''$, where the planes of $\mathcal{O}'$ and $\mathcal{O}''$ intersect in L'. Hence the 3-space Π_3' spanned by $\mathcal{O}'$ and $\mathcal{O}''$ contains at least $2q$ elements of $\mathcal{K}$. Consider all 4-spaces through Π_3' inside Π_5. By Lemma 4.2.10 we get at most $2q+2(q+1) = 4q+2$ points in $\Pi_5 \cap \mathcal{K}$, a contradiction since $q \geq 5$.

(ii.B.3) Finally, if p is the nucleus of both $\mathcal{O}$ and $\mathcal{O}'$, then consider a 3-space Π_3 spanned by $\mathcal{O}$ and a tangent L to $\mathcal{O}'$ through p. Consider a big 5-space Π_5 through Π_4. Consider all 4-spaces through Π_3 inside Π_5. No 4-space through Π_3 inside Π_5 different from Π_4 can intersect $\mathcal{K}$ in $2q+2$ points as well. Indeed, by Case (i) and the previous subcases of Case (ii) such a 4-space Π_4' again has to intersect $\mathcal{K}$ in two ovals $\mathcal{O}$ and $\mathcal{O}''$, contained in planes π and π'' respectively. The planes π' and π'' have to intersect in the tangent line L, and p again has to be the nucleus of both the ovals $\mathcal{O}$ and $\mathcal{O}''$.

But then the 3-space Π_3'' spanned by $\mathcal{O}'$ and $\mathcal{O}''$ contains at least $2q+1$ points of $\mathcal{K}$. Consider all 4-spaces through Π_3'' inside Π_5. Then by Lemma 4.2.10 $|\Pi \cap \mathcal{K}| \leq 2q+1+q+1 = 3q+2$, a contradiction since $q \geq 5$.

Consider now all 4-spaces through Π_3 inside Π_5. Exactly one of them intersects $\mathcal{K}$ in $2q+2$ points by the previous and all the others intersect $\mathcal{K}$ in at most $2q+1$ points. Hence, by an easy inspection, there is exactly one 4-space through Π_3 in Π_5 containing exactly $2q$ points of $\mathcal{K}$, but this yields a contradiction by the remark made at the end of Case (ii.A). □

Remark. A 4-space intersecting $\mathcal{K}$ in $2q+1$ points will be called a *big 4-space.*

Lemma 4.2.12 *(i) Inside a big 5-space* Π_5 *all 3-spaces contain at most* $q+2$ *points. Furthermore, all 4-spaces inside* Π_5 *through a 3-space intersecting*

$\mathcal{K}$ in $q+2$ points are big ones.

(ii) A big 4-space Π_4 contained in a big 5-space Π_5 intersects $\mathcal{K}$ in two ovals $\mathcal{O}_1, \mathcal{O}_2$ with $\mathcal{O}_1 \cap \mathcal{O}_2 = \{P\},\ P \in \mathcal{K}$.

Proof (i) Suppose a 3-space Π_3 of the big 5-space Π_5 intersects $\mathcal{K}$ in $q+2+x$ points, with $x \geq 0$. Then considering all 4-spaces in Π_5 through Π_3, we get at most $(2q+1-(q+2+x))(q+1)+q+2+x = q^2+q+1-xq$ points in $\Pi_5 \cap \mathcal{K}$ by Lemma 4.2.11, a contradiction if $x > 0$. The second part follows directly if $x = 0$.

(ii) By (i) of Lemma 4.2.11 there is a plane π in Π_4 which intersects $\mathcal{K}$ in an oval. We claim we can find a second plane in Π_4 which intersects $\mathcal{K}$ in an oval. Take 3 points contained in $\Pi_4 \cap \mathcal{K}$ not lying in π. These points span a plane π'. The space $\langle \pi, \pi' \rangle$ is a 4-space, otherwise we get a 3-space intersecting $\mathcal{K}$ in more than $q+2$ points, contradicting (i).

If π' contains exactly 3 points of $\mathcal{K}$ then consider all 3-spaces through π' in Π_4. If none of them contains at least 5 points of $\mathcal{K}$ we get at most $q+1+3 = q+4$ points in $\Pi_4 \cap \mathcal{K}$, a contradiction. So there is a 3-space Π_3 through π' in Π_4 containing more than 4 points of $\mathcal{K}$, hence by Conditions (P) and (S) we find a plane π'' containing $q+1$ points of $\mathcal{K}$ inside Π_3. Clearly π and π'' are different since π and π' span a 4-space.

If the two different planes π and π'' which intersect $\mathcal{K}$ in an oval intersect in a point, then we are done by Lemma 4.2.11. Suppose that π and π'' intersect in a line. Then the 3-space $\Pi_3' = \langle \pi, \pi'' \rangle$ intersects $\mathcal{K}$ in more than $q+2$ points, contradicting (i). □

Lemma 4.2.13 *Every 4-space contained in a big 5-space Π_5 intersects $\mathcal{K}$ in 1, $q+1$ or $2q+1$ points and each such big 5-space contains at least one 4-space intersecting $\mathcal{K}$ in exactly $2q+1$ points. Hence, each big 5-space intersects $\mathcal{K}$ in a $\mathcal{V}_2^4$.*

Proof Denote the number of points belonging to $\mathcal{K}$ contained in a 4-space $\Pi_i \subset \Pi_5$ by x_i; here Π_5 is a big 5-space. In the following sum and all the others below, i runs over all 4-spaces Π_i contained in Π_5. We have

$$\sum_i (x_i - 1)(x_i - (q+1))(x_i - (2q+1)) = 0. \tag{4.1}$$

Indeed, by a standard counting technique counting in two different ways respectively the number of pairs (p, Π) in Π_5, where $p \in \mathcal{K}$ and Π is a 4-space in Π_5, the number of triples $(p_1, p_2, \Pi), p_1 \neq p_2 \in \Pi \cap \mathcal{K}$ and Π a 4-space in

Π_5, and the quadruples $(p_1, p_2, p_3, \Pi), p_i \in \Pi \cap \mathcal{K}$, where the points p_i are all distinct and Π is a 4-space in Π_5 yields

$$\sum_i x_i = \frac{(q^2+q+1)\,(q^5-1)}{q-1}, \tag{4.2}$$

$$\sum_i x_i(x_i-1) = \frac{(q^2+q+1)\,(q^2+q)\,(q^4-1)}{q-1}, \tag{4.3}$$

$$\sum_i x_i(x_i-1)(x_i-2) = \frac{(q^2+q+1)\,(q^2+q)\,(q^2+q-1)\,(q^3-1)}{q-1}. \tag{4.4}$$

Now Equations (4.2), (4.3) and (4.4) together lead to Equation (4.1).

If a 4-space Π_4 inside a big 5-space contains more than $q+1$ points of $\mathcal{K}$, then it is a big one. Indeed, by Lemma 4.2.11 there is a plane in Π_4 intersecting $\mathcal{K}$ in an oval. Hence we can find a 3-space in Π_4 which intersects $\mathcal{K}$ in $q+2$ points. The claim now follows from (i) of Lemma 4.2.12.

Suppose $|\Pi_4 \cap \mathcal{K}| = x$, $\Pi_4 \subset \Pi_5$, with $4 \leq x < q+1$. Let Π_3 be a 3-space containing 4 points p_1, p_2, p_3, p_4 in $\Pi_4 \cap \mathcal{K}$. Hence, by Condition (S), $|\Pi_3 \cap \mathcal{K}| = 4$. Consider all 4-spaces through Π_3 inside Π_5. If there are less than 4 big ones among them, we get less than

$$3(2q-3) + (q-2)(q-3) + 4 = q^2 + q + 1$$

points in $\Pi_5 \cap \mathcal{K}$, a contradiction.

By (ii) of Lemma 4.2.12, in each of the at least 4 big 4-spaces inside Π_5 containing Π_3 the points p_1, p_2, p_3, p_4 are contained in 2 ovals. Hence either there is an oval containing 3 of them, which yields a contradiction, or there is a pair p_i, p_j contained in two different ovals. But the latter yields a contradiction by (i) of Lemma 4.2.12.

Suppose now that $|\Pi_4 \cap \mathcal{K}| = 3$. Consider a 3-space Π_3 in Π_4 containing the 3 points p_1, p_2, p_3 of $\Pi_4 \cap \mathcal{K}$ and all 4-spaces inside Π_5 containing Π_3. By the previous arguments these intersect $\mathcal{K}$ in 3, $q+1$ or $2q+1$ points. Denote the number of them intersecting $\mathcal{K}$ in $q+1$ and $2q+1$ points by α and β respectively. This yields the following equation

$$\alpha(q-2) + \beta(2q-2) + 3 = q^2 + q + 1.$$

We deduce that α is a multiple of $q-1$. If $\alpha = q-1$, then we get at most $(q-1)(q-2) + 2q + 1$ points in $\Pi_5 \cap \mathcal{K}$, a contradiction.

Hence, we find that $\alpha = 0$ and $\beta = \frac{q+2}{2}$. This already yields a contradiction if q is odd. As $q > 2$, the points p_1, p_2, p_3 are contained in 2 ovals in each of the at least 3 different big 4-spaces of Π_5 containing Π_3 by (ii) of Lemma 4.2.12. This yields a contradiction.

Finally, suppose that $|\Pi_4 \cap \mathcal{K}| = 2$. Consider a 3-space Π_3 in Π_4 containing the 2 points p_1, p_2 of $\Pi_4 \cap \mathcal{K}$ and all 4-spaces inside Π_5 containing Π_3. By the previous these all intersect $\mathcal{K}$ in 2, $q+1$ or $2q+1$ points. Denote the number of them intersecting $\mathcal{K}$ in $q+1$ and $2q+1$ points by α and β respectively. This yields the following equation,

$$\alpha(q-1) + \beta(2q-1) + 2 = q^2 + q + 1.$$

This yields that $\beta - 1$ is a multiple of $q-1$. If $\beta = 1$, we get at most $(q-1)(q-1) + 2q + 1 = q^2 + 2$ points of $\mathcal{K}$ in Π_5, a contradiction. If $\beta = q$, we get exactly $2q^2 - q + 2$ points in $\Pi_5 \cap \mathcal{K}$, also a contradiction.

In the previous paragraphs we proved that if a 4-space contains at least 2 points of $\mathcal{K}$, then it contains at least $q+1$ points of $\mathcal{K}$. By (i) of Lemma 4.2.12 and (ii) of Lemma 4.2.11 the only possibilities in this case are $q+1$ and $2q+1$. By Equation (4.1), this implies that there are no 4-spaces which have an empty intersection with $\mathcal{K}$.

Hence, every 4-space contained in Π_5 intersects $\mathcal{K}$ in 1, $q+1$ or $2q+1$ points.

We prove there is a 4-space contained in Π_5 which intersects $\mathcal{K}$ in $2q+1$ points. If this is not the case, then consider a 3-space in Π_5 containing $x > 1$ points of $\mathcal{K}$. We get the following equality:

$$(q+1)(q+1-x) + x = q^2 + q + 1,$$

hence $x = 1$, a contradiction.

Hence by Theorem 4.2.1, Π_5 intersects $\mathcal{K}$ in a Veronese variety $\mathcal{V}_2^4$. □

Theorem 4.2.14 *The set $\mathcal{K}$ is a Veronese variety $\mathcal{V}_n^{2^n}$.*

Proof We check the conditions of Theorem 4.2.3. The set $\mathcal{P}$ consists of all planes intersecting $\mathcal{K}$ in an oval.

Any two points of $\mathcal{K}$ are contained in at least one oval of $\mathcal{K}$ by Condition (P) and Lemma 4.2.9. If two points p_1, p_2 are contained in two ovals, namely $\mathcal{O}_1$ in the plane π_1 and $\mathcal{O}_2$ in the plane π_2, then these ovals span a 3-space Π_3 containing too many points of $\mathcal{K}$, a contradiction. Indeed, consider a point r on the intersection line L of π_1 and π_2 which is not the nucleus of $\mathcal{O}_1$ neither of $\mathcal{O}_2$ and two bisecants L_1 and L_2 through r to $\mathcal{O}_1$ and $\mathcal{O}_2$ respectively. Then the plane spanned by L_1 and L_2 contains at least 4 points of $\mathcal{K}$ and hence by Condition (P) $q+1$ points of $\mathcal{K}$. In this way we get at least $2q + q - 3 = 3q - 3 \geq 2q + 2$ (since $q \geq 5$) points in $\Pi_3 \cap \mathcal{K}$, a contradiction by Lemma 4.2.10. Hence, Property (U) is proved.

To prove Property (NE), consider two planes π_1 and π_2 which intersect $\mathcal{K}$ in an oval. If $\pi_1 \cap \pi_2$ is a point then the property follows directly from Lemma 4.2.11. If $\pi_1 \cap \pi_2$ is a line then we get a 3-space Π_3 containing at least and so exactly $2q+1$ points. But then there are 4-spaces through Π_3 containing more than $2q+1$ points of $\mathcal{K}$, a contradiction.

For Property (TP), take a point p not contained in a plane π which intersects $\mathcal{K}$ in an oval $\mathcal{O}_1$. Consider two points r and s on $\mathcal{O}_1$ and the ovals $\mathcal{O}_2$ and $\mathcal{O}_3$ which are uniquely determined by p and r, and p and s respectively. The point set of the ovals $\mathcal{O}_1$, $\mathcal{O}_2$ and $\mathcal{O}_3$ are contained in a 5-space Π_5 intersecting $\mathcal{K}$ in more than $2q+2$ points. Hence, by Lemma 4.2.13 $\Pi_5 \cap \mathcal{K}$ is a Veronesean $\mathcal{V}_2^4$. Take an arbitrary point t on $\mathcal{O}_1$ and consider the oval determined by p and t. Since $\Pi_5 \cap \mathcal{K}$ is a $\mathcal{V}_2^4$, this oval is contained in Π_5. For each of these ovals there is a tangent at p to these ovals. By Lemma 25.4.2 of [28] the union of these tangents forms a plane. □

4.2.2 Second characterization

In this section, we show that for $n > 2$, we can replace the set of conditions of Section 2 by the following set of conditions. Furthermore, we provide a counterexample for the case $n = 2$.

Consider a set $\mathcal{K}$ of $\frac{q^{n+1}-1}{q-1}$ points spanning $\mathbf{PG}(\frac{n(n+3)}{2}, q)$, with $n > 2$, such that

(P') If π is a plane then the intersection $\pi \cap \mathcal{K}$ contains at most $q+1$ points of $\mathcal{K}$.

(S') If a 3-space Π_3 intersects $\mathcal{K}$ in more than 4 points, then $|\Pi_3 \cap \mathcal{K}| \geq q+1$ and $\Pi_3 \cap \mathcal{K}$ is not a $(q+1)$-arc.

(V') If a 5-space Π_5 intersects $\mathcal{K}$ in more than $2q+2$ points then it intersects $\mathcal{K}$ in exactly q^2+q+1 points. Furthermore, any two points p_1, p_2 of $\mathcal{K}$ are contained in a 5-space containing q^2+q+1 points of $\mathcal{K}$.

Lemma 4.2.15 *Every 4-space contains at most $2q+2$ points of $\mathcal{K}$. Hence, a 3-space contained in a big 5-space contains at most $q+3$ points of $\mathcal{K}$.*

Proof Exactly the same as the proof of Lemma 4.2.10 using Condition (V'), since we only used there that part of Condition (V). □

Lemma 4.2.16 *For $n > 2$, $q > 7$, if a plane π contains at least 4 points of $\mathcal{K}$, then it contains exactly $q+1$ points of $\mathcal{K}$.*

Proof First suppose that $4 < |\pi \cap \mathcal{K}| < q+1$. Then all 3-spaces through π contain at least $q+1$ points. This yields at least $\frac{q^{\frac{n(n+3)}{2}-2}-1}{q-1}$ points for the set $\mathcal{K}$, a contradiction since $n > 2$.

Next, suppose that $|\pi \cap \mathcal{K}| = 4$. Consider points a, b and c of $\mathcal{K}$ such that $\langle \pi, a\rangle$, $\langle \pi, b\rangle$ and $\langle \pi, c\rangle$ are three different 3-spaces. By Condition (S') each of these three 3-spaces intersects $\mathcal{K}$ in at least $q+1$ points. Then the space $\langle \pi,\, a,\, b,\, c\rangle$ contains at least $3(q-3)+4$ points of $\mathcal{K}$. Hence, since $q > 7$, by Lemma 4.2.15 and Condition (V') it is a big 5-space Π_5.

By Lemma 4.2.15, a 3-space Π_3 in Π_5 contains at most $q+3$ points of $\mathcal{K}$.

From the previous paragraph it follows that we get the following inequality for the number x of 3-spaces Π_3^i through π inside the big 5-space Π_5 containing at least $q+1$ points of $\mathcal{K}$.

$$x(q-1) + 4 \geq q^2 + q + 1.$$

Hence we get $x \geq q + 2 - \frac{1}{q-1}$, this implies $x \geq q+2$ if $q > 2$.

Now consider a 3-space Π_3'' containing π and at least $q+1$ points of $\mathcal{K}$ which is not contained in Π_5 and consider also the 6-space $\Pi_6 = \langle \Pi_5, \Pi_3''\rangle$. Take one fixed 3-space Π_3^1 and consider the 5-spaces $\langle \Pi_3^1, \Pi_3'', \Pi_3^i\rangle$ with $i \neq 1$. Each of these 5-spaces intersects $\mathcal{K}$ in more than $2q+2$ points since $q > 7$ and hence is a big 5-space. It follows that $\Pi_6 \cap \mathcal{K}$ contains at least $(q+1)(q^2-q-1)+2q+2 = q^3+1$ points.

Repeating this reasoning yields inductively the following recursion formula for the number of points ϕ_{k+1} in $\Pi_{k+1} \cap \mathcal{K}$ where $\tilde{\Pi}_3$ is a 3-space containing π and at least $q+1$ points of $\mathcal{K}$ which is not contained in Π_k and where $\Pi_{k+1} = \langle \Pi_k, \tilde{\Pi}_3\rangle$, where $\phi_5 = q^2 + q + 1$.

$$\phi_{k+1} \geq (\frac{\phi_k - 4}{q-1} - 1)(q^2 - q - 1) + 2q + 2. \tag{4.5}$$

We will adapt the recursion formula to a recursion formula for numbers ψ_k such that $\psi_k \leq \phi_k$ for all $k \geq 5$.

First we rewrite the recursion formula for ϕ_k as follows.

$$\phi_{k+1} = (\phi_k - q - 3)\frac{q^2-q-1}{q-1} + 2q + 2.$$

Since $\frac{q^2-q-1}{q-1} > q-1$ if $q > 2$ we get after a little calculation

$$\phi_{k+1} > (q-1)\phi_k - q^2 + 5.$$

Since $\phi_5 = q^2 + q + 1$ we can even write for all integers $k \geq 5$

$$\phi_{k+1} > (q-2)\phi_k.$$

Now we set $\psi_5 = \phi_5$ and $\psi_{k+1} = (q-2)\psi_k$. Hence we get $\psi_N = (q-2)^{N-5}(q^2 + q + 1)$ for all $N \geq 5$. This yields the following inequality

$$(q-2)^{\frac{n(n+3)}{2}-5}(q^2+q+1) \leq \frac{q^{n+1}-1}{q-1}.$$

This is an equality if $n = 2$ and the left hand side increases faster than the right hand side if n increases, hence this yields a contradiction for $n > 2$. □

The remaining cases are $q = 5$ and $q = 7$. First we prove a lemma for $q = 5$.

Lemma 4.2.17 *Let $q = 5, n > 2$, and consider a plane π which intersects $\mathcal{K}$ in 4 points. If inside a big 5-space Π_5 there is a 4-space Π_4 through π intersecting $\mathcal{K}$ in 12 points then there are no 4-spaces through π inside Π_5 intersecting $\mathcal{K}$ in 11 or 10 points.*

Proof Suppose the contrary and consider a 6-space Π_6 containing Π_5 which intersects $\mathcal{K}$ in more than 31 points. Such a 6-space always exists otherwise we don't get enough points for the set $\mathcal{K}$.

If Π_5 contains a 4-space Π'_4 through π intersecting $\mathcal{K}$ in 11 points, then consider all 5-spaces through Π_4 and Π'_4 inside Π_6. By Conditions (S') and (V') the only ones which yield extra points are big 5-spaces. For take a 5-space with an extra point p, then we have at least two extra points. Namely, the 3-space $\langle \pi, p \rangle$ contains more than 4 points of $\mathcal{K}$ and hence by Condition (S') at least 6 points of $\mathcal{K}$.

Denote the number of big 5-spaces inside Π_6 through Π_4 and Π'_4 by α and β respectively. We get the following equation

$$19\alpha + 12 = 20\beta + 11$$

If we rewrite this as $1 + 19(\alpha - \beta) = \beta$, then clearly the only solution with $1 \leq \alpha,\ \beta \leq 6$ is $\alpha = \beta = 1$, a contradiction since Π_6 intersects $\mathcal{K}$ in more than 31 points.

If there is a 4-space Π'_4 in Π_5 through π intersecting $\mathcal{K}$ in 10 points then 5-spaces through Π'_4 inside Π_6 which yield extra points intersect $\mathcal{K}$ either in 12 or in 31 points by Condition (S') and Condition (V'). Denote the number of big 5-spaces through Π_4 inside Π_6 by x, the number of 5-spaces of Π_6 through Π'_4 intersecting $\mathcal{K}$ in 12 points by y and the number of big 5-spaces through Π'_4 inside Π_6 by z. Then the following equation is obtained

$$19x + 12 = 2y + 21z + 10, \text{ with } x \geq 1 \text{ and } x,\ y,\ z \leq 6.$$

The only solution is $x = z = 1$ and $y = 0$, a contradiction since Π_6 intersects $\mathcal{K}$ in more than 31 points. □

Lemma 4.2.18 *For $q = 5$ or $q = 7$ and $n > 2$, a plane π intersecting $\mathcal{K}$ in exactly 4 points is never contained in a big 5-space Π_5.*

Proof Case (a) $q = 5$:

Assume π is contained in a big 5-space Π_5. First of all, a 3-space in Π_5 contains at most 8 points of $\mathcal{K}$ by Lemma 4.2.15.

Project Π_5 from π onto a plane π' which is skew to π in Π_5. For the 3-spaces through π which contain 6, 7 or 8 points of $\mathcal{K}$, the projection in π' is given weight 2, 3 or 4 respectively.

First suppose there is a 3-space Π_3 in Π_5 which contains π and which intersects $\mathcal{K}$ in 8 points. Then five 4-spaces through Π_3 in Π_5 intersect $\mathcal{K}$ in 12 points and one 4-space through Π_3 in Π_5 intersects $\mathcal{K}$ in 11 points. But this yields a contradiction by Lemma 4.2.17.

Hence, from now on, we may assume that each 3-space through π inside a big 5-space which contains more than 4 points of $\mathcal{K}$ contains 6 or 7 points of $\mathcal{K}$. Hence if we denote the number of 3-spaces through π inside Π_5 which intersect $\mathcal{K}$ in 6 points by α and those which intersect $\mathcal{K}$ in 7 points by β, we get the following equation,

$$4 + 2\alpha + 3\beta = 31.$$

The rest of the proof is case-by-case analysis.

(A) $\beta \geq 7$:

In this case we have a set $\mathcal{P}$ of at least 7 points with weight 3 in π'. Since an oval in $\mathbf{PG}(2, 5)$ contains at most 6 points, three points of $\mathcal{P}$ will be collinear. But this implies that the 4-space spanned by the line L containing them and π intersects $\mathcal{K}$ in more than 12 points, a contradiction by Lemma 4.2.15.

(B) $\alpha = 6$, $\beta = 5$:

Consider a point p of weight 3 in π' and all lines $L_1, \cdots, L_6$ through it. On four of these lines, say $L_1, \cdots, L_4$ we have exactly one other point which has weight 3 otherwise we get a 4-space with more than 12 points. If none of $L_1, \cdots, L_4$ contains a point of weight 2 then the six points of weight 2 have to be distributed over the remaining two lines through p, a contradiction since then we get a 4-space intersecting $\mathcal{K}$ in more than 12 points of $\mathcal{K}$, a contradiction by Lemma 4.2.15. Hence we have already found a 4-space through π inside Π_5 which intersects $\mathcal{K}$ in 12 points. By Lemma 4.2.17, this implies that no 4-space through π inside Π_5 can intersect $\mathcal{K}$ in 10 or in 11 points. Now consider a point of weight 2 in π' and all lines through it. Then the 5 points of weight 3 are distributed over these lines as 2+2+1, as 2+1+1+1 or as 1+1+1+1+1. The latter two possibilities clearly yield a 4-space intersecting $\mathcal{K}$ in more than 12 points, a contradiction by Lemma 4.2.15. Namely, in the last case for instance, since no 4-space inside Π_5 is allowed to intersect $\mathcal{K}$ in exactly 11 points, all points of weight two are contained in one line through p in π'. The other case is similar.

But if it is always the 2+2+1 possibility then through each point of weight 2 there passes a line L containing 4 points of weight 2, which yields a contradiction.

(C) $\alpha = 9,\ \beta = 3:$

Consider a point p of weight 3 in π' and all lines through it. On two of these lines, L_1 and L_2, we have exactly one other point which has weight 3 otherwise we get a 4-space with more than 12 points. If there is no 4-space through π in Π_5 which intersects $\mathcal{K}$ in 12 points, then the 9 points of weight 2 have to be distributed over the remaining 4 lines, which again yields a too big 4-space. Hence there is a 4-space inside Π_5 intersecting $\mathcal{K}$ in 12 points, implying no 4-spaces through π inside Π_5 are allowed to intersect $\mathcal{K}$ in 10 or in 11 points by Lemma 4.2.17. This is impossible.

(D) $\alpha = 12,\ \beta = 1:$

Denote the 3-space through π inside Π_5 which intersects $\mathcal{K}$ in 7 points by Π_3. We have a set $\mathcal{P}$ of 13 points of weight 2 and 3 in π'. We claim that there has to be a line L containing 4 points of $\mathcal{P}$.

Indeed, consider an arbitrary point p contained in $\mathcal{P}$ and all lines through it. If there is no line which intersects $\mathcal{P}$ in 4 points then all lines of π' through p intersect $\mathcal{K}$ in 3 points. Since p was arbitrary this implies that all lines in π' intersect $\mathcal{P}$ in 0 or 3 points. But consider now a point r in π' not contained in $\mathcal{P}$ and all lines through it. Then we get a contradiction, since 3 does not divide 13. So we may assume that there is a line L in π' which intersects $\mathcal{P}$ in 4 points.

Hence, the 4-space spanned by L and π intersects $\mathcal{K}$ in 12 points. It has to be contained in another big 5-space otherwise we don't get enough points in $\mathcal{K}$. There again there has to be at least one 3-space, say Π_3', through π which intersects $\mathcal{K}$ in 7 points.

But now consider a space $\hat{\Pi}$ spanned by Π_3, Π_3' and another 3-space through π which contains at least 6 points of $\mathcal{K}$.

Then $\hat{\Pi}$ is certainly contained in a big 5-space, otherwise we don't have enough points in the set $\mathcal{K}$. But this is a contradiction since in any big 5-space we already excluded all cases with $\beta > 1$.

Case (b) $q = 7$:

Assume the plane π is contained in a big 5-space Π_5. First of all, a 3-space in Π_5 contains at most 10 points of $\mathcal{K}$ by Lemma 4.2.15.

Project Π_5 from π onto a plane π' which is skew to π in Π_5. For the 3-spaces through π which contain 8, 9 or 10 points of $\mathcal{K}$, the projection in π' is given weight 4, 5 or 6 respectively. Denote this set of points by $\mathcal{P}$.

First suppose there is a 3-space Π_3 in Π_5 which contains π and which intersects $\mathcal{K}$ in 10 points. Then seven 4-spaces through Π_3 in Π_5 intersect $\mathcal{K}$ in 16 points and one 4-space through Π_3 in Π_5 intersects $\mathcal{K}$ in 15 points. Consider all lines through the point p in π' corresponding with Π_3. There is exactly one line through p which contains one point p' of weight 5.

This implies that inside a big 5-space through Π_3 there is exactly one 3-space Π_3', namely the one which corresponds with p', which contains π and which intersects $\mathcal{K}$ in 9 points.

But a 4-space Π_4 through Π_3 intersecting $\mathcal{K}$ in 16 points has to be contained in at least one other big 5-space $\tilde{\Pi}_5$. Inside $\tilde{\Pi}_5$ we also find a 3-space $\tilde{\Pi}_3$ which contains π and which intersects $\mathcal{K}$ in 9 points. But now the big 5-space spanned by Π_3, Π_3' and $\tilde{\Pi}_3$ contains Π_3 and two 3-spaces which contain π and which intersect $\mathcal{K}$ in 9 points, a contradiction by the previous paragraph.

Hence, from now on, we may assume that each 3-space through π inside a big 5-space through π which contains more than 4 points of $\mathcal{K}$ contains 8 or 9 points of $\mathcal{K}$. Hence if we denote the number of 3-spaces through π inside Π_5 which intersect $\mathcal{K}$ in 8 points by α and those which intersect $\mathcal{K}$ in 9 points by β, we get the following equation,

$$4 + 4\alpha + 5\beta = 57.$$

Remark that inside π' each line through a point of weight 5 can contain at most one other point of weight 4 or 5 otherwise we get a 4-space which intersects $\mathcal{K}$ in more than 16 points. Hence $|\mathcal{P}| = \alpha + \beta \leq 1 + 8 \cdot 1 = 9$.

The only solutions of the above equation for (α, β) are the pairs $(12, 1)$, $(7, 5)$ and $(2, 9)$, which yields a contradiction by the previous paragraph. □

Remark 4.2.19 *The method of proof of the above theorem can also be used for the general case. However, Lemma 4.2.16 directly excludes all planes containing 4 points of* $\mathcal{K}$ *for* $q > 7$.

Lemma 4.2.20 *Any line* L *meets* $\mathcal{K}$ *in at most 2 points. Hence, a plane* π *with* $|\pi \cap \mathcal{K}| = q + 1$ *intersects* $\mathcal{K}$ *in an oval.*

Proof Similar to the proof of Lemma 4.2.9; use Lemma 4.2.15 and Lemma 4.2.16. □

Theorem 4.2.21 *If* $q \geq 5$ *and* $n > 2$, *then the set* $\mathcal{K}$ *is the point set of the Veronese variety of all quadrics of* $\mathbf{PG}(n, q)$.

Proof We check Conditions (P), (S) and (V) of Theorem 4.2.5. Conditions (S) and (V) are implied by Condition (S') and Theorem 1.5.8 and by Condition

(V') respectively. The first part of Condition (P) was proved in Lemma 4.2.16 for $q > 7$.

Furthermore, for $q = 5$ and $q = 7$ we proved the first part of Condition (P) for all planes which are contained in a big 5-space. In fact, we did only use Condition (P) for these planes in our first characterization.

The second part of Condition (P), namely that every 2 points of $\mathcal{K}$ are contained in an oval of $\mathcal{K}$, is never used to obtain Lemma 4.2.13 if $n > 2$. If $n = 2$, we did use Condition (P) for the proof of Lemma 4.2.10. Since every two points are contained in a big 5-space Π_5 by Condition (V), and since $\Pi_5 \cap \mathcal{K}$ is a Veronese variety $\mathcal{V}_2^4$ by Lemma 4.2.13 the second part of Condition (P) is proved. The proof is finished by Theorem 4.2.5. □

The counterexample for the case $n = 2$ is the following. Consider in $\mathbf{PG}(5, q)$ a point p on an ovoid $\mathcal{O}$ in $\mathbf{PG}(3, q)$ and a tangent line L to $\mathcal{O}$ at p. Furthermore, consider a 3-dimensional space Π'_3 intersecting Π_3 exactly in L and containing an oval $\mathcal{O}'$ which intersects L in p. Then the set $\mathcal{O} \cup \mathcal{O}'$ fulfills Conditions (P'), (S') and (V') but it is not a Veronesean $\mathcal{V}_2^4$.

Chapter 5

Characterizations of finite classical polar spaces by intersection numbers

5.1 Introduction

When Segre [51] proved his celebrated characterization of conics ("every set of $q+1$ points in $\mathbf{PG}(2,q)$, q odd, no three of which are collinear, is a conic"), he did more than proving a beautiful and interesting theorem; he in fact provided the starting point of a new direction in combinatorial geometry. In this branch of combinatorics the idea is to provide purely combinatorial characterizations of objects classically defined in an algebraic way. In Chapter 4 several such combinatorial characterizations of Veroneseans were obtained. In this chapter we again discuss several results of this kind, namely we characterize finite classical polar spaces by means of their intersection numbers with respect to certain subspaces. The work in this chapter is based on a result of Ferri and Tallini, stated later on, which provides a characterization of $Q(4,q)$ by intersection numbers with respect to planes and solids. This is a clear motivation to look at the following questions:

> Is it possible to characterize finite classical polar spaces by their intersection numbers with respect to planes and solids, respectively by their intersections with respect to hyperplanes and subspaces of codimension 2?

(Note that these questions of course do not make any sense for the polar space $W_{2n+1}(q)$, as this polar space comprises all points of its ambient projective space.)

The first question was answered affirmatively in Schillewaert [47], and Schillewaert and Thas [49]; the second question in [17]. Though it is possible to characterize certain polar spaces only by their line intersections, the existence (in abundance) of *quasi-quadrics* and *quasi-Hermitian varieties* shows that it is not possible to characterize them merely by their intersections with respect to hyperplanes. Here we define a quasi-quadric, respectively quasi-Hermitian variety, to be a subset of the set of points of a projective space having the same intersection numbers with respect to hyperplanes as a non-singular quadric, respectively a non-singular Hermitian variety. In the case of the parabolic quadric, this is a slight deviation of the standard definition as given in [14]. The concept of a quasi-Hermitian variety in fact does not appear in the literature, but it is very easy to show that examples can be constructed with the same techniques as those used to construct quasi-quadrics. For an overview on quasi-quadrics, we refer to [14].

5.2 Previous characterization results and main results

The following characterizations of quadrics and Hermitian varieties, which can be found in Hirschfeld and Thas [28], will be of great importance later on in this chapter. These theorems also provide nice examples of Segre-type theorems.

Definition 5.2.1 *A point set* $\mathcal{K}$ *in* $\mathbf{PG}(n,q)$ *is said to be of* type $(r_1, r_2, \cdots, r_s)$ *if* $|L \cap \mathcal{K}| \in \{r_1, r_2, \cdots, r_s\}$ *for all lines* L *of* $\mathbf{PG}(n,q)$*. A point* $p \in \mathcal{K}$ *is called* singular *with respect to* $\mathcal{K}$ *if all lines through* p *intersect* $\mathcal{K}$ *either in 1 or in* $q+1$ *points. If a set* $\mathcal{K}$ *contains a singular point, then* $\mathcal{K}$ *is called* singular.

The theorem below is an amalgamation of results of Tallini-Scafati [61], Hirschfeld and Thas [27], and Glynn [25].

Theorem 5.2.2 *Let* $\mathcal{K}$ *be a non-singular point set of type* $(1, r, q^2+1)$ *in* $\mathbf{PG}(n, q^2)$*,* $n \geq 4$ *and* $q > 2$*, satisfying the following properties:*

- $3 \leq r \leq q^2 - 1$*;*
- *there does not exist a plane* π *such that every line of* π *intersects* $\pi \cap \mathcal{K}$ *in* r *or* q^2+1 *points;*

Then the set $\mathcal{K}$ *is the point set of a non-singular Hermitian variety* $H(n, q^2)$*.*

The result below was obtained by Tallini in [58] and [59].

Theorem 5.2.3 *In* $\mathbf{PG}(n,q)$*, with* $n \geq 4$ *and* $q > 2$*, let* $\mathcal{K}$ *be a non-singular point set of type* $(0,1,2,q+1)$*.*
If $\frac{q^{n+1}-1}{q-1} > |\mathcal{K}| \geq \frac{q^n-1}{q-1}$*, then one of the following cases holds:*

(i) $|\mathcal{K}| = \frac{q^n-1}{q-1}$*,* n *is even, and* $\mathcal{K}$ *is the point set of a* $Q(n,q)$*.*

(ii) $|\mathcal{K}| = \frac{q^n-1}{q-1} + q^{\frac{n-1}{2}}$*,* n *is odd, and* $\mathcal{K}$ *is the point set of a* $Q^+(n,q)$*.*

(iii) $|\mathcal{K}| = \frac{q^n-1}{q-1} + 1$*,* q *is even, and* $\mathcal{K} = \Pi_t\mathcal{K}' \cup \{N\}$ *with* Π_t *some* $\mathbf{PG}(t,q) \subset \mathbf{PG}(n,q)$ *and with* $\mathcal{K}'$ *(the point set of) a* $Q(n-t-1,q)$ *in some* $(n-t-1)$*-dimensional subspace of* $\mathbf{PG}(n,q)$ *skew to* $\mathbf{PG}(t,q)$ *(hence* $n-t-1$ *is even) or with* $\mathcal{K}'$ *a* $(q+1)$*-arc in a plane skew to* $\mathbf{PG}(t,q)$ *if* $t = n-3$*. In each case,* N *is the nucleus of a particular chosen basis* $\mathcal{K}'$*.*

These two theorems provide characterizations of certain polar spaces by their line intersections. It is a natural question to ask whether polar spaces can also be characterized by their intersections with respect to other subspaces.

As a first result in this direction, we state the following result of Durante, Napolitano and Olanda [19].

Theorem 5.2.4 *Let* $\mathcal{K}$ *be a set of points in* $\mathbf{PG}(3,q)$*, with* $|\mathcal{K}| = q^2+q+1$*, and suppose that* $\mathcal{K}$ *contains at least two lines. Furthermore, suppose that* $\mathcal{K}$ *intersects every plane in* 1*,* $q+1$ *or* $2q+1$ *points. Then* $\mathcal{K}$ *is a cone projecting an oval in a plane* Π *from a point* v *not in* Π*.*

Ferri and Tallini proved the following nice characterization of the parabolic quadric $Q(4,q)$ in [23].

Theorem 5.2.5 *A set* $\mathcal{K}$ *of points in* $\mathbf{PG}(n,q)$*, with* $n \geq 4$ *and* $|\mathcal{K}| \geq q^3+q^2+q+1$*, intersecting all planes in* 1*,* a *or* b *points, where* $b \geq 2q+1$*, and intersecting every solid in* c*,* $c+q$ *or* $c+2q$ *points, where* $c \leq q^2+1$*, such that solids intersecting in* c *and solids intersecting in* $c+q$ *points exist, is a non-singular quadric of* $\mathbf{PG}(4,q)$*.*

We will prove the following corollary of this theorem in the following section.

Corollary 5.2.6 *If a set of points* $\mathcal{K}$ *in* $\mathbf{PG}(4,q)$ *is such that it intersects all planes in* 1*,* $q+1$*, or* $2q+1$ *points and all solids in* q^2+1*,* q^2+q+1 *or* q^2+2q+1 *points, then it is a parabolic quadric* $Q(4,q)$*.*

Further, we extend this theorem to a characterisation of quadrics in $\mathbf{PG}(n,q)$, $n \geq 4$, by all possible intersection numbers with planes and solids.

Theorem 5.2.7 *If a set $\mathcal{K}$ of points in $\mathbf{PG}(n,q)$, $n \geq 4$, intersects planes and solids in the same number of points as quadrics, then $\mathcal{K}$ is one of the following:*

(i) the projective space $\mathbf{PG}(n,q)$,

(ii) a hyperplane in $\mathbf{PG}(n,q)$,

(iii) a quadric in $\mathbf{PG}(n,q)$.

(iv) For q even,

(iv.1) a cone with vertex an $(n-3)$-dimensional space and base an oval,

(iv.2) a cone with vertex an $(n-4)$-dimensional space and base an ovoid.

Next, we prove the analogous result for Hermitian varieties, i.e. a characterization of Hermitian varieties in $\mathbf{PG}(n,q)$, $n \geq 4$, by their intersection numbers with respect to planes and solids.

Theorem 5.2.8 *If for a set $\mathcal{K}$ of points in $\mathbf{PG}(n,q^2)$, $n \geq 4$, the intersection numbers with planes and solids are also intersection numbers of planes and solids with a Hermitian variety, then $\mathcal{K}$ is either:*

(i) *the projective space $\mathbf{PG}(n,q^2)$,*

(ii) *a hyperplane in $\mathbf{PG}(n,q^2)$,*

(iii) *a Hermitian variety in $\mathbf{PG}(n,q^2)$,*

(iv) *a cone with vertex an $(n-2)$-dimensional space and base a line intersecting $\mathcal{K}$ in q or $q+1$ points,*

(v) *a cone with vertex an $(n-3)$-dimensional space and base a unital, or*

(vi) *a cone with vertex an $(n-3)$-dimensional space and base a set $\tilde{\mathcal{K}}$ of $\mathbf{PG}(2,q^2)$ intersecting each line of $\mathbf{PG}(2,q^2)$ in 1, q, $q+1$ or q^2+1 points and containing exactly one full line.*

Remark 5.2.9 *Let $\mathcal{M}$ be a* maximal $\{q^3-q^2+q;q\}$-arc *in $\mathbf{PG}(2,q^2)$, that is, a point set $\mathcal{M}$ of size q^3-q^2+q in $\mathbf{PG}(2,q^2)$ intersecting each line of $\mathbf{PG}(2,q^2)$ in either 0 or q points; such a set is known to exist for any $q=2^h$, see [30]. Let M be a line of $\mathbf{PG}(2,q^2)$ intersecting $\mathcal{M}$ in q points and let L be a line of $\mathbf{PG}(2,q^2)$ containing no points of $\mathcal{M}$. Then $\tilde{\mathcal{K}} = (\mathcal{M}\backslash M) \cup L$ can be taken as base of the cone described in Theorem 5.2.8 (vi).*

So far we extended the Corollary 5.2.6 of Theorem 5.2.5 of Ferri and Tallini to higher-dimensional quadrics and higher-dimensional Hermitian varieties allowing extra intersection numbers for the intersection with planes and solids. Another direction is to view intersections with planes and solids in 4-dimensional space more generally as intersections with hyperplanes and spaces of codimension 2 in higher-dimensional space. This viewpoint leads to a characterization of non-singular classical polar spaces except for the symplectic ones of course.

We show that non-singular quadrics and non-singular Hermitian varieties are completely characterized by their intersection numbers with respect to hyperplanes and spaces of codimension 2. This strongly generalizes the result Theorem 5.2.5 of Ferri and Tallini and also provides necessary and sufficient conditions for quasi-quadrics (respectively their Hermitian analogues) to be non-singular quadrics (respectively Hermitian varieties).

The following Segre-type characterization of polar spaces provides necessary and sufficient conditions for a quasi-quadric or a quasi-Hermitian variety to be a non-singular quadric or Hermitian variety.

Theorem 5.2.10 *If a point set $\mathcal{K}$ in $\mathbf{PG}(n,q)$, $n \geq 4$, $q > 2$, has the same intersection numbers with respect to hyperplanes and subspaces of codimension 2 as a polar space $P \in \{H(n,q), Q^+(n,q), Q^-(n,q), Q(n,q)\}$, then $\mathcal{K}$ is the point set of a non-singular polar space.*

Remark 5.2.11 *For $n = 3$, the conclusion of the above theorem remains true in the Hermitian and hyperbolic case. This is easily seen using Theorem 1.2.5. Also in the elliptic case the conclusion remains true, since an ovoid is a not a polar space. If $n = 4$, the conclusion of the theorem is true for all q. In the parabolic case, this is Theorem 5.2.6, and in the Hermitian case, this result is proved in Section 5.4.*

In the following sections, we give the proofs of the theorems above.

5.3 Proof of Theorem 5.2.7

5.3.1 A corollary of the theorem of Ferri and Tallini

Consider a set $\mathcal{K}$ of points in $\mathbf{PG}(4,q)$ intersecting every plane in 1, $q+1$ or $2q+1$ points, and every solid in q^2+1, q^2+q+1 or q^2+2q+1 points. Planes intersecting $\mathcal{K}$ in 1, $q+1$ and $2q+1$ points respectively will be called *small*, *medium* and *large* respectively. Solids intersecting $\mathcal{K}$ in q^2+1, q^2+q+1

and $q^2 + 2q + 1$ points respectively, will be called *small*, *medium* and *large* respectively.

We prove the conditions required for the characterization of Ferri and Tallini of $Q(4, q)$. Consider a given solid Π. First count how many small, medium and large planes there are in Π; call the number of them a, b and c respectively. Denote the number of points of $\mathcal{K}$ inside Π by γ. Counting the total number of planes in a solid, the incident pairs (p, α) where p is a point of $\mathcal{K}$ and α a plane, and the number of ordered triples (p, r, α) where p and r are distinct points of $\mathcal{K}$ lying in the plane α respectively, yields the following equations

$$a + b + c = (q + 1)(q^2 + 1),$$

$$a + b(q + 1) + c(2q + 1) = \gamma(q^2 + q + 1),$$

$$bq(q + 1) + c2q(2q + 1) = \gamma(\gamma - 1)(q + 1).$$

We can calculate a, b and c exactly for each value of γ; later on we will only use that $c = 0$ if $\gamma = q^2 + 1$, that a, b and c are all non-zero if $\gamma = q^2 + q + 1$, and that $a = 0$ if $\gamma = q^2 + 2q + 1$.

Note that it never occurs that two of the integers a, b and c are zero.

Lemma 5.3.1 *Small solids intersect $\mathcal{K}$ in an ovoid.*

Proof Consider a small solid Π and all planes through a line L inside Π, where we assume that L contains $x \geq 2$ points of $\mathcal{K}$. Since a small solid contains no large planes, we get exactly

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

points, hence $x = 2$. For $q = 2$, we have 5 points, no four coplanar. So, for all q, small solids intersect $\mathcal{K}$ in an ovoid. □

We first prove that the size assumption of Theorem 5.2.5 is fulfilled.

Lemma 5.3.2 *The set $\mathcal{K}$ contains $q^3 + q^2 + q + 1$ or $q^3 + q^2 + 2q + 1$ points.*

Proof (1) If a small plane α exists, then consider all solids through α inside the 4-dimensional space Δ. We obtain the following lower bound on the size of $\mathcal{K}$,

$$|\mathcal{K}| \geq 1 + (q + 1)q^2 = q^3 + q^2 + 1.$$

Equality holds if and only if all solids through α are small, and small solids are ovoids. Take a line L inside Δ. If L lies in a solid through α, then L contains at most 2 points of $\mathcal{K}$.

Next consider a line M not intersecting α and assume it contains a point x of

$\mathcal{K}$. Consider the small solid Π spanned by x and α. Inside Π one can find a small plane containing x. Hence, M lies in a small solid through a small plane, a case already treated. So all lines intersect $\mathcal{K}$ in at most 2 points. Hence, we would find a cap of size q^3+q^2+1. This yields a contradiction with Lemma 1.5.6.

So at least one solid through α is medium or large, so $|\mathcal{K}| \geq q^3+q^2+q+1$. In both cases, there is a large plane. Let π be this large plane. Look at all solids through π inside Δ. We get the inequality,

$$|\mathcal{K}| \leq (q+1)q^2+2q+1 = q^3+q^2+2q+1.$$

(2) If no small plane exists, then all 3-spaces are large ones. In this case, we get the following size for $\mathcal{K}$:

$$|\mathcal{K}| = (q+1)q^2+2q+1 = q^3+q^2+2q+1.$$

Taking an arbitrary plane and looking at all solids through it learns that the number of points in $\mathcal{K}$ is always 1 mod q, hence this lemma is proved. □

Lemma 5.3.3 *There exist small and medium solids.*

Proof We show that for both possible values of $|\mathcal{K}|$, there exist small and medium solids. Denote the number of small, medium and large solids in the 4-dimensional space by a, b and c respectively.

Counting the total number of solids Π in a 4-dimensional space, the number of incident pairs (p, Π) where $p \in \mathcal{K}$, and the number of ordered triples (p, r, Π) where p and r are distinct points of $\mathcal{K}$ incident with Π, yields the following equations

$$a+b+c = \frac{q^5-1}{q-1},$$

$$(q^2+1)a+(q^2+q+1)b+(q^2+2q+1)c = |\mathcal{K}|\frac{q^4-1}{q-1},$$

$$(q^2+1)q^2a+(q^2+q+1)(q^2+q)b+(q^2+2q+1)(q^2+2q)c = |\mathcal{K}|(|\mathcal{K}|-1)\frac{q^3-1}{q-1}.$$

Solving these equations yields that in both cases $a \neq 0$ and $b \neq 0$, so there exist small and medium solids. □

In our previous lemmas, we have proved all the necessary conditions for Theorem 5.2.5, hence we have the following result.

Theorem 5.3.4 *If a set $\mathcal{K}$ of points in* $\mathbf{PG}(4,q)$ *is such that it intersects all planes in 1, $q+1$, or $2q+1$ points and all solids in q^2+1, q^2+q+1 or q^2+2q+1 points, then it is a parabolic quadric $Q(4,q)$.*

It is this result we will extend in the next section to obtain a characterization of all quadrics by means of their intersection numbers with respect to planes and solids.

5.3.2 The characterization

Consider a set $\mathcal{K}$ of points in $\mathbf{PG}(n,q)$, $n \geq 4$, that has as intersection numbers with planes

$$1,\ q+1,\ 2q+1,\ q^2+q+1$$

and as intersection numbers with solids

$$q+1,\ q^2+1,\ q^2+q+1,\ q^2+2q+1,\ 2q^2+q+1,\ q^3+q^2+q+1.$$

We adopt the following terminology for the rest of this section. We call planes and solids that intersect the set $\mathcal{K}$ in i and j points respectively, *i-planes* and *j-solids* respectively. A line containing $q+1$ points of the set $\mathcal{K}$ is called a *full line*, a (q^2+q+1)-plane will be called a *full plane*, and a (q^3+q^2+q+1)-solid will be called a *full solid*.

Lemma 5.3.5 *A $(2q^2+q+1)$-solid meets the set $\mathcal{K}$ in the union of two full planes.*

Proof Consider a $(2q^2+q+1)$-solid Π, a line L contained in Π and look at all planes through L inside Π. Suppose that L contains x points of the set $\mathcal{K}$. Then, if we suppose that Π does not contain a full plane, we find at most

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

points. We find that $x \leq 2$, but then we would have a cap of size $2q^2+q+1$ in $\mathbf{PG}(3,q)$. This is impossible, hence Π does contain a full plane, say π. Next consider a point p in $\Pi\backslash\pi$ belonging to $\Pi\cap\mathcal{K}$, and let L be a line through p in Π such that L does not lie in a full plane of Π; hence L lies only in $(2q+1)$-planes of Π. Call x the number of points in $\mathcal{K}\cap L$. Then we get the following equality

$$x+(q+1)(2q+1-x)=2q^2+q+1.$$

Hence, $x=2$. If there is no full plane through p in Π, this would mean that $\mathcal{K}=\Pi\cup\{p\}$, which is a contradiction. Hence, we have shown that Π meets $\mathcal{K}$ in the union of two full planes. □

Lemma 5.3.6 *A $(q+1)$-solid meets $\mathcal{K}$ in a full line.*

Proof Since by assumption every plane is blocked, and since a $(q+1)$-solid contains only $q+1$ points of $\mathcal{K}$, the proof is finished by Theorem 1.4.8. □

Lemma 5.3.7 *If a solid* Π *contains a full plane* π *and a point* $p \in \mathcal{K}\backslash\pi$*, then* Π *is a* $(2q^2+q+1)$*-solid or a full solid.*

Proof Since Π already contains q^2+q+2 points of $\mathcal{K}$, we only have to prove that Π is not a (q^2+2q+1)-solid. Suppose it is a (q^2+2q+1)-solid. Consider a line N through p inside Π intersecting $\mathcal{K}$ in x points. Consider all planes through N inside Π. They all intersect $\mathcal{K}$ in at least $q+2$ points and hence in at least $2q+1$ points. Counting yields the following equality

$$(q+1)(2q+1-x)+x = q^2+2q+1.$$

This is only possible if $x = q+1$. Since N was an arbitrary line through p in Π, Π would intersect $\mathcal{K}$ in more than q^2+2q+1 points, a contradiction. □

Lemma 5.3.8 *There exist full lines.*

Proof If there exists a full plane or a $(q+1)$-solid, then we are done. So suppose that these do not exist. Then by the previous lemmas, there is a 4-dimensional space Δ whose planes are only 1-planes, $(q+1)$-planes and $(2q+1)$-planes, and whose solids are only (q^2+1)-solids, (q^2+q+1)-solids and (q^2+2q+1)-solids. But then by Theorem 5.2.6, Δ meets $\mathcal{K}$ in a parabolic quadric $Q(4,q)$; which contains lines. □

We define a point-line geometry $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathbf{I})$, where the points of $\mathcal{P}$ are the points of $\mathcal{K}$, where the lines of $\mathcal{B}$ are the full lines and where incidence is containment.

Theorem 5.3.9 *The geometry* $\mathcal{S}$ *is a Shult space.*

Proof We have already shown that there exist full lines, so $\mathcal{B}$ is non-empty. The different cases we consider in this proof will also show that $\mathcal{B}$ contains at least two lines.

Consider a point p of $\mathcal{S}$ and a line L of $\mathcal{S}$, such that p and L are not incident. We prove the axiom for the incidence relation of a Shult space, and we refer to it as the 1-or-all axiom (see Section 1.2 for the definition of a Shult space).

Consider the plane α generated by p and L. Since this plane contains at least $q+2$ points of $\mathcal{S}$, it is either a $(2q+1)$-plane or a full plane. If this plane is a full plane, then we have the all part of the 1-or-all axiom.

So suppose from now on that α is a $(2q+1)$-plane. We distinguish between several cases that cover all possible situations.

(1) Suppose that there exists a solid Π through α containing a full plane β. If Π was a full solid, then α would be a full plane. Since small solids intersect

$\mathcal{K}$ in an ovoid by Lemma 5.3.1, the solid Π either is a (q^2+2q+1)-solid or a $(2q^2+q+1)$-solid.

Since $\beta \neq \alpha$, Lemma 5.3.7 shows that Π is a $(2q^2+q+1)$-solid. By Lemma 5.3.5, Π contains two full planes, they both intersect α in a line, hence the 1-axiom is fulfilled.

(2) Suppose now that there exists a 4-space Δ containing α that does not contain full planes. Since $(2q^2+q+1)$-solids and full solids contain full planes, also these do not occur in this 4-space.

(a) Suppose that also no $(q+1)$-solids occur in Δ. Then we have exactly the intersection numbers with planes and solids as required for Theorem 5.2.6, so that $\mathcal{S}$ intersects Δ in a parabolic quadric $Q(4,q)$, which is a generalized quadrangle, so we have proved the 1-axiom.

(b) Suppose that a $(q+1)$-solid Π does occur in Δ, and that it intersects $\mathcal{S}$ in a full line M different from L. Consider all planes through M in Δ. Then we find at most

$$q^2(2q+1-(q+1))+(q+1)=q^3+q+1$$

points of $\mathcal{S}$ in Δ. Consider all lines through p inside α. One of them, say N, intersects $\mathcal{S}$ in exactly 2 points, otherwise α would intersect $\mathcal{S}$ in more than $2q+1$ points. Consider all planes through N inside Δ. Since α is a $(2q+1)$-plane, we find at least

$$(q^2+q)(q+1-2)+(2q+1-2)+2=q^3+q+1$$

points. Comparing these inequalities yields that all planes of Δ containing M and not contained in Π are $(2q+1)$-planes. Hence, all solids of Δ different from Π, intersecting Π in a plane that contains M, contain

$$q((2q+1)-(q+1))+q+1=q^2+q+1$$

points of $\mathcal{S}$. The line L and the solid Π intersect in a point r. Then $\{r\} = L \cap M$. If M lies in α, then we have proved the 1-axiom, so suppose that M does not lie in α.

Consider the solid Γ generated by α and M. This solid contains at least two lines, namely L and M, it intersects $\mathcal{K}$ in q^2+q+1 points and all planes of this solid are 1-planes, $(q+1)$-planes or $(2q+1)$-planes. Theorem 5.2.4 gives that Γ intersects $\mathcal{K}$ in a cone with as vertex r and base an oval. Hence, the line pr is the only line of $\mathcal{S}$ through p intersecting L. We have proved the 1-axiom.

(c) The remaining case is that the $(q+1)$-solids in Δ intersect $\mathcal{K}$ exactly in L. Let Π be such a $(q+1)$-solid of Δ through L. Considering all planes through L inside Δ yields as above that $\mathcal{K}$ intersects Δ in at most q^3+q+1 points. Consider a 1-plane β contained in Π, and consider all solids through

β in Δ. Since we know the $(q+1)$-solids contained in Δ contain L, we get at least

$$q(q^2)+q+1=q^3+q+1$$

points. Considering the two inequalities above learns us that they must be two equalities, so there pass q (q^2+1)-solids through β inside Δ. By Lemma 5.3.1, all (q^2+1)-solids through β inside Δ intersect $\mathcal{K}$ in an ovoid of $\mathbf{PG}(3,q)$.

We consider the union of all these ovoids and add one extra point of L; hence we have found a cap of size $q(q^2+1-1)+2=q^3+2$ in $\mathbf{PG}(4,q)$, yielding a contradiction with Lemma 1.5.6. Indeed, take any line N lying in Δ and not in Π. There always exists a solid Π' through N in Δ such that $\beta=\Pi'\cap\Pi$ intersects L in a point. So, Π' contains the 1-plane $\Pi\cap\Pi'$, hence as in the previous paragraph, Π' intersects $\mathcal{K}$ in an ovoid and hence N intersects $\mathcal{K}$ in at most 2 points.

(3) Consider now a 4-space Δ containing α such that no solid through α inside Δ contains a full plane, but Δ does. Call this full plane π.

(a) Suppose that $p\in\pi$. Then L does not intersect π. Take a point r on L and consider the solid Π'_r generated by r and π. By Lemma 5.3.7, Π' is a $(2q^2+q+1)$-solid or a full solid.

If a solid Π'_r is a full solid, then r is collinear with p in $\mathcal{S}$. Since α is a $(2q+1)$-plane, we have proved the 1-axiom. Suppose now that all solids Π'_r are $(2q^2+q+1)$-solids. If the full plane of Π'_r through r intersects π in a line through p, then we have again proved the 1-axiom. Suppose that this never happens. Then all the lines pr, $r\in L$, contain only two points of $\mathcal{S}$, namely p and r. But then α contains exactly $q+2$ points of $\mathcal{S}$, a contradiction.

(b) Suppose that $p\notin\pi$ and look at the solid generated by the point p and the plane π, call it Π.

Suppose that Π is a full solid. Then it does not contain α. It intersects α in a line of $\mathcal{S}$, hence we have proved the 1-axiom.

If Π is a $(2q^2+q+1)$-solid, then it intersects $\mathcal{K}$ in a union of two full planes. But then one of these planes contains p, and we are again in case (3)(a). □

Theorem 5.3.10 *If $\mathcal{S}$ is non-degenerate, then it is a non-singular quadric in $\mathbf{PG}(n,q)$, $n\geq 4$.*

Proof If there exists a full plane, then $\mathcal{S}$ is a non-degenerate Shult space of finite rank at least 3, and since all lines contain at least three points by definition, $\mathcal{S}$ with all its subspaces is a polar space. By Theorem 1.2.1, it is a finite classical polar space and by looking at the intersection numbers, we see that $\mathcal{S}$ is a non-singular quadric.

If there exists no full plane, then the previous arguments show we have proved for $\mathcal{S}$ axiom (GQ3) for generalized quadrangles. Clearly, there is a point p through which there pass two lines of $\mathcal{S}$. Hence, $\mathcal{S}$ is a generalized quadrangle.

By Theorem 1.1.2, it is a classical one; going through the list of classical generalized quadrangles yields it is the non-singular parabolic quadric $Q(4, q)$ or the non-singular elliptic quadric $Q^-(5, q)$. □

Suppose now that $\mathcal{S}$ is degenerate, so there exist points collinear with all other points. We call such points *singular* points.

Lemma 5.3.11 *The singular points of $\mathcal{S}$ form a subspace Π_k of $\mathbf{PG}(n, q)$.*

Proof Take two singular points p and r of $\mathcal{S}$ and consider a point t lying on the line $L = pr$. Surely, $t \in S$. All points on $\mathcal{S}$ are collinear with t. Take a point s of $\mathcal{S}$ not lying on L and consider the plane generated by s and L. This plane has to be a full one, hence s is collinear with t. □

Lemma 5.3.12 *If $\mathcal{S}$ contains singular points, then all lines not intersecting the subspace Π_k formed by the singular points, intersect $\mathcal{S}$ in 0, 1, 2 or $q + 1$ points.*

Proof Consider a line L not intersecting Π_k. Take a singular point p and consider the plane generated by p and L. Since this plane contains either 1, $q + 1$, $2q + 1$ or $q^2 + q + 1$ points of $\mathcal{S}$ by assumption, the statement is proved. □

Lemma 5.3.13 *If $n - k - 1 \geq 4$, then $\mathcal{S}$ is a cone with vertex a k-dimensional space and base a non-singular quadric.*

Proof If $\mathcal{S}$ is degenerate, then look at a complementary space $\mathbf{PG}(n-k-1, q)$ of the space Π_k. By assumption, this space does not contain singular points of $\mathcal{S}$. If $n - k - 1 \geq 4$, then Theorem 5.3.10 shows that $\mathcal{S}$ intersects this space in a non-singular quadric, hence $\mathcal{S}$ is a cone with vertex a k-dimensional space and base a non-singular quadric. □

Now we consider all other cases one by one.

(a) If $n - k - 1 = -1$, then $\mathcal{S}$ is the projective space $\mathbf{PG}(n, q)$.

(b) If $n - k - 1 = 0$, then $\mathcal{S}$ is a hyperplane of $\mathbf{PG}(n, q)$.

(c) If $n - k - 1 = 1$, then the complementary space is a line. If this line intersects $\mathcal{K}$ in zero points, we have an $(n - 2)$-dimensional space. If it intersects $\mathcal{K}$ in 2 points, we have the union of two hyperplanes.

(d) If $n-k-1=2$, then the complementary space is a plane π. Suppose that π intersects $\mathcal{S}$ in $q+1$ points. Since all lines intersect $\mathcal{K}\cap\pi$ in 0, 1, 2 or $q+1$ points, the intersection of π and $\mathcal{S}$ is an oval (a line is impossible otherwise we have extra singular points). Suppose that π intersects $\mathcal{K}$ in $2q+1$ points. Since π contains more than $q+2$ points of $\mathcal{K}$, π surely contains a line L of $\mathcal{S}$. Take a point $p \in S\cap\pi$ outside L. Considering all lines through p in π learns that one of them is a line of $\mathcal{S}$. The intersection of the two lines would be a singular point, this yields a contradiction.

(e) If $n-k-1=3$, then the complementary space is a solid Π. If this solid intersects $\mathcal{S}$ in q^2+1 points, it intersects $\mathcal{S}$ in an ovoid.

If this solid intersects $\mathcal{S}$ in q^2+q+1 points, it surely contains a line L of $\mathcal{S}$. Take a point p on $\mathcal{S}$, $p\notin L$, inside Π. Then the plane generated by p and L intersects $\mathcal{S}$ in two lines, as before. Hence, Π contains at least two lines. Theorem 5.2.4 learns that $\mathcal{S}$ intersects Π in a cone with vertex a point p and base an oval. This yields a contradiction, since the point p is then a singular point of $\mathcal{S}$.

Suppose Π intersects $\mathcal{S}$ in q^2+2q+1 points. By Lemma 5.3.7, we may assume Π intersects all planes in 1, $q+1$ or $2q+1$ points. Again we surely have lines of $\mathcal{S}$ lying in $\mathcal{S}\cap\Pi$.
Consider a point p of $\mathcal{S}\cap\Pi$ and a line L of $\mathcal{S}$, with $p\notin L$. The plane α generated by them is a $(2q+1)$-plane and the intersection sizes of lines immediately prove axiom (GQ3) for generalized quadrangles. By assumption, there is no point of $\mathcal{S}$ in Π collinear with all other points of $\Pi\cap S$.

So $\mathcal{S}\cap\Pi$ is a generalized quadrangle. Again by Theorem 1.1.2, it is a classical one and hence it is $Q^+(3,q)$.

If Π intersects $\mathcal{S}$ in $2q^2+q+1$ points, then, by Lemma 5.3.5, we get extra singular points, this yields a contradiction. Hence Theorem 5.2.7 is proved.

5.4 Proof of Theorem 5.2.8

Below we will prove the analogue of the above theorem for Hermitian varieties, i.e. we will characterize Hermitian varieties by means of their intersection numbers with respect to planes and solids.

5.4.1 Characterizations of $H(3,q^2)$ and $H(4,q^2)$

The classical generalized quadrangle $H(3,q^2)$

It is known that a non-singular Hermitian variety $H(3,q^2)$ in $\mathbf{PG}(3,q^2)$ intersects lines either in a point, a Baer subline or all q^2+1 points of the line. So the intersection numbers with lines are 1, $q+1$, and q^2+1. It intersects planes either in a non-singular Hermitian variety $H(2,q^2)$ or in a cone with vertex a point and as base a Baer subline. So the intersection numbers with planes are q^3+1 and q^3+q^2+1.

The following terminology is introduced for the considered set $\mathcal{K}$; it is also used in the next section. Lines intersecting $\mathcal{K}$ in one point are *tangent* lines, lines intersecting $\mathcal{K}$ in $q+1$ points *Baer* lines, and lines intersecting $\mathcal{K}$ in q^2+1 points *full* lines.

Planes that intersect our set $\mathcal{K}$ in q^3+1 points are called *non-singular* planes, and planes that intersect $\mathcal{K}$ in q^3+q^2+1 points are called *singular* planes. Denote the intersection of a plane α and the set $\mathcal{K}$ by $\mathcal{K}_\alpha$.

Theorem 5.4.1 *If the intersection numbers with lines and planes of the point set $\mathcal{K}$ of $\mathbf{PG}(3,q^2)$ are intersection numbers with lines and planes of $H(3,q^2)$, then $\mathcal{K}$ is a Hermitian variety $H(3,q^2)$.*

Proof Firstly, every plane α contains a tangent line. Suppose the contrary; then every line of α intersects $\mathcal{K}$ in at least $q+1$ points. This means that $\mathcal{K}_\alpha$ is a $(q+1)$-fold blocking set in α. By Theorem 1.4.6, $(q+1)$-fold blocking sets in $\mathbf{PG}(2,q^2)$ have size at least $(q+1)q^2+\sqrt{(q+1)q^2}+1$, which yields a contradiction with the assumptions on the intersection numbers with planes.

Next, there exists a full line. Suppose this is not the case, then we distinguish between two cases.

Either no singular plane exists in which case all planes are non-singular. In this case all lines must have the same intersection number with the set $\mathcal{K}$. Suppose the contrary, so assume that there exists at least one tangent line, and at least one Baer line, and consider all planes in $\mathbf{PG}(3,q^2)$ through a line L, respectively M, where we take L to be a tangent line and M to be a Baer line. This yields two different numbers for the size of $\mathcal{K}$, a contradiction. Since all planes contain at least one tangent line, this means that all lines are tangent ones. Then consider a plane α and a point p of $\mathcal{K}$ inside α. Look at all lines through p inside α. Then α would contain only the point p, a contradiction.

The other case is that there exists a singular plane α. Take a point p of $\mathcal{K}_\alpha$ lying on a tangent line L and consider all lines through p inside α. After counting we find at most $1+(q^2)q=1+q^3$ points, again a contradiction. So full lines certainly exist.

Also singular planes exist. To show this, consider a full line L and a point p of $\mathcal{K}$ which is not incident with L. Consider all lines through p in the plane α generated by p and L. All these lines contain at least 2 points hence they are Baer lines or full lines. So at least $1+q(q^2+1)=q^3+q+1$ points of the set $\mathcal{K}$ belong to α. Hence, α necessarily is a singular plane, and elementary counting yields that exactly one of the lines through p inside α is a full line, say M.

This line M intersects L in a point r. Consider a point p' in $\mathcal{K}_\alpha$ not lying on L or M. Through this point p' there goes a full line N in α by the previous arguments. The line N necessarily contains r, otherwise it intersects L and M in two different points s and t respectively, but then through $s \notin M$ there are two full lines in α that intersect M, namely L and N, a contradiction. Hence, all lines through r in α are either tangent lines or full lines, so counting yields that inside α there pass $q+1$ full lines through r.

One can also calculate the size of $\mathcal{K}$. Consider all planes through a full line; since they are all singular by the previous arguments, this yields

$$|\mathcal{K}| = (q^2+1)q^3 + q^2 + 1 = (q^3+1)(q^2+1).$$

Define $\mathcal{S}$ to be the incidence structure with as points the points of the set $\mathcal{K}$, as lines the full lines, and where a point p and a line L are said to be incident if L passes through p. We have already proved that axioms (GQ2) and (GQ3) for generalized quadrangles hold for $\mathcal{S}$.

It is impossible that one point p of $\mathcal{S}$ is collinear with all other points of $\mathcal{S}$. If this were the case, then consider a plane π not through p. Since this plane intersects $\mathcal{K}$ in either q^3+1 or q^3+q^2+1 points, $\mathcal{K}$ would contain either $1+q^2(q^3+1)$ or $1+q^2(q^3+q^2+1)$ points, which yields a contradiction with the size of $\mathcal{K}$.

Since it was proved that there exists a point p in $\mathcal{S}$ such that there go at least 3 lines of $\mathcal{S}$ through p, and since no point of $\mathcal{S}$ is collinear with all other points of $\mathcal{S}$, we have shown that the incidence structure $\mathcal{S}$ is a generalized quadrangle. Hence by Theorem 1.1.2 of Buekenhout and Lefèvre it is a classical one, and by looking at the different classical generalized quadrangles, it has to be $H(3,q^2)$. □

The classical generalized quadrangle $H(4,q^2)$

Consider a set $\mathcal{K}$ of points in $\mathbf{PG}(4,q^2)$, such that all intersection numbers with planes and solids are also intersection numbers with planes and solids of the non-singular Hermitian variety $H(4,q^2)$. We show that $\mathcal{K}$ has to be $H(4,q^2)$. Since $H(4,q^2)$ intersects a plane either in a line, a non-singular Hermitian variety $H(2,q^2)$, or a cone with vertex a point p and base a Baer subline $H(1,q^2)$, the intersection numbers with planes are

$$q^2+1,\ q^3+1,\ q^3+q^2+1.$$

Call planes with intersection number either q^2+1, q^3+1 or q^3+q^2+1, *small*, *medium* or *large*.

The intersection of a non-singular Hermitian variety $H(4,q^2)$ with a solid is either a non-singular Hermitian variety $H(3,q^2)$ or a cone with vertex a point p and base a non-singular Hermitian variety $H(2,q^2)$, so the intersection numbers with solids are

$$(q^2+1)(q^3+1),\ q^2(q^3+1)+1.$$

Call solids with intersection number $q^2(q^3+1)+1$ *singular*, the other ones *non-singular*. For a given plane α, the set of points belonging to $\mathcal{K}\cap\alpha$ will be denoted by $\mathcal{K}_\alpha$. A line L intersecting $\mathcal{K}$ in q^2+1 points is called a *full* line.

Theorem 5.4.2 *If each intersection number with planes and solids of a point set $\mathcal{K}$ in $\mathbf{PG}(4,q^2)$ is also an intersection number with planes and solids of $H(4,q^2)$, then $\mathcal{K}$ is a non-singular Hermitian variety $H(4,q^2)$.*

To prove Theorem 5.4.2, we first need a series of lemmas.

Lemma 5.4.3 *The set $\mathcal{K}$ contains $|H(4,q^2)|$ points.*

Proof Call $H_1=q^2(q^3+1)+1$ the number of points of $\mathcal{K}$ contained in a singular solid, $H_2=(q^2+1)(q^3+1)$ the number of points of $\mathcal{K}$ contained in a non-singular solid, and x the total number of points contained in the set $\mathcal{K}$. Call a the number of singular solids. Then counting the pairs (p,α) where p is a point and α a solid such that $p\in\mathcal{K}\cap\alpha$, respectively the triples (p,r,α) with $p,\ r\in\mathcal{K}\cap\alpha,\ p\neq r$, in two ways yields the following equations

$$aH_1+(\frac{q^{10}-1}{q^2-1}-a)H_2=x\frac{q^8-1}{q^2-1},$$

$$aH_1(H_1-1)+(\frac{q^{10}-1}{q^2-1}-a)H_2(H_2-1)=x(x-1)\frac{q^6-1}{q^2-1}.$$

From the first equation we obtain a in function of x. Substituting this in the second equation yields a quadratic equation in x. This equation has the following two solutions

$$x=q^7+q^5+q^2+1,\ \frac{q^9+q^8+q^7+2q^6+2q^5+2q^4+2q^3+2q^2+q+1}{q^2+q+1}.$$

The first solution is the desired one. The second one is not an integer, this proves the lemma. □

Consider a small plane α and look at all solids through α inside $\mathbf{PG}(4,q^2)$. Call the number of singular and non-singular ones a and b respectively, so $a+b=q^2+1$. An elementary counting yields the following equation

$$aq^5+b(q^5+q^3)+q^2+1=(q^5+1)(q^2+1).$$

Solving these equations yields $a=q^2+1$ and $b=0$. So all solids containing a small plane are singular. Similar calculations learn that the other planes are contained in both kinds of solids.

Lemma 5.4.4 *There exist solids of both kinds.*

Proof Suppose the contrary. Then the calculations above show that all planes are small and all solids are singular. Take a line L containing c points of the set $\mathcal{K}$. Consider all planes through L inside a solid. One gets the following equation,

$$(q^2+1)(q^2+1-c)+c = q^5+q^2+1.$$

This yields a contradiction for all c. Hence, there exist solids of both kinds. □

Lemma 5.4.5 *For a large plane α, the set $\mathcal{K}_\alpha$ is a blocking set in α.*

Proof Suppose that α contains a line L which is not blocked by $\mathcal{K}_\alpha$. Consider a large solid Π through α. Since through small planes, there only pass singular solids, all planes through L inside Π are medium or large ones, but then Π intersects the set $\mathcal{K}$ in more than $(q^2+1)(q^3+1)$ points, which yields a contradiction. □

Next we prove that also for small and medium planes α, the sets $\mathcal{K}_\alpha$ are blocking sets in α. The case $q = 2$ will be proved separately. First, the general case is proved.

Lemma 5.4.6 *Consider a medium plane α. If $q > 2$, then $\mathcal{K}_\alpha$ is a blocking set in α.*

Proof Suppose that $\mathcal{K}_\alpha$ is not a blocking set in α, meaning that α contains a line L which is not blocked by $\mathcal{K}_\alpha$. Consider a singular solid Π through α, and look at all planes through L inside Π. By the previous lemma, all these planes are small or medium. Call a the number of small ones, and b the number of medium ones. We obtain the following equation

$$a(q^2+1)+b(q^3+1) = q^2(q^3+1)+1.$$

Substituting $a = q^2+1-b$ in the above expression yields

$$b = q^2 - \frac{1}{q-1}.$$

Since b has to be an integer, this is a contradiction if $q > 2$. □

Lemma 5.4.7 *Consider a small plane α. If $q > 2$, then $\mathcal{K}_\alpha$ is a blocking set in α and hence the points belonging to $\mathcal{K}_\alpha$ form a line of α.*

Proof If α contains a line L which is not blocked by the set $\mathcal{K}_\alpha$, then by the previous lemmas all planes through L inside a solid Π on α must be small ones. But then Π intersects $\mathcal{K}$ in $(q^2+1)^2$ points, which yields a contradiction.

So $\mathcal{K}_\alpha$ is a blocking set in α, and blocking sets of size q^2+1 in a plane of order q^2 are lines by Theorem 1.4.8 of Bose and Burton. □

Next, the case $q = 2$.

Lemma 5.4.8 *Let $q = 2$ and consider a plane α that is either small or medium. Then the set $\mathcal{K}_\alpha$ is a blocking set for α. In particular, a small plane α intersects $\mathcal{K}$ in a line.*

Proof Suppose that a small plane α contains a line L which is not blocked by $\mathcal{K}_\alpha$. Consider a singular solid Π containing α, and call the number of small and medium planes through L inside Π, ϕ and ψ respectively. By Lemma 5.4.5, we know that $\phi + \psi = q^2 + 1$. Counting the number of intersection points of Π and $\mathcal{K}$ yields the following equation

$$\phi(q^2+1) + \psi(q^3+1) = q^2(q^3+1) + 1.$$

Substituting $q = 2$ into these equations, one obtains $\phi = 2$ and $\psi = 3$.

Next it is shown that the total number of small planes inside Π is 2. Call the number of small, medium and large planes inside Π, a, b and c respectively. Then by counting the total number of planes in a solid, the incident pairs (p, α), where p is a point of $\mathcal{K}$ and α a plane of Π, and the triples (p, r, α) where p and r are distinct points of $\mathcal{K}$ and α is a plane in Π containing p and r, in two ways, the following equations are obtained, where $k = q^2(q^3+1)+1$,

$$a + b + c = (q^2+1)(q^4+1),$$

$$a(q^2+1) + b(q^3+1) + c(q^3+q^2+1) = k(q^4+q^2+1),$$

$$a(q^2+1)q^2 + b(q^3+1)q^3 + c(q^3+q^2+1)(q^3+q^2) = k(k-1)(q^2+1).$$

Solving these equations yields $a = q(q-1)$, so if $q = 2$, then $a = 2$. This implies that all other lines inside α are blocked, otherwise at least 3 small planes are contained in Π, since each non-blocked line has two small planes through it in Π and only α can be counted twice.

This implies that by adding an arbitrary point r on L to $\mathcal{K}_\alpha$ a blocking set of size q^2+2 arises and so each such blocking set $\mathcal{K}_\alpha \cup \{r\}$ has to contain a line M_r by Theorem 1.4.4. Since the point r on L was arbitrary this means all these sets contain the same line M already contained in $\mathcal{K}_\alpha$, but then L is blocked by $\mathcal{K}_\alpha$, a contradiction.

Consider a line L in a medium plane α. Consider a singular solid Π containing α. The calculation in the beginning of the proof shows that if L is skew to $\mathcal{K}_\alpha$, then L is contained in a small plane. Hence, L is blocked. □

Remark 5.4.9 *It was already shown that singular solids exist, and by the previous proof all singular solids contain small planes. Since small planes intersect $\mathcal{K}$ in a full line, the set $\mathcal{K}$ contains full lines.*

Lemma 5.4.10 *Every line intersecting $\mathcal{K}$ in c points, where $2 \leq c < q^2+1$, is contained in at least one medium plane.*

Proof Suppose a line L intersects $\mathcal{K}$ in c points, with $2 \leq c < q^2+1$, and has no medium planes through it. Consider a solid Π containing L and look at all planes through L inside Π. So since none of these planes can be small since they share a full line with $\mathcal{K}$, by assumption all these planes are large ones, Π would contain $(q^2+1)(q^3+q^2+1-c)+c$ points belonging to the set $\mathcal{K}$. This yields a contradiction, even for a non-singular solid, unless $c = q^2+1$, a case which is excluded. □

Lemma 5.4.11 *If α is a medium plane, it contains no full lines.*

Proof A medium plane α is always contained in at least one non-singular solid Π. Suppose that L is a full line lying in α and consider all planes through L inside Π. The proof of the foregoing lemma immediately shows that all these planes have to be large ones, as $|\Pi \cap \mathcal{K}| = (q^2+1)(q^3+1) = (q^2+1)(q^3+q^2+1-|L|)+|L|$, a contradiction. □

Lemma 5.4.12 *If α is a medium plane, then $\mathcal{K}_\alpha$ is a minimal blocking set in α.*

Proof Consider a line L in α containing c points of the set $\mathcal{K}$, where $2 \leq c < q^2+1$. Note that such a line exists since a medium plane does not contain full lines by Lemma 5.4.11.

Consider a singular solid Π through α, and look at all planes through L inside Π. We get at least

$$(q^3+1-c)(q^2+1)+c$$

points belonging to $\Pi \cap \mathcal{K}$ because no small planes can contain L since all small planes intersect $\mathcal{K}$ in a line. This yields $c \geq q$ otherwise Π would not be a singular solid. The case $c = q$ cannot occur. Suppose the contrary. So take a line L such that L intersects $\mathcal{K}$ in q points. Consider a singular solid Π through L. The same counting argument as above yields that all planes through L inside Π must be medium planes. Since every plane through L is contained in at least one singular solid, $\mathcal{K}$ would contain

$$(q^4+q^2+1)(q^3+1-q)+q = q^7+q^4+q^2+1$$

points, which yields a contradiction. So, $c \geq q+1$. If $\mathcal{K}_\alpha$ would be a non-minimal blocking set, then there would be a point p of $\mathcal{K}_\alpha$ so that no line of α through p is a tangent one. Hence, all lines through p would contain at least $q+1$ points. But then counting yields that $\mathcal{K}_\alpha$ contains at least $1+(q^2+1)q = q^3+q+1$ points, a contradiction. □

Using the foregoing lemma, one can easily determine the intersection numbers with lines.

Lemma 5.4.13 *All lines intersect $\mathcal{K}$ in 1, $q+1$, or q^2+1 points.*

Proof Since every line intersecting $\mathcal{K}$ in c points, with $2 \leq c < q^2+1$, is contained in a medium plane and since medium planes intersect $\mathcal{K}$ in minimal non-trivial blocking sets, it follows from Theorem 1.4.4 that the blocking set is a unital and so $c = q+1$. □

Proof of Theorem 5.4.2. A line L intersecting $\mathcal{K}$ in $q+1$ points is called a *Baer* line; a line intersecting $\mathcal{K}$ in q^2+1 points is called a *full* line. For $q > 2$ the proof is easily finished by Theorem 23.5.19 in [28]. So an additional argument is necessary for $q = 2$. However, the following reasoning works for all q. Consider a point p in $\mathcal{K}$ and a line L in $\mathcal{K}$ which are not incident. By Lemma 5.4.11, the plane generated by them is a large one. The lines through p in that plane all are Baer lines or full lines. Elementary counting yields that exactly one of them is a full one.

Define $\mathcal{S}$ to be an incidence structure with as points the points of the set $\mathcal{K}$, as lines the full lines, and where a point p and a line L are said to be incident if L passes through p. We have already proved that axioms (GQ2) and (GQ3) for generalized quadrangles hold for $\mathcal{S}$. There is no point which is collinear with all others. If there was a point p collinear with all others, then consider a solid Π not incident with p. Since this solid contains either $q^2(q^3+1)+1$ or $(q^2+1)(q^3+1)$ points, then

$$|\mathcal{K}| \in \{1+q^2(q^2(q^3+1)+1), 1+q^2((q^2+1)(q^3+1))\}$$

This yields a contradiction with the size of $\mathcal{K}$. Next it will be shown that there is a point with at least three lines through it. Let p be a point of $\mathcal{K}$ and let L be a full line of $\mathcal{K}$ with p not on L. We know that every point p' of $\mathcal{K}\backslash L$ in $\langle p, L\rangle$ lies on exactly one full line intersecting L. Suppose that the full line through p intersecting L intersects L in r, then r already lies on two full lines. Consider a Baer line of $\langle p, L\rangle$ not through r. Every point of this Baer line is contained in a full line which intersects L which necessarily has to pass through r. So r is on at least 3 lines of $\mathcal{S}$. Hence, $\mathcal{S}$ is a generalized quadrangle. Theorem 1.1.2 implies that it is a classical one and by looking at the different classical ones, it has to be a non-singular Hermitian variety $H(4, q^2)$. □

5.4.2 Generalization

Consider a set $\mathcal{K}$ of points in $\mathbf{PG}(n,q^2)$, $n \geq 4$, for which each intersection number with planes and solids is also an intersection number with planes and solids of a Hermitian variety. First let us recall what the intersections of Hermitian varieties with planes and solids look like.

A plane lies on the Hermitian variety, or intersects it in either a non-singular Hermitian variety $H(2,q^2)$, a cone with vertex a point and base a non-singular Hermitian variety $H(1,q^2)$, or a line.

A solid lies on the Hermitian variety, or intersects it in either a non-singular Hermitian variety $H(3,q^2)$, a cone with vertex a point and base a non-singular Hermitian variety $H(2,q^2)$, a cone with vertex a line and base a non-singular Hermitian variety $H(1,q^2)$, or a plane.

So the intersection numbers of the set $\mathcal{K}$ with planes belong to

$$q^2+1, q^3+1, q^3+q^2+1, q^4+q^2+1,$$

and the intersection numbers of the set $\mathcal{K}$ with solids belong to

$$q^4+q^2+1, q^5+q^2+1, q^5+q^3+q^2+1, q^5+q^4+q^2+1, q^6+q^4+q^2+1.$$

Call a plane, a solid or a line intersecting the set $\mathcal{K}$ in i points an *i-plane*, *i-solid* or *i-line*. A plane intersecting the set $\mathcal{K}$ in q^4+q^2+1 points will be called a *full* plane, a solid intersecting the set $\mathcal{K}$ in $q^6+q^4+q^2+1$ points will be called a *full* solid, and a line intersecting the set $\mathcal{K}$ in q^2+1 points will be called a *full* line.

Lemma 5.4.14 *A (q^4+q^2+1)-solid Π intersects the set $\mathcal{K}$ in a full plane.*

Proof Suppose some line L in Π does not intersect $\mathcal{K}$. Consider all planes through L inside Π. Then at least $(q^2+1)^2$ points are contained in $\Pi \cap \mathcal{K}$, a contradiction. Hence all lines in Π are blocked by the set $\mathcal{K}$. Theorem 1.4.8 implies that $\Pi \cap \mathcal{K}$ is a plane. □

Lemma 5.4.15 *A $(q^5+q^3+q^2+1)$-solid Π does not contain full planes nor (q^2+1)-planes.*

Proof Let $H_1 = q^2+1$, $H_2 = q^3+1$, $H_3 = q^3+q^2+1$, $H_4 = q^4+q^2+1$ and $x = q^5+q^3+q^2+1$. Call the number of H_1-, H_2-, H_3- and H_4-planes inside Π, a, b, c and t respectively. It will be shown that the parameters a and t have to be zero.

By counting the total number of planes in a solid, the incident pairs (p,α), where p is a point of $\mathcal{K}$ and α a plane of Π, and the triples (p,r,α)

where p and r are distinct points of $\mathcal{K}$ and α is a plane in Π containing p and r, in two ways, the following equations are obtained.

$$a+b+c=\frac{q^8-1}{q^2-1}-t,$$

$$aH_1+bH_2+cH_3=x\frac{q^6-1}{q^2-1}-tH_4,$$

$$aH_1(H_1-1)+bH_2(H_2-1)+cH_3(H_3-1)=x(x-1)\frac{q^4-1}{q^2-1}-tH_4(H_4-1).$$

Solving these equations yields $a=-t(q^2-q+1)$, hence $t=0=a$. □

Lemma 5.4.16 *A* (q^5+q^2+1)*-solid* Π *contains at most* q *full planes. If it contains* q *full planes, then there are no* (q^3+q^2+1)*-planes contained in* Π*. Furthermore, a* (q^5+q^2+1)*-solid always contains* (q^2+1)*-planes.*

Proof Denote the number of full planes inside Π by t as above. Using the same counting techniques as above we find $a=q^3-tq^2+tq-t+1$, $b=q^3(q^3+t)$ and $c=q^4-(t+1)q^3+(1+t)q^2-tq$. Since c has to be positive, it follows that $t\leq q$. We see that $a>0$. □

Lemma 5.4.17 *If a* (q^5+q^2+1)*-solid* Π *does not contain lines intersecting* $\mathcal{K}$ *in* q *points then it does not contain full planes.*

Proof Suppose Π does contain a full plane π. By the proof of the previous lemma there exist (q^3+1)-planes in Π. Consider a (q^3+1)-plane α in Π and a point $p\in\mathcal{K}\cap\alpha$ outside π and a line L in α passing through p. If $|L\cap\mathcal{K}|=x$, the following inequality holds.

$$(q^2+1)(q^3+1-x)+x\leq q^5+q^2+1.$$

Hence $x\geq q$. Since we assume there are no q-lines in Π, it follows that $x\geq q+1$. Considering all lines through p inside α yields a contradiction. □

Lemma 5.4.18 *A* $(q^5+q^4+q^2+1)$*-solid contains* $q+1$ *full planes.*

Proof Apply exactly the same method as in the proofs of the lemmas above. Hence, $a=q^3+q^2-q-1-t(q^2-q+1)$ and $b=q^3(-q+t-1)$. The first equation implies $t\leq q+1$, while the second implies $t\geq q+1$, hence $t=q+1$.
□

Lemma 5.4.19 *A* $(q^5+q^4+q^2+1)$*-solid* Π *is a union of* $q+1$ *full planes all passing through the same line* L*.*

Proof Suppose there does not pass a full plane lying in Π through p, with $p \in \mathcal{K} \cap \Pi$. Consider an arbitrary line L in Π passing through p and intersecting $\mathcal{K}$ in x points. Consider all planes through L inside Π. Then at most

$$(q^2+1)(q^3+q^2+1-x)+x = q^5+q^4+q^2+1+q^3+(1-x)q^2$$

points belong to $\Pi \cap \mathcal{K}$. This implies $x \leq q+1$. Consider all lines through p in a fixed plane β of Π through p; they all contain at most $q+1$ points of $\mathcal{K}$, hence β contains at most $1+(q^2+1)q = q^3+q+1$, so at most q^3+1 points of the set $\mathcal{K}$. Hence all planes in Π through p would contain at most q^3+1 points. Consider again an arbitrary line L in Π passing through p and repeat the argument above. We get the inequality

$$(q^2+1)(q^3+1-x)+x \geq q^5+q^4+q^2+1.$$

This yields a contradiction. Hence through all points $p \in \Pi \cap \mathcal{K}$ there passes a full plane belonging to Π. So Π intersects $\mathcal{K}$ in a union of $q+1$ full planes. Since $|\Pi \cap \mathcal{K}| = q^5+q^4+q^2+1$, these planes all intersect in the same line, otherwise there would be fewer points contained in $\Pi \cap \mathcal{K}$. □

Lemma 5.4.20 *If a 4-space Δ is such that $|\Delta \cap \mathcal{K}| = (q^2+1)(q^5+1)$, then $\Delta \cap \mathcal{K}$ is a non-singular Hermitian variety $H(4,q^2)$.*

Proof Let $S_1 = q^4+q^2+1$, $S_2 = q^5+q^2+1$, $S_3 = q^5+q^3+q^2+1$, $S_4 = q^5+q^4+q^2+1$ $S_5 = q^6+q^4+q^2+1$ and $x = q^7+q^5+q^2+1$. Call the number of S_1-, S_2-, S_3-,S_4- and S_5-solids inside Π, a, b, c, t_1 and t_2, respectively. It will be shown that the parameters t_1 and t_2 have to be zero.

Then by counting the total number of solids in a 4-space, the incident pairs (p,Π), where p is a point of $\mathcal{K}$ and Π a solid of Δ, and the triples (p,r,Π) where p and r are distinct points of $\mathcal{K}$ and Π is a solid in Δ containing p and r, in two ways, we obtain the following equations

$$a+b+c = \frac{q^{10}-1}{q^2-1} - t_1 - t_2,$$

$$aS_1+bS_2+cS_3 = x\frac{q^8-1}{q^2-1} - t_1S_4 - t_2S_5,$$

$$aS_1(S_1-1)+bS_2(S_2-1)+cS_3(S_3-1) = x(x-1)\frac{q^6-1}{q^2-1} - t_1S_4(S_4-1) - t_2S_5(S_5-1).$$

Solving these equations yields $a = -\frac{t_2(q^4-q^3+2q^2-q+1)+t_1}{q^2-q+1}$. Hence, $t_1 = t_2 = a = 0$. So the only solids that occur in Δ are (q^5+q^2+1)- and $(q^5+q^3+q^2+1)$-solids. If Δ contains a full plane π, then consider all solids in Δ through π. We get at most

$$(q^2+1)(q^5+q^3-q^4)+q^4+q^2+1$$

points, a contradiction. Hence the intersection numbers with planes and solids are those of Theorem 5.4.2, so $\Delta \cap \mathcal{K}$ is a non-singular Hermitian variety $H(4, q^2)$. □

Lemma 5.4.21 *If a 4-space Δ contains a line L intersecting $\mathcal{K}$ in q points, then this line cannot be contained in a (q^2+1)-plane of Δ. Furthermore, if L is only contained in (q^3+1)-planes of Δ, then $|\mathcal{K} \cap \Delta| = q^7 + q^4 + q^2 + 1$.*

Proof Clearly L cannot be contained in full planes of Δ. First suppose that L is only contained in (q^3+1)-planes of Δ. Then $\mathcal{K} \cap \Delta = (q^4+q^2+1)(q^3+1-q)+q = q^7+q^4+q^2+1$. Next suppose that L is contained in a (q^2+1)-plane α of Δ. By Lemma 5.4.15, α is not contained in a $(q^5+q^3+q^2+1)$-solid of Δ. Since (q^4+q^2+1)- and $(q^5+q^4+q^2+1)$-solids do not contain lines intersecting $\mathcal{K}$ in q points, all solids through α in Δ are (q^5+q^2+1)-solids. Hence $|\Delta \cap \mathcal{K}| = (q^2+1)q^5 + (q^2+1)$. This is impossible by the previous lemma. □

Lemma 5.4.22 *In a 4-space Δ, a (q^3+q^2+1)-plane β does not contain a q-line.*

Proof By the previous lemma, a q-line cannot be contained in a (q^2+1)-plane. If in some 4-space Δ, a q-line L lies in a (q^5+q^2+1)-solid Π then an easy counting learns that inside Π, L is only contained in (q^3+1)-planes. Hence if a (q^3+q^2+1)-plane β lying in Δ contains L, then β is not contained in (q^5+q^2+1)-solids of Δ. Since $(q^5+q^4+q^2+1)$-solids do not contain q-lines, in this case

$$|\mathcal{K} \cap \Delta| = (q^2+1)q^5 + q^3 + q^2 + 1 = q^7 + q^5 + q^3 + q^2 + 1.$$

Suppose Δ contains a (q^2+1)-plane α and look at all solids through α inside Δ. A $(q^5+q^3+q^2+1)$-solid and a full solid do not contain (q^2+1)-planes, hence

$$aq^4 + bq^5 + (q^2+1-a-b)(q^5+q^4) + q^2 + 1 = q^7 + q^5 + q^3 + q^2 + 1.$$

Solving this equation yields $a = \frac{q^3+(1-b)q-1}{q^2}$, but this is never an integer, contradiction. Hence Δ does not contain (q^2+1)-planes. Since (q^4+q^2+1)-, (q^5+q^2+1)- and $(q^5+q^4+q^2+1)$-solids all contain (q^2+1)-planes, these solids do not occur in Δ.

Consider a $(q^5+q^3+q^2+1)$-solid in Δ. Such a solid contains (q^3+1)- and (q^3+q^2+1)-planes. Consider all solids through a (q^3+1)-plane inside Δ. By the previous all these solids are $(q^5+q^3+q^2+1)$-solids. Next, consider all solids through a (q^3+q^2+1)-plane inside Δ. Again these are all $(q^5+q^3+q^2+1)$-solids. This yields a contradiction since we get a different number of points in the respective cases. □

Lemma 5.4.23 *A 4-space Δ intersecting $\mathcal{K}$ in $q^7+q^4+q^2+1$ points contains at most q full solids. Furthermore, if Δ contains q full solids, then it contains no $(q^5+q^4+q^2+1)$-solids.*

Proof Let $S_1 = q^4+q^2+1$, $S_2 = q^5+q^2+1$, $S_3 = q^5+q^3+q^2+1$, $S_4 = q^5+q^4+q^2+1$ $S_5 = q^6+q^4+q^2+1$ and $x = q^7+q^4+q^2+1$. Call the number of S_1-, S_2-, S_3-,S_4- and S_5-solids inside Π, a, b, c, t_1 and t_2, respectively. The parameters t_1 and t_2 will be used in the calculations.

Then by counting the total number of solids in a 4-space, the incident pairs (p, Π), where p is a point of $\mathcal{K}$ and Π a solid of Δ, and the triples (p, r, Π) where p and r are distinct points of $\mathcal{K}$ and Π is a solid in Δ containing p and r, in two ways, one obtains the following equations

$$a+b+c = \frac{q^{10}-1}{q^2-1} - t_1 - t_2,$$

$$aS_1 + bS_2 + cS_3 = x\frac{q^8-1}{q^2-1} - t_1S_4 - t_2S_5,$$

$$aS_1(S_1-1)+bS_2(S_2-1)+cS_3(S_3-1) = x(x-1)\frac{q^6-1}{q^2-1} - t_1S_4(S_4-1) - t_2S_5(S_5-1).$$

Solving this yields $c = \frac{(q^4-(q^3-q^2)(1+t_2)-qt_2-t_1)q^3}{q^2-q+1}$. Since c must be non-negative, the proof is finished. □

Lemma 5.4.24 *Suppose all lines intersect $\mathcal{K}$ in 1, q, $q+1$ or q^2+1 points inside a (q^3+1)-plane α.*

(i) *If at least 2 lines in α intersect $\mathcal{K}$ in q^2+1 points, then α intersects $\mathcal{K}$ in a cone with vertex a point and base a line intersecting in $\mathcal{K}$ in q points.*

(ii) *If there is no line intersecting $\mathcal{K}$ in q points contained in α, then α intersects $\mathcal{K}$ in a unital.*

(iii) *If there is a line intersecting $\mathcal{K}$ in q points contained in α, then there is also a full line is contained in α.*

Proof (i) Assume that α contains more than one full line, so at least two, say L and M. These lines intersect in a point r. Take an arbitrary point p on L or M different from r. All lines through p inside α different from L or M intersect $\mathcal{K}$ in q points otherwise one gets more than $1+q^2+q^2(q-1) = q^3+1$ points. Consider now a point s in $\mathcal{K}\cap\alpha$ not lying on L or M. All lines through s inside α not through r intersect $\mathcal{K}$ in q points. Hence the line rs is a full line. Hence, the point r is collinear with all other points, proving our claim. (ii) and (iii) follow easily using standard counting techniques as in Lemma 5.4.23. □

Lemma 5.4.25 *If a 4-space Δ contains a line L intersecting $\mathcal{K}$ in q points, then it intersects $\mathcal{K}$ in $q^7+q^4+q^2+1$ points. Furthermore all lines in Δ intersect $\mathcal{K}$ in 1, q, $q+1$ or q^2+1 points and (q^3+q^2+1)-planes in Δ do not contain q-lines.*

Proof By Lemma 5.4.21 and Lemma 5.4.22, L is only contained in (q^3+1)-planes inside Δ. Then Lemma 5.4.21 shows that $|\Delta\cap\mathcal{K}| = q^7+q^4+q^2+1$. Consider all solids through a (q^3+1)-plane of Δ inside Δ. Then one gets at least

$$(q^2+1)(q^5+q^2-q^3)+q^3+1 = q^7+q^4+q^2+1$$

points. Hence, a (q^3+1)-plane of Δ is only contained in (q^5+q^2+1)-solids in Δ and not contained in a $(q^5+q^3+q^2+1)$-solid in Δ. This means there are no $(q^5+q^3+q^2+1)$-solids inside Δ, since by Lemma 5.4.15 such solids contain (q^3+1)-planes.

Consider a (q^2+1)-plane in Δ. If such a plane is not contained in a (q^4+q^2+1)-solid of Δ, then at least $(q^2+1)(q^5)+q^2+1$ points are contained in $\mathcal{K}\cap\Delta$, a contradiction. Hence (q^2+1)-planes contained in Δ intersect $\mathcal{K}$ in a line by Lemma 5.4.14.

Consider a (q^3+q^2+1)-plane β in Δ and all solids through it inside Δ. By Lemma 5.4.14, β is not contained in a (q^4+q^2+1)-solid, clearly β cannot be contained in a full solid and by the previous paragraph there are no $(q^5+q^3+q^2+1)$-solids inside Δ. Then counting yields there passes exactly one $(q^5+q^4+q^2+1)$-solid through β in Δ. Hence if a point p of $\mathcal{K}$ in Δ does belong to a (q^3+q^2+1)-plane of Δ, then there is a full plane through p in Δ by Lemma 5.4.19. Suppose there is a point p of $\mathcal{K}$ in Δ such that there does not pass a full plane through p in Δ. Then also no (q^3+q^2+1)-plane passes through p in Δ. Consider a line through p in Δ that contains x points of $\mathcal{K}$. This yields the following inequality

$$(q^4+q^2+1)(q^3+1-x)+x \geq q^7+q^4+q^2+1.$$

Hence $x\leq q$. Consider all lines through p inside a fixed plane π through p lying in Δ. Then π contains at most $(q^2+1)(q-1)+1$ points, hence π should be a (q^2+1)-plane, but such a plane contains a full line, a contradiction. Hence through all points $p\in\mathcal{K}\cap\Delta$, there passes a full plane. Hence it follows that a (q^5+q^2+1)-solid of Δ is the union of full lines.

In a (q^4+q^2+1)-, a $(q^5+q^4+q^2+1)$-, and a full solid of Δ, all lines intersect $\mathcal{K}$ in 1, $q+1$ or q^2+1 points. Hence if a line in Δ does not intersect $\mathcal{K}$ in 1, $q+1$ or q^2+1 points, then it lies in a (q^5+q^2+1)-solid Π inside Δ since there are no $(q^5+q^3+q^2+1)$-solids inside Δ.

Consider a point $p\in\mathcal{K}\cap\Pi$. Consider a line L through p in Π containing x points of $\mathcal{K}$, where x is different from 1, $q+1$ and q^2+1. Consider all planes through L inside Π. Assume, by way of contradiction, that L is contained in a (q^3+q^2+1)-plane of Δ. As such a plane is contained in one $(q^5+q^4+q^2+1)$-solid of Δ, we have $x \in \{1, q+1, q^2+1\}$ by Lemma 5.4.19, a contradiction. Hence, all planes of Π containing L are (q^3+1)-planes. This implies

$$(q^2+1)(q^3+1-x)+x = q^5+q^2+1.$$

Hence $x = q$, so all lines in Δ intersect $\mathcal{K}$ in 1, q, $q+1$ or q^2+1 points. □

5.4.3 Case 1: There is no line intersecting $\mathcal{K}$ in q points

In this section it is assumed that no line intersects the set $\mathcal{K}$ in q points. Define a point-line geometry $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathbf{I})$, where the points of P are the points of $\mathcal{K}$, where the lines of $\mathcal{B}$ are the full lines and where incidence is containment.

Theorem 5.4.26 *The geometry $\mathcal{S}$ is a Shult space.*

Proof Consider a point p of $\mathcal{S}$ and a line L of $\mathcal{S}$, such that p and L are not incident. We prove the main axiom for the incidence relation of a Shult space, referring to it as the 1-or-all axiom; see Section 1.2 for the definition of a Shult space.

Consider the plane α generated by p and L and let Δ be a 4-dimensional subspace containing α. Several cases are distinguished.

By Lemma 5.4.17 all (q^5+q^2+1)-solids in Δ do not contain full planes.

1) Suppose there is a solid Π containing α in Δ that contains a full plane β. Then Π intersects $\mathcal{K}$ either in β, a $(q^5+q^4+q^2+1)$-solid, which is the union of $q+1$ full planes through a line M, or a full solid. In all cases the 1-or-all axiom holds.

2) Suppose Δ does not contain full planes. Then Δ also does not contain (q^4+q^2+1)- or $(q^5+q^4+q^2+1)$-solids. By Theorem 5.4.2 Δ intersects $\mathcal{K}$ in a non-singular Hermitian variety $H(4,q^2)$, hence the 1-or-all axiom holds.

3) Suppose Δ contains a full plane β, but no solid containing α inside Δ contains a full plane. Consider a solid Π in Δ containing β. If L belongs to Π then it is contained in a full plane lying in Π bringing us back to Case 1. So assume L and Π intersect in a point s. This point belongs to a full plane γ in Π, which might be equal to β. Consider the solid generated by p and γ. This solid is either a $(q^5+q^4+q^2+1)$-solid or a full solid. Inside this solid there is a full plane ψ that passes through p. If L intersects ψ we are back in Case 1, so assume $L \cap \psi = \emptyset$. Consider an arbitrary point $r \in L$ and the solid Π_r generated by r and ψ. This solid intersects $\mathcal{K}$ in a full solid or in a cone with vertex a line and base a line intersecting $\mathcal{K}$ in $q+1$ points. Hence the line rp intersects $\mathcal{K}$ in $q+1$ or q^2+1 points. Consider all lines through p inside α;

then the assumptions on the intersection sizes of planes with the set $\mathcal{K}$ imply that the 1-or-all axiom holds. $\square$

Theorem 5.4.27 *If $\mathcal{S}$ is non-degenerate, then it is a non-singular Hermitian variety in $\mathbf{PG}(n, q^2)$, $n \geq 4$.*

Proof If there exists a full plane, then $\mathcal{S}$ is a non-degenerate Shult space of finite rank at least 3, and since all lines contain at least three points by definition, $\mathcal{S}$ with all its subspaces is a polar space. By Theorem 1.2.1 it is a finite classical polar space and by looking at the intersection numbers, $\mathcal{S}$ is a non-singular Hermitian variety.

If there exists no full plane, then the previous arguments show we have proved that axiom (GQ3) for generalized quadrangles is satisfied for $\mathcal{S}$. Clearly, there is a point p through which there pass three lines of $\mathcal{S}$. Hence, $\mathcal{S}$ is a generalized quadrangle.

By Theorem 1.1.2, it is a classical one; going through the list of classical generalized quadrangles yields it is the non-singular Hermitian variety $H(4, q^2)$. $\square$

Suppose now that $\mathcal{S}$ is degenerate, so there exist points collinear with all other points. Such points are called *singular points.*

Lemma 5.4.28 *The singular points of $\mathcal{S}$ form a subspace Π_k of $\mathbf{PG}(n, q^2)$.*

Proof Take two singular points p and r of $\mathcal{S}$ and consider a point t lying on the line $L = pr$. We claim that t is a singular point. Since p and r are both singular, all the points of L belong to $\mathcal{S}$, so $t \in S$. Let $M \neq L$ be an arbitrary line through t and consider the plane α generated by L and M. If α intersects $\mathcal{S}$ in L then M intersects $\mathcal{S}$ in 1 point. If α contains a point n of $\mathcal{S}$ not belonging to L, then through n there pass at least two full lines in α since p and r are singular points. Since we have the 1-or-all axiom all lines through n in α are full lines. Hence α is a full plane and M is a line of $\mathcal{S}$. So every line through t intersects $\mathcal{S}$ either in 1 or in $q^2 + 1$ points. $\square$

Lemma 5.4.29 *If $\mathcal{S}$ contains singular points, then all lines not intersecting the subspace Π_k formed by the singular points, intersect $\mathcal{S}$ in 1, $q+1$, or q^2+1 points.*

Proof Consider a line L not intersecting Π_k. Take a singular point p and consider the plane generated by p and L. Since this plane contains either $q^2 + 1$, $q^3 + 1$, $q^3 + q^2 + 1$ or $q^4 + q^2 + 1$ points of $\mathcal{S}$ by assumption, the lemma is proved. $\square$

Lemma 5.4.30 *If $n-k-1 \geq 4$, then $\mathcal{S}$ is a cone with vertex a k-dimensional space and base a non-singular Hermitian variety.*

Proof If $\mathcal{S}$ is degenerate, then look at a complementary space $\mathbf{PG}(n-k-1, q^2)$ of the space Π_k. By assumption, this space does not contain singular points of $\mathcal{S}$. If $n-k-1 \geq 4$, then Theorem 5.4.27 shows that $\mathcal{S}$ intersects this space in a non-singular Hermitian variety, hence $\mathcal{S}$ is a cone with vertex a k-dimensional space and base a non-singular Hermitian variety. □

Now, consider all other cases one by one.

(a) If $n-k-1 = -1$, then $\mathcal{S}$ is the projective space $\mathbf{PG}(n, q^2)$.

(b) If $n-k-1 = 0$, then $\mathcal{S}$ is a hyperplane of $\mathbf{PG}(n, q^2)$.

(c) If $n-k-1 = 1$, then the complementary space is a line. If this line intersects $\mathcal{K}$ in one or in q^2+1 points, a contradiction. If it intersects $\mathcal{K}$ in $q+1$ points, it is the union of $q+1$ hyperplanes.

(d) If $n-k-1 = 2$, then the complementary space is a plane π. By Lemma 5.4.29 all lines intersect in 1, $q+1$ or q^2+1 points.

(1) Suppose that π intersects $\mathcal{S}$ in q^2+1 points. Since all lines are blocked, this intersection has to be a line, but then there are singular points in the base, a contradiction.

(2) Suppose that π intersects $\mathcal{S}$ in q^3+1 points. Since we assume no lines intersect $\mathcal{K}$ in q points, all lines in π intersect $\mathcal{S}$ in 1 or in $q+1$ points, hence π intersects $\mathcal{S}$ in a unital. Indeed, if there would be a full line L in π then consider a point p in $\pi \cap S$ not belonging to L, and consider all lines through p in π. At least $1+(q^2+1)q = q^3+q+1$ points would be contained in $\pi \cap \mathcal{S}$, a contradiction.

(3) Suppose that π intersects $\mathcal{S}$ in q^3+q^2+1 points. Since there is no line in π that intersects $\mathcal{K}$ in q points, the 1-axiom for generalized quadrangles is fulfilled. Hence some point $s \in S \cap \pi$ is collinear with all other points in $\mathcal{S} \cap \pi$ otherwise we have a generalized quadrangle fully embedded in π, which yields a contradiction. But then s is a singular point, which is impossible.

(e) If $n-k-1 = 3$, then the complementary space is a solid Π.

By assumption, the solid Π does not contain a line intersecting $\mathcal{S}$ in q points. If Π contains a full plane then by Lemmas 5.4.15 and 5.4.17 it is either a (q^4+q^2+1)-solid, a $(q^5+q^4+q^2+1)$-solid or a full solid. In all cases there are singular points in the base, a contradiction. Hence Π does not contain full planes. Then Lemma 5.4.1 implies that $\Pi \cap \mathcal{K} = H(3, q^2)$.

Theorem 5.4.31 *If a set $\mathcal{K}$ of points in $\mathbf{PG}(n, q^2)$, $n \geq 4$, contains no lines intersecting $\mathcal{K}$ in q points, and if the intersection numbers of $\mathcal{K}$ with planes and solids are also intersection numbers of planes and solids with a Hermitian variety in $\mathbf{PG}(n, q^2)$, then $\mathcal{K}$ is either*

(i) *the projective space* $\mathbf{PG}(n, q^2)$,

(ii) *a hyperplane in* $\mathbf{PG}(n, q^2)$,

(iii) *a Hermitian variety in* $\mathbf{PG}(n, q^2)$.

(iv) *a cone with vertex an* $(n-2)$*-dimensional space and base a line intersecting* $\mathcal{K}$ *in* $q+1$ *points.*

(v) *a cone with vertex an* $(n-3)$*-dimensional space and base a unital.*

5.4.4 Case 2: There is a line intersecting $\mathcal{K}$ in q points

In this section it is assumed that there is a line intersecting the set $\mathcal{K}$ in q points. Since every line M together with a q-line lie in a 4-space Δ, by Lemma 5.4.25 every line intersects the set $\mathcal{K}$ either in 1, q, $q+1$ or q^2+1 points. Consequently, by Theorem 1.4.8, a (q^2+1)-plane intersects $\mathcal{K}$ in a line. Again by Lemma 5.4.25 a line intersecting $\mathcal{K}$ in q points is only contained in (q^3+1)-planes. The following notations are introduced:

$$H_1(k) = \frac{q^{2k}-1}{q^2-1},$$

$$H_2(k) = q^{2k-1} + \frac{q^{2k-2}-1}{q^2-1},$$

$$H_3(k) = q^{2k-1} + \frac{q^{2k}-1}{q^2-1},$$

$$H_4(k) = \frac{q^{2k+2}-1}{q^2-1}.$$

Lemma 5.4.32 *Assume* $\mathcal{K}$ *is contained in* $\Pi_n = \mathbf{PG}(n, q^2)$.

(i) *Then* $|\mathcal{K}| = H_2(n)$.

(ii) *Next, consider any subspace* Π_l *of dimension* l *in* Π_n*, with* $l \geq 2$*. Then* $|\Pi_l \cap \mathcal{K}| \in \{H_1(l),\ H_2(l),\ H_3(l),\ H_4(l)\}$.

(iii) *If* $|\mathcal{K} \cap \Pi_l| = H_1(l)$*,* $l \geq 1$*, then* $\mathcal{K} \cap \Pi_l$ *is an* $(l-1)$*-dimensional space.*

(iv) *If* $|\mathcal{K} \cap \Pi_l| = H_3(l)$*,* $l \geq 1$*, then* $\mathcal{K} \cap \Pi_l$ *is a union of* $q+1$ $(l-1)$*-dimensional spaces containing a common space* Π_{l-2} *of dimension* $l-2$.

(v) *If* $|\mathcal{K} \cap \Pi_l| = H_4(l)$*,* $l \geq 1$*, then* $\mathcal{K} \cap \Pi_l$ *is the* l*-dimensional space* Π_l.

(vi) *If in a space of dimension $l+2$ which intersects $\mathcal{K}$ in $H_2(l+2)$ points an l-dimensional space Π_l is only contained in $(l+1)$-dimensional spaces which intersect $\mathcal{K}$ in $H_2(l+1)$ points, then Π_l intersects $\mathcal{K}$ in $H_2(l)$ points.*

Proof (i) Since a q-line of Π_n is only contained in (q^3+1)-planes, necessarily

$$|\Pi_n \cap \mathcal{K}| = (q^3+1-q)\frac{q^{2n-2}-1}{q^2-1} + q = H_2(n).$$

(ii) Consider a (q^3+1)-plane α and all solids through α inside Π_n. By Lemma 5.4.14 and Lemma 5.4.19, α can only be contained in (q^5+q^2+1)- and $(q^5+q^3+q^2+1)$-solids. An elementary counting yields that only the former occurs. This also implies that there are no $(q^5+q^3+q^2+1)$-solids contained in Π_l, since such solids always contain (q^3+1)-planes by Lemma 5.4.15.

If a (q^3+1)-plane α is contained in Π_l, then since all solids through α inside Π_l are (q^5+q^2+1)-solids, we find that $|\Pi_l \cap \mathcal{K}|$ is equal to

$$\frac{q^{2l-4}-1}{q^2-1}(q^5+q^2-q^3)+q^3+1 = H_2(l).$$

If there is no (q^3+1)-plane contained in Π_l, then by Lemma 5.4.25 all lines intersect $\mathcal{K}$ in $1, q+1$ or q^2+1 points. Now for $l \geq 4$, Lemma 5.4.31 proves (iii), (iv) and (v) of this Lemma.

For $l=3$, (iii) is the statement of Lemma 5.4.14, (iv) is the statement of Lemma 5.4.19, and (v) is obvious.

To prove (vi), denote the number of points in $\Pi_l \cap \mathcal{K}$ by x. Then we get the following equation

$$(q^2+1)(q^{2l+1}+\frac{q^{2l}-1}{q^2-1}-x)+x = q^{2l+3}+\frac{q^{2l+2}-1}{q^2-1}.$$

Solving yields $x = H_2(l)$. □

Theorem 5.4.33 *If there is a line intersecting $\mathcal{K}$ in q points, then the set $\mathcal{K}$ is a cone with vertex an $(n-3)$-dimensional space and base a (q^3+1)-plane.*

Proof (1) Suppose $\mathcal{K}$ does not contain a hyperplane. In this case, there are only three types of hyperplane intersections by Lemma 5.4.32. With a standard counting technique as in Lemma 5.4.23 we can determine that there are exactly q^3+1 hyperplanes which intersect $\mathcal{K}$ in a space of codimension 2 and there exists a hyperplane Π_{n-1} which intersects $\mathcal{K}$ in $H_3(n-1)$ points, and by Lemma 5.4.32 (iv) Π_{n-1} intersects $\mathcal{K}$ in a union of $q+1$ $(n-2)$-dimensional spaces

$\Pi_{n-2,i}$ through a common $(n-3)$-dimensional space Π_{n-3}. Let Π'_{n-1} be one of the (q^3+1) hyperplanes which intersect $\mathcal{K}$ in an $(n-2)$-dimensional space Π_{n-2}. Every space $\Pi_{n-2,i}$ intersects Π_{n-1} in at least an $(n-3)$-dimensional space which has to be completely contained in Π_{n-2}. This implies that Π_{n-2} contains Π_{n-3} completely. Because, either there are two $\Pi_{n-2,i}$ which share the same $(n-3)$-dimensional space with Π_{n-2}, which then must be Π_{n-3} or all $\Pi_{n-2,i}$ share different $(n-3)$-dimensional spaces with Π_{n-2}. But this implies that Π_{n-2} is completely contained in Π_{n-1}, so Π_{n-3} again is contained in Π_{n-2}. Hence, in this case, $\mathcal{K}$ is a union of q^3+1 spaces of dimension $(n-2)$ which have an $(n-3)$-dimensional space in common. Since for such a cone, the size is $H_2(n)$, which is also the size of $\mathcal{K}$, $\mathcal{K}$ is necessarily equal to this cone.

(2) Suppose $\mathcal{K}$ does contain a hyperplane Π_{n-1}. Consider a point $p \notin \Pi_{n-1}$. We claim that p is contained in an $(n-2)$-dimensional space Π_{n-2} which is completely contained in $\mathcal{K}$. If this would not be the case, then all hyperplanes through p would intersect $\mathcal{K}$ in $H_2(n-1)$ points, since cases (iii), (iv) and (v) of Lemma 5.4.32 are unions of $(n-2)$-dimensional spaces and reasoning inductively using (vi) of Lemma 5.4.32 all lines through p would intersect $\mathcal{K}$ in q points, a contradiction.

The space Π_{n-2} through p intersects Π_{n-1} in an $(n-3)$-dimensional space Π_{n-3}. Take an arbitrary point $r \in \Pi_{n-3}$, a point $s \in \mathcal{K}\backslash(\Pi_{n-1} \cup \Pi_{n-2})$, and a point t in $\Pi_{n-2}\backslash\Pi_{n-3}$. Consider the plane π_{rst} generated by r, s and t. This plane intersects Π_{n-1} in a full line. Hence, this plane contains at least two full lines. If π_{rst} is a (q^3+1)-plane, then due to Lemma 5.4.24 the line rs is a full line. If π_{rst} is a (q^3+q^2+1)-plane, then π_{rst} intersects $\mathcal{K}$ in $q+1$ lines through a common point. Indeed, since π_{rst} contains already two full lines, it is easy to deduce from the fact that all lines intersect $\mathcal{K}$ in 1, $q+1$ or q^2+1 points that every point is collinear with the intersection point of these two full lines. This finishes the proof. □

In the case that there are no lines intersecting $\mathcal{K}$ in q points, Theorem 5.4.31 leads us to cases (i), (ii), (iii), (iv) where the base intersects $\mathcal{K}$ in $q+1$ points and (v) of Theorem 5.2.8. If there is a line intersecting $\mathcal{K}$ in q points, Theorem 5.4.33 shows that $\mathcal{K}$ is a cone with vertex an $(n-3)$-dimensional space and base a q^3+1-plane α. The plane α necessarily contains a full line by Lemma 5.4.24. If there is exactly one full line contained in α we have (vi) of Theorem 5.2.8 and if there are at least two full lines contained in α we are lead to (iv) of Theorem 5.2.8 where the base contains q points.

5.5 Proof of Theorem 5.2.10

Below we will handle the four different types of polar spaces one by one. The basic idea is to study certain structures in the dual projective space. However the elliptic and parabolic case will turn out to be harder than the other two cases, and especially the parabolic case will be more complex and interesting (this is basically due to the fact that there are more intersections with respect to hyperplanes).

Remark 5.5.1 *Throughout this section we will use the usual notations for non-singular polar spaces. A cone with vertex a point p or a line L over a non-singular polar space, e.g. over a $Q(2n, q)$ will be denoted by $pQ(2n, q)$, respectively $LQ(2n, q)$ (a small letter will always indicate that the vertex of the cone is a point, while a capital letter will indicate that the vertex is a line). With these conventions, the notations will always immediately tell whether the considered polar space is singular or non-singular. Only in the statements of our lemmas and theorems we will explicitly mention the (non-)singular character of the considered polar spaces.*

From here on we always assume that we work in a projective space of dimension at least four and that $q > 2$.

5.5.1 Hermitian varieties

Let us first recall the intersections of a Hermitian variety $H(n, q^2)$ in $\mathbf{PG}(n, q^2)$ with hyperplanes and subspaces of codimension 2. A hyperplane intersects $H(n, q^2)$ either in $H(n-1, q^2)$ or in a cone $pH(n-2, q^2)$. A subspace of codimension 2 intersects $H(n, q^2)$ either in $H(n-2, q^2)$, in a cone $pH(n-3, q^2)$ or in a cone $LH(n-4, q^2)$. Hence the intersection numbers with hyperplanes in $\mathbf{PG}(n, q^2)$ are

$$H_1 = \frac{(q^n - (-1)^n)(q^{n-1} + (-1)^n)}{q^2 - 1}, H_2 = 1 + \frac{q^2 (q^{n-1} + (-1)^n)(q^{n-2} - (-1)^n)}{q^2 - 1}.$$

and the intersection numbers with subspaces of codimension 2 are

$$C_1 = \frac{(q^{n-1} + (-1)^n)(q^{n-2} - (-1)^n)}{q^2 - 1}, C_2 = 1 + \frac{q^2 (q^{n-2} - (-1)^n)(q^{n-3} + (-1)^n)}{q^2 - 1},$$

$$C_3 = 1 + q^2 + \frac{q^4 (q^{n-3} + (-1)^n)(q^{n-4} - (-1)^n)}{q^2 - 1}.$$

From now on, let $\mathcal{K}$ be a point set in $\mathbf{PG}(n, q^2)$ having the above intersection numbers with respect to hyperplanes and subspaces of codimension 2. We want to prove that $\mathcal{K}$ is the point set of a Hermitian variety $H(n, q^2)$. We will call subspaces intersecting $\mathcal{K}$ in a given number m of points, *subspaces of type m*. For obvious reasons a hyperplane intersecting $\mathcal{K}$ in H_2 points will also be called a *tangent hyperplane*.

Lemma 5.5.2 *The set $\mathcal{K}$ contains $|H(n, q^2)|$ points. There are $|H(n, q^2)|$ tangent hyperplanes.*

Proof We count in two ways the pairs (p, α) where p is a point of $\mathcal{K}$ and α a hyperplane such that $p \in \alpha$, respectively the triples (p, r, α) where $p \neq r$ are points of $\mathcal{K}$ and α a hyperplane such that $p, r \in \alpha$. Denote by h_1 the number of hyperplanes intersecting $\mathcal{K}$ in H_1 points and by x the size of $\mathcal{K}$. We obtain:

$$x\frac{q^{2n}-1}{q^2-1} = h_1H_1 + (\frac{q^{2n+2}-1}{q^2-1} - h_1)H_2, \tag{5.1}$$

and

$$x(x-1)\frac{q^{2n-2}-1}{q^2-1} = h_1H_1(H_1-1) + (\frac{q^{2n+2}-1}{q^2-1} - h_1)H_2(H_2-1). \tag{5.2}$$

Solving the first equation for h_1 and substituting this value in the second equation yields a quadratic equation in x. The solutions are $x_1 = |H(n, q^2)|$ and x_2, which is a tedious expression in q, however easily computed with any computer algebra package.

We show the latter solution is impossible. So suppose by way of contradiction that the set $\mathcal{K}$ contains x_2 points. Consider a subspace Π of codimension 2 intersecting the set $\mathcal{K}$ in C_i points. Denote by k_i the number of non-tangent hyperplanes containing Π. We obtain the following equation:

$$k_i(H_1 - C_i) + (q^2 + 1 - k_i)(H_2 - C_i) + C_i = x_2.$$

Solving this equation in k_i for $i = 1, 2, 3$ yields respectively

$$k_1 = \frac{q^n - (-1)^n(q^2 - q + 1)}{q^{n-1} - (1)^n};\ k_2 = \frac{2\,q^n - (-1)^n(q^2+1)}{q^{n-1} - (-1)^n};$$

$$k_3 = -\frac{q^{n+1} - 2\,q^n + (-1)^n}{q^{n-1} - (-1)^n}.$$

These are not integers if $n > 2$, proving x_2 cannot occur.

The second assertion follows by substituting $x = |H(n, q^2)|$ in Equation (5.1). □

Remark 5.5.3 *Notice that for $n = 2$, we would obtain integers and in that case we have $x_2 = q^2 + q + 1$, that is, exactly the number of points of a Baer subplane, which was to be expected.*

Lemma 5.5.4 *Through a space of codimension 2 of type C_1, C_2, C_3, there pass respectively $T_1 = q + 1$, $T_2 = 1$, $T_3 = q^2 + 1$ tangent hyperplanes.*

Proof Let Π be a codimension 2-space intersecting $\mathcal{K}$ in C_i points and let T_i denote the number of tangent hyperplanes containing Π. We obtain the following equation:

$$C_i + T_i(H_2 - C_i) + (q^2 + 1 - T_i)(H_1 - C_i) = |\mathcal{K}|.$$

Solving the equation in T_i for $i = 1, 2, 3$ yields the result. □

Lemma 5.5.5 *Each tangent hyperplane contains A_i subspaces of codimension 2 intersecting $\mathcal{K}$ in C_i points, where*

$$A_1 = q^{2n-2},\ A_2 = \frac{q^{n-2}\left(q^{n-1} + (-1)^n\right)}{q+1},$$

$$A_3 = \frac{(q^{n-1} + (-1)^n)(q^{n-2} - (-1)^n)}{q^2 - 1}.$$

.

Proof Consider any tangent hyperplane Π. Denote by A_i the number of codimension 2 subspaces of type C_i contained in Π. Then

$$\sum_i A_i = \frac{q^{2n} - 1}{q^2 - 1}.$$

We count in two ways the pairs (p, Δ), $p \in \Delta \subset \Pi$, with p a point of $\mathcal{K}$ and Δ a subspace of codimension 2. We obtain

$$\sum_i A_i C_i = H_2 \frac{q^{2n-2} - 1}{q^2 - 1}.$$

Next we count in two ways the triples (p, r, Δ), with $p, r \in \Delta \subset \Pi$, with $p \neq r$ points of $\mathcal{K}$ and Δ a subspace of codimension 2. We obtain

$$\sum_i A_i C_i (C_i - 1) = H_2(H_2 - 1) \frac{q^{2n-4} - 1}{q^2 - 1}.$$

The obtained system of three linear equations in A_1, A_2 and A_3 can easily be solved, yielding the desired result. □

Lemma 5.5.6 *Each point of $\mathcal{K}$ is contained in H_2 tangent hyperplanes, while each point not in $\mathcal{K}$ is contained in H_1 tangent hyperplanes.*

Proof We need to show that each point of $\mathcal{K}$ is contained in H_2 tangent hyperplanes. Set $\mathcal{K} = \{p_1, \cdots, p_{|H(n,q^2)|}\}$. Let a_i denote the number of tangent hyperplanes containing the point p_i. Counting pairs (p, τ), $p \in \mathcal{K}$, $p \in \tau$, τ a tangent hyperplane, we obtain:

$$\sum_i a_i = |H(n,q^2)|H_2. \tag{5.3}$$

Next we count triples (p, τ_1, τ_2), $p \in \mathcal{K}$, $p \in \tau_i$, τ_i a tangent hyperplane, $i = 1, 2$, $\tau_1 \neq \tau_2$. This yields the following equation:

$$\sum_i a_i(a_i - 1) = \left|H(n,q^2)\right| \left(\sum_j A_j(T_j - 1)C_j \right), \tag{5.4}$$

where as before T_i denotes the number of tangent hyperplanes containing a fixed codimension 2-space Π of type C_i and A_i is the number of codimension 2 subspaces of type C_i in a tangent hyperplane.

From Equations (5.3) and (5.4), we can compute

$$\left|H(n,q^2)\right| \sum_i a_i^2 - (\sum_i a_i)^2 = 0,$$

from which we deduce, using the variance trick, that a_i is a constant equal to H_2.

The second assertion is proved in a similar way. □

Denote by $\mathcal{H}$ the set of tangent hyperplanes of $\mathcal{K}$. Let $\delta : \mathbf{PG}(n,q^2) \rightarrow \mathbf{PG}(n,q^2)^D$ be any fixed chosen duality of $\mathbf{PG}(n,q^2)$.

Lemma 5.5.7 *The point set $\mathcal{K}' := \mathcal{H}^\delta$ is a $(1, q+1, q^2+1)$-set in $\mathbf{PG}(n,q^2)^D$.*

Proof As by Lemma 5.5.4, a codimension 2 subspace is contained in either 1, $q+1$ or q^2+1 tangent hyperplanes, applying δ immediately yields the result. □

Lemma 5.5.8 *The set $\mathcal{K}'$ is the point set of a non-singular Hermitian variety $H(n,q^2)$ in $\mathbf{PG}(n,q^2)^D$.*

Proof We will check the conditions of Theorem 5.2.2. Since every tangent hyperplane contains subspaces of type C_1 (by Lemma 5.5.5), we see that every point of $\mathcal{K}'$ is contained in lines intersecting $\mathcal{K}'$ in exactly $q+1$ points. Hence $\mathcal{K}'$ is non-singular. As $q > 2$ also the first condition is satisfied. Now assume there would be a plane π intersecting $\mathcal{K}'$ in a point set such that every line of π would intersect $\mathcal{K}' \cap \pi$ in $q+1$ or q^2+1 points. Then $\mathcal{K}' \cap \pi$ would be the complement of a maximal (q^2-q)-arc in π, implying that q^2-q divides q^2, a contradiction since $q > 2$. Consequently, also the second condition of Theorem 5.2.2 is satisfied and $\mathcal{K}'$ is the point set of a non-singular Hermitian variety in $\mathbf{PG}(n, q^2)$. □

Theorem 5.5.9 *The set $\mathcal{K}$ is the point set of a non-singular Hermitian variety $H(n, q^2)$.*

Proof Clearly, $\mathcal{K}'$ is a point set satisfying the same conditions on intersections with hyperplanes and subspaces of codimension 2 as $\mathcal{K}$ in $\mathbf{PG}(n, q^2)$. Since the tangent hyperplanes to $\mathcal{K}'$ are exactly those hyperplanes containing H_2 points of $\mathcal{K}'$, we find that if we apply the duality δ^{-1} to $\mathbf{PG}(n, q)^D$, the tangent hyperplanes to $\mathcal{K}'$ are mapped bijectively to the points of $\mathcal{K}$ (see Lemma 5.5.6). Hence, we can now apply Lemma 5.5.8 with $\mathcal{K}'$ in $\mathbf{PG}(n, q^2)^D$ replaced by $\mathcal{K}$ in $\mathbf{PG}(n, q^2)$. We conclude that $\mathcal{K}$ is the point set of a Hermitian variety $H(n, q^2)$. □

5.5.2 Hyperbolic quadrics

First of all let us recall what the intersections of a hyperbolic quadric $Q^+(2n+1, q)$ with hyperplanes and spaces of codimension 2 look like. A hyperplane can intersect $Q^+(2n+1, q)$ in $Q(2n, q)$ or in a cone $pQ^+(2n-1, q)$. A space of codimension 2 can intersect $Q^+(2n+1, q)$ either in $Q^-(2n-1, q)$, in a cone $pQ(2n-2, q)$, in $Q^+(2n-1, q)$ or in a cone $LQ^+(2n-3, q)$.

So the intersection numbers with hyperplanes are

$$H_1 = \frac{q^{2n}-1}{q-1},\ H_2 = 1 + q\frac{(q^n-1)(q^{n-1}+1)}{q-1}.$$

The intersection numbers with spaces of codimension 2 are

$$C_1 = \frac{(q^n+1)(q^{n-1}-1)}{q-1},\ C_2 = 1 + \frac{q\,(q^{2\,n-2}-1)}{q-1},$$

$$C_3 = \frac{(q^n-1)\,(q^{n-1}+1)}{q-1}, C_4 = 1 + q + \frac{q^2\,(q^{n-1}-1)\,(q^{n-2}+1)}{q-1}.$$

From now on let $\mathcal{K}$ be a set of points in $\mathbf{PG}(2n+1,q)$ having the same intersection numbers with hyperplanes and codimension 2-spaces as a $Q^+(2n+1,q)$. We want to prove that $\mathcal{K}$ is the point set of a hyperbolic quadric $Q^+(2n+1,q)$. We will call subspaces intersecting $\mathcal{K}$ in a given number m of points, *subspaces of type m*. For obvious reasons, a hyperplane intersecting $\mathcal{K}$ in H_2 points will also be called a *tangent hyperplane*.

Lemma 5.5.10 *The set $\mathcal{K}$ has size $|Q^+(2n+1,q)|$. Furthermore, there are $|Q^+(2n+1,q)|$ tangent hyperplanes.*

Proof We count in two ways the pairs (p,α), where p is a point of $\mathcal{K}$ and α a hyperplane such that $p \in \alpha$, respectively the triples (p,r,α) where $p \neq r$ are points of $\mathcal{K}$ and α a hyperplane such that $p,r \in \alpha$. Call h_1 the number of hyperplanes intersecting $\mathcal{K}$ in H_1 points and x the size of $\mathcal{K}$. This yields the following equations

$$h_1H_1 + (\frac{q^{2n+2}-1}{q-1} - h_1)H_2 = x\frac{q^{2n+1}-1}{q-1}, \tag{5.5}$$

$$h_1H_1(H_1-1) + (\frac{q^{2n+2}-1}{q-1} - h_1)H_2(H_2-1) = x(x-1)\frac{q^{2n}-1}{q-1}. \tag{5.6}$$

Solving h_1 in terms of x from the first equation and substituting this in the second equation yields a quadratic equation in x. The solutions are $x_1 = |Q^+(2n+1,q)|$ and x_2, which is, as in the Hermitian case, an easily computed but tedious expression in q.

We show that the latter solution cannot occur. So suppose the set $\mathcal{K}$ contains x_2 points. Consider a space Π of codimension 2 intersecting the set $\mathcal{K}$ in C_i points. Denote by k_i the number of non-tangent hyperplanes containing Π. Then we obtain

$$k_i(H_1 - C_i) + (q+1-k_i)(H_2 - C_i) + C_i = x_2.$$

Solving this equation in k_i for $i = 1,2,3,4$ yields

$$k_1 = 3 + \frac{q-1}{q^n+1},\ k_2 = q\frac{q^{n-1}+1}{q^n+1},$$

$$k_3 = \frac{2q^n+q+1}{q^n+1},\ k_4 = -\frac{q^{n+1}-2\,q^n-1}{q^n+1}.$$

These are not integers; the desired contradiction.

The second assertion follows by substituting $x = |Q^+(2n+1,q)|$ in Equation (5.5). □

Lemma 5.5.11 *Through a space of codimension 2 of type C_1, C_2, C_3, C_4, there pass respectively $T_1 = 0$, $T_2 = 1$, $T_3 = 2$ and $T_4 = q + 1$ tangent hyperplanes.*

Proof Let Π be a codimension 2 space intersecting $\mathcal{K}$ in C_i points and let T_i denote the number of tangent hyperplanes containing Π. We obtain the following equation:

$$C_i + T_i(H_2 - C_i) + (q + 1 - T_i)(H_1 - C_i) = |\mathcal{K}|.$$

Solving the equation in T_i for $i = 1, 2, 3, 4$ yields the result. □

Lemma 5.5.12 *Each tangent hyperplane contains A_i subspaces of codimension 2 intersecting $\mathcal{K}$ in C_i points, where*

$$A_1 = 0,\ A_2 = q^{n-1}(q^n - 1),\ A_3 = q^{2n},$$

$$A_4 = \frac{(q^n - 1)(q^{n-1} + 1)}{q - 1}.$$

Proof Consider any tangent hyperplane Π. By the previous lemma, $A_1 = 0$. Hence,

$$\sum_{i=2}^{4} A_i = \frac{q^{2n+1} - 1}{q - 1}.$$

We count in two ways the pairs (p, Δ), $p \in \Delta \subset \Pi$, with p a point of $\mathcal{K}$ and Δ a subspace of codimension 2. We obtain

$$\sum_{i=2}^{4} A_i C_i = H_2 \frac{q^{2n} - 1}{q - 1}.$$

Next we count in two ways the triples (p, r, Δ), with $p, r \in \Delta \subset \Pi$, with $p \neq r$ points of $\mathcal{K}$ and Δ a subspace of codimension 2. We obtain

$$\sum_{i=2}^{4} A_i C_i (C_i - 1) = H_2(H_2 - 1)\frac{q^{2n-1} - 1}{q - 1}.$$

The obtained system of three linear equations in A_2, A_3 and A_4 can easily be solved, yielding the desired result. □

Lemma 5.5.13 *Each point of $\mathcal{K}$ is contained in H_2 tangent hyperplanes, while each point not in $\mathcal{K}$ is contained in H_1 tangent hyperplanes.*

Proof We need to show that each point of $\mathcal{K}$ is contained in H_2 tangent hyperplanes. Set $\mathcal{K} = \{p_1, \cdots, p_{|Q^+(2n+1,q)|}\}$. Let a_i denote the number of tangent hyperplanes containing the point p_i. Counting pairs (p, τ), $p \in \mathcal{K}$, $p \in \tau$, τ a tangent hyperplane, we obtain:

$$\sum_i a_i = |Q^+(2n+1,q)|H_2. \tag{5.7}$$

Next we count triples (p, τ_1, τ_2), $p \in \mathcal{K}$, $p \in \tau_i$, τ_i a tangent hyperplane, $i = 1, 2$, $\tau_1 \neq \tau_2$. As before, T_i denotes the number of tangent hyperplanes containing a fixed codimension 2 space Π of type C_i. We obtain the following equation:

$$\sum_i a_i(a_i - 1) = \left|Q^+(2n+1,q)\right| \left(\sum_j A_j(T_j - 1)C_j \right). \tag{5.8}$$

From Equations (5.7) and (5.8), we can compute

$$\left|Q^+(2n+1,q)\right| \sum_i a_i^2 - (\sum_i a_i)^2 = 0,$$

from which we deduce that a_i is a constant equal to H_2.

The second assertion is proved in a similar way. □

Denote by $\mathcal{H}$ the set of tangent hyperplanes of $\mathcal{K}$. Let $\delta : \mathbf{PG}(2n+1,q) \to \mathbf{PG}(2n+1,q)^D$ be any fixed chosen duality of $\mathbf{PG}(2n+1,q)$.

Lemma 5.5.14 *The set $\mathcal{K}' := \mathcal{H}^\delta$ is the point set of a non-singular hyperbolic quadric $Q^+(2n+1,q)$ in $\mathbf{PG}(2n+1,q)^D$.*

Proof This is an immediate consequence of Lemma 5.5.11, Lemma 5.5.12 and Theorem 5.2.3. □

Theorem 5.5.15 *The set $\mathcal{K}$ is the point set of a non-singular hyperbolic quadric $Q^+(2n+1,q)$ in $\mathbf{PG}(2n+1,q)$, $q > 2$.*

Proof Clearly $\mathcal{K}'$ is a point set satisfying the same conditions on intersections with hyperplanes and subspaces of codimension 2 as $\mathcal{K}$ in $\mathbf{PG}(2n+1,q)$. Since the tangent hyperplanes to $\mathcal{K}'$ are exactly those hyperplanes containing H_2 points of $\mathcal{K}'$, we find that if we apply the duality δ^{-1} to $\mathbf{PG}(2n+1,q)^D$, the tangent hyperplanes to $\mathcal{K}'$ are mapped bijectively to the points of $\mathcal{K}$ (see Lemma 5.5.13). Hence, we can now apply Lemma 5.5.14 with $\mathcal{K}'$ in $\mathbf{PG}(2n+1,q)^D$ replaced by $\mathcal{K}$ in $\mathbf{PG}(2n+1,q)$. We conclude that $\mathcal{K}$ is the point set of a hyperbolic quadric $Q^+(2n+1,q)$. □

5.5.3 Elliptic quadrics

First of all, let us recall what the intersections of an elliptic quadric $Q^-(2n+1,q)$ with hyperplanes and spaces of codimension 2 look like. A hyperplane of $\mathbf{PG}(2n+1,q)$ can intersect $Q^-(2n+1,q)$ either in $Q(2n,q)$ or in a cone $pQ^-(2n-1,q)$.

A space of codimension 2 can intersect $Q^-(2n+1,q)$ either in $Q^+(2n-1,q)$, a cone $pQ(2n-2,q)$, $Q^-(2n-1,q)$ or a cone $LQ^-(2n-3,q)$.

So the intersection numbers with hyperplanes are

$$H_1 = \frac{q^{2n}-1}{q-1}, H_2 = 1 + q\frac{(q^n+1)(q^{n-1}-1)}{q-1}.$$

The intersection numbers with spaces of codimension 2 are

$$C_1 = \frac{(q^n-1)\,(q^{n-1}+1)}{q-1},\ C_2 = 1 + q\frac{(q^{2\,n-2}-1)}{q-1},$$

$$C_3 = \frac{(q^n+1)\,(q^{n-1}-1)}{q-1},\ C_4 = 1+q+q^2\frac{(q^{n-1}+1)\,(q^{n-2}-1)}{q-1}.$$

From now on, let $\mathcal{K}$ be a set of points in $\mathbf{PG}(2n+1,q)$, $n \geq 2$ having the same intersection numbers with hyperplanes and codimension 2 spaces as an elliptic quadric $Q^-(2n+1,q)$. We want to prove that $\mathcal{K}$ is the point set of a non-singular elliptic quadric. We will call subspaces intersecting $\mathcal{K}$ in a given number m of points, *subspaces of type m*. For obvious reasons, a hyperplane intersecting $\mathcal{K}$ in H_2 points will also be called a *tangent hyperplane.*

Lemma 5.5.16 *The set $\mathcal{K}$ has size $|Q^-(2n+1,q)|$. Furthermore, there are $|Q^-(2n+1,q)|$ tangent hyperplanes.*

Proof This is proved in a similar way as Lemma 5.5.10. □

Lemma 5.5.17 *Through a space of codimension 2 of type C_1, C_2, C_3, C_4, there pass respectively $T_1 = 0$, $T_2 = 1$, $T_3 = 2$ and $T_4 = q+1$ tangent hyperplanes.*

Proof This is completely analogous to the proof of Lemma 5.5.11. □

Lemma 5.5.18 *Each tangent hyperplane contains A_i subspaces of codimension 2 intersecting $\mathcal{K}$ in C_i points, where*

$$A_1 = 0,\ A_2 = q^{n-1}(q^n+1),\ A_3 = q^{2n},$$

$$A_4 = \frac{(q^n+1)(q^{n-1}-1)}{q-1}.$$

Proof The proof is similar to the proof of Lemma 5.5.12. □

Lemma 5.5.19 *Each point of $\mathcal{K}$ is contained in H_2 tangent hyperplanes, while each point not in $\mathcal{K}$ is contained in H_1 tangent hyperplanes.*

Proof This is proved as for Lemma 5.5.13. □

Denote by $\mathcal{H}$ the set of tangent hyperplanes of $\mathcal{K}$. Let $\delta : \mathbf{PG}(2n+1,q) \rightarrow \mathbf{PG}(2n+1,q)^D$ be any fixed chosen duality of $\mathbf{PG}(2n+1,q)$.

By Lemma 5.5.17, the set $\mathcal{K}' := \mathcal{H}^\delta$ is a $(0,1,2,q+1)$-set in $\mathbf{PG}(2n+1,q)^D$. We want to show that $\mathcal{K}'$ is the point set of an elliptic quadric. Notice however that $\mathcal{K}'$ does not satisfy the conditions of Theorem 5.2.3. By Lemma 5.5.19, the intersection numbers of $\mathcal{K}'$ with respect to hyperplanes are H_1 and H_2.

We define a point-line geometry $\mathcal{S}$, with point set $\mathcal{K}'$ and line set those lines of $\mathbf{PG}(2n+1,q)^D$ intersecting $\mathcal{K}'$ in $q+1$ points (the incidence is the natural one).

Theorem 5.5.20 *The geometry $\mathcal{S}$ is a Shult space such that no point of $\mathcal{S}$ is collinear with all other points of $\mathcal{S}$ if $q > 2$.*

Proof Consider a point p of $\mathcal{S}$ and a line L of $\mathcal{S}$, such that p and L are not incident. Consider the plane α generated by p and L.

If this plane contains another point r of $\mathcal{S}$, then the fact that $\mathcal{K}'$ is a $(0,1,2,q+1)$-set implies that α intersects $\mathcal{S}$ either in two intersecting lines or is fully contained in $\mathcal{S}$ (notice that $q > 2$ is necessary here). In both cases, the "1-or-all axiom" holds.

Next suppose that α intersects $\mathcal{S}$ only in p and L. Assume that α would not be contained in a hyperplane of type H_1. We count pairs (u,H), with u a point of $\mathcal{S}$ not in α and H a hyperplane containing u and α. We obtain

$$\left(|Q^-(2n+1,q)| - q - 2\right)\frac{q^{2n-2}-1}{q-1} = \frac{q^{2n-1}-1}{q-1}(H_2 - q - 2),$$

a contradiction. Hence, α is contained in at least one hyperplane Π of type H_1. By Theorem 5.2.3, the $(0,1,2,q+1)$-set $\mathcal{K}' \cap \Pi$ is the point set of a non-singular parabolic quadric. We conclude that in $\mathcal{S}$ the point p is collinear with 1 or all points of L. Since each point of $\mathcal{S}$ is contained in at least one hyperplane of type H_1, no point of $\mathcal{S}$ is collinear with all other points of $\mathcal{S}$. We still have to prove that through every point of $\mathcal{S}$ there passes a constant number of lines in order to conclude that $\mathcal{S}$ is a Shult space (using our definition from the introduction of Shult-space which is slightly different from the original one). Consider first two non-collinear points p and r. Then for every line containing

p there is exactly one line M through r intersecting L. Hence, through p and r there pass the same number of lines. Next consider two collinear points p and r. Considering all planes containing the line pr, it is clear that one can find a point s which is both non-collinear with p and r. By the above, there pass equally many lines through p and r. □

Corollary 5.5.21 *The point set $\mathcal{K}'$ forms the point set of a non-singular elliptic quadric $Q^-(2n+1,q)$, $q>2$.*

Proof This is an immediate consequence of $|\mathcal{K}'| = |Q^-(2n+1,q)|$, the previous lemma and Theorem 1.2.5. □

Theorem 5.5.22 *The set $\mathcal{K}$ is the point set of a non-singular elliptic quadric $Q^-(2n+1,q)$ in $\mathbf{PG}(2n+1,q)$, $q>2$.*

Proof Clearly $\mathcal{K}'$ is a point set satisfying the same conditions on intersections with hyperplanes and subspaces of codimension 2 as $\mathcal{K}$ in $\mathbf{PG}(2n+1,q)$. Since the tangent hyperplanes to $\mathcal{K}'$ are exactly those hyperplanes containing H_2 points of $\mathcal{K}'$, we find that if we apply the duality δ^{-1} to $\mathbf{PG}(2n+1,q)^D$, the tangent hyperplanes to $\mathcal{K}'$ are mapped bijectively to the points of $\mathcal{K}$ (see Lemma 5.5.19). Hence we can now apply Corollary 5.5.21 with $\mathcal{K}'$ in $\mathbf{PG}(2n+1,q)^D$ replaced by $\mathcal{K}$ in $\mathbf{PG}(2n+1,q)$. We conclude that $\mathcal{K}$ is the point set of an elliptic quadric $Q^-(2n+1,q)$. □

5.5.4 Parabolic quadrics

First of all let us recall what the intersections of a parabolic quadric $Q(2n,q)$ with hyperplanes and spaces of codimension 2 look like. A hyperplane can intersect $Q(2n,q)$ either in $Q^+(2n-1,q)$, $Q^-(2n-1,q)$ or in a cone $pQ(2n-2,q)$.

A space of codimension 2 can intersect a parabolic quadric $Q(2n,q)$ either in $Q(2n-2,q)$, a cone $pQ^+(2n-3,q)$, a cone $pQ^-(2n-3,q)$ or a cone $LQ(2n-4,q)$ (notice that this cone contains the same number of points as $Q(2n-2,q)$). So the intersection numbers with hyperplanes are

$$H_1 = \frac{(q^n-1)(q^{n-1}+1)}{q-1}, H_2 = \frac{(q^n+1)(q^{n-1}-1)}{q-1},$$

$$H_3 = 1 + q\frac{q^{2n-2}-1}{q-1}.$$

The intersection numbers with spaces of codimension 2 are

$$C_1 = \frac{q^{2n-2}-1}{q-1},\ C_2 = 1 + q\frac{(q^{n-1}-1)(q^{n-2}+1)}{q-1},$$

$$C_3 = 1 + q\frac{(q^{n-1}+1)(q^{n-2}-1)}{q-1}.$$

From now on, let $\mathcal{K}$ be a set of points in $\mathbf{PG}(2n,q)$ having the same intersection numbers with hyperplanes and codimension 2 spaces as $Q(2n,q)$. We want to prove that $\mathcal{K}$ is the point set of a parabolic quadric $Q(2n,q)$. We will call subspaces intersecting $\mathcal{K}$ in a given number m of points, *subspaces of type m*. For obvious reasons a hyperplane intersecting $\mathcal{K}$ in H_3 points will also be called a *tangent hyperplane*.

Lemma 5.5.23 *The set $\mathcal{K}$ contains $|Q(2n,q)|$ points.*

Proof Let h_i, respectively c_i, denote the number of hyperplanes of type H_i, respectively the number of codimension 2 spaces of type C_i. By counting pairs and triples as in Lemma 5.5.10, but now with respect to hyperplanes as well as with respect to codimension 2 spaces, we obtain

$$\sum_i h_i = \frac{q^{2n+1}-1}{q-1}, \tag{5.9}$$

$$\sum_i h_i H_i = \frac{q^{2n}-1}{q-1}\,|\mathcal{K}|, \tag{5.10}$$

$$\sum_i h_i H_i (H_i - 1) = \frac{q^{2n-1}-1}{q-1}\,|\mathcal{K}|\,(|\mathcal{K}|-1), \tag{5.11}$$

$$\sum_i c_i = \frac{(q^{2n+1}-1)(q^{2n}-1)}{(q^2-1)(q-1)}, \tag{5.12}$$

$$\sum_i c_i C_i = |\mathcal{K}|\,\frac{(q^{2n}-1)(q^{2n-1}-1)}{(q^2-1)(q-1)}, \tag{5.13}$$

$$\sum_i c_i C_i (C_i - 1) = |\mathcal{K}|\,(|\mathcal{K}|-1)\frac{(q^{2n-1}-1)(q^{2n-2}-1)}{(q^2-1)(q-1)}. \tag{5.14}$$

Now consider a hyperplane Π of type H_j and denote by m_i^j the number of codimension 2 spaces of type C_i it contains. By counting pairs (p,Δ) and triples (p,r,Δ), with $p \neq r$ points of $\mathcal{K}\cap\Pi$, $\Delta \subset \Pi$ a codimension 2 space, and $p,r \in \Delta$, we obtain

$$\sum_i m_i^j = \frac{q^{2n}-1}{q-1},$$

$$\sum_i m_i^j C_i = H_j\frac{q^{2n-1}-1}{q-1},$$

$$\sum_i m_i^j C_i(C_i - 1) = H_j(H_j - 1)\frac{q^{2n-2} - 1}{q - 1}.$$

From these equations, all values m_i^j can easily be determined. As $m_2^2 = 0$ we see that the number of hyperplanes of type H_1 through a codimension 2 space of type C_2 is a constant $f(|\mathcal{K}|)$ depending only on the size of $\mathcal{K}$.

By counting pairs (H, Δ), with H a hyperplane of type H_1, $\Delta \subset H$ a codimension 2 space of type C_2, we obtain

$$h_1 m_2^1 = c_2 f(|\mathcal{K}|). \tag{5.15}$$

From Equation (5.15) we can solve h_1 in function of c_2 and $|\mathcal{K}|$, say $h_1 = h_1(c_2, |\mathcal{K}|)$. From Equations (5.12), (5.13) and (5.14) we can obtain an expression for c_2 depending only on $|\mathcal{K}|$, say $c_2 = c_2(\mathcal{K})$. From Equations (5.9), (5.10) and (5.11) we can now obtain a quadratic equation in $|\mathcal{K}|$ of the form $s\,|\mathcal{K}|^2 + t\,|\mathcal{K}| + u(h_1) = 0$, where the Maple calculations show that s and t are independent of h_1 and $u(h_1)$ is a function of h_1. By substitution of $h_1 = h_1(c_2, |\mathcal{K}|)$ we obtain

$$s\,|\mathcal{K}|^2 + t\,|\mathcal{K}| + u(h_1(c_2, |\mathcal{K}|)) = 0, \tag{5.16}$$

which turns out to be a cubic equation in $|\mathcal{K}|$. One simply checks that $|\mathcal{K}| = \frac{q^{2n}-1}{q-1}$ is a solution of Equation (5.16).

We want to exclude the other roots of Equation (5.16) as possible sizes for the set $\mathcal{K}$.

Though Maple is not able to directly calculate the other roots for general n and q it is not too hard to determine the product and sum of the roots of Equation (5.16) with Maple.

One obtains that the three roots have product

$$-\frac{u(h_1(c_2(\mathcal{K})))}{s} = \frac{q^{4n-2} + q^{2n+1} - 3q^{2n} + q^{2n-1} - q^{2n-2} + 1}{(q-1)^3\,(q^{2\,n-1} - 1)},$$

and sum

$$-\frac{t}{s} = 3\,\frac{(q^n + 1)\,(q^n - 1)}{q - 1}.$$

From the above expressions, one can deduce that the other roots are complex, non-real, numbers, a contradiction. □

Lemma 5.5.24 *There are exactly $\frac{q^{2n}-1}{q-1}$ tangent hyperplanes. Furthermore, every codimension 2 space of type C_2 or C_3 is contained in exactly one tangent hyperplane.*

Proof The first assertion follows from Equations (5.9), (5.10) and (5.11) once we know $|\mathcal{K}| = \frac{q^{2n}-1}{q-1}$. To prove the second assertion, we notice that $m_3^1 = m_2^2 = 0$. Hence, if T_i denotes the number of tangent hyperplanes containing a given codimension 2 space of type C_i, $i = 2, 3$, then

$$T_i(H_3 - C_i) + (q + 1 - T_i)(H_{i-1} - C_i) + C_i = |\mathcal{K}| .$$

We obtain $T_2 = T_3 = 1$. □

Lemma 5.5.25 *For every codimension* 2 *space of type C_1, the number of hyperplanes of type H_1 containing it is equal to the number of hyperplanes of type H_2 in which it is contained.*

Proof One notices that $|\mathcal{K}| = (q+1)(H_3-C_1)+C_1$ and that $(H_1+H_2)/2 = H_3$. The lemma follows. □

Lemma 5.5.26 *Let γ be a codimension* 3 *space contained in a hyperplane H of type H_1. Suppose that γ is contained in N_H codimension* 2 *spaces α of type C_2, such that $\gamma \subset \alpha \subset H$. Then $|\gamma \cap \mathcal{K}| = q^{n-2}N_H + \frac{(q^{n-1}+1)(q^{n-2}-1)}{q-1}$. Furthermore, if γ is also contained in a hyperplane E of type H_2, then $N_H \leq 2$.*

Proof Let X denote the number of points of $\mathcal{K}$ contained in γ. As $m_3^1 = 0$ we have

$$(q + 1 - N_H)(C_1 - X) + N_H(C_2 - X) + X = H_1.$$

It follows that

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

Next let E be a hyperplane of type H_2 containing γ and let N_E be the number of codimension 2 spaces β of type C_3 such that $\gamma \subset \beta \subset E$. Since $m_2^2 = 0$ we obtain that

$$(q + 1 - N_E)(C_1 - X) + N_E(C_3 - X) + X = H_2.$$

Substitution of the higher obtained expression for X in terms of N_H yields

$$N_E = 2 - N_H.$$

As $N_E \geq 0$, the lemma follows. □

Lemma 5.5.27 *A codimension* 3 *space that is contained in a hyperplane of type H_1 contains $Nq^{n-2} + \frac{(q^{n-1}+1)(q^{n-2}-1)}{q-1}$ points of $\mathcal{K}$, with $N \in \{0, 1, 2, q+1\}$.*

Proof Let γ be any codimension 3 space contained in a hyperplane H of type H_1, and set $X = |\gamma \cap \mathcal{K}|$. If γ is contained in hyperplanes of type H_1 as well as of type H_2 there is nothing to prove because of the previous lemma.

If γ is contained in no hyperplane of type H_2, then γ cannot be contained in a codimension 2 space of type C_3 (since through each codimension 2 space of type C_3, there passes a hyperplane of type H_2, which follows from $m_3^1 = 0$). Furthermore, since the number of H_2 hyperplanes containing a given codimension 2 space of type C_1 equals the number of H_1 hyperplanes containing it, γ cannot be contained in a codimension 2 space α of type C_1 such that $\gamma \subset \alpha \subset H$. Hence, in H, all codimension 2 spaces containing γ must be of type C_2. By the previous lemma, we obtain that $X = (q+1)q^{n-2} + \frac{(q^{n-1}+1)(q^{n-2}-1)}{q-1}$. □

Corollary 5.5.28 *Every hyperplane of type H_1 intersects $\mathcal{K}$ in the point set of a non-singular hyperbolic quadric $Q^+(2n-1,q)$.*

Proof By the previous lemma the conditions of Theorem 5.5.15 and Section 5.5.2 are satisfied in each hyperplane of type H_1, whenever $n > 2$. If $n = 2$, the corollary follows by the remark after Theorem 5.2.10. □

Lemma 5.5.29 *Every point of $\mathcal{K}$ is contained in at least one hyperplane of type H_1.*

Proof Let p be any point of $\mathcal{K}$. Assume by way of contradiction that p is only contained in hyperplanes of type H_2 and H_3. Then, by counting pairs (r, H), $r \in \mathcal{K}$, $r \neq p$, $p, r \in H$, H a hyperplane, we obtain

$$l_2(H_2 - 1) + \left(\frac{q^{2n}-1}{q-1} - l_2\right)(H_3 - 1) = \left(\frac{q^{2n}-1}{q-1} - 1\right)\frac{q^{2n-1}-1}{q-1},$$

with l_2 the number of hyperplanes of type H_2 containing p. It follows that $l_2 < 0$, an absurdity. □

Theorem 5.5.30 *The set $\mathcal{K}$ is the point set of a non-singular parabolic quadric.*

Proof Let L be any line of $\mathbf{PG}(2n,q)$, and suppose that $|L \cap \mathcal{K}| = x$, with $x \geq 3$. Suppose there would be no hyperplane of type H_1 containing L. Then, if n_2 would be the number of hyperplanes of type H_2 containing L, we obtain by counting pairs (r, H), $r \in \mathcal{K}$, $r \notin L$, H a hyperplane containing r and L,

$$n_2(H_2 - x) + \left(\frac{q^{2n-1}-1}{q-1} - n_2\right)(H_3 - x) = \left(\frac{q^{2n}-1}{q-1} - x\right)\frac{q^{2n-2}-1}{q-1}.$$

This implies that $n_2 < 0$, a contradiction. Hence, L is contained in a hyperplane of type H_1. Corollary 5.5.28 implies that $x = q + 1$. Consequently, $\mathcal{K}$ is a $(0, 1, 2, q + 1)$-set in $\mathbf{PG}(2n, q)$. By combining Lemma 5.5.29 and Corollary 5.5.28, we also see that each point of $\mathcal{K}$ is contained in a line M such that $|M \cap \mathcal{K}| = 2$. Hence, $\mathcal{K}$ is non-singular. It follows that $\mathcal{K}$ satisfies the conditions of Theorem 5.2.3. As $|\mathcal{K}| = \frac{q^{2n}-1}{q-1}$, the theorem follows. □

The Main Theorem 5.2.10 is now an immediate consequence of Theorems 5.5.9, 5.5.15, 5.5.22 and 5.5.30.

Appendix A

Nederlandstalige samenvatting

In de appendix zullen we een overzicht geven van het algemeen wiskundig kader en van de specifieke resultaten bekomen in deze thesis. De bedoeling is dus niet om volledig te zijn of in detail te gaan, zo zijn er geen vertalingen van de bewijzen in de engelstalige tekst, maar wel om summier de gebruikte methoden en de hoofdstellingen te bespreken. We zullen wel dezelfde structuur aanhouden als voor de engelstalige tekst. De engelstalige termen waarvoor geen geijkte nederlandstalige vertaling is gekend, worden onvertaald gelaten, daar dit enkel kan leiden tot gekunstelde termen en verwarring.

A.1 Inleiding

In het eerste hoofdstuk wordt kort de context geschetst waarin het onderzoek te situeren is en worden gekende zaken die verder in het werk gebruikt worden vermeld. Zo komen veralgemeende vierhoeken, klassieke polaire ruimten, blocking sets en de Veroneseanen aan bod. We zullen de begrippen die expliciet aan bod komen in de nederlandstalige tekst hier vastleggen.

A.1.1 Veralgemeende vierhoeken

Definitie A.1.1 *Een* veralgemeende vierhoek $\mathbf{VV}$ *van de orde* (s,t) *is een incidentiestructuur* $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathbf{I})$ *waarin* $\mathcal{P}$ *en* $\mathcal{B}$ *verschillende niet-ledige verzamelingen van objecten zijn die respectievelijk* punten *en* rechten *worden genoemd, en waarvoor* $\mathbf{I}$ *een symmetrische punt-rechte incidentierelatie is die aan volgende axioma's voldoet:*

(VV1) Elk punt is incident met $t+1$ *rechten* $(t \geq 1)$ *en twee verschillende punten zijn incident met hoogstens 1 gemeenschappelijke rechte.*

(VV2) Elke rechte is incident met $s+1$ punten en twee verschillende rechten zijn incident met hoogstens 1 gemeenschappelijk punt.

(VV3) Als p een punt is en L een rechte niet incident met p, dan bestaat er een uniek punt-rechte paar (q, M) zodat $p \mathbf{I} M \mathbf{I} q \mathbf{I} L$.

Definitie A.1.2 *Een* automorfisme *van een* **VV** *is een permutatie van $\mathcal{P} \cup \mathcal{B}$ die $\mathcal{P}$, $\mathcal{B}$ en* **I** *behoudt. De verzameling automorfismen van een* **VV** *$\mathcal{S}$ vormt een groep, de* automorfismengroep *van de veralgemeende vierhoek, genoteerd als $Aut(\mathcal{S})$.*

Definitie A.1.3 *Een* deelvierhoek *$\mathcal{S}' = (\mathcal{P}', \mathcal{B}', \mathbf{I}')$ van een veralgemeende vierhoek $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathbf{I})$ is een veralgemeende vierhoek waarvoor $\mathcal{P}' \subseteq \mathcal{P}$, $\mathcal{B}' \subseteq \mathcal{B}$, en waarvoor $\mathbf{I}'$ de restrictie is van $\mathbf{I}$ tot $(\mathcal{P}' \times \mathcal{B}') \cup (\mathcal{B}' \times \mathcal{P}')$.*

Definitie A.1.4 *Een* ovoïde *van een veralgemeende vierhoek $\mathcal{S}$ is een verzameling $\mathcal{O}$ van punten van $\mathcal{S}$ zodat elke rechte van $\mathcal{S}$ incident is met een uniek punt van $\mathcal{O}$.*

De klassieke veralgemeende vierhoeken. Beschouw een niet-singuliere kwadriek met Witt index 2, dus met projectieve index 1, in $\mathbf{PG}(3, q)$, $\mathbf{PG}(4, q)$ en $\mathbf{PG}(5, q)$. De punten en rechten van deze kwadrieken vormen veralgemeende vierhoeken die we noteren als $Q^+(3, q)$, $Q(4, q)$ en $Q^-(5, q)$, en zijn van orde $(q, 1)$, (q, q) en (q, q^2) respectievelijk. Vervolgens, zij H een niet-singuliere Hermitische variëteit in $\mathbf{PG}(3, q^2)$ of $\mathbf{PG}(4, q^2)$. De punten en rechten van H vormen een veralgemeende vierhoek $H(3, q^2)$ of $H(4, q^2)$, met orde (q^2, q) of (q^2, q^3) respectievelijk. De punten van $\mathbf{PG}(3, q)$ samen met de totaal isotrope rechten met betrekking tot een symplectische polariteit vormen een **VV**, genoteerd als $W(q)$, en ze heeft orde (q, q). De hier gedefinieerde veralgemeende vierhoeken worden de *klassieke veralgemeende vierhoeken* genoemd.

Definitie A.1.5 *Zij V een vectorruimte over een lichaam, niet noodzakelijk eindig dimensionaal. Een veralgemeende vierhoek $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathbf{I})$ is* volledig ingebed *in de projectieve ruimte $\mathbf{PG}(V)$ als er een afbeelding π van $\mathcal{P}$ naar de verzameling punten en van $\mathcal{B}$ naar de verzameling rechten van $\mathbf{PG}(V)$ bestaat waarvoor:*

(i) π injectief is op de punten,

(ii) als $x \in \mathcal{P}$ en $L \in \mathcal{B}$ met $x \mathbf{I} L$, dan $x^\pi \in L^\pi$,

(iii) de verzameling punten x^π, met $x \in \mathcal{P}$, brengt $\mathbf{PG}(V)$ voort,

(iv) elk punt in $\mathbf{PG}(V)$ *gelegen op het beeld van een rechte* L *van de vierhoek is ook het beeld van een punt op de rechte* L *van de vierhoek.*

De volgende mooie stelling is van Buekenhout en Lefèvre [11].

Theorem A.1.6 *Elke eindige veralgemeende vierhoek die volledig is ingebed in een projectieve ruimte* $\mathbf{PG}(V)$ *is klassiek.*

A.1.2 Klassieke polaire ruimten

Polaire ruimten werden voor het eerst axiomatisch beschreven door Veldkamp [72]. We herhalen de definite van Tits van polaire ruimten.

Een *polaire ruimte* van *rang* n, $n > 2$, is een puntenverzameling $\mathcal{P}$ samen met een familie van deelverzamelingen van $\mathcal{P}$, *deelruimten* genoemd, die aan volgende axioma's voldoen.

(i) Een deelruimte, samen met de deelruimten die ze bevat, is een d-dimensionale projectieve ruimte waarvoor $-1 \leq d \leq n-1$; d wordt de *dimensie* van de deelruimte genoemd.

(ii) De intersectie van twee deelruimten is een deelruimte.

(iii) Voor een deelruimte van dimensie $n-1$ en een punt $p \in \mathcal{P}\backslash V$ bestaat er een unieke deelruimte W van dimensie $n-1$ zodat $p \in W$ en zodat $V \cap W$ dimensie $n-2$ heeft; W bevat alle punten van V die verbonden zijn met p door een deelruimte van dimensie 1, ook *rechte* genoemd.

(iv) Er bestaan twee disjuncte deelruimten van dimensie $n-1$.

De polaire ruimten van rang 2 zijn per definitie de veralgemeende vierhoeken.

De *eindige klassieke polaire ruimten* zijn de volgende structuren.

(i) De niet-singuliere hyperbolische en elliptische kwadrieken in oneven dimensie $Q^+(2n+1,q), n \geq 1$, en $Q^-(2n+1,q), n \geq 2$, samen met de deelruimten die ze bevatten, vormen een polaire ruimte van rang $n+1$ en n, respectievelijk. De niet-singuliere parabolische kwadrieken $Q(2n,q), n \geq 2$, in even dimensie, samen met de deelruimten die ze bevatten, vormen een polaire ruimte van rang n.

(ii) De niet-singuliere Hermitische variëteiten in $\mathbf{PG}(2n,q^2)$, $n \geq 2$, samen met de deelruimten die ze bevatten, vormen een polaire ruimte van rang n; de niet-singuliere Hermitische variëteiten in $\mathbf{PG}(2n+1,q^2)$, $n \geq 1$, samen met de deelruimten die ze bevatten, vormen een polaire ruimte van rang $n+1$.

(iii) De punten van $\mathbf{PG}(2n+1,q), n \geq 1$, samen met de totaal isotrope deelruimten van een niet-singuliere symplectische polariteit van $\mathbf{PG}(2n+1,q)$, vormen een polaire ruimte van rang $n+1$.

Door stellingen van Veldkamp en Tits zijn alle polaire ruimten van eindige rang tenminste drie geclassificeerd. In het eindig geval, dit is als de polaire ruimte slechts een eindig aantal punten bevat, geldt de volgende stelling, zie [71].

Stelling A.1.7 *Elke eindige polaire ruimte van rang tenminste drie is klassiek.*

Buekenhout en Shult beschrijven polaire ruimten als punt-rechte meetkunden.

Definitie A.1.8 *Een* Shult ruimte *is een punt-rechte meetkunde $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathbf{I})$, met $\mathcal{B}$ een niet-ledige verzameling van deelverzamelingen van $\mathcal{P}$ van cardinaliteit tenminste 2, zodat de incidentierelatie $\mathbf{I}$, die hier bevatten is, aan het volgende axioma voldoet. Voor elke rechte $L \in \mathcal{B}$ en voor elk punt $p \in \mathcal{P} \backslash L$ is het punt p collineair met ofwel één punt van L of met alle punten van L.*

Een Shult ruimte is *niet-singulier* als geen enkel punt collineair is met alle andere punten.
Een *deelruimte* van een Shult ruimte $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathbf{I})$ is een deelverzameling W van $\mathcal{P}$ zodat elke twee punten van W op een gemeenschappelijke rechte liggen en zodat elke rechte die verschillende punten van W bevat volledig bevat is in W. Een Shult ruimte is *lineair* als twee rechten in ten hoogste 1 punt snijden. Buekenhout en Shult bewezen de volgende fundamentele stelling [12].

Stelling A.1.9 (i) *Elke niet-singuliere Shult ruimte is lineair.*

(ii) *Als $\mathcal{S}$ een niet-singuliere Shult ruimte is van eindige rang tenminste 3, en als alle rechten tenminste drie punten bevatten, dan is de Shult ruimte samen met al haar deelruimten een polaire ruimte.*

We hebben dus de volgende stelling.

Stelling A.1.10 *Veronderstel dat $\mathcal{S}$ een eindige niet-singuliere Shult ruimte van rang tenminste 3 is, en zodat elke rechte tenminste drie punten bevat. Dan is $\mathcal{S}$ isomorf aan de punt-rechte meetkunde van een eindige klassieke polaire ruimte.*

Als een Shult ruimte volledig is ingebed in een projectieve ruimte, dan volgt volgende stelling uit Buekenhout en Lefèvre [11], en Lefèvre-Percsy [37, 38].

Theorem A.1.11 *Veronderstel dat $\mathcal{S}$ een niet-singuliere eindige Shult ruimte is. Als $\mathcal{S}$ volledig is ingebed in een projectieve ruimte, dan bestaat $\mathcal{S}$ uit de punten en rechten van een eindige klassieke polaire ruimte. Hier betekent volledig ingebed dat de verzameling rechten van $\mathcal{S}$ een deelverzameling is van de verzameling rechten van een projectieve ruimte en dat de puntenverzameling van $\mathcal{S}$ de verzameling is van alle punten bevat in deze rechten.*

A.1.3 Veroneseanen en veralgemeende (duale) bogen

In deze deelsectie definiëren we veralgemeende (duale) bogen en een algebraïsch object waarmee ze kunnen geconstrueerd worden, de veralgemeende Veroneseaan.

Definitie A.1.12 *Een* veralgemeende duale boog $\mathcal{F}$ *van* graad d *met dimensies* $n = n_0 > n_1 > n_2 > \cdots > n_{d+1} > -1$ *in* $\mathbf{PG}(n, q)$ *is een verzameling* n_1*-dimensionale deelruimten van* $\mathbf{PG}(n, q)$ *waarvoor:*

1. *elke j van deze deelruimten snijden in een deelruimte van dimensie n_j, $1 \leq j \leq d + 1$,*
2. *elke $d + 2$ van deze deelruimten hebben een ledige intersectie.*

We noemen $(n = n_0, n_1, \ldots, n_{d+1})$ *het* type *van de veralgemeende duale boog.*

Verder in de tekst is er sprake van reguliere en sterk reguliere veralgemeende duale bogen. Dit zijn bijkomende technische voorwaarden die we stellen aan veralgemeende duale bogen. Ze zijn echter niet essentieel om het hoofdidee te volgen.

Definitie A.1.13 *Een* veralgemeende boog $\mathcal{A}$ *van* graad d *met dimensies* $n_1 < n_2 < \cdots < n_{d+1}$ *in* $\mathbf{PG}(n, q)$ *is een verzameling* n_1*-dimensionale deelruimten van* $\mathbf{PG}(n, q)$ *waarvoor:*

1. *elke j van deze deelruimten brengen een deelruimte van dimensie n_j, $1 \leq j \leq d + 1$, voort,*
2. *elke $d + 2$ van deze deelruimten brengen $\mathbf{PG}(n, q)$ voort.*

We noemen $(n, n_1, \ldots, n_{d+1})$ *het* type *van de veralgemeende boog.*

De kwadratische Veroneseaan wordt als volgt gedefinieerd.

Definitie A.1.14 *De Veronese variëteit $\mathcal{V}_n^{2^n}$ van alle kwadrieken van* $\mathbf{PG}(n,q)$*,* $n \geq 1$*, is de variëteit*

$$\mathcal{V}_n^{2^n} = \{p(x_0^2, x_1^2, \cdots, x_n^2, x_0x_1, x_0x_2, \cdots, x_{n-1}x_n) \mid\mid (x_0, \cdots, x_n) \in \mathbf{PG}(n,q)\}$$

in $\mathbf{PG}(\frac{n(n+3)}{2}, q)$*; deze variëteit heeft dimensie n en orde 2^n. Het natuurlijk getal n wordt de* index *van $\mathcal{V}_n^{2^n}$ genoemd.*

Het beeld van een willekeurig hypervlak van $\mathbf{PG}(n,q)$ onder de Veronese afbeelding is een kwadratische Veroneseaan $\mathcal{V}_{n-1}^{2^{n-1}}$, en de deelruimte erdoor voortgebracht heeft dimensie $N_{n-1} = \frac{(n-1)(n+2)}{2}$. Zo een deelruimte wordt een $\mathcal{V}_{n-1}$-*deelruimte* genoemd. In het bijzonder voor $n = 2$ worden de $\mathcal{V}_1$-deelruimten *kegelsnedevlakken* genoemd.

Het beeld van een rechte van $\mathbf{PG}(n,q)$ is een kegelsnede, en als q even is, dan vormt de verzameling van kernen van al deze kegelsneden een Grassmanniaan van rechten van $\mathbf{PG}(n,q)$ en brengt bijgevolg een ruimte voort van dimensie $\frac{(n-1)(n+2)}{2}$, die we de *kernruimte* van $\mathcal{V}_n^{2^n}$ noemen, zie [65].

Definitie A.1.15 *De raakruimte aan $\mathcal{V}_n^{2^n}$ in $p \in \mathcal{V}_n^{2^n}$ is de unie van alle raaklijnen in p aan de kegelsneden op $\mathcal{V}_n^{2^n}$ door p (voor $q = 2$ beschouwt men de kegelsneden die het beeld zijn van rechten van* $\mathbf{PG}(n,2)$*).*

Deze kwadratische Veroneseaan kan ook aan de hand van matrices worden bestudeerd, zie [28].

Stelling A.1.16 *De kwadratische Veroneseaan $\mathcal{V}_n^{2^n}$ in* $\mathbf{PG}(n,q)$ *bestaat uit alle punten $p(y_{0,0}, \cdots, y_{n,n}, y_{0,1}, \cdots, y_{n-1,n})$ in* $\mathbf{PG}(\frac{n(n+3)}{2}, q)$ *waarvoor $[y_{i,j}]$, met $y_{i,j} = y_{j,i}$ als $i \neq j$, een symmetrische matrix is van rang 1.*

Een uitbreiding van deze definitie kan als volgt bekomen worden. Zij $\mathbf{PG}(V)$ een n-dimensionale ruimte met basis e_i $(0 \leq i \leq n)$. Zij $\mathbf{PG}(W)$ een $\left(\binom{n+d+1}{d+1} - 1\right)$-dimensionale ruimte met basis $e_{i_0,\ldots,i_d}$ $(0 \leq i_0 \leq i_1 \leq \cdots \leq i_d \leq n)$.

Definitie A.1.17 *De* veralgemeende Veroneseaan *is de puntenverzameling die het beeld is van de volgende afbeelding. Definieer $\zeta : \mathbf{PG}(V) \to \mathbf{PG}(W)$ als*

$$\zeta : [\sum_{i=0}^{n} x_i e_i] \mapsto [\sum_{0 \leq i_0 \leq \cdots \leq i_d \leq n} x_{i_0} \cdots x_{i_d} e_{i_0,\ldots,i_d}].$$

Aan een veralgemeende Veroneseaan kunnen we veralgemeende bogen en veralgemeende duale bogen hechten. We starten met de constructie van de veralgemeende duale bogen.

Noteer het standaard scalair product van V en W als b en B respectievelijk, i.e.,

$$b(\sum_{i=0}^{n} x_i e_i, \sum_{i=0}^{n} y_i e_i) = \sum_{i=0}^{n} x_i y_i,$$

en

$$B(\sum_{0\le i_0\le\cdots\le i_d\le n} x_{i_0,\ldots,i_d} e_{i_0,\ldots,i_d}, \sum_{0\le i_0\le\cdots\le i_d\le n} y_{i_0,\ldots,i_d} e_{i_0,\ldots,i_d}) = \sum_{0\le i_0\le\cdots\le i_d\le n} x_{i_0,\ldots,i_d} y_{i_0,\ldots,i_d}.$$

Constructie A.1.18 *Voor elke $x \in V$ noteren we de deelruimte van V die orthogonaal staat op x met betrekking tot b als $x^\perp$. Met andere woorden*

$$x^\perp = \{y \in V \mid\mid b(x, y) = 0\}.$$

Voor elk punt $p = [x]$ van $\mathbf{PG}(V)$ definiëren we een deelruimte $D(p)$ van $\mathbf{PG}(W)$ door

$$D(p) = \{z \in W \mid\mid B(z, \zeta(y)) = 0 \textit{ voor alle } y \in x^\perp\}. \tag{A.1}$$

We noteren deze verzameling deelruimten $\{D(p) \mid\mid p \in \mathbf{PG}(V)\}$ als $\mathcal{D}$.

Hieronder geven we een voorbeeld van deze algemene constructie.

Voorbeeld A.1.19 *Beschouw de afbeelding $\zeta : \mathbf{PG}(2, q) \to \mathbf{PG}(5, q)$ waarbij*

$$\zeta([x_0, x_1, x_2]) = [x_0^2, x_1^2, x_2^2, x_0x_1, x_0x_2, x_1x_2]$$

de kwadratische Veroneseaan $\mathcal{V}_2^4$ definieert.

Als $p = [a, b, c]$, dan hebben de vlakken $D(p)$ volgende voorstelling:

$$D(p) = \{[ax_0, bx_1, cx_2, ax_1 + bx_0, ax_2 + cx_0, bx_2 + cx_1] \mid\mid x_0, x_1, x_2 \in \mathbb{F}_q\}\ .$$

Deze vlakken vormen een sterk reguliere veralgemeende boog van q^2+q+1 vlakken van type $(5, 2, 0)$.

Een alternatieve beschrijving van $D(p)$ is de volgende.

Voor elke permutatie σ, stel $e_{i_{\sigma(0)},\ldots,i_{\sigma(d)}}$ gelijk aan $e_{i_0,\ldots,i_d}$, $0 \le i_0 \le i_1 \le \cdots \le i_d \le n$.

Zij $\theta : V^{d+1} \to W$ de multilineaire afbeelding

$$\theta : (\sum_{i=0}^{n} x_i^{(0)} e_i, \ldots, \sum_{i=0}^{n} x_i^{(d)} e_i) \mapsto \sum_{0 \leq i_0 \leq \cdots \leq i_d \leq n} x_{i_0}^{(0)} \cdot \ldots \cdot x_{i_d}^{(d)} e_{i_0,\ldots,e_d}. \qquad \text{(A.2)}$$

Eenvoudige controle leert ons dat als $b(x, y) = 0$, dan geldt

$$B(\theta(x, v_1, \ldots, v_d), \zeta(y)) = 0$$

voor alle vectoren $v_1, \ldots, v_d$ van V.

Dus voor $p = (x)$ hebben we

$$\langle \theta(x, v_1, \ldots, v_d) \mid\mid v_1, \ldots, v_d \in V \rangle \subseteq D(p) \ .$$

Aangezien de vectorruimte $\langle \theta(x, v_1, \ldots, v_d) \mid\mid v_1, \ldots, v_d \in V \rangle$ dimensie $\binom{n+d}{d}$ heeft (kies $v_1, \ldots, v_d$ als eenheidsvectoren), vinden we

$$\langle \theta(x, v_1, \ldots, v_d) \mid\mid v_1, \ldots, v_d \in V \rangle = D(p) \ . \qquad \text{(A.3)}$$

In [36] bewezen we de volgende stelling.

Stelling A.1.20 *De verzameling $\mathcal{D} = \{D(p) \mid\mid p \in \mathbf{PG}(V)\}$ is een sterk reguliere veralgemeende duale boog met dimensies $n_i = \binom{n+d+1-i}{d+1-i} - 1, i = 0, \cdots, d+1$.*

De verzameling $\mathcal{D}$ gedefinieerd door Constructie A.1.18 noemen we een *duale Veronese boog.*

Duaal aan Constructie A.1.18 hebben we volgende constructie van veralgemeende bogen.

Constructie A.1.21 *We behouden de notaties van Constructie A.1.18. Voor elke $x \in V$, zij $x^\perp$ de deelruimte van V die orthogonaal is ten opzichte van x met betrekking tot b. Met andere woorden*

$$x^\perp = \{y \in V \mid\mid b(x, y) = 0\}.$$

Voor elk punt $p = (x)$ van $\mathbf{PG}(V)$ definiëren we een deelruimte $A(p)$ van $\mathbf{PG}(W)$ door

$$A(p) = \left\langle \zeta(y) \mid\mid y \in x^\perp \right\rangle. \qquad \text{(A.4)}$$

Stelling A.1.22 *De verzameling $\mathcal{A} = \{A(p) \mid\mid p \in \mathbf{PG}(n, q)\}$ uit Constructie A.1.21, is een veralgemeende boog met dimensies $n_i = \binom{n+d+1}{d+1} - \binom{n+d+1-i}{d+1-i} - 1$, $i = 1, \ldots, d+1$.*

De veralgemeende duale boog beschreven in Constructie A.1.18 is het duale van deze boog.

Opmerking A.1.23 *De elementen $A(p)$ zijn precies de $\mathcal{V}_{n-1}$-deelruimten hoger gedefinieerd. Bijgevolg is de verzameling $\mathcal{D}$ uit Constructie A.1.18 het duale van deze verzameling $\mathcal{V}_{n-1}$-deelruimten.*

A.2 Authenticatiecodes

Hier bespreken we belangrijke toepassingen van de meetkunden bestudeerd in deze thesis, namelijk authenticatiecodes en secret sharing schemes. Authentiecatiecodes werden ingevoerd door Simmons in [53]. Voor een goed overzicht van de huidige status verwijzen we naar Pei [42].

We starten met de beschrijving van authenticatiecodes met of zonder arbitrage en vermelden enkele van hun belangrijke eigenschappen. Deze concepten worden geïllustreerd aan de hand van enkele eenvoudige schema's in de engelstalige tekst. In deze samenvatting zullen we vooral ons eigen werk toelichten, in het bijzonder tonen we aan dat veralgemeende duale bogen geschikt zijn om authenticatiecodes te construeren. Tot slot bespreken we enkele andere meetkundige constructies van authenticatiecodes en de performantie van onze schema's met betrekking tot de in het begin vermelde eigenschappen.

A.2.1 Authenticatie zonder arbitrage

In bepaalde situaties waar informatie wordt uitgewisseld, zoals overschrijvingen, wil men zekerheid hebben over de identiteit van de andere persoon. Daartoe kunnen zender en ontvanger op voorhand een sleutel afspreken die toelaat elkaar te herkennen. Dit model heet authenticatie zonder arbitrage. In bepaalde situaties faalt dit model als zender en ontvanger elkaar niet kunnen vertrouwen, bijvoorbeeld op de beurs als er zich hevige koersschommelingen voordoen. In dit geval dient het model uitgebreid te worden tot een model met een onafhankelijke betrouwbare derde partij, de *scheidsrechter*.

Meer formeel definieert men een message authentication code (MAC) als volgt.

Definitie A.2.1 *Een* message authentication code (MAC) *is een* 4*-tal* $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$ *met*

1. *$\mathcal{S}$ een eindige verzameling bronboodschappen,*

2. *$\mathcal{A}$ een eindige verzameling geëncodeerde boodschappen (authenticatiezegels),*

3. *$\mathcal{K}$ een eindige verzameling sleutels,*

4. *voor elke sleutel $K \in \mathcal{K}$ is er een encodeerregel $e_K \in \mathcal{E}$ met $e_K : \mathcal{S} \to \mathcal{A}$.*

We veronderstellen steeds een uniforme distributie voor de encodeerregels. Dit is geen essentiële beperking, maar het vermijdt ingewikkelder berekeningen waardoor de hoofdideeën van de schema's beter naar voor komen.

Bovendien is er geen enkele reden om a priori bepaalde regels boven andere te verkiezen.

Een belangrijk aspect bij MAC's is de veiligheid gemeten aan de hand van volgende aanvalswaarschijnlijkheden.

Definitie A.2.2 *Zij P_i de kans voor een tegenstander om een paar $(s, e_K(s))$ te construeren zonder de sleutel K te kennen, nadat hij i paren $(s_j, e_K(s_j))$ heeft gezien. De kleinste waarde r waarvoor $P_{r+1} = 1$ is de* orde *van het schema.*

Voor $r = 1$ is P_0 de waarschijnlijkheid van een impersonation attack*, het zich voordoen als iemand anders, genoemd en P_1 de waarschijnlijkheid van een* substitution attack*, het vervangen van een geziene boodschap door een andere. We veronderstellen steeds dat een* replay attack*, dit is het opnieuw sturen van een reeds gezien paar (boodschap, authenticatiezegel), zich niet kan voordoen.*

In volgende stelling wordt formeel duidelijk gemaakt dat men niet kan verwachten dat de aanvalswaarschijnlijkheden laag zijn als men niet over voldoende sleutels beschikt. Voor $r = 1$ en $P_0 = P_1$ werd dit bewezen in [24], en voor willekeurige r met $P_0 = P_1 = \cdots = P_r$, in [20].

Stelling A.2.3 *Als een MAC aanvalswaarschijnlijkheden $P_i = 1/n_i$ $(0 \leq i \leq r)$ heeft, dan geldt $|\mathcal{K}| \geq n_0 \cdots n_r$.*

Een MAC die gelijkheid bereikt in bovenstaande stelling wordt *perfect* genoemd.

Volgende stelling toont aan dat ook het aantal boodschappen beperkt is.

Stelling A.2.4 *Zij $P_i = 1/n_i$ met $n_i \in \mathbb{N}$. Als voor een MAC geldt dat $|\mathcal{K}| = n_0 \cdot \ldots \cdot n_r$, dan $|\mathcal{S}| \leq \frac{n_{r-1}n_r - 1}{n_r - 1} + r - 1$.*

Een MAC wordt *Cartesisch* genoemd als elke geëncodeerde boodschap het beeld is van een unieke bronboodschap.

Het blijkt dat veralgemeende duale bogen uitermate geschikt zijn om MAC's te construeren. Hier vermelden we enkel de stelling; in de sectie hieronder over authenticatie met arbitrage geven we meer uitleg.

Stelling A.2.5 *Zij Π een hypervlak van $\mathbf{PG}(n+1, q)$ en zij $\mathcal{D}$ een veralgemeende duale boog van graad l in Π van het type $(n, n_1, \ldots, n_{l+1})$.*

De elementen van $\mathcal{D}$ zijn de boodschappen en de punten van $\mathbf{PG}(n+1, q)$ niet in Π zijn de sleutels. De encodering van een boodschap met een sleutel is de $(n_1 + 1)$-dimensionale deelruimte voortgebracht door de boodschap en de sleutel.

Dit definieert een perfecte MAC van orde $r = l + 1$ met aanvalswaarschijnlijkheden

$$P_i = q^{n_{i+1} - n_i}.$$

A.2.2 Authenticatie met arbitrage

Zoals reeds vermeld in voorgaande deelsectie zijn er situaties waarin de communicatoren elkaar niet vertrouwen. In het geval van een geschil tussen beiden dienen we een mechanisme ter beschikking te hebben om uit deze impasse te geraken. Een integere scheidsrechter wordt aan het systeem toegevoegd. Meer formeel gesproken is een MAC met arbitrage of een A^2-code als volgt gedefinieerd.

Definitie A.2.6 *Een* authenticatiecode met arbitrage *of* A^2-code *bestaat uit:*

- $\mathcal{S}$*: een verzameling bronboodschappen,*
- $\mathcal{M}$*: een verzameling geëncodeerde boodschappen,*
- $\mathcal{E}_\mathcal{T}$*: een verzameling encodeerregels: bijecties van* $\mathcal{S}$ *naar* $\mathcal{M}$*,*
- $\mathcal{E}_\mathcal{R}$*: een verzameling decodeerregels: afbeeldingen van* $\mathcal{M}$ *naar* $\mathcal{S}$ *of een afwijzing.*

Dit schema wordt in twee stappen opgezet. De ontvanger Bob kiest een decodeerregel en overhandigt deze aan de scheidsrechter. Voor elke gekozen decodeerregel heeft de scheidsrechter een aantal encodeerregels ter beschikking. Hij kiest er één uit en overhandigt deze aan de zender Alice. Bob aanvaardt een geëncodeerde boodschap als geldig als hij niet wordt afgewezen door zijn decodeerregel. In het geval van betwisting tussen Alice en Bob beslist de scheidsrechter dat Alice de geëncodeerde boodschap heeft gestuurd indien deze boodschap correspondeert met de encodeerregel die hij aan haar heeft overhandigd.

In dit schema hebben we de aanvalswaarschijnlijkheden P_{O_i} voor een tegenstander, die gedefinieerd zijn zoals in het model zonder scheidsrechter. Daarnaast zijn er nog de aanvalswaarschijnlijkheden voor de ontvanger P_{R_r}, dit is de kans dat de ontvanger erin slaagt na het observeren van r paren die bestaan uit een bronboodschap en een geëncodeerde boodschap, de scheidsrechter te doen beslissen dat de zender een bericht heeft gestuurd terwijl dit niet het geval is en de aanvalswaarschijnlijkheid P_T, dit is de kans dat de zender erin slaagt om de ontvanger een boodschap die niet aan zijn encodeerregels voldoet als geldig te laten aanzien.

Net als bij de authenticatiecodes zonder arbitrage zijn er grenzen op het aantal encodeerregels en hier bovendien ook op het aantal decodeerregels.

Stelling A.2.7 *We hebben de volgende benedengrenzen voor het aantal encodeer- en decodeerregels:*

$$|\mathcal{E}_R| \geq (P_{O_0} P_{O_1} \cdots P_{O_{t-1}} P_T)^{-1},$$
$$|\mathcal{E}_T| \geq (P_{O_0} P_{O_1} \cdots P_{O_{t-1}} P_{R_0} P_{R_1} \cdots P_{R_{t-1}})^{-1}.$$

Als de gelijkheid optreedt in beide ongelijkheden, dan is het arbitrageschema *t-voudig perfect*.

Hieronder tonen we aan dat veralgemeende duale bogen geschikt zijn om een MAC met arbitrage te construeren.

Beschouw de ruimte Π_n opgespannen door een veralgemeende duale boog van type $(n = n_0, n_1, \ldots, n_{l+1})$ en bed deze ruimte in een $(n+2)$-dimensionale ruimte Π_{n+2} in. De bronboodschappen zijn de n_1-dimensionale deelruimten die element zijn van de veralgemeende duale boog, de decodeerregels zijn de punten in $\Pi_{n+2}\backslash\Pi_n$, de encodeerregels zijn de rechten in Π_{n+2} scheef aan Π_n, en de boodschappen zijn de (n_1+2)-dimensionale ruimten voortgebracht door een bronboodschap en een sleutel. We veronderstellen hierbij dat zender Alice en ontvanger Bob elkaar niet vertrouwen. Wanneer Alice en Bob wensen te communiceren, kiest Bob een punt p in $\Pi_{n+2}\backslash\Pi_n$ als decodeerregel en stuurt dit door naar de integere scheidsrechter. Deze kiest een rechte L door p scheef aan Π_n als encodeerregel en stuurt L naar Alice. Als Bob een (n_1+2)-dimensionale ruimte Π_{n_1+2} ontvangt, controleert Bob als $p \in \Pi_{n_1+2}$. Als dit het geval is, dan aanvaardt hij de boodschap; in het andere geval verwerpt hij ze.

Het doel voor een opponent is dus om een paar (Π_{n_1}, Π_{n_1+2}) te produceren zodat $p \in \Pi_{n_1+2}$.

Als er een discussie ontstaat tussen Alice en Bob over een geldige boodschap, dan controleert de scheidsrechter als de encodeerregel L die hij aan Alice overhandigde, bevat is in Π_{n_1+2}. Als dit het geval is wordt er van uitgegaan dat Alice de boodschap heeft gestuurd, anders niet.

Als Alice Bob wil bedriegen, moet ze dus een ruimte Π_{n_1+2} construeren die p bevat maar niet L. Als Bob Alice wil bedriegen dient hij een ruimte Π_{n_1+2} te construeren die de rechte L bevat.

Het aantal encodeerregels voor de zender is het aantal rechten scheef aan Π_n; dit is gelijk aan $|\mathcal{E}_R| = q^{2n+2}$. Het aantal decodeerregels is het aantal punten in $\Pi_{n+2}\backslash\Pi_n$; dit is $(q+1)q^{n+1}$.

Als een opponent wil bedriegen, dan moet hij een (n_1+2)-dimensionale ruimte produceren die het punt p bevat. Zijn kansen om dit te doen na het zien van i paren zijn $P_{O_i} = q^{n_i - n_{i-1}}$. Als Alice Bob wil bedriegen, moet ze raden welk punt op de rechte L de decodeerregel van Bob vormt. Dus haar kans is $P_T = \frac{1}{q+1}$. Tot slot is de kans voor Bob om vals te spelen na het zien van i paren gelijk aan $q^{n_i - n_{i-1}}$.

Dit schema is dus perfect met betrekking tot de benedengrenzen hoger gegeven.

A.2.3 Schema's afkomstig van veralgemeende vierhoeken

In deze deelsectie illustreren we dat ook veralgemeende vierhoeken geschikt zijn om authenticatiecodes te construeren. We starten met het eerste gekende voorbeeld van een authenticatiecode gebaseerd op veralgemeende vierhoeken van De Soete [16]; vervolgens beschrijven we twee schema's die we samen met K. Thas hebben gevonden [46].

Het schema van De Soete

Neem een vast punt p in een veralgemeende vierhoek van de orde (s, t). De bronboodschappen zijn de $t + 1$ rechten van de veralgemeende vierhoek door p, de encodeerregels (sleutels) zijn de punten die niet-collineair zijn met p, en de boodschappen de punten collineair met p maar verschillend van p. Als Alice een boodschap stuurt naar Bob dan kiest ze een rechte L door p als bronboodschap. Vanuit de afgesproken sleutel k is er juist 1 rechte M die L snijdt in een punt r. Alice stuurt het punt-rechte paar (r, L) door naar Bob die vervolgens controleert als r incident is met L en k. Dit geeft een Cartesische authenticatiecode waarbij $|\mathcal{S}| = t + 1$, $|\mathcal{M}| = (t + 1)s$, $\mathcal{E} = ts^2$ en $P_0 = P_1 = 1/s$.

Schema's gebaseerd op deelvierhoeken

Eerst stellen we een schema zonder arbitrage voor gebaseerd op ovoïdes in deelvierhoeken. Dit schema levert een zeer lage P_0. Zij $\mathcal{S}$ een veralgemeende vierhoek van de orde (s, t). Veronderstel dat $\mathcal{S}'$ een deelvierhoek is van de orde $(s, t/s)$ van $\mathcal{S}$. Dan toont een eenvoudige telling aan dat elke rechte van $\mathcal{S}$ de deelvierhoek $\mathcal{S}'$ snijdt in 1 of $s + 1$ punten. Zij x een punt in $\mathcal{S} \backslash \mathcal{S}'$. Dan vormen de $t + 1$ punten van $\mathcal{S}'$ collineair met x een ovoïde $\mathcal{O}_x$ van $\mathcal{S}'$. We zeggen dat de ovoïde $\mathcal{O}_x$ ondersteund wordt door x.

Veronderstel nu dat $\{\mathcal{S}_1, \mathcal{S}_2, \cdots, \mathcal{S}_r\}$ een verzameling verschillende deelvierhoeken van orde $(s, t/s)$ is van de vierhoek van de orde (s, t), waarbij $s \neq 1 \neq t$. Zij Σ het aantal punten in $\cup_{i=1}^{r} \mathcal{S}_i$. De $\mathcal{S}_j$'s zijn de bronboodschappen. De sleutels zijn de punten in $\mathcal{S} \backslash \cup_{i=1}^{r} \mathcal{S}_i$ en de boodschappen zijn de ovoïdes in de deelvierhoeken $\mathcal{S}_j$ die ondersteund worden door een punt buiten de unie. Zij k het maximaal aantal punten buiten de unie dat dezelfde ovoïde van een zekere $\mathcal{S}_j$ ondersteunt. Dan geldt

$$P_0 \leq \frac{s^2/t + 1}{(s + 1)(st + 1) - \Sigma}.$$

Op deze manier krijgen we Cartesische schema's die bovendien perfect zijn als elke ovoïde door hetzelfde aantal punten wordt ondersteund. In de engelstalige tekst staan dergelijke situaties beschreven.

Nu beschrijven we een schema met arbitrage: beschouw $\{\S_1, \S_2, \cdots, \S_r\}$, een verzameling verschillende $Q(4,q)$-deelvierhoeken in een niet-singuliere elliptische kwadriek $Q^-(5,q)$. Zij x een punt van $Q^-(5,q)$ buiten de unie van de deelvierhoeken gekozen door Bob. Voor een dergelijk punt x en een bronboodschap $\S_j$, zij O_x de ovoïde op $\S_j$ ondersteund door x. De scheidsrechter kiest een punt c_j van $\S_j$ op de ovoïde gelegen.

Voor het systeem kiezen we een lijst $\mathbf{H}$ van deelgroepen van $\mathrm{Aut}(\mathbf{Q}^-(5,q))$, zijnde $\mathcal{O}^-(6,q) \rtimes \mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_p)$ (q is een macht van het priemgetal p). Bob kiest een vaste deelgroep H in $\mathbf{H}$. Bob geeft H en zijn gekozen punt x aan de scheidsrechter. De deelgroep H heeft verschillende banen op $\mathbf{Q}^-(5,q)$. De scheidsrechter overhandigt c_j en de baan onder H van c_j, genoteerd c_j^H, als encodeerregel aan Alice voor een gegeven bronboodschap $\mathcal{S}_j$. Als Alice een boodschap naar Bob stuurt, dan kiest ze een bronboodschap $\mathcal{S}_j$ en stuurt ze het drietal $(\mathcal{S}_j, c_j, c_j^H)$ naar Bob.

Als hij een tripel (a,b,c) ontvangt, dan beschouwt Bob dit als geldig als b op de ovoïde van a gelegen is en c de baan onder H van b is.

In geval van een geschil aangaande een tripel (a,b,c), controleert de scheidsrechter als b het punt is horende bij a dat hij Alice overhandigde en als c de baan is onder H van b. Als dit zo is, beslist hij dat Alice de boodschap heeft gestuurd, anders niet.

Als Bob wil valsspelen, moet hij het punt c_j raden.

Als Alice wil valsspelen, dan moet ze de goede baan raden. Het is vrijwel onmogelijk voor Alice om dit te doen, behalve misschien door een exhaustieve zoektocht doorheen alle deelgroepen van $\mathrm{Aut}(\mathbf{Q}^-(5,q))$ in het geval er slechts een beperkt aantal deelgroepen zijn die dezelfde baan leveren als diegene die ze observeert. De scheidsrechter kan dit echter voorkomen door de gepaste punten op de ovoïdes te kiezen.

Een opponent moet zowel het punt c_j als de groep H raden, een schier onmogelijke taak.

We maken geen expliciete berekeningen, maar door de lijst van deelgroepen gepast te kiezen kan men dit schema naar zijn eigen behoeften aanpassen en zo bijvoorbeeld de lengte van de banen regelen.

A.3 Secret sharing schemes

Definitie A.3.1 *Een* secret sharing scheme *is een systeem om een geheim te verspreiden onder een groep deelnemers door elke deelnemer een* share *te geven op een dusdanige manier dat enkel welbepaalde gespecifieerde deelverzamelingen van deelnemers (vastgelegd door de* toegangsstructuur*) het geheim kunnen* *terugvinden door hun shares samen te leggen.*

Secret sharing schemes worden gebruikt in situaties waar het niet raadzaam is om één enkele persoon een geheim volledig toe te vertrouwen, bijvoorbeeld een code om nucleaire wapens af te vuren of voor bankrekeningen van grote organisaties. In dergelijke omstandigheden is het beter om een geheim over verschillende mensen te verspreiden zodat de kans op crimineel gedrag wordt beperkt.

De toegangsstructuur van een secret sharing scheme bepaalt welke deelverzamelingen van deelnemers toegelaten zijn om een geheim te reconstrueren; de zogenaamde *authorised sets*. De andere deelverzamelingen van deelnemers worden *unauthorised* genoemd. Een goed secret sharing scheme bezit de volgende twee eigenschappen:

(i) *Privaatheid*: unauthorised verzamelingen mogen het geheim niet terugvinden.

(ii) *Herconstrueerbaarheid*: authorised deelverzamelingen moeten een methode ter beschikking hebben om het geheim te reconstrueren aan de hand van hun shares.

De meeste secret sharing schemes worden verondersteld te beschikken over een *monotone toegangsstructuur*, dit wil zeggen dat als een verzameling deelnemers A een geheim kan reconstrueren dat dan ook elke verzameling deelnemers die A volledig bevat het geheim kan reconstrueren. De *dealer* van het secret sharing scheme is een volledig vertrouwde instantie, die verantwoordelijk is voor het opstarten van het systeem, wat inhoudt dat hij het geheim en de shares genereert, en elke deelnemer zijn of haar shares toevertrouwt. De *combiner* is de persoon die de shares van een gegeven verzameling deelnemers verzamelt en tracht het geheim te reconstrueren.

Een secret sharing scheme wordt *perfect* genoemd als unauthorised verzamelingen niets te weten komen over het geheim, dus ook geen partiële informatie.

Het meest natuurlijk voorbeeld van een secret sharing scheme is het (k, n)*-threshold scheme*, ook *k uit n secret sharing scheme* genoemd. Hierbij hebben we een monotone toegangsstructuur met n deelnemers waarbij elke k deelnemers het geheim kunnen reconstrueren en geen enkele groep van $k-1$ deelnemers dit kan.

A.3.1 Meetkundige secret sharing schemes

We onderzoeken hier toepassingen van veralgemeende bogen in secret sharing schemes. Een uitstekend overzicht van secret sharing en de verbanden met meetkunde is terug te vinden in [32].

Stelling A.3.2 *Kies in* $\mathbf{PG}(n+1,q)$ *een* n*-dimensionale ruimte* Π *als geheim. Kies in* Π *een veralgemeende boog* $\mathcal{A}$ *van graad* $k-2$ *met* n' *elementen en type* $(n, n_1, \ldots, n_{k-1})$*. De elementen van* $\mathcal{A}$ *zijn de shares. Dit beschrijft een* (k, n')*-threshold scheme met aanvalswaarschijnlijkheden*

$$P_i = \frac{q-1}{q^{n+1-n_i}-1}$$

voor $0 \leq i < k$ *(formeel stellen we* $n_0 = -1$*).*

Stelling A.3.3 *Kies in* $\mathbf{PG}(n+1,q)$ *een* (n_1+1)*-dimensionale deelruimte* π' *en maak deze publiek. Kies verder een* n_1*-dimensionale deelruimte* π *in* π' *als geheim. Kies om het even welk hypervlak* Π *van* $\mathbf{PG}(n+1,q)$ *dat* π *bevat maar niet* π'*. Zij verder* $\mathcal{A}$ *een veralgemeende boog van* Π *van de orde* $k-2$ *met* $n'+1$ *elementen en met type* $(n, n_1, \ldots, n_{k-1})$*. De deelruimte* π *wordt verondersteld een element van de boog* $\mathcal{A}$ *te zijn. De* n' *elementen van* $\mathcal{A}$ *verschillend van* π *zijn de shares. Dit beschrijft een* k *uit* n *secret sharing scheme met aanvalswaarschijnlijkheden*

$$P_i = \frac{q-1}{q^{n_{i+1}-n_i+1}-1}$$

voor $0 \leq i < k-1$ *(formeel stellen we* $n_0 = -1$ *en* $n_k = n$*).*

A.4 Minimale codewoorden

A.4.1 Probleemstelling

In het derde hoofdstuk bestuderen we minimale codewoorden. Deze zijn ingevoerd door Massey [40] voor cryptografische doeleinden. Ze worden gebruikt in welbepaalde secret sharing schemes, om de toegangsstructuur te modelleren. We bestuderen minimale codewoorden in binaire Reed-Muller codes. Een classificatieresultaat van Kasami, Tokura en Azumi [34] over Booleaanse functies zal ons toelaten om ons probleem in een equivalent meetkundig probleem te vertalen. In deze meetkundige context zullen we het aantal niet-minimale codewoorden berekenen. Dit laat ons toe om in de gevallen waar de gewichtsdistributie van de code gekend is het aantal minimale codewoorden te vinden. De bekomen resultaten verbeteren theoretische resultaten bekomen door Borissov, Manev en Nikova [5], en computerondersteunde resultaten van Borissov en Manev [4].

Eerst en vooral geven we de definities en stellingen nodig voor een goede formulering van het probleem. We zullen een meetkundige interpretatie geven aan de codewoorden, en vervolgens ons probleem vertalen naar een equivalent probleem in eindige meetkunde.

Definitie A.4.1 *Voor elke m en r, $0 \leq r \leq m$, wordt de* binaire r-de orde Reed-Muller code RM(r, m) *gedefinieerd als de verzameling van alle binaire vectoren f van lengte $n = 2^m$ geassocieerd aan Booleaanse veeltermen $f(x_1, x_2, ..., x_m)$ van graad ten hoogste r.*

Definitie A.4.2 *Als $f(x_1, ..., x_m)$ een Booleaanse functie is, dan is $T(f)$ de verzameling vectoren $X = (x_1, ..., x_m)$ zodat $f(X) = 1$.*

Definitie A.4.3 *De* drager *van een codewoord c, genoteerd als supp(c), is de verzameling van posities in het codewoord c die een niet-nul symbool bevatten.*

Definitie A.4.4 *Zij C een q-aire lineaire code. Een niet-nul codewoord $c \in C$ wordt* minimaal *genoemd als zijn meest linkse niet-nul component een 1 is en als hij een drager heeft die geen enkele drager van een ander niet-nul codewoord met als meest linkse niet-nul component een 1 als echte deelverzameling bevat. De drager van een minimaal codewoord wordt* minimaal *genoemd met betrekking tot de code C.*

Het verband met het vorige hoofdstuk wordt gelegd door de volgende stelling van Massey [40], en geeft aan waarom het interessant is om minimale codewoorden te bestuderen.

Stelling A.4.5 *De toegangsstructuur van een secret sharing scheme dat correspondeert met een lineaire q-aire $[n, k]$-code C wordt gespecifieerd door de minimale codewoorden in de duale code $C^\perp$ waarvoor de eerste component een* 1 *is, in de zin dat de verzameling shares bepaald door elk dergelijk minimaal codewoord in de duale code de verzameling shares is corresponderend met de posities na de eerste waar het minimaal codewoord een niet-nul element bezit.*

Volgende eigenschappen zijn te vinden in [1]; de tweede is diegene die essentieel is voor ons resultaat.

Lemma A.4.6 *Zij C een binaire lineaire $[n, k, d]$-code.*

(i) *De drager van een codewoord van gewicht $\leq 2d - 1$ is minimaal met betrekking tot C.*

(ii) *Het codewoord c is een niet-minimaal codewoord in C als en slechts als er een paar niet-nul codewoorden c_1, c_2 bestaat, met onderling disjuncte dragers beide bevat in de drager van c, zodat $c = c_1 + c_2$.*

(iii) *Als c een minimaal codewoord is in C, dan geldt $wt(c) \leq n - k + 1$.*

De natuurlijke vraag die opduikt, is wat er gebeurt tussen deze grenzen. Het kleinste niet-triviale geval is $wt(c) = 2d$. Dit werd opgelost door Borissov, Manev, en Nikova [5] voor RM(r, m), door een meetkundige interpretatie van de minimale codewoorden. Eerst voeren we enkele notaties in om hun resultaat compact te kunnen noteren.

Definitie A.4.7 *De q-*aire Gaussiaanse coëfficiënt *wordt als volgt gedefinieerd:* $\begin{bmatrix} m \\ i \end{bmatrix} = \prod_{j=0}^{i-1} \frac{q^m - q^j}{q^i - q^j}$, $\begin{bmatrix} m \\ 0 \end{bmatrix} = 1$, *voor* $i = 1, 2, \cdots, m$.

Verder gebruiken we de volgende notaties:

$$A_{r,m} = 2^{r-1} \begin{bmatrix} m \\ m-r+1 \end{bmatrix}.$$

$$B_{r,m} = \frac{2^{r+1} - 4}{4} \begin{pmatrix} 2^{r+1} \\ 3 \end{pmatrix} \begin{bmatrix} m \\ m-r-1 \end{bmatrix}.$$

$$S_{r,m} = (2^{m-r+1} - 1)A_{r,m} + 3B_{r,m}.$$

$$E_{r,m} = \sum_{k=\max\{0, m-2r\}}^{m-r} 2^{(m-r-k)(m-r-k+1)} \begin{bmatrix} m-r \\ k \end{bmatrix} \begin{bmatrix} r \\ m-r-k \end{bmatrix}.$$

$$P_{r,m} = 2^{r-1} \begin{bmatrix} m \\ m-r \end{bmatrix} (2^r \begin{bmatrix} m \\ m-r \end{bmatrix} - E_{r,m}).$$

De hoofdstelling van Borissov, Manev en Nikova [5] luidt als volgt.

Stelling A.4.8 *Het aantal niet-minimale codewoorden van gewicht $2d = 2^{m-r+1}$ in RM(r, m) is $A_{r,m} + B_{r,m} + P_{r,m} - S_{r,m}$.*

We vermelden het volgende classificatieresultaat van Kasami, Tokura en Azumi [34] over Booleaanse functies dat de sleutel vormt voor onze meetkundige vertaling van het probleem.

Stelling A.4.9 *Zij $f(x_1, ..., x_m)$ een Booleaanse functie van graad ten hoogste r, met $r \geq 2$, zodat $|T(f)| < 2^{m-r+1}$. Dan kan f affien getransformeerd worden naar één van de volgende vormen:*

$$f = x_1 \cdots x_{r-2}(x_{r-1}x_r + \cdots + x_{r+2\mu-3}x_{r+2\mu-2}),\ 2 \leq 2\mu \leq m - r + 2,$$

$$f = x_1 \cdots x_{r-\mu}(x_{r-\mu+1} \cdots x_r + x_{r+1} \cdots x_{r+\mu}),\ 3 \leq \mu \leq r, \mu \leq m - r.$$

We zullen codewoorden van de vormen hierboven respectievelijk *codewoorden van eerste en tweede type* noemen. Het is welbekend dat de vectoren van kleinste gewicht 2^{m-r} in RM(r, m) geïnterpreteerd kunnen worden als de incidentievectoren van $(m-r)$-dimensionale affiene ruimten.

Met een codewoord van het eerste type correspondeert meetkundig een kwadriek Ψ met als top een $(m-r+1-2\mu)$-dimensionale ruimte $\mathbf{PG}(m-r+1-2\mu, 2)$ volledig op oneindig gelegen en als basis een 2μ-dimensionale niet-singuliere parabolische kwadriek $Q(2\mu, q)$ die de ruimte op oneindig in een niet-singuliere hyperbolische kwadriek $Q^+(2\mu-1, q)$ snijdt.

Met een codewoord van het tweede type correspondeert meetkundig een verzameling affiene punten die exact gelijk is aan de verzameling affiene punten bevat in de unie van twee $(m-r)$-dimensionale ruimten, maar niet in hun doorsnede. We noemen dit een *symmetrisch verschil*.

A.4.2 De meetkundige context

Hier beschrijven we welke verschillende meetkundige situaties zich voordoen. In deze nederlandstalige samenvatting zullen we ons tot deze beschrijving beperken, aangezien zowel de uitwerking van de beschrijving als de formules zeer lang en technisch zijn, en weinig verhelderend. Voor de precieze formules verwijzen we de lezer naar de engelstalige tekst.

We bestuderen de gevallen $c = c_1 + c_2$ uit Lemma A.4.6, met $wt(c) \leq 3 \cdot 2^{m-r}$. Dit impliceert dat we kunnen onderstellen dat $wt(c_1) = 2^{m-r}$ en $wt(c_2) = \frac{3}{2}2^{m-r}$. Eerst en vooral maken we onderscheid tussen twee gevallen naargelang de keuze van het codewoord c_2.

Het codewoord c_2 is een kwadriek Ψ

Zij Π de $(m-r+2)$-dimensionale projectieve ruimte die de kwadriek Ψ bevat en zij α de projectieve sluiting van de $(m-r)$-dimensionale affiene ruimte die correspondeert met het codewoord van kleinste gewicht c_1. De doorsnijding van Π met de ruimte op oneindig wordt genoteerd als Π_∞. Merk op dat Ψ een $(m-r-2\mu+1)$-dimensionale top Γ op oneindig bezit. Noteer de 2μ-dimensionale ruimte die de basis vormt van de kwadriek Ψ met B, en de doorsnijding van B met Π_∞ als B_∞.

Eerst en vooral beschrijven we de verschillende situaties in $\mathbf{AG}(m, q)$ die zich voordoen indien we de paren (Ψ, α) die geen affiene punten gemeen hebben willen tellen, waar Ψ de kwadriek is en waar α een projectieve ruimte $\mathbf{PG}(m-r, q)$ is, niet volledig op oneindig gelegen. Merk op dat in het geval $q = 2$, het affien gedeelte van α het codewoord c_1 definieert en het affien gedeelte van Ψ het codewoord c_2.

Geval 1) De ruimten α en Π hebben geen punten gemeenschappelijk. Dan heeft α zeker geen affiene punten gemeen met Ψ.

Geval 2) De ruimten α en Π snijden in een x-dimensionale ruimte, $x \geq 0$, die compleet op Π_∞ ligt. Al deze ruimten α hebben geen affiene punten gemeen met Ψ. Om het aantal dergelijke ruimten te vinden, beschouwen we een vaste x-dimensionale ruimte Π_x, gelegen in Π_∞, en tellen we hoeveel $(m-r)$-dimensionale ruimten een projectieve sluiting hebben die Π exact in Π_x snijdt.

Geval 3) De ruimten α en Π snijden in een l-dimensionale ruimte Π_l, $l \geq 0$, niet compleet op Π_∞ gelegen. Als $l = 0$, dan tellen we hoeveel $(m-r)$-dimensionale affiene ruimten een projectieve sluiting hebben die Π exact snijden in een affien punt niet gelegen op Ψ.

Veronderstel dus vanaf nu dat $l > 0$, dan komen we tot volgende twee gevallen.

Lemma A.4.10 *Zij α een $(m-r)$-dimensionale affiene ruimte in $\mathbf{AG}(m,q)$ die een niet-ledige intersectie heeft met de $(m-r+2)$-dimensionale affiene ruimte Π die de kwadriek Ψ bevat. Veronderstel dat $\alpha \cap \Pi$ scheef is aan Ψ, dan is $\alpha \cap \Pi_\infty$ ofwel bevat in $\Psi \cap \Pi_\infty$ ofwel is $\alpha \cap \Pi_\infty \cap \Psi$ een hypervlak in $\alpha \cap \Pi_\infty$.*

Bij alle berekeningen vertrekken we van de doorsnijding in Π_∞. Deze doorsnijding moet de ruimte op oneindig vormen van een affiene ruimte die geen punten gemeen heeft met de kwadriek Ψ. Om dergelijke affiene ruimten te bekomen, dienen we externe rechten aan de kwadriek te beschouwen door een punt p op oneindig gelegen. Het aantal dergelijke rechten hangt af van de verschillende specifieke situaties die we hier niet in detail behandelen.

Het codewoord c_2 is een symmetrisch verschil

Noteer de twee $(m-r)$-dimensionale ruimten die het symmetrisch verschil c_2 vormen als β en γ, en zij α de $(m-r)$-dimensionale projectieve ruimte corresponderend met het codewoord c_1. We starten van een vast symmetrisch verschil en tellen hoeveel $(m-r)$-dimensionale affiene ruimten α geen affiene punten gemeen hebben met dit symmetrisch verschil. We onderscheiden volgende gevallen.

Geval 1) Er zijn geen snijpunten van α met β of γ. Dan zijn er zeker ook geen affiene snijpunten.

Geval 2) De enige snijpunten van α met β of γ liggen in $\beta \cap \gamma$. Dus de doorsnijding is een k-dimensionale ruimte gelegen in $\beta \cap \gamma$.

Geval 3) Er zijn snijpunten van α met β of γ niet gelegen in $\beta \cap \gamma$. Bijgevolg liggen alle snijpunten van α met $\beta \cup \gamma$ op oneindig, anders krijgen we affiene snijpunten niet gelegen in $\beta \cap \gamma$.

De gevallen 2) en 3) worden op analoge wijze opgelost gebruikmakend van projecties. We starten van gegeven snijruimten $\alpha \cap \beta$ en $\alpha \cap \gamma$. Dit noemen we een *startconfiguratie*. We tellen hoe vaak elke startconfiguratie kan voorkomen. Dan breiden we zo een startconfiguratie geleidelijk uit tot we een $(m-r)$-dimensionale affiene ruimte α bekomen. In elke stap projecteren we op een ruimte complementair aan de ruimte tot dusver geconstrueerd. We tellen hoeveel uitbreidingsmogelijkheden er zijn bij elke stap. Dit levert een inductieve formule op, waaruit we het gevraagde aantal $(m-r)$-dimensionale affiene ruimten die geen affiene punten gemeen hebben met het gegeven symmetrisch verschil kunnen berekenen.

Verwisselingen

Nadat al deze tellingen zijn gebeurd, dienen we nog de situaties te beschouwen die we eventueel meerdere malen hebben geteld. Om uit te zoeken wanneer dit gebeurt, veronderstellen we dat we een gegeven niet-minimaal codewoord c op twee verschillende wijzen kunnen schrijven als een paar niet-nul codewoorden met disjuncte drager, dus we veronderstellen dat

$$c = c_1 + c_2 = c_3 + c_4.$$

Hierbij veronderstellen we de codewoorden c_1 en c_3 van minimaal gewicht. Zij stemmen dus overeen met $(m-r)$-dimensionale affiene ruimten in $\mathbf{AG}(m, q)$. We veronderstellen dat c_1 en c_3 in een t-dimensionale ruimte snijden. Deze parameter t legt onmiddellijk sterke restricties op voor de intersectiemogelijkheden.

In het geval dat c_2 een kwadriek Ψ is, bewijzen we eerst dat de projectieve sluiting van de $(m-r)$-dimensionale affiene ruimte c_3 de top Γ van de kwadriek c_2, dus Ψ, volledig moet bevatten, opdat een verwisseling zou mogelijk zijn. In een zeer beperkt aantal gevallen, voor de waarden $q = 2$ en $q = 3$, treedt er ook effectief een verwisseling op. In al deze gevallen blijkt c_4 ook een kwadriek te zijn.

Als c_2 een symmetrisch verschil is, zijn er ook in een beperkt aantal situaties paren dubbelgeteld waarbij wegens voorgaande paragraaf c_4 terug een symmetrisch verschil moet zijn.

A.5 Karakteriseringen van Veroneseanen

In [65] wordt een karakterisering van de eindige kwadratische Veroneseaan $\mathcal{V}_n^{2^n}$ aan de hand van de $\mathcal{V}_{n-1}$-deelruimten gegeven. Deze $\mathcal{V}_{n-1}$-deelruimten vormen een sterk reguliere veralgemeende boog. In [35] en [36] bewezen we een extensieresultaat voor sterk reguliere veralgemeende bogen, dat ons toelaat om een vergelijkbare karakterisering van de veralgemeende Veroneseaan te bekomen.

A.5.1 Gekende verwante resultaten

In 1947 bestudeerde Bose ovalen en hyperovalen in [6]. Daar bewees hij dat elke verzameling punten in $\mathbf{PG}(2,q)$, waarvan er geen drie op een rechte liggen, ten hoogste $q+1$ punten bezit als q oneven is en ten hoogste $q+2$ als q even is. Verzamelingen waarvoor deze grenzen worden bereikt worden respectievelijk *ovalen* en *hyperovalen* genoemd.

Speciale gevallen van veralgemeende duale bogen hebben een lange voorgeschiedenis. Zo is een veralgemeende duale boog van graad 0 een (partiële) spread van $\mathbf{PG}(n,q)$. De veralgemeende boog van graad $n-1$ in $\mathbf{PG}(n,q)$ en van type $(n,n-1,\ldots,1,0)$ is niets anders dan het duale van een gewone boog in $\mathbf{PG}(n,q)$.

Veralgemeende duale bogen van graad 1 met $n_2 = 0$ zijn bekend als n_1-dimensionale duale bogen. Het is welbekend dat de dimensie n van de omgevende ruimte $\mathbf{PG}(n,q)$ van een n_1-dimensionale duale boog voldoet aan $2n_1 \leq n \leq \frac{1}{2}n_1(n_1+3)$ (zie [73]).

We hebben volgende stelling over deze duale Veronese boog nodig.

Stelling A.5.1 *Voor q oneven is de duale Veronese boog maximaal, en voor q even kan ze uitgebreid worden met de kernruimte tot een duale boog van grootte q^2+q+2.*

De verzameling $\mathcal{F}$ van q^2+q+1 vlakken in $\mathbf{PG}(5,q)$ uit Voorbeeld A.1.19 bezit de volgende eigenschappen:

(P1) elke twee van deze vlakken snijden in een punt,

(P2) elke drie van deze vlakken bezitten een ledige doorsnede.

Als q oneven is, dan is $D(p)$ het raakvlak aan $\mathcal{V}_2^4$ in p.

In 1958 toonde Tallini [60] (zie ook [28]) dat elke verzameling van q^2+q+1 vlakken in $\mathbf{PG}(5,q)$, q oneven, die voldoet aan (P1) en (P2), isomorf is aan de verzameling $\mathcal{F}$ uit Voorbeeld A.1.19, dus isomorf met de verzameling raakvlakken van $\mathcal{V}_2^4$.

Bovendien zijn raakvlakken gerelateerd aan kegelsnedevlakken, dit is Stelling 25.1.18 uit [28].

Stelling A.5.2 *Als q oneven is, dan bezit $\mathbf{PG}(5,q)$ een polariteit die de kegelsnedevlakken van $\mathcal{V}_2^4$ op de verzameling raakvlakken aan $\mathcal{V}_2^4$ afbeeldt.*

Dit laat toe om een duale versie van de stelling van Tallini te formuleren.

Stelling A.5.3 *Zij $\mathcal{L}$ een verzameling van q^2+q+1 vlakken van $\mathbf{PG}(5,q)$, q oneven, die volgende eigenschappen heeft.*

(i) *Elke twee verschillende elementen uit $\mathcal{L}$ hebben juist 1 punt gemeen.*

(ii) *Elke drie verschillende elementen uit $\mathcal{L}$ brengen $\mathbf{PG}(5,q)$ voort.*

(iii) *Geen enkel punt behoort tot alle elementen uit $\mathcal{L}$.*

Dan is $\mathcal{L}$ de verzameling kegelsnedevlakken aan een Veroneseaan $\mathcal{V}_2^4$.

Dit resultaat werd veralgemeend naar hogere dimensies en naar q even in [65]. Zij bekwamen de volgende karakterisering van de eindige kwadratische Veroneseaan $\mathcal{V}_n^{2^n}$.

Stelling A.5.4 *Zij $\mathcal{F}$ een verzameling van $\frac{q^{n+1}-1}{q-1}$ deelruimten van dimensie $\frac{(n-1)(n+2)}{2}$ in $\mathbf{PG}(N=\frac{n(n+3)}{2},q)$ met de volgende eigenschappen:*

(VS1) Elke twee elementen van $\mathcal{F}$ brengen een hypervlak van $\mathbf{PG}(n,q)$ voort.

(VS2) Elke drie elementen van $\mathcal{F}$ brengen $\mathbf{PG}(N,q)$ voort.

(VS3) Geen enkel punt is bevat in elk element van $\mathcal{F}$.

(VS4) De doorsnede van elke niet-ledige verzameling van elementen van $\mathcal{F}$ is een deelruimte van dimensie $N_i=\frac{i(i+3)}{2}$ voor een $i\in\{-1,0,1,\cdots,n-1\}$.

(VS5) Er zijn drie elementen Ω_1, Ω_2, Ω_3 in $\mathcal{F}$ waarvoor $\Omega_1\cap\Omega_2=\Omega_2\cap\Omega_3=\Omega_3\cap\Omega_1$.

Dan is $\mathcal{F}$ ofwel de verzameling $\mathcal{V}_{n-1}$-deelruimten aan een kwadratische Veroneseaan $\mathcal{V}_n^{2^n}$, of q is even, er bestaan twee elementen $\Omega_1,\Omega_2\in\mathcal{F}$ zodat de $\frac{(n-2)(n+1)}{2}$-dimensionale doorsnede $\Omega_1\cap\Omega_2$ in geen enkel element van $\mathcal{F}$ is bevat en er is een unieke deelruimte Ω van dimensie $\frac{(n-1)(n+2)}{2}$ zodat $\mathcal{F}\cup\{\Omega\}$ de verzameling $\mathcal{V}_{n-1}$-deelruimten samen met de kernruimte is van een kwadratische Veroneseaan $\mathcal{V}_n^{2^n}$.

In het bijzonder, als $n=2$, dan is de stelling geldig zonder dat we $(VS4)$ hoeven te onderstellen.

Voor $d=1$ en q even zijn er niet-Veronese duale bogen met de eigenschap dat elke ruimte opgespannen door twee elementen van $\mathcal{F}$ enkel deze twee elementen van $\mathcal{F}$ bevat. Voor $n=2$ is het mogelijk om alle voorbeelden te classificeren die niet aan (VS5) voldoen door een resultaat uit [15]; het blijkt dat er enkel mogelijkheden zijn voor $q = 2$ en $q = 4$. De classificatie blijft een open probleem voor $n \geq 3$, hoewel een oneindige klasse aan voorbeelden is gekend, beschreven in [65].

Wij werken in de duale ruimte. In Opmerking A.1.23 zagen we dat de duale Veronese boog het duale is van de verzameling van $\mathcal{V}_{n-1}$ deelruimten.

De duale formulering van bovenstaande stelling luidt als volgt. Wij bewijzen een uitbreiding van deze duale versie.

Stelling A.5.5 *Zij $\mathcal{F}$ een verzameling van $\frac{q^{n+1}-1}{q-1}$ n-dimensionale ruimten in* $\mathbf{PG}(\frac{n(n+3)}{2}, q)$ *die voldoen aan*

(VS1) Elke twee elementen uit $\mathcal{F}$ snijden in een punt.

(VS2) Elke drie elementen uit $\mathcal{F}$ hebben een ledige doorsnede.

(VS3) De elementen uit $\mathcal{F}$ brengen $\mathbf{PG}(\frac{n(n+3)}{2}, q)$ voort.

(VS4) Elke eigenlijke deelruimte van $\mathbf{PG}(\frac{n(n+3)}{2}, q)$ opgespannen door een verzameling elementen uit $\mathcal{F}$ is een deelruimte van dimensie $\frac{i(2n-i+3)}{2} - 1$, voor een zekere $i \in \{0, \ldots, n\}$.

(VS5) Als q even is, dan bestaat er tenminste een deelruimte voortgebracht door twee elementen uit $\mathcal{F}$ die meer dan twee elementen van $\mathcal{F}$ bevat.

Dan is $\mathcal{F}$ de duale Veronese boog gedefinieerd door Constructie A.1.18 of q is even, en er zijn twee elementen $\Omega_1, \Omega_2 \in \mathcal{F}$ zodat de $2n$-dimensionale ruimte $\langle \Omega_1, \Omega_2 \rangle$ slechts twee elementen van $\mathcal{F}$ bevat en er is een unieke deelruimte Ω van dimensie n zodat $\{\Omega\} \cup \mathcal{F}$ de unie is van een Veroneseane duale boog gedefinieerd in Constructie A.1.18 samen met zijn kernruimte. In het bijzonder, als $n = 2$, is de stelling geldig onder de zwakkere voorwaarden dat $\mathcal{F}$ voldoet aan $(VS1)$, $(VS2)$, $(VS3)$ en $(VS5)$.

A.5.2 Algebraische karakterisering van duale bogen

Het hoofdresultaat van deze deelsectie is het volgende. Het bewijs van deze stelling is sterk geïnspireerd op de methode gebruikt in [65].

Stelling A.5.6 *Veronderstel dat $d+\delta \leq \frac{q-5}{2}$ als q oneven is en dat $d+\delta \leq \frac{q-6}{2}$ als q even is.*

Zij $\mathcal{F}$ een sterk reguliere veralgemeende duale boog van grootte $\frac{q^{n+1}-1}{q-1} - \delta$ en van type $(n_0, \ldots, n_{d+1})$ waarbij $n_i = \binom{n+d+1-i}{n} - 1$.

Daarenboven veronderstellen we dat elke eigenlijke deelruimte opgespannen door een verzameling elementen uit $\mathcal{F}$ een dimensie $\binom{n+d+1}{d+1} - \binom{n+d+1-i}{d+1} - 1$

voor een $i \in \{0, \ldots, n\}$ heeft. Deze veronderstelling noemen we **eigenschap (P)***.*

Als q even is, veronderstellen we daarenboven dat er twee elementen $\Omega_0, \Omega_1 \in \mathcal{F}$ bestaan zodat $\langle \Omega_0, \Omega_1 \rangle$ tenminste drie elementen van $\mathcal{F}$ bevat.

Dan is $\mathcal{F}$ uitbreidbaar tot een sterk reguliere veralgemeende duale boog van grootte $\frac{q^{n+1}-1}{q-1}$.

Als q even is en $d = 1$, dan is de duale boog zelfs uitbreidbaar tot één van grootte $\frac{q^{n+1}-1}{q-1} + 1$. In alle gevallen is de duale boog een deelverzameling van de maximale duale boog beschreven in 1.3.5 of van de duale Veronese boog plus de kernruimte in het geval $d = 1$, q even.

Hoewel eigenschap (P) ietwat gekunsteld lijkt, kunnen we aantonen dat als q voldoende groot is, meer precies als $q \geq n$, dat eigenschap (P) dan voldaan is voor elke sterke reguliere veralgemeende duale boog.

Het bewijs van Stelling A.5.6 bestaat uit twee grote delen, die we iets nader zullen toelichten in de twee volgende deelsecties. Hieronder geven we eerst een ruwe schets van het bewijs.

Voor het geval $d = 1$ bewijzen we dat voor een deficiëntie $\delta > 0$, met δ klein een duale boog van graad 2 met type (n_0, n_1, n_2) en van grootte $\frac{q^{n+1}-1}{q-1} - \delta$ niet maximaal is.

Voor $d > 1$ gebruiken we inductie op d. Het hoofdidee van dit stuk is het volgende. In Constructie A.1.18 hadden we $n + 1$ speciale elementen van de boog, namelijk die van de vorm $D((0, \ldots, 0, 1, 0, \ldots, 0))$. In elk van deze elementen induceren de andere elementen van de boog een duale boog van grootte $\frac{q^{n+1}-1}{q-1} - 1$. Dus elk element $(n, n_1, \ldots, n_d)$ van de boog bevat een extensieruimte. Binnen deze extensieruimte kunnen we opnieuw kijken naar de geinduceerde boog om opnieuw een extensieruimte te vinden, enzovoort.

Het idee van het bewijs is om $n+1$ elementen van de duale boog te vinden die de ruimte volledig opspannen. Deze elementen zullen blijken de elementen van de vorm $(n, n_1, \ldots, n_d)$ te zijn. Daarnaast kiezen we nog een $(n + 2)$-de element dat intuïtief correspondeert met een eenheidspunt van $\mathbf{PG}(n, q)$. Vervolgens gebruiken we inductief de gekende algebraische karakterisering van de duale bogen van graad $d - 1$ om de Veroneseaan terug te vinden.

A.5.3 Het geval $d = 1$

Voor $d = 1$ reduceert onze hoofdstelling zich tot de volgende stelling. Bemerk hierbij dat de voorwaarden exact dezelfde zijn als die van Stelling A.5.4.

Stelling A.5.7 *Veronderstel dat $\delta \leq \frac{q-5}{2}$ als q oneven is en dat $\delta \leq \frac{q-6}{2}$ als q even is, en zij $\mathcal{F}$ een verzameling van $\frac{q^{n+1}-1}{q-1} - \delta$ verschillende n-dimensionale ruimten in $\mathbf{PG}(\frac{n(n+3)}{2}, q)$ met de volgende eigenschappen:*

(VS1) Elke twee elementen van $\mathcal{F}$ snijden in een punt.

(VS2) Elke drie elementen van $\mathcal{F}$ hebben een ledige intersectie.

(VS3) De elementen van $\mathcal{F}$ spannen de ruimte $\mathbf{PG}(\frac{n(n+3)}{2}, q)$ op.

(VS4) Elke eigenlijke deelruimte van $\mathbf{PG}(\frac{n(n+3)}{2}, q)$ opgespannen door een verzameling elementen uit $\mathcal{F}$ is een deelruimte van dimensie $\frac{i(2n-i+3)}{2} - 1$, voor een $i \in \{0, \ldots, n\}$.

(VS5) Als q even is, dan bestaat er tenminste één ruimte opgespannen door twee elementen uit $\mathcal{F}$ die meer dan twee elementen uit $\mathcal{F}$ bevat.

Dan is $\mathcal{F}$ een sterk reguliere veralgemeende duale boog van grootte $\frac{q^{n+1}-1}{q-1} - \delta$ van graad 2 en type (n_0, n_1, n_2), waarbij $n_i = \binom{n+2-i}{n} - 1$, uitbreidbaar tot een sterk reguliere veralgemeende duale boog van grootte $\frac{q^{n+1}-1}{q-1}$. In het geval q even is het bovendien geweten dat elke duale boog van grootte $\frac{q^{n+1}-1}{q-1}$ uitbreidbaar is tot een duale boog van grootte $\frac{q^{n+1}-1}{q-1} + 1$.

Opnieuw geldt dat als $q \geq n$ dat dan (VS4) automatisch volgt uit (VS1), (VS2) en (VS3).

In het geval van de Veroneseaan geldt dat elk element van $\mathcal{F}$ correspondeert met een punt van de projectieve ruimte $\mathbf{PG}(n, q)$. De $2n$-dimensionale ruimten opgespannen door twee elementen van $\mathcal{F}$ corresponderen met rechten van $\mathbf{PG}(n, q)$. In dit geval zijn de mogelijkheden voor het aantal elementen van $\mathcal{F}$ bevat in een $2n$-ruimte dus beperkt.

Volgend lemma vormt een eerste stap in deze richting en toont ook al een eerste keer aan dat er een verschil zal optreden tussen de gevallen q even en q oneven. Het geval q even vraagt wat meer werk omdat daar een kern kan optreden; deze kan geïdentificeerd worden waarna we kunnen verder werken zoals in het geval q oneven. We zullen in deze appendix hier niet op ingaan.

Lemma A.5.8 *Elke $2n$-dimensionale ruimte bevat $0, 1, 2$ of tenminste $q - \delta$ ($\delta \leq \frac{q-7}{2}$ als q oneven is en $\delta \leq \frac{q-8}{2}$ als q even is) elementen van $\mathcal{F}$. Als q oneven is, kan het geval 2 zich bovendien niet voordoen.*

We zullen een $2n$-ruimte *groot* noemen als het tenminste $q - \delta$ elementen van $\mathcal{F}$ bevat. Een volgend lemma legt in elke grote $2n$-ruimte een speciaal vlak vast, dat heel wat structurele informatie in zich draagt.

Lemma A.5.9 *Zij Π een grote $2n$-dimensionale ruimte. Dan bevat Π een vlak $\bar{\pi}$ dat de elementen van $\mathcal{F}$ in Π in rechten snijdt. De elementen van $\mathcal{F}$, niet in Π, snijden Π in een rechte die $\bar{\pi}$ niet snijdt.*

Het volgend lemma is een eerste aanwijzing van het feit dat de *contactpunten*, dit zijn de punten bevat in exact één element van $\mathcal{F}$, die we her en der zien, gestructureerd liggen.

Lemma A.5.10 *Zij $\pi \in \mathcal{F}$. Beschouw alle grote $2n$-dimensionale ruimten door π. Dan snijden de vlakken $\bar{\pi}$ bevat in deze ruimten de ruimte π in verschillende rechten door een zelfde punt.*

We slaan hier in de appendix enkele technische stappen over. Hierin wordt bewezen dat de rechten die we zien in de vlakken $\bar{\pi}$ de gewenste structuur bezitten. Na dit technisch stuk zijn we in staat om het volgende te doen.

We definiëren een lineaire ruimte $\mathcal{L}$ met als *punten* de elementen van $\mathcal{F}$ en de $2n$-dimensionale ruimten voortgebracht door twee elementen van $\mathcal{F}$ als *rechten*. Als *vlakken* definiëren we de $(3n-1)$-dimensionale ruimten voortgebracht door drie elementen van $\mathcal{F}$.

Lemma A.5.11 *Elk vlak van $\mathcal{L}$ is een projectief vlak van de orde q met enkele gaten.*

Onderstaand lemma vervolledigt het bewijs van Stelling A.5.7.

Lemma A.5.12 *Zij $\mathcal{F}$ een duale boog die aan de veronderstellingen van Stelling A.5.7 voldoet. Als $\delta > 0$, dan is $\mathcal{F}$ niet maximaal.*

A.5.4 Het geval $d \geq 2$

We geven een summiere schets van de structuur van het bewijs voor het geval $d \geq 2$ zonder volledig te willen zijn. Zo zullen we bijvoorbeeld de technische moeilijkheden voor het geval q even met een eventuele kern niet aankaarten. In het eerste deel van deze deelsectie tonen we aan dat bepaalde onderstellingen over $\mathcal{F}$ blijven gelden in deelstructuren; dit is noodzakelijk om inductie te kunnen toepassen. Fixeer een element $\Omega \in \mathcal{F}$ en definieer $\mathcal{F}_\Omega = \{\Omega \cap \Omega_i || \Omega_i \in \mathcal{F} \backslash \{\Omega\}\}$. We vatten deze resultaten samen in onderstaande lemmata.

Lemma A.5.13 *Als $\mathcal{F}$ sterk regulier is, dan is $\mathcal{F}_\Omega$ sterk regulier. Hieruit volgt dat als $\mathcal{F}$ een sterk reguliere veralgemeende duale boog is met $q \geq n$ dat $\mathcal{F}$ dan voldoet aan eigenschap (P). Bovendien geldt als $\mathcal{F}$ sterk regulier is en aan eigenschap (P) voldoet, dat dan ook $\mathcal{F}_\Omega$ aan eigenschap (P) voldoet.*

Lemma A.5.14 *Zij q even en veronderstel dat $\mathcal{F}$ een sterk reguliere veralgemeende duale boog is, die voldoet aan eigenschap (P) en drie speciale elementen $\Omega_1', \Omega_2', \Omega_3'$ bevat met $\Omega_3' \subset \langle \Omega_1', \Omega_2' \rangle$. Dan bezit $\mathcal{F}_\Omega$ drie elementen $\Omega_1 \cap \Omega, \Omega_2 \cap \Omega, \Omega_3 \cap \Omega$ zodat $\Omega_3 \cap \Omega$ bevat is in $\langle \Omega_1 \cap \Omega, \Omega_2 \cap \Omega \rangle$.*

De volgende stelling toont aan dat de boog geconstrueerd aan de hand van de Veroneseaan niet kan uitgebreid worden.

Stelling A.5.15 *Zij $d \geq 2$. Dan is de sterk reguliere veralgemeende duale boog gedefinieerd via Constructie A.1.18 maximaal.*

Hiermee is het bewijs van Stelling A.5.6 voltooid.

A.5.5 Open problemen

Voor sommige van onze onderstellingen zijn ons geen tegenvoorbeelden gekend. Het is heel interessant om te weten of dergelijke voorbeelden bestaan of anders of het mogelijk is om deze onderstellingen uit de andere onderstellingen te bewijzen. In het bijzonder krijgen we volgende vragen:

- Er zijn ons geen voorbeelden bekend van reguliere duale bogen die niet sterk regulier zijn. Bestaan dergelijke voorbeelden?
- Voor $d = 1$ hebben we voorbeelden van niet-Veronese duale bogen waarvoor geen enkele $2n$-ruimte meer dan twee elementen van de boog bevat. Wat gebeurt er in het geval $d > 1$?
- We hebben eigenschap (P) bewezen voor $q \geq n$. Bestaan er tegenvoorbeelden van eigenschap (P) als $q < n$?

A.5.6 Een karakterisering van de Veroneseaan aan de hand van intersectiegetallen

In deze sectie bekomen we een combinatorische karakterisering van de Veroneseaan aan de hand van intersectiegetallen. Het resultaat steunt op een gelijkaardig resultaat voor de Veroneseaan $\mathcal{V}_2^4$ door Ferri [22], Hirschfeld en Thas [28], en Thas en Van Maldeghem [66], en een structurele karakterisering van de Veroneseaan door Thas en Van Maldeghem [65].

We starten met de karakterisering van $\mathcal{V}_2^4$ aan de hand van intersectiegetallen met vlakken en 4-ruimten.

Stelling A.5.16 *Zij $\mathcal{K}$ een verzameling van k punten in $\mathbf{PG}(5,q)$, $q \neq 2,4$, die aan volgende voorwaarden voldoet:*

(i) $|\Pi_4 \cap \mathcal{K}| = 1,\ q+1,\ 2q+1$ *voor elk hypervlak* Π_4 *van* $\mathbf{PG}(5,q)$ *en er bestaat een hypervlak* Π_4 *waarvoor* $|\Pi_4 \cap \mathcal{K}| = 2q+1$.

(ii) Elk vlak van $\mathbf{PG}(5,q)$ dat vier punten van $\mathcal{K}$ bevat, bevat tenminste $q+1$ punten van $\mathcal{K}$.

Dan is $\mathcal{K}$ de puntenverzameling van een Veroneseaan $\mathcal{V}_2^4$.

Een stelling van Zanella [76] levert een bovengrens op het aantal punten van de kwadratische Veroneseaan dat kan bevat zijn in een k-dimensionale ruimte. Ze luidt als volgt.

Stelling A.5.17 *Beschouw de Veroneseaan $\mathcal{V}_n$ gedefinieerd door de afbeelding*

$$\zeta : \mathbf{PG}(n,q) \to \mathbf{PG}(\frac{n(n+3)}{2}, q) :$$

$$(x_0, x_1, \cdots, x_n) \mapsto (x_0^2, \cdots, x_n^2, x_0x_1 \cdots, x_{n-1}x_n).$$

Zij k, n, a natuurlijke getallen zodat $k+1 \leq \frac{(a+3)(a+2)}{2}$, dan bevatten de doorsnedes $\Pi_k \cap \mathcal{V}_n$ ten hoogste

$$\frac{q^{a+1}-1}{q-1} + q^{k-\frac{(a+2)(a+1)}{2}}$$

punten.

Toegepast op lage dimensies levert dit de bovengrenzen $q+1$, $q+2$, $2q+1$ en q^2+q+1 voor $k=2$, $k=3$, $k=4$ en $k=5$ respectievelijk.

De volgende structuurstelling werd bewezen door Thas en Van Maldeghem in [66].

Stelling A.5.18 *Zij X een verzameling punten in $\Pi := \mathbf{PG}(M,q)$, $M > 2$, die Π opspant, en zij $\mathcal{P}$ een verzameling vlakken zodat voor elke $\pi \in \mathcal{P}$ de doorsnede $X \cap \pi$ een ovaal is in π. Voor elke $\pi \in \mathcal{P}$ en elke $x \in X \cap \pi$ noteren we de raaklijn in x aan $X \cap \pi$ als $T_x(\pi)$. Onderstel volgende drie eigenschappen:*

(i) Elke twee punten $x, y \in X$ zijn bevat in een uniek element van $\mathcal{P}$, genoteerd als $[x,y]$.

(ii) Als $\pi_1, \pi_2 \in \mathcal{P}$ en $\pi_1 \cap \pi_2$ is niet leeg, dan geldt $\pi_1 \cap \pi_2 \subset X$.

(iii) Als $x \in X$ en $\pi \in \mathcal{P}$ waarbij $x \notin \pi$, dan is elk van de rechten $T_x([x,y])$, $y \in X \cap \pi$, bevat in een vast vlak van Π, genoteerd $T(x,\pi)$.

Dan bestaat er een natuurlijk getal $n \geq 2$ (dat de index *van X wordt genoemd), een projectieve ruimte $\Pi' := \mathbf{PG}(\frac{n(n+3)}{2}, q)$ die Π bevat, en een kwadratische Veroneseaan $\mathcal{V}_n$ van index n in Π', met $R \cap \mathcal{V}_n = \emptyset$, zodat X de (bijectieve) projectie van $\mathcal{V}_n$ vanuit R op Π is. De deelruimte R kan leeg zijn; in dit geval is X projectief equivalent met $\mathcal{V}_n$.*

Onze karakterisering wordt hieronder beschreven. Zij $\mathcal{K}$ een verzameling van $\frac{q^{n+1}-1}{q-1}$ punten die $\mathbf{PG}(\frac{n(n+3)}{2}, q)$, met $n \geq 2$, opspant waarvoor geldt:

(i) Als een vlak π minstens vier punten van $\mathcal{K}$ bevat, dan bevat het exact $q+1$ punten van $\mathcal{K}$. Bovendien onderstellen we dat elke twee punten van $\mathcal{K}$ bevat zijn in een vlak dat $\mathcal{K}$ in $q+1$ punten snijdt.

(ii) Als in een 3-ruimte Π_3 geldt dat $|\Pi_3 \cap \mathcal{K}| \geq 5$, dan zijn er vier punten van $\mathcal{K}$ bevat in een vlak gelegen in Π_3. In het bijzonder volgt hier wegens (i) uit dat als $|\Pi_3 \cap \mathcal{K}| > 4$, dan $|\Pi_3 \cap \mathcal{K}| \geq q+1$.

(iii) Als een 5-ruimte Π_5 de verzameling $\mathcal{K}$ in meer dan $2q+2$ punten snijdt, dan snijdt ze $\mathcal{K}$ in exact q^2+q+1 punten.

Opmerking A.5.19 *Bemerk dat voor $n = 2$ de derde voorwaarde ledig is.*

Als $\mathcal{K}$ aan bovenstaande voorwaarden voldoet, dan geldt de volgende stelling.

Stelling A.5.20 *Als $q \geq 5$, dan is de verzameling $\mathcal{K}$ de puntenverzameling van de Veroneseaan van alle kwadrieken van $\mathbf{PG}(n, q)$.*

Een tegenvoorbeeld voor $q = 2$, $n > 2$, voor bovenstaande stelling wordt gegeven door een punt in een Veronese variëteit te vervangen door een punt dat correspondeert met een matrix van maximale rang, gebruikmakende van de correspondentie gegeven in Stelling A.1.16.

Een tegenvoorbeeld voor $q = 3$, $n = 2$, wordt gegeven door de puntenverzameling van een elliptische kwadriek $\mathcal{E}$ in een 3-ruimte $\Pi_3 \subset \mathbf{PG}(5, 3)$ gelegen en 3 punten op een rechte $L \subset \mathbf{PG}(5, 3)$ die Π_3 niet snijdt.

Het bewijs verloopt in verschillende stappen. Eerst wordt bewezen dat een 4-ruimte voldoet aan de grenzen van Stelling A.5.17 van Zanella. Vervolgens tonen we aan dat elke 5-ruimte die $\mathcal{K}$ in $q^2 + q + 1$ punten snijdt een kwadratische Veroneseaan $\mathcal{V}_2^4$ is. Dit laat toe om Stelling A.5.18 toe te passen.

Voorwaarde (i) is een sterke voorwaarde aangezien ze a priori al de 'kegelsnedes' de structuur laat binnen sluipen. Als $n > 2$, dan kunnen we echter onze voorwaarden afzwakken tot de volgende:

Zij $\mathcal{K}$ een verzameling van $\frac{q^{n+1}-1}{q-1}$ punten die $\mathbf{PG}(\frac{n(n+3)}{2}, q)$, met $n > 2$, opspant en waarvoor geldt:

(i') Een vlak π snijdt $\mathcal{K}$ in hoogstens $q+1$ punten.

(ii') Als in een 3-ruimte Π_3 geldt dat $|\Pi_3 \cap \mathcal{K}| \geq 5$, dan geldt dat $|\Pi_3 \cap \mathcal{K}| \geq q+1$ en er is een vlak in Π_3 dat minstens 4 punten van $\mathcal{K}$ bevat.

(iii') Als een 5-ruimte Π_5 de verzameling $\mathcal{K}$ in meer dan $2q + 2$ punten snijdt, dan snijdt ze $\mathcal{K}$ in exact $q^2 + q + 1$ punten. Bovendien geldt dat elke twee punten p_1, p_2 van $\mathcal{K}$ bevat zijn in een 5-ruimte die $q^2 + q + 1$ punten van $\mathcal{K}$ bevat.

Een tegenvoorbeeld voor $n = 2$ is het volgende. Beschouw in $\mathbf{PG}(5, q)$ een punt p op een ovoïde $\mathcal{O}$ in $\Pi_3 = \mathbf{PG}(3, q)$ en een raaklijn L aan $\mathcal{O}$ in p. Bekijk vervolgens een vlak π dat Π_3 exact in L snijdt en een ovaal $\mathcal{O}'$ bevat die L in p snijdt. Dan voldoet $\mathcal{O} \cup \mathcal{O}'$ aan (i'), (ii') en (iii'), maar het is geen kwadratische Veroneseaan $\mathcal{V}_2^4$.

A.6 Karakteriseringen van klassieke polaire ruimten door intersectiegetallen

A.6.1 Inleiding

Het beroemde resultaat van Segre [51] dat elke $q + 1$ punten in $\mathbf{PG}(2, q)$, q oneven, waarvan geen drie punten collineair zijn, een kegelsnede vormen, stond aan de wieg van de combinatorische meetkunde en sindsdien hebben combinatorische karakteriseringen van objecten die klassiek algebraisch gedefinieerd worden de interesse gewekt van velen; niet alleen omwille van de estheticiteit maar ook omdat deze karakteriseringen vele nuttige toepassingen hebben in aanverwante disciplines zoals bijvoorbeeld de codeertheorie.

Het volgende karakteriseringsresultaat van Ferri en Tallini [23] van de parabolische kwadriek $Q(4, q)$ vormde de start van ons onderzoek.

Stelling A.6.1 *Een verzameling punten K in $\mathbf{PG}(n, q)$, met $n \geq 4$ en $|K| \geq q^3 + q^2 + q + 1$, die elk vlak in 1, a of b punten snijdt, met $b \geq 2q + 1$, en die elke 3-dimensionale ruimte in c, $c + q$ of $c + 2q$ punten snijdt, met $c \leq q^2 + 1$, zodat er 3-dimensionale ruimten bestaan die K in c en $c + q$ punten snijden, is een niet-singuliere kwadriek van $\mathbf{PG}(4, q)$.*

Via eenvoudige telargumenten kan men volgende stelling bewijzen als gevolg van het voorgaande. Dit gevolg vormt het uitgangspunt van de resultaten bekomen in dit hoofdstuk.

Gevolg A.6.2 *Als een verzameling punten in $\mathbf{PG}(n, q)$, $n \geq 4$, elk vlak in $1, q{+}1,$ of $2q{+}1$ punten snijdt en elke 3-dimensionale ruimte in $q^2{+}1, q^2{+}q{+}1$ of $q^2{+}2q{+}1$ punten snijdt, dan is $\mathcal{K}$ de puntenverzameling van een parabolische kwadriek $Q(4, q)$.*

Deze stelling roept natuurlijkerwijze de volgende vragen op.

> Is het mogelijk om andere eindige klassieke polaire ruimten te karakteriseren aan de hand van hun intersectiegetallen ten opzichte van vlakken en 3-dimensionale ruimten, respectievelijk, is het mogelijk om ze te karakteriseren aan de hand van hun intersectiegetallen ten opzichte van hypervlakken en ruimten van codimensie 2.

Merk hierbij op dat deze vragen uiteraard weinig zin hebben voor de symplectische polaire ruimte $W_{2n+1}(q)$, daar deze polaire ruimte alle punten bevat van de projectieve ruimte die zij opspant.

De eerste vraag werd positief beantwoord in [47] voor kwadrieken, en in [49] voor Hermitische variëteiten, de tweede in [17]. De bewijsmethode om de eerste vraag te beantwoorden bestaat erin uit de intersectiegetallen de voorwaarden van de Stellingen A.1.6, A.1.7, A.1.9, A.1.10 en A.1.11 die veralgemeende vierhoeken, Shult ruimten en polaire ruimten karakteriseren af te leiden. Voor de tweede vraag wordt een dualiteit gebruikt, en voorgaande karakteriseringen van polaire ruimten aan de hand van intersectiegetallen.

Hoewel het mogelijk is om polaire ruimten enkel en alleen aan de hand van hun intersectiegetallen met rechten te karakteriseren, is het onmogelijk om enkel de intersectiegetallen met hypervlakken te gebruiken voor een karakterisering van polaire ruimten. Dit omdat er een vrije constructie bestaat waarmee men in overvloed *quasi-kwadrieken* en *quasi-Hermitische variëteiten* kan construeren. Hierbij definiëren we een quasi-kwadriek, respectievelijk een quasi-Hermitische variëteit als een deelverzameling van de puntenverzameling van de projectieve ruimte die dezelfde intersectiegetallen heeft met hypervlakken als een niet-singuliere kwadriek, respectievelijk, een niet-singuliere Hermitische variëteit. In het parabolisch geval is er een lichte afwijking van de originele definitie zoals gegeven in [14]. In dit laatste artikel worden quasi-Hermitische variëteiten niet gedefinieerd, maar met zeer analoge constructies als diegene die daar aangewend worden voor quasi-kwadrieken kan men deze objecten construeren.

A.7 Resultaten

Volgende karakteriseringen van kwadrieken en Hermitische variëteiten, die men kan vinden in [28], zijn van groot belang voor de resultaten later bekomen in het hoofdstuk. Op zich vormen ze ook mooie voorbeelden van Segre-type stellingen.

Definitie A.7.1 *Een puntenverzameling $\mathcal{K}$ in $\mathbf{PG}(n,q)$ is van* type $(r_1, r_2, \cdots, r_s)$ *als* $|L\cap\mathcal{K}| \in \{r_1, r_2, \cdots, r_s\}$ *voor alle rechten L in $\mathbf{PG}(n,q)$.*

Een punt $p \in \mathcal{K}$ is singulier *ten opzichte van $\mathcal{K}$ als alle rechten door p de verzameling $\mathcal{K}$ in 1 of $q+1$ punten snijden. Als de verzameling $\mathcal{K}$ een singulier punt bevat, dan wordt $\mathcal{K}$* singulier *genoemd.*

Volgende stelling is een amalgaam van resultaten bekomen door Tallini-Scafati [61], Hirschfeld en Thas [27], en Glynn [25].

Stelling A.7.2 *Zij $\mathcal{K}$ een niet-singuliere puntenverzameling van type $(1, r, q^2+1)$ in $\mathbf{PG}(n, q^2)$, $n \geq 4$ en $q > 2$, die voldoet aan volgende eigenschappen:*

- *$3 \leq r \leq q^2 - 1$;*
- *Er is geen vlak π zodat elke rechte bevat in π de verzameling $\mathcal{K}$ in r of $q^2 + 1$ punten snijdt.*

Dan is de verzameling $\mathcal{K}$ de puntenverzameling van een niet-singuliere Hermitische variëteit $H(n, q^2)$.

Het resultaat hieronder werd bekomen door Tallini in [58] en [59].

Stelling A.7.3 *Zij $\mathcal{K}$ een niet-singuliere puntenverzameling van type $(0, 1, 2, q+1)$ in $\mathbf{PG}(n, q)$ met $n \geq 4$ en $q > 2$.*
Als $\frac{q^{n+1}-1}{q-1} > |\mathcal{K}| \geq \frac{q^n-1}{q-1}$, dan geldt één van de volgende gevallen:

(i) *$|\mathcal{K}| = \frac{q^n-1}{q-1}$, n is even, en $\mathcal{K}$ is de puntenverzameling van een parabolische kwadriek $Q(n, q)$.*

(ii) *$|\mathcal{K}| = \frac{q^n-1}{q-1} + q^{\frac{n-1}{2}}$, n is oneven, en $\mathcal{K}$ is de puntenverzameling van een hyperbolische kwadriek $Q^+(n, q)$.*

(iii) *$|\mathcal{K}| = \frac{q^n-1}{q-1} + 1$, q is even, en $\mathcal{K} = \Pi_t\mathcal{K}' \cup \{N\}$ waarbij Π_t een $\mathbf{PG}(t, q) \subset \mathbf{PG}(n, q)$ is, en met $\mathcal{K}'$ de puntenverzameling van een parabolische kwadriek $Q(n-t-1, q)$ in een $(n-t-1)$-dimensionale deelruimte van $\mathbf{PG}(n, q)$ scheef aan $\mathbf{PG}(t, q)$ (bijgevolg is $n-t-1$ even) of waarbij $\mathcal{K}'$ een $(q+1)$-boog is in een vlak scheef aan $\mathbf{PG}(t, q)$ als $t = n-3$. In beide gevallen is N de kern van een vooraf gekozen basis $\mathcal{K}'$.*

De volgende stelling geeft een karakterisering van kwadrieken aan de hand van de intersectiegetallen met vlakken en 3-dimensionale ruimten.

Stelling A.7.4 *Als elk intersectiegetal van een puntenverzameling $\mathcal{K}$ in $\mathbf{PG}(n, q)$, $n \geq 4$, met vlakken en 3-dimensionale ruimten ook een intersectiegetal is van kwadrieken met vlakken en 3-dimensionale ruimten, dan is $\mathcal{K}$ één van de volgende verzamelingen:*

(i) de projectieve ruimte $\mathbf{PG}(n,q)$,

(ii) een hypervlak in $\mathbf{PG}(n,q)$,

(iii) een kwadriek in $\mathbf{PG}(n,q)$,

(iv) met q even,

(iv.1) een kegel met top een $(n-3)$-dimensionale ruimte en basis een ovaal.

(iv.2) een kegel met top een $(n-4)$-dimensionale ruimte en basis een ovoïde.

Voor Hermitische variëteiten bewezen we volgende twee stellingen, die nuttig zijn als hulpmiddel voor de algemene karakterisering van Hermitische variëteiten aan de hand van hun intersectiegetallen met vlakken en 3-dimensionale ruimten, waarbij de tweede stelling het analogon is van Stelling A.6.2 voor kwadrieken.

Stelling A.7.5 *Als elk intersectiegetal met vlakken en 3-dimensionale ruimten van een puntenverzameling $\mathcal{K}$ in $\mathbf{PG}(3,q^2)$ ook een intersectiegetal met vlakken en 3-dimensionale ruimten van $H(3,q^2)$ is, dan is $\mathcal{K}$ een Hermitische variëteit $H(3,q^2)$.*

Stelling A.7.6 *Als elk intersectiegetal met vlakken en 3-dimensionale ruimten van een puntenverzameling $\mathcal{K}$ in $\mathbf{PG}(4,q^2)$ ook een intersectiegetal met vlakken en 3-dimensionale ruimten van $H(4,q^2)$ is, dan is $\mathcal{K}$ een niet-singuliere Hermitische variëteit $H(4,q^2)$.*

Bovenstaande hulpresultaten leiden mede tot de volgende karakterisering aan de hand van intersectiegetallen met vlakken en 3-dimensionale ruimten.

Stelling A.7.7 *Als elk intersectiegetal met vlakken en 3-dimensionale ruimten van een puntenverzameling $\mathcal{K}$ in $\mathbf{PG}(n,q^2)$, $n \geq 4$, ook een intersectiegetal met vlakken en 3-dimensionale ruimten van een Hermitische variëteit is, dan is $\mathcal{K}$ één van de volgende verzamelingen:*

(i) *de projectieve ruimte $\mathbf{PG}(n,q^2)$,*

(ii) *een hypervlak in $\mathbf{PG}(n,q^2)$,*

(iii) *een Hermitische variëteit in $\mathbf{PG}(n,q^2)$,*

(iv) *een kegel met top een $(n-2)$-dimensionale ruimte en basis een rechte die $\mathcal{K}$ in q of $q+1$ punten snijdt,*

(v) *een kegel met top een* $(n-3)$*-dimensionale ruimte en basis een unitaal,*

(vi) *een kegel met top een* $(n-3)$*-dimensionale ruimte en basis een verzameling* $\tilde{\mathcal{K}}$ *van* $\mathbf{PG}(2,q^2)$ *die elke rechte van* $\mathbf{PG}(2,q^2)$ *in* 1, q, $q+1$ *of* q^2+1 *punten snijdt en exact één rechte volledig bevat.*

Opmerking A.7.8 *Zij* $\mathcal{M}$ *een* maximale $\{q^3-q^2+q;q\}$-boog *in* $\mathbf{PG}(2,q^2)$*, dit is een puntenverzameling* $\mathcal{M}$ *van grootte* q^3-q^2+q *in* $\mathbf{PG}(2,q^2)$ *die elke rechte van* $\mathbf{PG}(2,q^2)$ *in* 0 *of* q *punten snijdt; een dergelijke verzameling bestaat voor elke* $q=2^h$*, zie [30]. Zij* M *een rechte van* $\mathbf{PG}(2,q^2)$ *die* $\mathcal{M}$ *in* q *punten snijdt and zij* L *een rechte van* $\mathbf{PG}(2,q^2)$ *die geen punten van* $\mathcal{M}$ *bevat. Dan kan* $\tilde{\mathcal{K}}=(\mathcal{M}\backslash M)\cup L$ *als basis genomen worden voor de kegel in Stelling A.7.7 (vi).*

Tot dusver hebben we het gevolg van Stelling A.6.1 van Ferri en Tallini uitgebreid tot hoger-dimensionale kwadrieken en Hermitische variëteiten waarbij we extra intersectiegetallen voor vlakken en 3-dimensionale ruimten hebben toegelaten. Een andere richting is om intersecties met vlakken en 3-dimensionale ruimten in een 4-dimensionale ruimte meer algemeen te zien als intersecties met hypervlakken en ruimten van codimensie 2 in hoger-dimensionale ruimten. Deze richting leidt tot een karakterisering van niet-singuliere klassieke polaire ruimten, uiteraard met uitzondering van de symplectische polaire ruimten.

We tonen aan dat niet-singuliere kwadrieken en niet-singuliere Hermitische variëteiten volledig gekarakteriseerd worden door hun intersectiegetallen met hypervlakken en ruimten van codimensie 2. Dit veralgemeent sterk Stelling A.6.1 van Ferri en Tallini en bezorgt nodige en voldoende voorwaarden voor quasi-kwadrieken (quasi-Hermitische variëteiten) om niet-singuliere kwadrieken (niet-singuliere Hermitische variëteiten) te zijn.

Dit wordt precies gemaakt in de volgende stelling.

Stelling A.7.9 *Als een puntenverzameling* $\mathcal{K}$ *in* $\mathbf{PG}(n,q)$*,* $n\geq 4$*,* $q>2$*, dezelfde intersectiegetallen heeft met hypervlakken en ruimten van codimensie 2 als een polaire ruimte* $P\in\{H(n,q),Q^+(n,q),Q^-(n,q),Q(n,q)\}$*, dan is* $\mathcal{K}$ *de puntenverzameling van een dergelijke niet-singuliere polaire ruimte* P*.*

Bibliography

[1] A. Ashikhmin and B. Barg. Minimal vectors in linear codes. *IEEE Trans. Inform. Theory*, **44**, (1998), 2010–2017.

[2] S. Ball. Multiple blocking sets and arcs in finite planes. *J. London Math. Soc.*, **54**, (1996), 581–593.

[3] A. Blokhuis, L. Storme, and T. Szőnyi. Lacunary polynomials, multiple blocking sets and Baer subplanes. *J. London Math. Soc.*, **60** (1999) 321–332.

[4] Y. Borissov and N. Manev. Minimal codewords in linear codes. *Serdica Math. J.*, **30**, (2004), 303–324.

[5] Y. Borissov, N. Manev and S. Nikova. On the non-minimal codewords in binary Reed-Muller codes. *Discrete Appl. Math.*, **128**, (2003), 65–74.

[6] R. C. Bose. Mathematical theory of the symmetrical factorial design. *Sankhyā*, (1947), 107–166.

[7] 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.

[8] A. A. Bruen. Baer subplanes and blocking sets. *Bull. Amer. Math. Soc.*, **76**, (1970), 342–344.

[9] A. A. Bruen. Polynomial multiplicities over finite fields and intersection sets. *J. Combin. Theory Ser. A*, **60**, (1992), 19–33.

[10] A. A. Bruen and J. A. Thas. Blocking sets. *Geom. Dedicata*, **6**, (1977), 193–203.

[11] F. Buekenhout and C. Lefèvre. Generalized quadrangles in projective spaces. *Arch. Math.*, **25**, (1974), 540–552.

[12] F. Buekenhout and E. E. Shult. On the foundations of polar geometry. *Geom. Dedicata*, **3**, (1974), 155–170.

[13] L. R. A. Casse, J. A. Thas, and P. R. Wild. $(q^n + 1)$-sets of $\mathbf{PG}(3n-1,q)$, generalized quadrangles and Laguerre planes. *Simon Stevin*, **59**, (1985), 21–42.

[14] F. De Clerck, N. Hamilton, C. O'Keefe, and T. Penttila. Quasi-quadrics and related structures. *Australas. J. Combin.*, **22**, (2000), 151–166.

[15] A. Del Fra. On d-dimensional dual hyperovals, *Geom. Dedicata*, **79**, (2000), 157–178.

[16] M. De Soete. Some construction for authentication-secrecy codes. *Advances in cryptology—EUROCRYPT '88* (Davos, 1988), 57–75.

[17] S. De Winter and J. Schillewaert. A characterization of finite polar spaces by intersection numbers. *Combinatorica*, submitted.

[18] S. De Winter and J. Schillewaert. A note on singular quasi-quadrics and quasi-Hermitian varieties. preprint.

[19] N. Durante, V. Napolitano, and D. Olanda. On quadrics of $\mathbf{PG}(3,q)$. preprint, 2006.

[20] V. Fȧk. Repeated use of codes which detect deception. *IEEE Trans. Inform. Theory* **25**, (1979), no. 2, 233–234.

[21] R. Feng and Z. Wan. A construction of Cartesian authentication codes from geometry of classical groups. *Journal of Combinatorics, Information & System Sciences* **20**, (1995), 197–270.

[22] O. Ferri. Su di una caratterizzazione grafica della superficie di Veronese di un $S_{5,q}$. *Atti Accad. Naz. Lincei Rend.*, **61** (1976), 603–610.

[23] O. Ferri and G. Tallini. A characterization of nonsingular quadrics in $\mathbf{PG}(4,q)$. *Rend. Mat. Appl.* **11** (1991), no. 1, 15–21.

[24] E. N. Gilbert, F. J. MacWilliams, and N. J. A. Sloane. Codes which detect deception. *The Bell System Technical Journal* **53**, (1974), 405–424.

[25] D. Glynn. On the characterization of certain sets of points in finite projective geometry of dimension three. *Bull. London Math. Soc.*, **15**, (1983), 31–34.

[26] J. W. P. Hirschfeld and L. Storme. The packing problem in statistics, coding theory and finite projective spaces: update 2001. (English summary) Finite geometries, 201–246, Dev. Math., 3, Kluwer Acad. Publ., Dordrecht, 2001.

[27] J. W. P. Hirschfeld and J. A. Thas. Sets of type $(1, n, q+1)$ in $\mathbf{PG}(d, q)$. *Proc. London Math. Soc. (3)*, **41**, (1980), 254–278.

[28] J. W. P. Hirschfeld and J. A. Thas. *General Galois geometries.* Oxford University Press, Oxford, 1991.

[29] J. W. P. Hirschfeld. *Finite projective spaces of three dimensions, second edition.* Oxford University Press, Oxford, 1985.

[30] J. W. P. Hirschfeld. *Projective geometries over finite fields, second edition.* Oxford University Press, Oxford, 1998.

[31] B. Huppert. *Endliche gruppen I.* Springer-Verlag, Berlin, 1967.

[32] W. A. Jackson, K. M. Martin, and C. M. O'Keefe. Geometrical contributions to secret sharing theory. *J. of Geom.*, **79**, (2004), 102–133.

[33] T. Johansson. Contributions to unconditionally secure authentication. *PhD Thesis*, Lund University, Sweden, 1994.

[34] T. Kasami, N. Tokura and S. Azumi. On the weight enumeration of weights less than $2.5d$ of Reed-Muller codes. *Inform. control*, **30**, (1976), 380–395.

[35] A. Klein, J. Schillewaert, and L. Storme. Generalized dual arcs and Veronesean surfaces, with applications to cryptography. *J. Combin. Theory, Ser. A*, accepted.

[36] A. Klein, J. Schillewaert, and L. Storme. Generalized Veroneseans. *Proc. London Math. Soc.*, submitted.

[37] C. Lefèvre-Percsy. Sur les semi-quadriques en tant qu'espaces de Shult projectifs. *Acad. Roy. Belg. Bull. Cl. Sci.*, **63**, (1977), 160–164.

[38] C. Lefèvre-Percsy. Semi-quadriques en tant que sous-ensembles des espaces projectifs. *Bull. Soc. Math. Belg.*, **29**, (1977), 175–183.

[39] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes. I+II.*, North-Holland Publishing Co., Amsterdam, 1977.

[40] J. L. Massey. Minimal codewords and secret sharing. *Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory*, (1993), 276–279.

[41] S. E. Payne and J. A. Thas. *Finite generalized quadrangles.* Research Notes in Mathematics **110**, Pitman Advanced Publishing Program, Boston/London/Melbourne, 1984.

[42] D. Pei. *Authentication codes and combinatorial designs.* Discrete mathematics and its applications, Chapman & Hall/CRC, Boca Raton, FL, 2006.

[43] B. Qvist. Some remarks concerning curves of the second degree in a finite plane. *Ann. Acad. Sci. Fennicae. Ser. A. I. Math.-Phys. 1952*, **134**, (1952), 27 pp.

[44] J. Schillewaert. Generalised dual arcs and Veronesean surfaces, with applications to cryptography. *Proceedings Optimal Codes and related topics*, (2007), 126–131.

[45] J. Schillewaert Geometric authentication codes. Proceedings of the Academy Contact Forum *Coding Theory and Cryptography II* at the *Royal Flemish Academy of Belgium for Science and the Arts* (September 21, 2007), (2008), 101–112.

[46] J. Schillewaert and K. Thas. Authentication codes from Generalized quadrangles. *J. Cryptology*, submitted.

[47] J. Schillewaert. A characterization of quadrics by intersection numbers. *Des. Codes and Cryptogr.*, accepted.

[48] J. Schillewaert,L. Storme and J. A. Thas Minimal codewords in binary Reed-Muller codes. *Des, Codes and Cryptogr.*, submitted.

[49] J. Schillewaert and J. A. Thas. Characterizations of Hermitian varieties by intersection numbers. *Des, Codes and Cryptogr.*, accepted.

[50] J. Schillewaert, J. A. Thas and H. Van Maldeghem A characterization of the finite Veronesean by intersection properties. *Annals Combin.*, submitted.

[51] B. Segre. Ovals in a finite projective plane. *Canad. J. Math.*, **7**, (1955), 414–416.

[52] A. Shamir. How to share a secret. *Communications of the ACM*, **22**, (1979), 612–613.

[53] G. L. Simmons. *Authentication theory/coding theory.* Advances in Cryptology-Crypto '84, Lecture notes in computer science, **196**, (1985), 411–431.

[54] D. R. Stinson. Some constructions and bounds for authentication codes. *J. Cryptology*, **1** (1988), 37–52.

[55] D. R. Stinson. A construction for authentication and secrecy codes. *J. Cryptology*, **2** (1988), 199–127.

[56] D. R. Stinson. The combinatorics of authentication and secrecy codes. *J. Cryptology*, **2**, (1990), 23–49.

[57] D. R. Stinson. An explication of secret sharing schemes. *Des. Codes Cryptogr.*, **2**, (1992), no. 4, 357–390.

[58] G. Tallini. Sulle k-calotte degli spazi lineari finiti. I, *Atti Accad. Naz. Lincei. Rend. Cl. Sci. Fis. Mat. Nat.*, **8**, (1956), 311–317.

[59] G. Tallini. Caratterizzazione grafica delle quadriche ellittiche negli spazi finiti. *Rend. Mat. e Appl. (5)*, **5**, (1957), 328–351.

[60] G. Tallini. Una proprietà grafica caratteristica della superficie di Veronese negli spazi finiti. I, II. *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat. (8)*, **24**, (1958), 19–23, 135–138.

[61] M. Tallini Scafati. Caratterizzazione grafica delle forme hermitiane di un $S_{r,q}$. *Rend. Mat. e Appl. (5)*, **26**, (1967), 273–303.

[62] J. A. Thas. Series of lectures at Ghent University. Unpublished manuscript, 1976.

[63] J. A. Thas. Some results on quadrics and a new class of partial geometries. *Simon Stevin*, **55**, (1981), 129–139.

[64] J.A. Thas, K. Thas, and H. Van Maldeghem. *Translation Generalized Quadrangles.* Series in Pure Mathematics **26**, World Scientific, Singapore, 2006.

[65] J. A. Thas and H. Van Maldeghem. Characterizations of the finite quadric Veroneseans $V_n^{2^n}$. *The Quarterly Journal of Mathematics.* **55**, (2004), 99–113.

[66] J. A. Thas and H. Van Maldeghem. Classification of finite Veronesean caps. *European J. Combin.*, **25**, (2004), 275-285.

[67] J. A. Thas and H. Van Maldeghem. On Ferri's characterization of the finite quadric Veronesean $\mathcal{V}_2^4$. *J. Combin. Theory, Ser. A*, **2**, (2005), 217–221.

[68] K. Thas. Translation generalized quadrangles for which the translation dual arises from a flock. *Glasgow Math. J.*, **45**, (2003), 457–474.

[69] K. Thas. *Symmetry in Finite Generalized Quadrangles.* Monograph, Frontiers in Mathematics **1**, Birkhäuser, 2004.

[70] K. Thas. A stabilizer lemma for translation generalized quadrangles. *European J. Combin.*, **28**, (2007), 1–16.

[71] J. Tits. *Buildings of spherical type and finite BN-pairs.* Springer-Verlag, Berlin, Lecture Notes in Mathematics, Vol. 386, 1974.

[72] F. D. Veldkamp. Polar geometry, i-v. *Indag. Math.*, **21**, (1959), 512–551.

[73] S. Yoshiara. Ambient spaces of dimensional dual arcs. *J. Algebraic Combin.*, **19**, (2004), 5–23.

[74] M. Walker. A class of translation planes. *Geom. Dedicata* **5**, (1976), 135–146.

[75] Z. Wan, B. Smeets, and P. Vanroose. On the construction of Cartesian authentication codes over symplectic spaces. *IEEE Trans. Inform. Theory*, **40**, (1994), 920–929.

[76] C. Zanella. Linear sections of the finite Veronese varieties and authentication systems defined using geometry. *Des. Codes Cryptogr.*, **13**, (1998), 199–212.