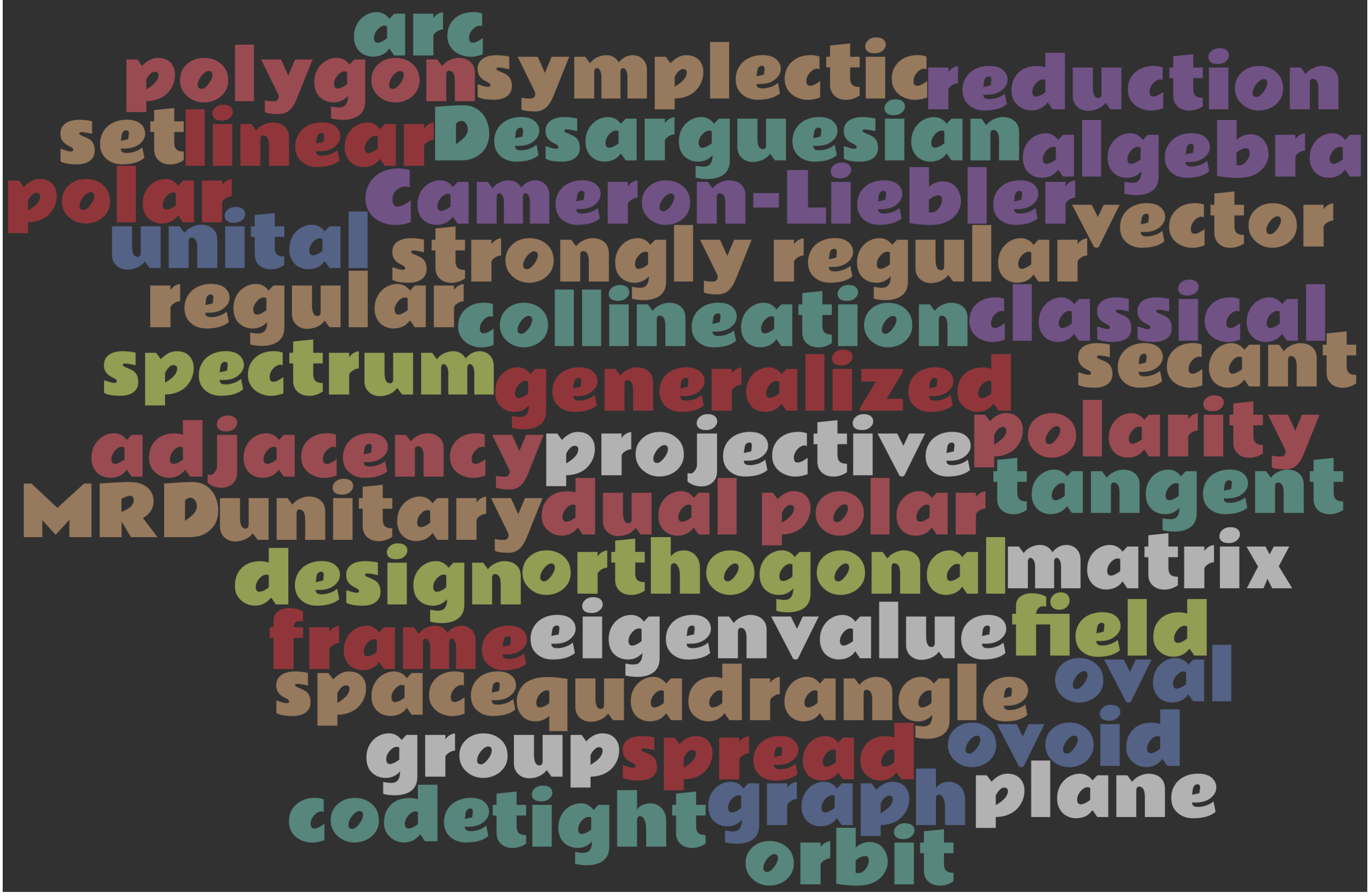
FINITE GEOMETRY & FRIENDS

A BRUSSELS SUMMER SCHOOL ON FINITE GEOMETRY

17-21 June, 2019
Vrije Universiteit Brussel
Brussels
Belgium



arc
polygon symplectic reduction
set linear Desarguesian algebra
polar Cameron-Liebler
unital strongly regular vector
regular collineation classical
spectrum generalized secant
adjacency projective polarity
MRD unitary dual polar tangent
design orthogonal matrix
frame eigenvalue field
space quadrangle oval
group spread ovoid
code tight graph plane
orbit

VUB DOCTORAL SCHOOL OF NATURAL SCIENCES & (BIOSCIENCE) ENGINEERING

fwo

Summer School

Finite Geometry and Friends

Vrije Universiteit Brussel

Brussels, Belgium

June 17-21, 2019

Lecture notes

Aida Abiad
Maastricht University

Nicola Durante
Università degli Studi di Napoli "Federico II"

Francesco Pavese
Politecnico di Bari

Geertrui Van de Voorde
University of Canterbury, Christchurch

Contents

Preface

These are the lectures notes of the summer school

Finite Geometry and Friends.

held from 17–21 June 2019 at the Vrije Universiteit Brussel, Belgium. Four young, yet established researchers will each deliver four hours of lectures on their topics, supplemented by two hours of exercise sessions. Each of them has written a set of notes to accompany the lectures.

First up is Aida Abiad from the University of Maastricht, who will introduce the students to topics in spectral graph theory. The two main topics that will be treated are eigenvalue interlacing and cospectral graphs. These ideas have found many applications to finite geometries, which makes a good introduction to this topic ever so interesting.

Next in line is Nicola Durante from Università degli Studi di Napoli "Federico II" in Naples, Italy, who will lecture on the the geometry of non-reflexive sesquilinear forms. Amongst the objectives are the classification of geometric objects related to such forms in small dimension, and to exploit the connection of such objects with "modern" objects from finite geometry such as hyperovals, spreads, $\mathbb{F}_q$-linear sets, semifield flocks, and MRD-codes.

Francesco Pavese, from Politecnico di Bari, Italy, will lecture on the actions of groups on finite projective and polar spaces. He will show that a good understanding of these actions and groups can help to construct subsets of points (or lines or planes or ...) with particular properties. These constructions can be useful in a variety of situations, of which we will see a coding theoretical application and a more geometrical one.

Finally we have Geertrui van de Voorde, from the University of Canterbury in New Zealand who will introduce us the theory of linear sets. This relatively new topic has been very active in the last few decades and a lot of progress has been made on several problems involving them. A large part of its success and attractiveness is due to its relation with a wide variety of topics in finite geometry such as blocking sets, direction problems and hyperovals and arcs. A few of these will be treated more in depth.

In summary, in these notes you will find a well-rounded and varied menu of topics presented by four excellent researchers. We hope that they form a helpful introduction to people who are new to the research fields and can motivate them to partake in future research.

The organisers,

Jan De Beule
Sam Mattheus

Part I

Eigenvalue techniques and their applications to graph theory

Aida Abiad

QE / Operations research, Quantitative Economics,
School of Business and Economics,
Maastricht University
Tongersestraat 53,
6211 LM Maastricht,
The Netherlands

email: aidaabiad@gmail.com

Contents

Preface

The object of these lecture notes is to give an introduction to two eigenvalue methods and to show some of their applications to combinatorics. The notes are intended to be used as course notes and should provide material for about 4 hours of lectures and 2 hours of exercises.

Chapter 2 contains an introduction to eigenvalue interlacing, together with an illustration of how it can be used to obtain new results in graph theory.

Chapter 3 looks at constructions of graphs with the same spectrum (cospectral graphs), in particular to Godsil-McKay switching. Its highlight is an application to construct new strongly regular graphs.

There are many topics in spectral graph theory that have not been touched upon in these notes. It should not be inferred that the topics covered in these notes are more interesting or relevant than those not covered. I have taken material from a number of sources all of which will provide further reading and references.

Aida Abiad, Eindhoven, May 2019.

Chapter 1

Introduction

Spectral graph theory studies the relation between structural properties of the graph and the eigenvalues of associated matrices. Graphs are often studied by their adjacency matrix, a square zero-one matrix whose rows and columns are both indexed in the same order by the vertices of the graph, with a 1 in a given position if and only if the corresponding vertices are adjacent. In this notes we will also consider other types of matrices (Laplacian matrix). If we do not specify the matrix, we assume we are dealing with the adjacency matrix.

The spectrum of a finite graph is by definition the spectrum of the adjacency matrix, that is, its set of eigenvalues together with their multiplicities. Just as astronomers study stellar spectra to determine the make-up of distant stars, one of the main goals in graph theory is to deduce the principal properties and structure of a graph from its graph spectrum (or from a short list of easily computable invariants). Eigenvalues are closely related to almost all major invariants of a graph, linking one extremal property to another. For example, we can see from the spectrum whether the graph is regular, or bipartite. The spectrum contains a lot of information of the graph, but in general it does not determine the graph (up to isomorphism). So a central question is:

Given the spectrum of a graph, what can be said about its structure?

Spectral graph theory looks at answering questions of this type.

Sometimes the eigenvalues uniquely determine the graph. If that is the case we say that the graph is determined by the spectrum (DS for short). On the other hand, for graphs with a very special structure, such as trees and strongly regular graphs, it has been proved that they are almost never determined by the spectrum (see [28], [33]). For many graphs, it has been established whether they are determined by the spectrum or not. However, for many other interesting graphs the problem is still open.

Two graphs with the same spectrum for some type of matrix are called cospectral with respect to the corresponding matrix. Cospectral graphs help us understand "weaknesses" in identifying structures only using the spectrum, and this will be the main highlight in the second part of these lecture notes.

There exist several algebraic methods to prove theorems in combinatorics. One of them is eigenvalue interlacing, a tool that gives information about substructures in graphs . This will be the main highlight of the first part of these lecture notes.

All graphs will be undirected, without loops and multiple edges. We shall denote by $\mathbf{1}$ and $\mathbf{0}$ the all-one and the zero vector, respectively. We denote the all-one matrix by J, the identity matrix by I and the all-zero matrix by O. For details and an overview of the results on spectra of graphs, we refer to the book by Brouwer and Haemers [9].

Chapter 2

Eigenvalue interlacing

In this chapter we introduce an important spectral technique: eigenvalue interlacing.

2.1 Preliminaries

Consider two sequences of real numbers: $\lambda_1 \geq \cdots \geq \lambda_n$ and $\mu_1 \geq \cdots \geq \mu_m$ with $m < n$. The second sequence is said to *interlace* the first one whenever

$$\lambda_i \geq \mu_i \geq \lambda_{n-m+i} \quad \text{for } i = 1, \ldots, m.$$

The interlacing is called *tight* if there exist an integer $k \in [0, m]$ such that

$$\lambda_i = \mu_i \text{ for } 1 \leq i \leq k \quad \text{and} \quad \lambda_{n-m+i} = \mu_i \text{ for } k+1 \leq i \leq m.$$

If $m = n-1$, the interlacing inequalities become $\lambda_1 \geq \mu_1 \geq \lambda_2 \geq \mu_2 \geq \cdots \geq \mu_m \geq \lambda_n$, which clarifies the name. Throughout, the λ_is and the μ_is will be eigenvalues of matrices A and B, respectively.

Theorem 2.1.1. [18][Interlacing] *Let A be a real symmetric $n \times n$ matrix with eigenvalues $\lambda_1 \geq \cdots \geq \lambda_n$. For some $m < n$, let S be a real $n \times m$ matrix with orthonormal columns, $S^\top S = I$. Define $B = S^\top AS$ and let B have eigenvalues $\mu_1 \geq \cdots \geq \mu_m$ with respective eigenvectors $v_1, \ldots, v_m$. Then,*

(i) *the eigenvalues of B interlace those of A, that is,*

$$\lambda_i \geq \mu_i \geq \lambda_{n-m+i}, \qquad i = 1, \dots, m, \tag{2.1}$$

(ii) *if $\mu_i = \lambda_i$ or $\mu_i = \lambda_{n-m+i}$ for some $i \in [1, m]$, then B has a μ_i-eigenvector v such that Sv is a μ_i-eigenvector of A.*

(iii) *If for some integer l, $\mu_i = \lambda_i$, for $i = 1, \dots, l$ (or $\mu_i = \lambda_{n-m+i}$ for $i = l, \dots, m$) then Sv_i is a μ_i-eigenvector of A for $i = 1, \dots, l$ (respectively $i = l, \dots, m$).*

(iv) *if the interlacing is tight, then $SB = AS$.*

Two interesting particular cases of interlacing are obtained by choosing appropriately the matrix S.

If $S = [\,I \;\; O\,]^\top$, then B is just a principal submatrix of A and we have:

Corollary 2.1.2. *If B is a principal submatrix of a symmetric matrix A, then the eigenvalues of B interlace the eigenvalues of A.*

If $\mathcal{P} = \{X_1, \dots, X_m\}$ is a partition of the vertex set V, with each $X_i \neq \emptyset$, we can take for $\widetilde{B}$ the so-called quotient matrix of A with respect to $\mathcal{P}$. Let A be partitioned according to $\mathcal{P}$:

$$A = \begin{bmatrix} A_{1,1} & \cdots & A_{1,m} \\ \vdots & & \vdots \\ A_{m,1} & \cdots & A_{m,m} \end{bmatrix},$$

where $A_{i,j}$ denotes the submatrix (block) of A formed by rows in X_i and columns in X_j. The *characteristic matrix* $\widetilde{S}$ is the $n \times m$ matrix whose j^{th} column is the characteristic vector of X_j ($j = 1, \dots, m$).

Then, the *quotient matrix* of A with respect to $\mathcal{P}$ is the $m \times m$ matrix $\widetilde{B}$ whose entries are the average row sums of the blocks of A, more precisely:

$$(\widetilde{B})_{i,j} = \frac{1}{|U_i|}\mathbf{1}^\top A_{i,j}\mathbf{1} = \frac{1}{|U_i|}(\widetilde{S}^\top A \widetilde{S})_{i,j}.$$

The partition is called *equitable* (or *regular*) if each block $A_{i,j}$ of A has constant row (and column) sum, that is, $\widetilde{S}\widetilde{B} = A\widetilde{S}$.

Corollary 2.1.3. *Suppose $\widetilde{B}$ is the quotient matrix of a symmetric partitioned matrix A.*

(i) *The eigenvalues of $\widetilde{B}$ interlace the eigenvalues of A.*

(ii) *If the interlacing is tight then the partition is regular.*

Proof. Take $D = \operatorname{diag}(|X_1|, \dots, |X_m|) = \widetilde{S}^\top \widetilde{S}$, $S = \widetilde{S}D^{-1/2}$ and $B = S^\top AS$. Then, since $B = D^{1/2}\widetilde{B}D^{-1/2}$, B and $\widetilde{B} = D^{-1/2}BD^{1/2}$ have the same spectrum, and the eigenvalues of $B = S^\top AS$ interlace those of A, which proves (i). For (ii) note that if the interlacing is tight, then $SB = AS$; hence, $\widetilde{S}\widetilde{B} = A\widetilde{S}$. □

Note that $\widetilde{B}$ need not to be a symmetric matrix. However, the proof of Corollary 2.1.3 shows that $\widetilde{B}$ is diagonally similar to B, which is symmetric.

Note also that the converse of Corollary 2.1.3.(ii) is not true: a regular partition does not imply tight interlacing.

2.2 A generalization of Grone's result

A third particular case of interlacing, which is a mix of both types, was used in [5] for obtaining lower and upper bounds for the sums of Laplacian eigenvalues of graphs. This lead to generalizations of a theorem by Grone, as we shall see below.

Let G be a graph on n vertices, with degrees $d_1 \geq d_2 \geq \cdots \geq d_n$, and Laplacian matrix L with eigenvalues $\theta_1 \geq \theta_2 \geq \cdots \geq \theta_n (= 0)$, it is known that, for $1 \leq m \leq n$,

$$\sum_{i=1}^{m} \theta_i \geq \sum_{i=1}^{m} d_i. \tag{2.2}$$

This is a consequence of Schur's theorem [31] stating that the spectrum of any symmetric, positive definite matrix majorizes its main diagonal. In particular, note that if $m = n$ we have equality in (2.2), because both terms correspond to the trace of L. To prove (2.2) by using interlacing, let B be a principal $m \times m$ submatrix of L indexed by the subindeces corresponding to the m higher degrees, with eigenvalues $\mu_1 \geq \mu_2 \geq \cdots \geq \mu_m$. Then,

$$\operatorname{tr} B = \sum_{i=1}^{m} d_i = \sum_{i=1}^{m} \mu_i,$$

and, by interlacing, $\theta_{n-m+i} \leq \mu_i \leq \theta_i$ for $i = 1, \ldots, m$, whence (2.2) follows. Similarly, reasoning with the principal submatrix B (of L) indexed by the m vertices with lower degrees we get:

$$\sum_{i=1}^{m} \theta_{n-m+i} \leq \sum_{i=1}^{m} d_{n-m+i}. \tag{2.3}$$

The next result, which is an improvement of (2.2), is due to Grone [16], who proved that if G is connected and $m < n$ then,

$$\sum_{i=1}^{m} \theta_i \geq \sum_{i=1}^{m} d_i + 1. \tag{2.4}$$

In [9], Brouwer and Haemers gave two different proofs of (2.4), both using eigenvalue interlacing. In [5], Abiad, Fiol, Haemers and Perarnau extended the ideas of these two proofs and found a generalization of Grone's result (2.4), see details below.

Given a graph G with a vertex subset $U \subset V$, let ∂U be the *vertex-boundary* of U, that is, the set of vertices in $\overline{U} = V \backslash U$ with at least one adjacent vertex in U. Also, let $\partial(U, \overline{U})$ denote the *edge-boundary* of U, which is the set of edges which connect vertices in U with vertices in $\overline{U}$.

Theorem 2.2.1. *[5] Let G be a connected graph on $n = |V|$ vertices, having Laplacian matrix L with eigenvalues $\theta_1 \geq \theta_2 \geq \cdots \geq \theta_n (= 0)$. For any given vertex subset $U = \{u_1, \ldots, u_m\}$ with $0 < m < n$, we have*

$$\sum_{i=1}^{m} \theta_{n-i} \leq \sum_{u \in U} d_u + \frac{|\partial(U, \overline{U})|}{n-m} \leq \sum_{i=1}^{m} \theta_i. \tag{2.5}$$

Proof. Consider the partition of the vertex set V into $m+1$ parts: $U_i = \{u_i\}$ for $u_i \in U$, $i = 1, \ldots, m$, and $U_{m+1} = \overline{U}$. Then, the corresponding quotient matrix is

$$\boldsymbol{B} = \left[\begin{array}{ccc|c} & & & b_{1,m+1} \\ & L_U & & \vdots \\ & & & b_{m,m+1} \\ \hline b_{m+1,1} & \cdots & b_{m+1,m} & b_{m+1,m+1} \end{array}\right],$$

where L_U is the principal submatrix of L, with rows and columns indexed by the vertices in U, $b_{i,m+1} = (n-m)b_{m+1,i} = -|\partial(U_i, \overline{U})|$, and $b_{m+1,m+1} = |\partial(U, \overline{U})|/(n-$

m) (because $\sum_{i=1}^{m+1} b_{m+1,i} = 0$). Let $\mu_1 \geq \mu_2 \geq \cdots \geq \mu_{m+1}$ be the eigenvalues of B. Since B has row sum 0, we have $\mu_{m+1} = \theta_n = 0$. Moreover,

$$\sum_{i=1}^{m} \mu_i = \sum_{i=1}^{m+1} \mu_i = \operatorname{tr} B = \sum_{u \in U} d_u + b_{m+1,m+1},$$

Then, (2.5) follows by applying interlacing, $\theta_i \geq \mu_i \geq \theta_{n-m-1+i}$ and adding up for $i = 1, 2, \ldots, m$. □

If the vertex degrees of G are $d_1 \geq d_2 \geq \cdots \geq d_n$, one can choose conveniently the m vertices of U (that is, those with higher or lower degrees) to obtain the best inequalities in (2.5). Namely,

$$\sum_{i=1}^{m} \theta_i \geq \sum_{i=1}^{m} d_i + \frac{|\partial(U, \overline{U})|}{n-m}, \tag{2.6}$$

and

$$\sum_{i=1}^{m} \theta_{n-i} \leq \sum_{i=1}^{m} d_{n-i+1} + \frac{|\partial(U, \overline{U})|}{n-m}. \tag{2.7}$$

Note that (2.7), together with (2.3) for $m+1$, yields

$$\sum_{i=0}^{m} \theta_{n-m+i} = \sum_{i=1}^{m} \theta_{n-i} \leq \sum_{i=1}^{m} d_{n-i+1} + \min\left\{ d_{n-m}, \frac{|\partial(U, \overline{U})|}{n-m} \right\}. \tag{2.8}$$

If we have more information on the structure of the graph, one can improve the above results by either bounding $|\partial(U, \overline{U})|$ or 'optimizing' the ratio $b = |\partial(U, \overline{U})|/(n-m)$. In fact, the right inequality in (2.5) (and, hence, (2.6)) can be improved when $\overline{U} \neq \partial U$. Simply first delete the vertices (and corresponding edges) of $\overline{U} \setminus \partial U$, and then apply the inequality. Then $d_1, \ldots, d_m$ remain the same and $\lambda_1, \ldots, \lambda_m$ do not increase. Thus the following holds:

Theorem 2.2.2. *[5] Let G be a connected graph on $n = |V|$ vertices, with Laplacian eigenvalues $\theta_1 \geq \theta_2 \geq \cdots \geq \theta_n (= 0)$. For any given vertex subset $U = \{u_1, \ldots, u_m\}$ with $0 < m < n$, we have*

$$\sum_{i=1}^{m} \theta_i \geq \sum_{u \in U} d_u + \frac{|\partial(U, \overline{U})|}{|\partial U|}. \tag{2.9}$$

Similarly as it was done in (2.6), if one chooses the m vertices of U such that they are those with maximum degree, then we can write:

$$\sum_{i=1}^{m} \theta_i \geq \sum_{i=1}^{m} d_i + \frac{|\partial(U, \overline{U})|}{|\partial U|}.$$

Notice that Grone's result (2.4) follows as a corollary, since always $|\partial(U, \overline{U})| \geq |\partial U|$.

2.3 Some applications of interlacing

Eigenvalue interlacing provides a handy tool for obtaining inequalities and regularity results concerning the structure of graphs in terms of eigenvalues of a matrix associated to a graph (often the adjacency and the Laplacian matrix).

In this section we shall see some old and new applications of eigenvalue interlacing to matrices associated to graphs. Bounds are obtained for characteristic numbers of graphs, such as the independence number, the chromatic number or the isoperimetric number.

Cliques and cocliques

A *clique* in a graph is a set of pairwise adjacent vertices. A *coclique* (or *independent set*) in a graph is a set of pairwise nonadjacent vertices. The *clique number* $\omega(G)$ is the size of the largest clique in G. The *independence number* $\alpha(G)$ is the size of the largest coclique in G.

Let G be a graph on n vertices (undirected, simple and loopless) having an adjacency matrix A with eigenvalues $\lambda_1 \geq \cdots \geq \lambda_n$. Both Corollaries 2.1.2 and 2.1.3 lead to a bound for $\alpha(G)$.

Theorem 2.3.1. *[12]*

$$\alpha(G) \leq |\{i|\lambda_i \geq 0\}| \text{ and } \alpha(G) \leq |\{i|\lambda_i \leq 0\}|.$$

Proof. A has a principal submatrix $B = O$ of size $\alpha = \alpha(G)$. Corollary 2.1.2 gives $\lambda_\alpha \geq \mu_\alpha = 0$ and $\lambda_{n-\alpha+1} \geq \mu_1 = 0$. □

Theorem 2.3.2. *If G is regular, then*

$$\alpha(G) \leq n\frac{-\lambda_n}{\lambda_1 - \lambda_n}$$

and if a coclique C meets this bound, then every vertex not in C is adjacent to precisely $-\lambda_n$ vertices of C.

Proof. We apply Corollary 2.1.3. Let $k = \lambda_1$, be the degree of G and put $\alpha = \alpha(G)$. The coclique gives rise to a partition of A with quotient matrix

$$B = \begin{bmatrix} 0 & k \\ \frac{k\alpha}{n-\alpha} & k - \frac{k\alpha}{n-\alpha} \end{bmatrix}.$$

B has eigenvalues $\mu_1 = k$ (row sum) and $\mu_2 = -k\alpha/(n-\alpha)(\mathrm{tr}(B) - k)$ and so $\lambda_n \leq \mu_2$ gives the required inequality. If equality holds, then $\mu_2 = \lambda_n$, and since $\lambda_1 = \mu_1$, the interlacing is tight and hence the partition is regular. □

The first bound is due to Cvetković [12]. The second bound is an unpublished result of Hoffman known as the *Hoffman bound* or *ratio bound*. There are many examples where equality holds. For instance, a 4-coclique in the Petersen graph is tight for both bounds.

The Hoffman bound was generalised to the nonregular case by Haemers [18] as follows.

Theorem 2.3.3. *[18] If G has smallest degree δ, then*

$$\alpha(G) \leq n\frac{-\lambda_1\lambda_n}{\delta^2 - \lambda_1\lambda_n}.$$

Proof. Now we let k denote the average degree of the vertices of the coclique. Then the quotient matrix B is the same as above, except maybe for the entry $(B)_{2,2}$.

Interlacing gives

$$-\lambda_1\lambda_n \geq -\mu_1\mu_2 = -\det(B) = \frac{k^2\alpha}{n-\alpha} \geq \frac{\delta^2\alpha}{n-\alpha},$$

which yields the required inequality. □

If G is regular of degree k, then $\delta = k = \lambda_1$ and Theorem 2.3.3 reduces to Hoffman's bound (Theorem 2.3.2).

Chromatic number

The *chromatic number* of a graph G is the smallest number of colors needed to color the vertices of so that no two adjacent vrtices share the same color, i.e., the smallest value k possible to obtain a k-coloring. A *coloring* of a graph G is a partition of its vertices into cocliques (color classes). Therefore, the number of color classes, and hence the chromatic number $\chi(G)$ of G, is bounded below by $n/\alpha(G)$. Thus upper bounds for $\alpha(G)$ give lower bounds for $\chi(G)$. For instance, if G is regular, Theorem 2.3.2 implies that $\chi(G) \geq 1-(\lambda_1/\lambda_n)$. This bound, however, remains valid for nonregular graphs [18] (but note that it does not follow from Theorem 2.3.3).

Theorem 2.3.4. *[18]*

(i) *If G is not the empty graph, then $\chi(G) \geq 1 - (\lambda_1/\lambda_n)$.*

(ii) *If $\lambda_2 > 0$, then $\chi(G) \geq 1 - \lambda_{n-\chi(G)+1}/\lambda_2$.*

Proof. Let $\chi = \chi(G)$.

(i) Let $X_1, \dots, X_\chi$ denote the color classes of G and let $u_1, \dots, u_n$ be an orthonormal set of eigenvectors of S (where u_i corresponds to λ_i). For $i = 1, \dots, \chi$, let s_i denote the restriction of u_1 to X_i, that is

$$(s_i)_j = \begin{cases} (u_1)_j & \text{if } j \in X_i \\ 0 & \text{otherwise} \end{cases}$$

and put $\widetilde{S} = [s_1 \cdots s_\chi]$ (if some $s_i = 0$, we delete it from $\widetilde{S}$ and proceed similarly) and $D = \widetilde{S}^\top \widetilde{S}$, $S = \widetilde{S} D^{-\frac{1}{2}}$, and $B = S^\top A S$. Then B has zero diagonal (since each color class corresponds to a zero submatrix of A) and an eigenvalue λ_1 ($d = D^{-\frac{1}{2}}\mathbf{1}$ is a λ_1-eigenvector of B). Moreover, interlacing Theorem 2.1.1 gives that the remaining eigenvalues of B are at least λ_n. Hence

$$0 = \operatorname{tr}(B) = \mu_1 + \cdots + \mu_\chi \geq \lambda_1 + (\chi - 1)\lambda_n,$$

which proves (i), since $\lambda_n < 0$.

(ii) The proof of (ii) is similar, but a little bit more complicated. With $s_1, \dots, s_\chi$ as above, choose a nonzero vector s in

$$\langle u_{n-\chi+1}, \dots, u_n \rangle \cap \langle s_1, \dots, s_\chi \rangle^\perp.$$

The two spaces have nontrivial intersection since the dimensions add up to n and u_1 is orthogonal to both. Redefine s_i to be the restriction of s to X_i, and let $\widetilde{S}$, D, S and d be analogous to above. Put $A' = A - (\lambda_1 - \lambda_2)u_1 u_1^\top$. Then the largest eigenvalue of A' equals λ_2, but all other eigenvalues of A are also eigenvalues of A' with the same eigenvectors. Define $B = S^\top A' S$. Now again B has zero diagonal (since $u_1^\top S = 0$). Moreover, B has smallest eigenvalue $\mu_\chi \leq \lambda_{n-\chi+1}$, because

$$\mu_\chi \leq \frac{d^\top B d}{d^\top d} = \frac{s^\top A' s}{s^\top s} \leq \lambda_{n-\chi+1}.$$

So interlacing gives

$$0 = \mathrm{tr}(B) = \mu_1 + \ldots + \mu_\chi \leq \lambda_{n-\chi+1} + (\chi - 1)\lambda_2.$$

Since $\lambda_2 > 0$, (ii) follows.

□

The inequality (i) is due to Hoffman [22], and its proof is due to Haemers [18] and is a customary illustration of interlacing. The condition $\lambda_2 > 0$ of (ii) is not strong; only the complete multipartite graphs, possibly extended with some isolated vertices, have $\lambda_2 \leq 0$. The inequality (ii) looks a bit awkward, but can be made more explicit if the smallest eigenvalue λ_n has large multiplicity m_n, say. Then (ii) yields $\chi \geq \min\{1 + m_n, 1 - (\lambda_n/\lambda_2)\}$ (indeed if $\chi \leq m_n$, then $\lambda_n = \lambda_{n-\chi+1}$, hence $\chi \geq 1 - (\lambda_n/\lambda_2)$). For strongly regular graphs with $\lambda_2 > 0$, it is shown in [17], that the minimum is always taken by $1 - (\lambda_n/\lambda_2)$, except for the pentagon. So the next corollary follows.

Corollary 2.3.5. *[18] If G is a strongly regular graph, not the pentagon or a complete multipartite graph, then*

$$\chi \geq 1 - \frac{\lambda_n}{\lambda_2}.$$

A natural generalization of a regular partition, which makes sense also for non-regular graphs, is the so-called *weight-regular partition*. Its definition is based on giving to each vertex $u \in V$ a weight which equals the corresponding entry ν_u of the Perron eigenvector ν. Such weights "regularize" the graph, leading to a kind of regular partition that can be useful for general graphs. For more details on weight-regular partitions see [14, 13]. In [1] it was shown that Hoffman's bound can be improved for certain classes of graphs by using interlacing and weight-regular partitions.

Corollary 2.3.6. *[1] If G has at least one edge and the vertex partition defined by the χ color classes is not weight-regular, then*

$$\chi(G) \geq 2 - \frac{\lambda_1}{\lambda_n}.$$

Isoperimetric number

The *isoperimetric number* $i(G)$ is defined as

$$i(G) = \min_{U \subset V} \left\{ |\partial(U, \overline{U})| / |U| : 0 < |U| \leq n/2 \right\}.$$

For example, the isoperimetric numbers of the complete graph, the path and the cycle are, respectively, $i(K_n) = \lceil \frac{n}{2} \rceil$, $i(P_n) = 1/\lfloor \frac{n}{2} \rfloor$, and $i(C_n) = 2/\lfloor \frac{n}{2} \rfloor$.

Given a graph G on n vertices and Laplacian eigevalues $\theta_1 \geq \theta_2 \geq \cdots \geq \theta_n (= 0)$. For general graphs, Mohar [29] proved the following spectral bounds.

$$\frac{\theta_{n-1}}{2} \leq i(G) \leq \sqrt{\theta_{n-1}(2d_1 - \theta_{n-1})}. \tag{2.10}$$

Using the eigenvalue inequalities from Theorem 2.2.1, Abiad, Fiol, Haemers and Perarnau showed the following bound [5], which in some situations is better than Mohar's upper bound.

Proposition 2.3.7. *[5]*

$$i(G) \leq \min_{\frac{n}{2} \leq m < n} \sum_{i=1}^{m} (\theta_i - d_i). \tag{2.11}$$

Proof. Apply (2.6) taking into account that $i(G) \leq \frac{|\partial(\overline{U}, U)|}{|\overline{U}|}$ when $0 < |\overline{U}| \leq \frac{n}{2}$. □

Example 2.3.8. Consider the graph join G of the complete graph K_p with the empty graph $\overline{K_q}$, so $n = p + q$. The Laplacian spectrum and the degree sequence are

$$\{n^p, p^{q-1}, 0^1\} \text{ and } \{(n-1)^p, p^q\},$$

respectively. Equation (2.11) gives $i(G) \leq \min\{p, \lceil \frac{n}{2} \rceil\}$, which is better than Mohar's upper bound (2.10) for all $0 \leq q < n$.

2.4 Exercises and open problems

Exercise 2.4.1. Let A be a real symmetric matrix of order n with eigenvalues $\lambda_1 \geq \cdots \lambda_n$. Let $\{X_1, \ldots, X_m\}$ be a partition of the index set for row and columns of A, and let B be the corresponding quotient matrix, with eigenvalues $\mu_1 \geq \cdots \geq \mu_m$. Show that if $\lambda_i = \mu_i$ for some i, then A has a λ_i-eigenvector that is constant on each part X_j.

Exercise 2.4.2. Let B denote the quotient matrix of a symmetric matrix A whose rows and columns are partitioned according to a partitioning $\{X_1, \ldots, X_m\}$.

(i) Give an example, where the eigenvalues of B are a sub(multi)set of the eigenvalues of A, whilst the partition is not equitable.

(ii) Give an example where the partition is equitable, whilst the interlacing is not tight.

Exercise 2.4.3. [4] The *k-independence number* of a graph is the maximum size of a set of vertices at pairwise distance greater than k. Generalize Cvetković's bound from Theorem 2.3.1 for the k-independence number.

Exercise 2.4.4. [29] Let G be a graph with Laplacian eigenvalues $\theta_1 \geq \theta_2 \geq \cdots \geq \theta_n (= 0)$ and isoperimetric number $i(G)$. Show Mohar's lower bound (2.10), that is, $i(G) \geq \theta_{n-1}/2$.

Exercise 2.4.5. [5] For a given integer k, a *k-dominating set* in a graph G is a vertex subset $D \subseteq V$ such that every vertex not in D has at least k neighbors in D. Apply Theorem 2.2.1 to deduce an inequality for the first m largest Laplacian eigenvalues of a graph G in terms of a k-dominating set of G.

Open problem 2.4.6. Find new examples of tight interlacing for weight-regular partitions, analogous to Proposition 5.3 (i) from [1], for other graph parameters.

Chapter 3

Cospectral graphs

Consider the two graphs shown in Figure 3.1.

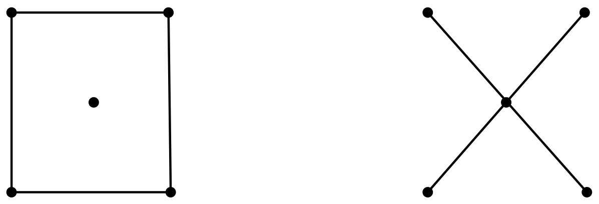


Figure 3.1: Two cospectral graphs on 5 vertices.

It is easily checked that the corresponding adjacency matrices have spectrum

$$\{2^1, 0^3, -2^1\},$$

where the exponents indicate multiplicities. Two graphs with the same spectrum for some type of matrix are called *cospectral* with respect to the corresponding matrix. This is the first example of nonisomorphic cospectral graphs found by Collatz and Sinogowitz [11] in 1957. For graphs on less than five vertices, no pair with cospectral adjacency matrix exists, so any graph with less than five vertices is determined by its spectrum.

If a graph is not determined by the spectrum, this can be proved by constructing a nonisomorphic cospectral mate. In this chapter we will see some tools for constructing cospectral graphs; the most important one is the switching method of Godsil and McKay [15]. Godsil-McKay switching is an operation on a graph that does not change the spectrum of the adjacency matrix (though it was invented to make cospectral graphs with respect to the adjacency matrix, the idea also works for the Laplacian matrix). Godsil-McKay switching was generalized by Abiad and Haemers in [6].

Constructing cospectral graphs is not only important for disproving that a graph is determined by its spectrum. In several cases such a graph can be important in its own right. Good examples are the twisted Grassmann graphs, found by Van Dam and Koolen [35], which form a new family of distance-regular graphs and which are cospectral with Grassmann graphs.

Consider two graphs G and G' with adjacency matrices A and A', respectively. As it was just mentioned, the graphs G and G' are called *cospectral* if A and A' have the same spectrum.

For a graph G with adjacency matrix A, any matrix of the form $M = xI + yJ + zA$ with $x, y, z \in \mathbb{R}$, $z \neq 0$ is called a *generalized adjacency matrix* of G. Since we are interested in the relation between G and the spectrum of M, we can restrict to generalized adjacency matrices of the form $yJ - A$ without loss of generality. As we shall see in Theorem 3.0.1, Johnson and Newman [26] proved that if $yJ - A$ and $yJ - A'$ are cospectral for two distinct values of y, then they are cospectral for all y, and hence they are cospectral with respect to all generalized adjacency matrices. In this case we will call G and G' $\mathbb{R}$-*cospectral*. So if $yJ - A$ and $yJ - A'$ are cospectral for some but not all values of y, they are cospectral for exactly one value $\widehat{y}$ of y. Then we say that G and G' are $\widehat{y}$-*cospectral*. Thus cospectral graphs (in the usual sense) are either 0-cospectral or $\mathbb{R}$-cospectral.

For a graph G with adjacency matrix A, the polynomial $p(x, y) = \det(xI + yJ - A)$ will be called the *generalized characteristic polynomial* of $A - yJ$, and $p(x, 0) = p(x)$ is the characteristic polynomial of A.

An orthogonal matrix Q is *regular* if it has constant row sum, that is, $Q\mathbf{1} = r\mathbf{1}$.

Theorem 3.0.1. *[26] If G and G' are graphs with adjacency matrices A and A', respectively, then the following are equivalent.*
(i) The graphs G and G' are cospectral, and so are their complements.
(ii) The graphs G and G' are $\mathbb{R}$-cospectral.
(iii) There exists a regular orthogonal matrix Q, such that $Q^{\top}AQ = A'$.

Proof. First, we shall prove that if $yJ - A$ and $yJ - A'$ are cospectral for two distinct values of y, then they are cospectral for all y, and hence they are cospectral with respect to all generalized adjacency matrices. Let G and G' be graphs with generalized characteristic polynomials $p(x, y)$ and $p'(x, y)$, respectively. Note that for fixed y, $p(x, y)$ is the characteristic polynomial of $A - yJ$. Since J has rank 1, the degree in y of $p(x, y)$ is 1 (this follows from Gaussian elimination in $xI + yJ - A$), so there exist integers $a_0, \ldots, a_n$ and $b_0, \ldots, b_n$ such that

$$p(x, y) = \sum_{i=0}^{n} (a_i + b_i y) x^i.$$

It is clear that $p(x, y) \equiv p'(x, y)$ if and only if G and G' are $\mathbb{R}$-cospectral, and G and G' are $\widehat{y}$-cospectral if and only if $p(x, \widehat{y}) = p'(x, \widehat{y})$ for all $x \in \mathbb{R}$, whilst $p(x, y) \not\equiv p'(x, y)$ (indeed, if G and G' are y cospectral for some $\widehat{y}$ but not for all y, then the corresponding polynomials $p(x, y)$ and $p'(x, y)$ are not identical, whilst $p(x, \widehat{y}) = p'(x, \widehat{y})$). If this is the case, then $a_i + \widehat{y} b_i = a'_i + \widehat{y} b'_i$ with $(a_i, b_i) \neq (a'_i, b'_i)$ for some i $(0 \leq i \leq n - 3)$. This implies $\widehat{y} = -(a_i - a'_i)/(b_i - b'_i)$ is unique and rational. Thus we proved the equivalence between (i) and (ii). Finally, it easily follows that G and G' are $\mathbb{R}$-cospectral if Q is regular, since $Q^\top \mathbf{1} = \mathbf{1}$ implies $Q^\top (yJ - A) Q = yJ - A'J$, so $yJ - A$ and $yJ - A'$ are cospectral for every $y \in \mathbb{R}$. By taking $y = 1$ we see that $\mathbb{R}$-cospectral graphs have cospectral complements. □

The spectrum of a graph G together with that of its complement will be referred to as the *generalized spectrum* of G. We say that a given graph G is *determined by its spectrum* (DS for short) if every graph cospectral with G is isomorphic with G. A graph G is said to be *determined by its generalized spectrum* (DGS for short) if every graph $\mathbb{R}$-cospectral with G is isomorphic with G, or equivalently, if every graph cospectral with G and with complement cospectral to $\overline{G}$ is isomorphic to G.

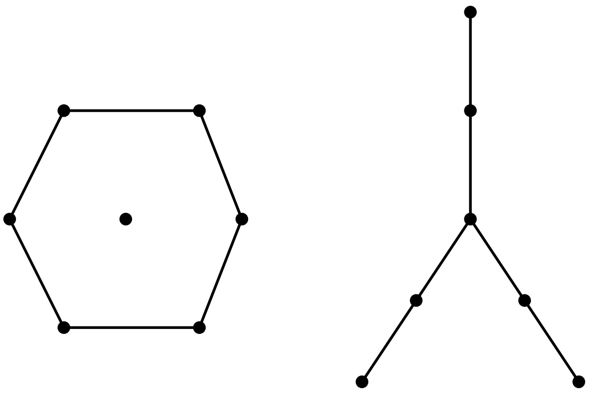


Figure 3.2: A pair of $\mathbb{R}$-cospectral graphs.

3.1 Constructing cospectral graphs: GM switching

Several constructions of cospectral graphs are known. Here we focus on a method introduced by Godsil and McKay [15], which seems to be the most productive one. At several points in the rest of these notes we will make use of it, and it will be referred to simply as GM switching. Godsil and McKay gave the conditions under which the adjacency spectrum is unchanged by this operation.

Lemma 3.1.1. [15][GM switching] *Let G be a graph and let $\{X_1, \dots, X_\ell, Y\}$ be a partition of the vertex set $V(G)$ of G. Suppose that for every vertex $x \in Y$ and every $i \in \{1, \dots, \ell\}$, x has either 0, $\frac{1}{2}|X_i|$ or $|X_i|$ neighbors in X_i. Moreover, suppose that for all $i, j \in \{1, \dots, \ell\}$ the number of neighbors of an arbitrary vertex of X_i that are contained in X_j, depends only on i and j and not on the vertex. Make a new graph G' from G as follows. For each $x \in Y$ and $i \in \{1, \dots, \ell\}$ such that x has $\frac{1}{2}|X_i|$ neighbors in X_i delete the corresponding $\frac{1}{2}|X_i|$ edges and join x instead to the $\frac{1}{2}|X_i|$ other vertices in X_i. Then G and G' are cospectral (with cospectral complements).*

Proof. Let A and A' be the adjacency matrices of G and G', respectively (the vertex ordering is assumed to be in accordance with the partition). Let n be the number of vertices of G and G'. For $i = 1, \dots, m$ define the $|V_i| \times |V_i|$ matrix $R_i = \frac{2}{|V_i|}J - I$, and the $n \times n$ block diagonal matrix $Q = \operatorname{diag}(R_1, \dots, R_m, I)$. Then Q is orthogonal and regular, and it follows straightforwardly that $Q^\top AQ = A'$, and more generally, that $Q^\top(A + yJ)Q = A' + yJ$ for every $y \in \mathbb{R}$. □

The operation that changes G into G' is called *Godsil-McKay switching*. Note that the pair of graphs in Figure 3.2 is related by GM switching ($\ell = 1$ and X_1 is a 4-coclique), and hence has cospectral complements. The pair of graphs in Figure 3.1 does not have cospectral complements and hence does not arise by GM switching.

If $\ell = 1$ and $|X_1| = 2$, then GM switching interchange the two vertices in X_1, so G and G' are isomorphic, and we call the switching trivial. But if $\ell = 1$ and $|X_1| \geq 4$, then GM switching usually produces nonisomorphic graphs [21].

3.2 Some applications of GM switching

Finding switching partitions that make the Godsil-McKay switching work (the so-called *Godsil-McKay switching sets*) in a given family of graphs is a nontrivial problem that has only been solved in some special cases, like for the Johnson graphs $J(n, k)$ with $n/2 \geq k \geq 3$ [34] and some Kneser graphs $K(n, k)$ [20], which are both families of graphs belonging to the Johnson association scheme. Some graphs in the Johnson scheme are determined by its spectrum, like $K(2k + 1, k)$ [23] (also known as Odd graphs, whose vertices represent the k-element subsets of a $(2k + 1)$-element set, where two vertices are adjacent if and only if their corresponding subsets are disjoint) and $J(n, 2)$ for $n \neq 8$ (see for example [36]). But for most graphs in the Johnson association scheme it is not known if such Godsil-McKay switching set exists. This provided the initial motivation for [7], where such a switching set is found for the symplectic graphs over $\mathbb{F}_2$.

New strongly regular graphs

A graph (simple, undirected and loopless) of order v is *strongly regular* with parameters (n, k, λ, μ) whenever it is not complete or edgeless and
(i) each vertex is adjacent to k vertices,
(ii) for each pair of adjacent vertices there are λ vertices adjacent to both,
(iii) for each pair of non-adjacent vertices there are μ vertices adjacent to both.
For example, the pentagon is strongly regular with parameters $(n, k, \lambda, \mu) = (5, 2, 0, 1)$.

The theory of strongly regular graphs sits at the core of algebraic combinatorics. These structures are interesting mathematical objects and their study has important applications in coding theory, combinatorics and computer science among others. Recently, strongly regular graphs have been used to construct the smallest known counterexamples to Borsuk's conjecture. Moreover, constructing new strongly regular graphs may be useful for the graph isomorphism problem, since distinguishing them is the main challenge.

It is well-known that if a graph G' has the same spectrum as a strongly regular graph G, then G' is also strongly regular with the same parameters as G (see for example [9]). Therefore Godsil-McKay switching also provides a tool to construct new strongly regular graphs from known ones. However, again there is no guarantee that the switched graph is nonisomorphic with the original graph. The necessary conditions for isomorphism after switching shown in [2] do not apply here, since the graphs are strongly regular and have a lot of structure. Hence some creativity is needed for proving nonsimorphism after switching. In [7], for instance, the 2-rank of the graph (the rank of the adjacency matrix over the finite field $\mathbb{F}_2$) is used to prove nonisomorphism after switching.

Recently, many researchers constructed strongly regular graphs with the same parameters as the collinearity graphs of finite classical polar spaces. This was triggered by a result of Abiad and Haemers, who used Godsil-McKay switching [7] to obtain strongly regular graphs with the same parameters as the symplectic graph $Sp(2\nu, 2)$ for all $\nu \geq 3$. In particular, it is shown that the 2-rank of the graph increases after switching. This implies that the switched graph is a new strongly regular graph with the same parameters as $Sp(2\nu, 2)$.

Barwick et al. [8] generalized this, also using Godsil–McKay switching, to quadrics of rank at least 3 over $\mathbb{F}_2$. Ihringer [25] generalized the results obtained by switching to all finite classical polar spaces of rank at least 3 over $\mathbb{F}_q$ by using purely geometrical arguments. More new graphs with the same parameters as $Sp(2\nu, 2)$ or related graphs were found also in [27], [24] and [3].

In [7], the following results are proven, providing an illustration of the use of Godsil-McKay switching to obtain new strongly regular graphs.

Let A and A' be the adjacency matrices of G and G', respectively, and assume that the first $|S|$ rows (and columns) of A and A' correspond to the switching set S and the last h rows correspond to the vertices outside S with exactly $\frac{1}{2}|S|$ neighbors in S. Then

$$A' = A + K \pmod 2, \quad \text{where } K = \begin{bmatrix} O & O & J \\ O & O & O \\ J^\top & O & O \end{bmatrix},$$

and J is the $|S| \times h$ all-ones matrix. Since 2-rank$(K) = 2$, the 2-ranks of A and A' differ by at most 2. It is well-known that the 2-rank of any adjacency matrix is even (see [10]), thus we have the following result.

Proposition 3.2.1. *[7] Suppose* 2*-rank*$(A) = r$*, then* r *is even and* 2*-rank*$(A') = r - 2$*,* r*, or* $r + 2$*.*

Let $\mathbb{F}_2^{2\nu}$ be the 2ν-dimensional vector space over $\mathbb{F}_2$, and let $K = I_\nu \otimes (J_2 - I_2)$, where I_ν is the identity matrix of order ν, and J denotes the all-ones matrix of order 2. The *symplectic graph* $Sp(2\nu, 2)$ over $\mathbb{F}_2$ is the graph whose vertices are the nonzero vectors of $\mathbb{F}_2^{2\nu}$, where two vertices x and y are adjacent whenever $x^\top K y = 1$. Equivalently, $x = [x_1 \ \dots \ x_{2\nu}]^\top$ and $y = [y_1 \ \dots \ y_{2\nu}]^\top$ are adjacent if

$$(x_1y_2 + x_2y_1) + (x_3y_4 + x_4y_3) + \cdots + (x_{2\nu-1}y_{2\nu} + x_{2\nu}y_{2\nu-1}) = 1.$$

For $\nu \geq 2$, it is known (see for example [30]) that the symplectic graph $Sp(2\nu, 2)$ is a strongly regular graph with parameters

$$\left(2^{2\nu} - 1,\ 2^{2\nu-1},\ 2^{2\nu-2},\ 2^{2\nu-2}\right),$$

and eigenvalues $2^{2\nu-1}$, $2^{\nu-1}$, $-2^{\nu-1}$ with multiplicities 1, $2^{2\nu-1} - 2^{\nu-1} - 1$, $2^{2\nu-1} + 2^{\nu-1} - 1$, respectively.

For $\nu \geq 3$, we define the following vectors in $\mathbb{F}_2^{2\nu}$:

$$v_1 = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ z \end{bmatrix}, v_2 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ z \end{bmatrix}, v_3 = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ z \end{bmatrix}, v_4 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ z \end{bmatrix},$$

where z is an arbitrary vector in $\mathbb{F}_2^{2\nu-6}$.

Proposition 3.2.2. *The set $S = \{v_1, v_2, v_3, v_4\}$ is a Godsil-McKay switching set of $Sp(2\nu, 2)$ for $\nu \geq 3$.*

Proof. Any two vertices from S are nonadjacent, so the subgraph of $Sp(2\nu, 2)$ induced by S is a coclique, and therefore regular. Consider an arbitrary vertex $x \notin S$. Then

$$\overset{\top}{x} K v_1 + \overset{\top}{x} K v_2 + \overset{\top}{x} K v_3 + \overset{\top}{x} K v_4 = \overset{\top}{x} K(v_1 + v_2 + v_3 + v_4) = \overset{\top}{x} K \mathbf{0} = 0.$$

This implies that the number of edges between x and S is even, and therefore S is a switching set. □

Let G' be the graph obtained from $G = Sp(2\nu, 2)$ by switching with respect to S. We shall now prove that G and G' are non-isomorphic.

Theorem 3.2.3. *For $\nu \geq 3$, the graph G' obtained from $Sp(2\nu, 2)$ by switching with respect to the switching set S given above, is strongly regular with the same parameters as $Sp(2\nu, 2)$, but with 2-rank equal to $2\nu + 2$.*

Proof. Let A be the adjacency matrix of $G = Sp(2\nu, 2)$, and assume that the first four rows and columns correspond to S. Then 2-rank$(A) = 2\nu$ and A has $2^{2\nu} - 1$ rows. This implies that, over $\mathbb{F}_2$, every possible nonzero linear combination of a basis of the row space of A is a row of A. Therefore the sum (mod 2) of any two rows of A is again a row of A. Let r_1 and r_2 be rows of A corresponding to the vertices $v_5 = [100000z^\top]^\top$ and $v_6 = [001000z^\top]^\top$, respectively. Then r_1 starts with 0011 and r_2 starts with 0101. It follows that $r_7 = r_5 + r_6$ is also a row of A starting with 0110. After switching only the first four entries of r_5, r_6 and r_7 change and become 1100, 1010 and 1001, respectively. Let r_i' denote the switched version of r_i ($i = 5, 6$ or 7). Then $v = r_5' + r_6' + r_7' = 11110\ldots0$. So v is in the row space of the switched matrix A', but it is not a row of A'. So G' is not isomorphic to G, and by Theorem 5.3 from [30] and Proposition 3.2.1 the 2-rank of A' equals $2\nu + 2$. □

The switching set S given above, is not the only one. There are many more (indeed, for any three independent vectors v_1, v_2 and $v_3 \in \mathbb{F}_2^{2\nu}$, the set $\{v_1, v_2, v_3, v_1 + v_2 + v_3\}$ is a Godsil-McKay switching set) and many remain a switching set after switching with respect to S. Therefore we can apply switching several times. However it is not true in general that a second switching increases the 2-rank again, and it looks difficult to make a general statement like in the above theorem.

Abiad, Butler and Haemers generalised some results from [7] to strongly regular graphs coming from certain graphical Hadamard matrices [3].

3.3 Other constructions of cospectral graphs

In [6], Abiad and Haemers presented a new method to construct families of cospectral graphs that generalizes Godsil-McKay switching. To do so, regular (constant row sum) orthogonal matrices of level 2 were used. We say that a matrix Q has *level l* if l is the smallest positive integer such that lQ is an integral matrix. Since A and A' are symmetric, G and G' are cospectral precisely when A and A' are similar, that is, there exists an orthogonal matrix Q such that $A' = Q^\top AQ$. If Q is a permutation matrix (i.e. Q is regular of level 1) then G and G' are isomorphic. So the next natural step is to study the case when G is nonisomorphic with G'. If G and G' are nonisomorphic, and there exist a regular orthogonal matrix Q of level 2 such that $A' = Q^\top AQ$, we call G and G' *semi-isomorphic*. Semi-isomorphic graphs are $\mathbb{R}$-cospectral, which means that the matrices $xI + yJ + zA$ and $xI + yJ + zA'$ have the same spectrum for every $x, y, z \in \mathbb{R}$, $z \neq 0$, where J and I are the all-one matrix and the identity matrix, respectively.

Johnson and Newman [26] show that being $\mathbb{R}$-cospectral is equivalent to being cospectral with cospectral complements, see Theorem 3.0.1 in these notes. It has been conjectured by Van Dam and Haemers that almost every graph is determined by its spectrum [32], or equivalently, that the proportion of graphs on n vertices that are determined by their spectrum goes to 1 as $n \to \infty$. A weaker version states that almost every graph is determined by its spectrum together with that of its complement. Both conjectures are still open, but Wang and Xu [39] have a number of results that support them. They prove that for almost no graph there exists a graph semi-isomorphic with it, and in addition they provide experimental evidence showing that a positive fraction of all pairs of nonisomorphic $\mathbb{R}$-cospectral graphs, are in fact semi-isomorphic. This makes it interesting to investigate the concept of semi-isomorphism in [6]. By using the classification of regular orthogonal matrices of level 2 [38], [6] works out the requirements for this switching operation to work in case Q has one nontrivial indecomposable block of size 4, 6, 7, or 8. Size 4 corresponds to Godsil-McKay switching of level 2. The other cases provide new methods for constructing $\mathbb{R}$-cospectral graphs.

A variation of GM switching is described in [37] by Wang, Qiu and Hu. This counterpart of the well-known GM switching method for generating cospectral graphs (with cospectral complements), can be used to construct pairs of non-isomorphic cospectral graphs that are not obtainable by the original GM switching method.

Theorem 3.3.1. *[37] Let G be a graph whose vertex set is partitioned as $C_1 \cup C_2 \cup D$. Assume that $|C_1| = |C_2|$ and that $C_1 \cup C_2$ is an equitable partition of the induced subgraph on $C_1 \cup C_2$ (that is, any two vertices in C_1 have same number of neighbors in C_1 and in C_2, and any two vertices in C_2 have same number of neighbors in C_2 and in C_1), and that all $x \in D$ satisfy one of the following:*

1. $|G(x) \cap C_1| = |G(x) \cap C_2|$*, or*
2. $G(x) \cap (C_1 \cup C_2) \in \{C_1, C_2\}$.

Construct a graph G' from G by modifying the edges between $C_1 \cup C_2$ and D as follows:

$$G'(x) \cap (C_1 \cup C_2) = \begin{cases} C_1 & \text{if } G(x) \cap (C_1 \cup C_2) = C_2 \\ C_2 & \text{if } G(x) \cap (C_1 \cup C_2) = C_1 \\ G(x) \cap (C_1 \cup C_2) & \text{otherwise} \end{cases}$$

for $x \in D$. Then G' is cospectral with G.

3.4 Exercises and open problems

Exercise 3.4.1. [2] Let $\lambda_G(x, y)$ denote the number of common neighbors of two vertices x and y in G, and let X be a switching set in a graph G (following the notation of Lemma 3.1.1). Show that the following conditions are sufficient for two cospectral graphs G and G' being non-isomorphic.
(i) The multiset of degrees (in G) of the vertices in X changes after switching.
(ii) The multiset $\Lambda_G = \{\lambda_G(x, y) \mid x \in X, y \in V(G)\}$ changes after switching.
(iii) The vertices of X all have the same degree, and the multiset $\overline{\Lambda}_G = \{\lambda_G(x, y) \mid x \in X, y \in Y\}$ changes after switching.

Exercise 3.4.2. [20] Let G be the Kneser graph $K(m, k)$ with vertex set $\binom{X}{k}$, where $|X| = m = 3k - 1$ $(k \geq 2)$. Fix $Y \subset X$ with $|Y| = k - 1$ and consider the subset

W of vertices of G consisting of the k-subsets of X containing Y. Prove that Wsatisfies the conditions for GM switching, and that the switching produces a graph nonisomorphic to G, provided $k \geq 3$.

Open problem 3.4.3. For Godsil-McKay switching to work the graph needs a special structure, called a Godsil-McKay switching partition. This switching partition of the vertices of a graph makes it possible to switch some of the edges such that the spectrum of the adjacency matrix does not change. However, the presence of this structure does not imply that the graph is not determined by its spectrum; it may be that after switching the graph is isomorphic with the original one. In [2] this phenomenon is investigated by obtaining some elementary necessary conditions for isomorphism after switching and showing how they can be used to guarantee nonisomorphism after switching for some graph products. Investigate whether new analogous sufficient or necessary conditions can be obtained for the switching presented in [37].

Open problem 3.4.4. [19] Study whether being regular with vertex or edge connectivity 1 is characterized by the spectrum.

References

[1] A. Abiad. A characterization and an application of weight-regular partitions of graphs. *Linear Algebra Appl.*, 569:164–174, 2019.

[2] A. Abiad, A. E. Brouwer, and W. H. Haemers. Godsil-McKay switching and isomorphism. *Electron. J. Linear Algebra*, 28:4–11, 2015.

[3] A. Abiad, S. Butler, and W. H. Haemers. Graph switching, 2-ranks, and graphical Hadamard matrices. *Discrete Math.*, to appear.

[4] A. Abiad, S. Cioaba, and M. Tait. Spectral bounds for the k-independence number of a graph. *Linear Algebra Appl.*, 510:160–170, 2016.

[5] A. Abiad, M. A. Fiol, W. H. Haemers, and G. Perarnau. An Interlacing Approach for Bounding the Sum of Laplacian Eigenvalues of Graphs. *Linear Algebra Appl.*, 34:11–21, 2014.

[6] A. Abiad and W. H. Haemers. Cospectral graphs and regular orthogonal matrices of level 2. *Electron. J. Comb.*, 19(3), 2012.

[7] A. Abiad and W. H. Haemers. Switched symplectic graphs and their 2-ranks. *Des. Codes Crypt.*, 81(1):35–41, 2016.

[8] S. G. Barwick, W. A. Jackson, and T. Penttila. New families of strongly regular graphs. *Australasian Journal of Combinatorics*, 67(3):486–507, 2017.

[9] A. E. Brouwer and W. H. Haemers. *Spectra of Graphs*. Springer, 2012.

[10] A. E. Brouwer and C. A. van Eijl. On the p-rank of the adjacency matrices of strongly regular graphs. *J. Alg. Comb.*, 1:329–346, 1992.

[11] L. Collatz and U. Sinogowitz. Spektren endlicher grafen. *Abh. Math. Sem. Univ. Hamburg*, 21:63–77, 1957.

[12] D. M. Cvetković. Graphs and their spectra. *Publ. Elektrotehn. Fak. Ser. Mut. Fiu.*, 354–356:1–50, 1971.

[13] M. A. Fiol. Eigenvalue interlacing and weight parameters of graphs. *Linear Algebra Appl.*, 290:275–301, 1999.

[14] M. A. Fiol and E. Garriga. On the algebraic theory of pseudo-distance-regularity around a set. *Linear Algebra Appl.*, 298:115–141, 1999.

[15] C. D. Godsil and B. D. McKay. Constructing cospectral graphs. *Aequationes Math.*, 25:257–268, 1982.

[16] R. Grone. Eigenvalues and the degree seqences of graphs. *Linear and Multilinear Algebra*, 39:133–136, 1995.

[17] W. H. Haemers. *Eigenualue Techniques in Design and Graph Theoy*. Math. Centre Tract 121, Mathematical Centre, Amsterdam, 1980.

[18] W. H. Haemers. Interlacing eigenvalues and graphs. *Linear Algebra Appl.*, 226-228:593–616, 1995.

[19] W. H. Haemers. Cospectral pairs of regular graphs with different connectivity. *preprint*, 2019.

[20] W. H. Haemers and F. Ramezani. Graphs cospectral with Kneser graphs. *Combinatorics and Graphs, AMS, Contemporary Mathematics*, 531:159–164, 2010.

[21] W. H. Haemers and E. Spence. Enumeration of cospectral graphs. *European J. Combin.*, 25:199–211, 2004.

[22] A. J. Hoffman. On eigenvalues and colourings of graphs. pages 79–91, 1970.

[23] T. Huang and C. Liu. Spectral characterization of some generalized Odd graphs. *Graphs Combin.*, 15:195–209, 1999.

[24] A. M. W. Hui and B. Rodrigues. Switched graphs of some strongly regular graphs related to the symplectic graph. *Des. Codes Cryptography*, 86:179–194, 2018.

[25] F. Ihringer. A switching for all strongly regular collinearity graphs from polar spaces. *J. Algebr. Comb.*, 46:263–274, 2017.

[26] C. R. Johnson and M. Newman. A note on cospectral graphs. *J. Combin. Theory Ser. B*, 28:96–103, 1980.

[27] S. Kubota. Strongly regular graphs with the same parameters as the symplectic graph. *preprint*, 2017.

[28] B. D. McKay. On the spectral characterisation of trees. *Ars Combin.*, 3:219–232, 1979.

[29] B. Mohar. Isoperimetric numbers of graphs. *J. Combin. Theory Ser. B*, 47:274–291, 1989.

[30] M. J. P. Peeters. Uniqueness of strongly regular graphs having minimal p-rank. *Linear Algebra Appl.*, 226-228:9–31, 1995.

[31] I. Schur. Über eine Klasse von Mittelbildungen mit Anwendungen die Determinanten. *Theorie Sitzungsber. Berlin. Math. Gessellschaft*, 22:9–20, 1923.

[32] E. R. van Dam and W. H. Haemers. Which graphs are determined by their spectrum? *Linear Algebra Appl.*, 373:241–272, 2003.

[33] E. R. van Dam and W. H. Haemers. Developments on spectral characterizations of graphs. *Discrete Math.*, 309:576–586, 2009.

[34] E. R. van Dam, W. H. Haemers, J. H. Koolen, and E. Spence. Characterizing distance-regularity of graphs by the spectrum. *J. Combin. Theory Ser. A*, 113:1805–1820, 2006.

[35] E. R. van Dam and J. H. Koolen. A new family of distance-regular graphs with unbounded diameter. *Invention. Math.*, 162:189–193, 2005.

[36] J. H. van Lint and R. M. Wilson. *A Course in Combinatorics*. Cambridge University Press, 1992.

[37] W. Wang, L. Qiu, and Y. Hu. Cospectral graphs, GM-switching and regular rational orthogonal matrices of level p. *Linear Algebra Appl.*, 563:154–177, 2019.

[38] W. Wang and C. X. Xu. An excluding algorithm for testing whether a family of graphs are determined by their generalized spectra. *Linear Algebra Appl.*, 418:62–74, 2006.

[39] W. Wang and C. X. Xu. On the asymptotic behavior of graphs determined by their generalized spectra. *Discrete Math.*, 310:70–76, 2010.

Part II

Geometry of sesquilinear forms

Nicola Durante

Dipartimento di Matematica e Applicazioni "Renato Caccioppoli"
Via Cintia – Complesso Monte S. Angelo, 26
Napoli
Italy

email: ndurante@unina.it

Contents

Preface

Geometries of reflexive sesquilinear forms of a vector space over a field have been intensively studied in the last decades since they give rise to the well known objects in projective spaces called quadrics, symplectic geometries and Hermitian varieties.

With these notes we study the geometries of non-reflexive sesquilinear forms of a vector space over a finite field. We will be able to classify the geometric objects related to such forms in the finite projective line $\mathrm{PG}(1, q^n)$ and, assuming the form is degenerate, also in the finite projective plane $\mathrm{PG}(2, q^n)$ and in the threedimensional finite projective space $\mathrm{PG}(3, q^n)$.

We will see that the geometric objects that come out are related to both some very old geometric constructions of conics and quadrics due to J. Steiner and F. Seydewitz almost 200 year ago and to very new arguments such as hyperovals, spreads, $\mathbb{F}_{||}$-linear sets, semifield flocks, MRD-codes, and more.

Finally everything is known (thanks to the huge work of B. Kestenband), but difficult to handle with, also in the case of non-degenerate, non-reflexive sesquilinear forms of a vector space of dimension three over a finite field, hence in the finite projective plane $\mathrm{PG}(2, q^n)$.

Chapter 1

Preliminary results

1.1 Finite fields

Definition 1.1.1. Let $\mathbb{F}$ be a field. If

$$c \in \mathbb{N},\ ca = 0\ \forall\, a \in \mathbb{F} \implies c = 0,$$

then $\mathbb{F}$ has *characteristic* 0 and we write $\mathrm{char}(\mathbb{F}) = 0$, otherwise $\mathbb{F}$ has *positive characteristic*, being the smallest positive integer p such that:

$$pa = 0\ \forall\, a \in \mathbb{F}.$$

In this case we write $\mathrm{char}(\mathbb{F}) = p$.

Let $\mathbb{F}$ be a field and let $\mathbb{K}$ be a subfield of $\mathbb{F}$. The field $\mathbb{F}$ is also called an *extension* of the field $\mathbb{K}$.

Definition 1.1.2. A field $\mathbb{F}$ with no proper subfields is a *prime* field.

Examples 1.1.3. The field $\mathbb{Q}$, of rational numbers, and the field $\mathbb{Z}_p$, of integers modulo a prime number p, are examples of prime fields.

There are no other prime fields than $\mathbb{Q}$ and $\mathbb{Z}_p$.

Definition 1.1.4. Let $\mathbb{F}$ be a field. The intersection of all subfields of $\mathbb{F}$ is the *prime* or *fundamental* subfield of $\mathbb{F}$.

Proposition 1.1.5. *Let $\mathbb{F}$ be a field. The prime field of $\mathbb{F}$ is either $\mathbb{Q}$ or $\mathbb{Z}_p$. In the first case char$(\mathbb{F}) = 0$, in the second case char$(\mathbb{F}) = p$.*

Definition 1.1.6. Let $\mathbb{F}$ be a field and let $\mathbb{K}$ be a subfield of $\mathbb{F}$. Let a be an element of $\mathbb{F} \setminus \mathbb{K}$. The intersection of all subfields of $\mathbb{F}$ containing $\mathbb{K}$ and a is denoted by $\mathbb{K}(a)$ and it is called the *extension* of the field $\mathbb{K}$ by adding a.

If the field $\mathbb{F}$ is an extension of a field $\mathbb{K}$, then $\mathbb{F}$ is a vector space of dimension $[\mathbb{F} : \mathbb{K}]$ over $\mathbb{K}$.

Definition 1.1.7. Let p be a prime number, for every $h \in \mathbb{N}$ there is a field of order $q = p^h$, called the *Galois* field of order q, that we will denote by $\mathbb{F}_q$. It is unique, up to isomorphisms, and it is an extension of the field $\mathbb{Z}_p$. The prime p is the characteristic of $\mathbb{F}_q$.

The elements of $\mathbb{F}_q$ are characterized to be the q distinct roots of the polynomial $x^q - x$. The multiplicative group $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ of the field $\mathbb{F}_q$ is a cyclic group and any element generating it is a *primitive element* of $\mathbb{F}_q$. Let $g \in \mathbb{Z}_p[x]$ be an irreducible polynomial of degree $h > 1$ over $\mathbb{Z}_p$ and let a be a root of g in an extension of $\mathbb{Z}_p$. The extension of $\mathbb{Z}_p$ by adding a is:

$$\mathbb{Z}_p(a) = \{m_0 + m_1 a + \cdots + m_{h-1} a^{h-1}\}_{m_j \in \mathbb{Z}_p}$$

and it is a field isomorphic to the Galois field of order $q = p^h$. The followings hold:

Proposition 1.1.8. *Let $\mathbb{F}_q$ be a finite field of order $q = p^h$. For every $h'|h$ there is a subfield $\mathbb{F}_{q'}$, of order $q' = p^{h'}$, of $\mathbb{F}_q$.*

Proposition 1.1.9. *Let $a_1, \ldots, a_{q-1}$ be the elements of $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. Then:*

$$a^{q-1} = 1 \qquad \forall a \in \mathbb{F}_q^*,$$

$$a^q = a \qquad \forall a \in \mathbb{F}_q,$$

$$a_1 \cdots a_{q-1} = -1.$$

Proposition 1.1.10. *Let $\mathbb{F}_{q^n}$ be a finite field of order q^n. For every integer m with $0 \leq m < n$ the map $\sigma_m : x \in \mathbb{F}_{q^n} \longrightarrow x^{q^m} \in \mathbb{F}_{q^n}$ is an automorphism of $\mathbb{F}_{q^n}$ with $Fix(\sigma_m) = \mathbb{F}_{q^{(m,n)}}$.*

The map σ_m of the previous proposition is called the *m-th Frobenius' automorphism* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Proposition 1.1.11. *The group $Aut(\mathbb{F}_q)$ of all the automorphisms of $\mathbb{F}_q$, $q = p^h$, is a cyclic group of order h. It is generated by the first Frobenius' automorphism of $\mathbb{F}_q$ over $\mathbb{Z}_p$.*

Definition 1.1.12. Let $\mathbb{F} = \mathbb{F}_{q^n}$ be an extension of the field $\mathbb{K} = \mathbb{F}_q$, $q = p^h$. For every $a \in \mathbb{F}$ the *trace* of a over $\mathbb{K}$ is the element

$$Tr_{\mathbb{F}/\mathbb{K}}(a) = Tr(a) = a + a^q + \cdots + a^{q^{n-1}}.$$

If $\mathbb{K} = \mathbb{F}_p$, then $Tr_{\mathbb{F}/\mathbb{K}}$ is the *absolute trace*. The *norm* of a over $\mathbb{K}$ is the element

$$N_{\mathbb{F}/\mathbb{K}}(a) = N(a) = a \cdot a^q \cdots a^{q^{n-1}} = a^{(q^n-1)/(q-1)}.$$

If $\mathbb{K} = \mathbb{F}_p$, then $N_{\mathbb{F}/\mathbb{K}}$ is the *absolute norm*.

Definition 1.1.13. A *reduced* polynomial of $\mathbb{F}_q[x]$ is either 0 or a polynomial of degree at most $q-1$.

Definition 1.1.14. A *skew field* $\mathbb{F}$ satisfies all the axioms for a field except (possibly) commutativity of multiplication.

Theorem 1.1.15 (J.H.M. Wedderburn [64]). *Every finite skew field is a field.*

Remark 1.1.16. Let $\mathbb{F}_q$ be a finite field of order $q = p^h$, p a prime.

- If q is odd, then $\frac{q-1}{2}$ elements of $\mathbb{F}_q^*$ are non-squares and $\frac{q-1}{2}$ elements of $\mathbb{F}_q^*$ are squares.
- If q is even, then all elements of $\mathbb{F}_q$ are squares.

For the proofs of the results in this section see e.g. [70].

1.2 Linear, semilinear and $\mathbb{F}_q$-linear maps

Let V be a vector space over a field $\mathbb{F}$ (also called $\mathbb{F}$-vector space) and let $H \subset V$. In the remaining part we will denote by $\langle H \rangle$ the subspace spanned by H.

Definition 1.2.1. Let V and W be two finite dimensional vector spaces over a field $\mathbb{F}$. A *linear map* $f : V \longrightarrow W$ satisfies:

$$f(au + bv) = af(u) + bf(v) \;\; \forall a, b \in \mathbb{F} \;\text{ and }\; \forall u, v \in V.$$

If f is bijective, then it is an *isomorphism* between V and W. If f is an isomorphism of V into itself, then f is an *automorphism* of V. The *linear group* of V, denoted by $\mathrm{GL}(V)$, contains all the automorphisms of V.

If $\mathcal{B} = (e_1, e_2, \dots, e_{d+1})$ is an ordered basis of V, so that $d+1$ is the *dimension* of V as $\mathbb{F}$-vector space, then $v = x_1e_1 + x_2e_2 + \cdots + x_{d+1}e_{d+1}$, and we will denote by X the column of *coordinates* $(x_1, x_2, \dots, x_{d+1})_t$ of v, w.r.t. $\mathcal{B}$. For every automorphism f of V, there is a non-singular square matrix A_f of order $d+1$ such that $X' = A_fX$, where $X' = (x'_1, x'_2, \dots, x'_{d+1})_t$ denotes the column of coordinates of $f(v)$ w.r.t. $\mathcal{B}$. Let $\mathrm{GL}(d+1, \mathbb{F})$ be the group of non-singular square matrices of order $d+1$ with elements in $\mathbb{F}$. It is $\mathrm{GL}(V) \cong \mathrm{GL}(d+1, \mathbb{F})$.

Definition 1.2.2. Let V and W be two finite dimensional $\mathbb{F}$-vector spaces and let σ be an automorphism of $\mathbb{F}$. A *semilinear* map $f : V \longrightarrow W$, with σ as *companion automorphism*, or *σ-linear* map satisfies:

$$f(au + bv) = a^\sigma f(u) + b^\sigma f(v), \ \ \forall a, b \in \mathbb{F} \ \text{ and } \ \forall u, v \in V.$$

The *Kernel* of f is the subspace of V defined as $\ker(f) = \{v \in V : f(v) = 0\}$. The *Image* of f is the subspace of W defined as $Imf = \{f(v) : v \in V\}$.
If f is a bijective map, then it is a *semilinear isomorphism* between V and W. If f is a semilinear isomorphism of V into itself, then f is a semilinear *automorphism* of V. The *semilinear group* of V, denoted by $\Gamma\mathrm{L}(V)$, contains all the semilinear automorphisms of V. It is $\Gamma\mathrm{L}(V) \cong \mathrm{GL}(V) \rtimes Aut(\mathbb{F})$.

Let σ be an automorphism of $\mathbb{F}$ and let $\mathcal{B}$ be an ordered basis of V. If $v \in V$ and $X = (x_1, x_2, \dots, x_{d+1})_t$ are the coordinates of v, w.r.t $\mathcal{B}$, then we will denote by v^σ the vector of V with coordinates $X^\sigma = (x_1^\sigma, x_2^\sigma, \dots, x_{d+1}^\sigma)_t$ w.r.t. $\mathcal{B}$.
If $f : V \longrightarrow V$ is an automorphism of V, then the map

$$f_\sigma : v \in V \longrightarrow f(v^\sigma) \in V,$$

is a σ-linear automorphism w.r.t. $\mathcal{B}$. If X and X' are the vectors of coordinates of v and $f_\sigma(v)$, w.r.t. $\mathcal{B}$, then it is

$$X' = A_f X^\sigma.$$

Definition 1.2.3. Let V and W be two finite dimensional $\mathbb{F}_{q^n}$-vector spaces. An $\mathbb{F}_q$-*linear* map $f : V \longrightarrow W$ satisfies:

$$f(au + bv) = af(u) + bf(v), \ \ \forall a, b \in \mathbb{F}_q \ \text{ and } \ \forall u, v \in V.$$

For more details on this section see e.g. [6],[46].

1.3 Desarguesian projective and affine spaces

Let V be a $(d+1)$-dimensional vector space over a (skew) field $\mathbb{F}$. We will denote by $\mathrm{PG}(V)$ the set of 1-dimensional subspaces of V, that will be called *points* of

$\mathrm{PG}(V)$. We will call *lines, planes, m-dimensional projective subspaces, hyperplanes* respectively the 2-dimensional, 3-dimensional, $(m+1)$-dimensional, d-dimensional subspaces of V seen as set of points of $\mathrm{PG}(V)$. We consider the empty set as a projective subspace of dimension -1. If H is any subset of points of $\mathrm{PG}(V)$, then we will denote by $\langle H\rangle$ the projective subspace spanned by H. Denote by $\mathcal{S}_j$ the set of all subspaces of $\mathrm{PG}(V)$ with dimension j, for every $j \in \{-1, 0, 1, \ldots, d\}$.

Definition 1.3.1. The pair $(\mathrm{PG}(V), (\mathcal{S}_{-1}, \mathcal{S}_0, \mathcal{S}_1, \ldots, \mathcal{S}_d))$ is the *d-dimensional projective space associated* to V, also called either the *d-dimensional projective space over* $\mathbb{F}$ or the *d-dimensional Desarguesian projective space*. We will often denote just by $\mathrm{PG}(V)$ the projective space associated to V. We will denote by $\mathrm{PG}(d, \mathbb{F})$ the d-dimensional projective space associated to $V = \mathbb{F}^{d+1}$ and we will use $\mathrm{PG}(d, q)$ instead of $\mathrm{PG}(d, \mathbb{F}_q)$. If $d = 1$, then $\mathrm{PG}(1, \mathbb{F})$ is called the *projective line* over $\mathbb{F}$. If $d = 2$, then $\mathrm{PG}(2, \mathbb{F})$ is called the *projective plane* over $\mathbb{F}$.

Definition 1.3.2. If $f : V \longrightarrow W$ is an isomorphism between two $\mathbb{F}$-vector spaces V and W, then the bijection

$$\langle v\rangle \in \mathrm{PG}(V) \longrightarrow \langle f(v)\rangle \in \mathrm{PG}(W),$$

is the *projectivity* between $\mathrm{PG}(V)$ and $\mathrm{PG}(W)$ *induced* by f. The *projective general linear* group of $\mathrm{PG}(V)$, denoted by $\mathrm{PGL}(V)$, contains all the projectivities of $\mathrm{PG}(V)$. If $V = \mathbb{F}_q^{d+1}$, then $\mathrm{PGL}(V)$ is denoted by $\mathrm{PGL}(d+1, q)$.

Definition 1.3.3. Let $f : V \longrightarrow W$ be a linear map with $\ker(f) \neq \{0\}$. The map

$$\langle v\rangle \in \mathrm{PG}(V) \setminus \ker(f) \longrightarrow \langle f(v)\rangle \in \mathrm{PG}(W),$$

will be called a *degenerate projectivity* between $\mathrm{PG}(V)$ and $\mathrm{PG}(W)$.

Definition 1.3.4. Let $P_1 = \langle v_1\rangle, P_2 = \langle v_2\rangle, \ldots, P_m = \langle v_m\rangle$ be points of $\mathrm{PG}(V)$. They are either *linearly dependent*, respectively *linearly independent* if the vectors $v_1, v_2, \ldots, v_m$ are linearly dependent, respectively linearly independent.

Definition 1.3.5. If V has dimension $d+1$, then any ordered set of $d+2$ points $\mathcal{R} = (A_1, A_2, \ldots, A_{d+1}, A)$ of $\mathrm{PG}(V)$ such that any $d+1$ of them are linearly independent is a *projective frame* of $\mathrm{PG}(V)$. The points $A_1, \ldots, A_{d+1}$ are the *fundamental points* and A is the *unit point* of the frame $\mathcal{R}$.

Definition 1.3.6. Let $\mathcal{B} = (e_1, e_2, \ldots, e_{d+1})$ be an ordered basis of V. The ordered set $\mathcal{R}(\mathcal{B}) = (\langle e_1\rangle, \langle e_2\rangle, \ldots, \langle e_{d+1}\rangle, \langle e_1 + e_2 + \cdots + e_{d+1}\rangle)$ is called the *associated* frame of $\mathrm{PG}(V)$. For every point $P = \langle x_1e_1 + \cdots + x_{d+1}e_{d+1}\rangle$ the vector $X = (x_1, \ldots, x_{d+1})_t$, defined up to a non-zero scalar multiple, is the vector of the *projective coordinates* of P w.r.t. the frame $\mathcal{R}$. In what follows, we will denote by $X = (x_1, \ldots, x_{d+1})_t$, instead of $\langle(x_1, \ldots, x_{d+1})_t\rangle$, a point of $\mathrm{PG}(d, q)$. Sometimes, we will omit the symbol t of transposition, whenever it does not affect what follows.

Definition 1.3.7. Let V and W be two $\mathbb{F}$-vector spaces with dimension greater than two. A bijection $g : \mathrm{PG}(V) \longrightarrow \mathrm{PG}(W)$ is a *collineation* if g, together with g^{-1}, maps lines into lines. If V and W have dimension two, then a *collineation* is a map $\langle v \rangle \in \mathrm{PG}(V) \longrightarrow \langle f(v) \rangle \in \mathrm{PG}(W)$, induced by a bijective semilinear map $f : V \longrightarrow W$. The *collineation group* of $\mathrm{PG}(V)$, denoted by $\mathrm{P\Gamma L}(V)$, contains all the collineations of $\mathrm{PG}(V)$. If $V = \mathbb{F}_q^{d+1}$, then we use $\mathrm{P\Gamma L}(d+1,q)$ instead of $\mathrm{P\Gamma L}(V)$. It is $\mathrm{P\Gamma L}(d+1,q) \cong \mathrm{PGL}(d+1,q) \rtimes Aut(\mathbb{F}_q)$.

Theorem 1.3.8. (*Fundamental Theorems*)

1. *Let $\mathcal{R}$ and $\mathcal{R}'$ be two projective frames of* $\mathrm{PG}(V)$, *there is a unique projectivity that maps $\mathcal{R}$ into $\mathcal{R}'$.*
2. *Let V and W be two $\mathbb{F}$-vector spaces. Every collineation between* $\mathrm{PG}(V)$ *and* $\mathrm{PG}(W)$ *is induced by a semilinear map $f : V \longrightarrow W$.*

Definition 1.3.9. *Projective geometry* is the study of properties of subsets of $\mathrm{PG}(V)$ invariant under the group $\mathrm{PGL}(V)$. *Incidence geometry* in $\mathrm{PG}(V)$ is the study of properties of subsets of $\mathrm{PG}(V)$ invariant under the group $\mathrm{P\Gamma L}(V)$.

Hence we can always fix a frame of $\mathrm{PG}(V)$ in order to study subsets of $\mathrm{PG}(V)$.

Definition 1.3.10. Let $f : V \longrightarrow W$ be a semilinear map, with $\ker(f) \neq \{0\}$. The map

$$\langle v \rangle \in \mathrm{PG}(V) \setminus \ker(f) \longrightarrow \langle f(v) \rangle \in \mathrm{PG}(W),$$

will be called a *degenerate collineation* between $\mathrm{PG}(V)$ and $\mathrm{PG}(W)$.

Definition 1.3.11. Let S_m be a subspace of dimension m, $0 \leq m \leq d-2$, of $\mathrm{PG}(d,q)$ and consider the following geometry:

- the points are the $(m+1)$-dimensional subspaces containing S_m,
- the lines are the $(m+2)$-dimensional subspaces containing S_m.

This geometry, denoted by $\mathrm{PG}(d,q)/S_m$, is called the *quotient geometry* of $\mathrm{PG}(d,q)$ w.r.t. S_m and it is isomorphic to a $\mathrm{PG}(d-m-1,q)$.

If $m = 0$ and $d > 2$, then $\mathrm{PG}(d,q)/S_0$ is called the *star of lines with centre the point* S_0 and in what follows will be also denoted by $\mathcal{S}_{S_0}$. If $d = 2$, then $\mathrm{PG}(2,q)/S_0$ is called the *pencil of lines with centre the point* S_0 and will be also denoted by $\mathcal{P}_{S_0}$.

If $m = d-2$, then $\mathrm{PG}(d,q)/S_{d-2}$ is called the *pencil of hyperplanes with axis* S_{d-2} and in what follows will be also denoted by $\mathcal{P}_{S_{d-2}}$.

Definition 1.3.12. Let $\mathrm{PG}(d, q^n)$ be the projective geometry of dimension d over $\mathbb{F}_{q^n}$. Let S_m be a subspace of dimension m of $\mathrm{PG}(d, q^n)$.

A *subgeometry of order* q of S_m is the set of points of S_m, say S'_m, whose projective coordinates, with respect to a fixed frame of S_m, are in $\mathbb{F}_q$.

If S is either a line or a plane of $\mathrm{PG}(d, q^n)$, then S' is called respectively an $\mathbb{F}_q$-*subline* or an $\mathbb{F}_q$-*subplane* of S.

If $n = 2$, then S'_m is a *Baer* subgeometry of S_m.

Let π_∞ be a selected hyperplane of the projective space $\mathrm{PG}(d, \mathbb{F})$. The points of $\mathrm{AG}(d, \mathbb{F}) = \mathrm{PG}(d, \mathbb{F}) \setminus \pi_\infty$ are the *affine* points of $\mathrm{PG}(d, \mathbb{F})$ w.r.t. π_∞, and for every m-dimensional projective subspace S_m of $\mathrm{PG}(d, \mathbb{F})$, not contained in π_∞, the set $A_m = S_m \setminus \pi_\infty$ is an *m-dimensional affine subspace* of $\mathrm{AG}(d, \mathbb{F})$. We will call *lines, planes, hyperplanes*, respectively, affine subspaces of dimension $1, 2, d-1$. We consider the empty set as an affine subspace of dimension -1. The points of π_∞ are also called either the *improper* points or the *directions* of $\mathrm{AG}(d, \mathbb{F})$. Any affine line $A_1 = S_1 \setminus \pi_\infty$ has a unique improper point $S_1 \cap \pi_\infty$. For every $m > 1$, the subspace of π_∞ given by $S_m \cap \pi_\infty$ is the *improper subspace* of $A_m = S_m \setminus \pi_\infty$. Any two affine subspaces of dimension greater than zero are *parallel* subspaces if the improper subspace of one of them contains the improper subspace of the other one. It is easy to see that if two affine subspaces are parallel subspaces, then either they have empty intersection or one of them is contained in the other one.

Definition 1.3.13. Let $\mathcal{A}_j$ be the family of affine subspaces of $\mathrm{AG}(d, \mathbb{F})$, for every $j \in \{-1, 0, 1, \ldots, d\}$. An *affine space* of *dimension* d over $\mathbb{F}$ or *Desarguesian affine space* is the pair

$$(\mathrm{AG}(d, \mathbb{F}), (\mathcal{A}_{-1}, \mathcal{A}_0, \ldots, \mathcal{A}_d)),$$

often denoted just by $\mathrm{AG}(d, \mathbb{F})$. If $\mathbb{F} = \mathbb{F}_q$, then we will use $\mathrm{AG}(d, q)$ instead of $\mathrm{AG}(d, \mathbb{F})$. If $d = 1$, then $\mathrm{AG}(1, \mathbb{F})$ is called the *affine line* over $\mathbb{F}$. If $d = 2$, then $\mathrm{AG}(2, \mathbb{F})$ is called the *affine plane* over $\mathbb{F}$

For the proofs of the results in this section see e.g. [3],[8],[30],[33],[46],[49].

1.4 Characterizations of affine and projective spaces

In this section we will give a more general definition of projective and affine planes. We start with the definition of an incidence structure.

Definition 1.4.1. Let $\mathcal{P}$ be a non-empty set, whose elements are called *points*, and let $\mathcal{L}$ be a non-empty set, whose elements are called either *lines* or *blocks*. Denote by I an *incidence* relation between $\mathcal{P}$ and $\mathcal{L}$ that we will consider symmetric. We will denote by $(\mathcal{P}, \mathcal{L}, I)$ an *incidence structure*.

The incidence relation will be often either $\subseteq$ or $\supseteq$. In these cases we will omit I and denote the incidence geometry by $(\mathcal{P}, \mathcal{L})$ and either the set $\mathcal{L}$ of lines will be identified with a set of subsets of $\mathcal{P}$, with the incidence being $\subseteq$ or the set $\mathcal{P}$ of points will be identified with a set of subsets of $\mathcal{L}$, with the incidence being $\supseteq$. Moreover when a point P is incident with a line ℓ we will use the usual terminology: the point P is on the line ℓ, the line ℓ passes through the point P etc.

Definition 1.4.2. A *linear space* is an incidence structure $(\mathcal{P}, \mathcal{L})$ of points and lines satisfying the following properties:

- any two distinct points are incident with a unique line,
- every line is incident with at least two distinct points,
- there are at least two distinct lines.

Next the definition of projective plane.

Definition 1.4.3. A *projective plane* is a linear space $(\mathcal{P}, \mathcal{L})$ such that:

- any two distinct lines meet at a unique point,
- every line is incident with at least three distinct points.

Finally, the definition of affine plane.

Definition 1.4.4. An *affine plane* is a linear space $(\mathcal{P}, \mathcal{L})$ such that:

- through any point not on a line ℓ there is a unique line disjoint from ℓ.

There are examples of both affine and projective planes not isomorphic to $\mathrm{AG}(2, \mathbb{F})$ and to $\mathrm{PG}(2, \mathbb{F})$, respectively, for any (skew) field $\mathbb{F}$; they are called *non-desarguesian* planes. (see e.g. [8], [50]). In [8],[95],[102] it is proved the following characterization theorem for projective spaces:

Theorem 1.4.5. *Let $(\mathcal{P}, \mathcal{L})$ be a linear space. If the following hold:*

(i) [*Veblen-Young axiom*] *let ℓ and ℓ' be two lines meeting at a point P and let $A_1, A_2 \in \ell \setminus \{P\}$, $B_1, B_2 \in \ell' \setminus \{P\}$. The lines A_1B_1 and A_2B_2 have a common point,*

(ii) *every line contains at least three distinct points,*

then $(\mathcal{P}, \mathcal{L})$ is either a Desarguesian projective space $\mathrm{PG}(d, \mathbb{F})$*, $d \geq 3$, for some (skew) field $\mathbb{F}$ or it is a projective plane.*

In [69] H. Lenz proved the following characterization theorem for affine spaces:

Theorem 1.4.6. *Let $(\mathcal{P}, \mathcal{L})$ be a linear space with an equivalence relation, called parallelism, among its lines. If the following hold:*

(i) [*Playfair axiom*] *through any point not on a line ℓ there is a unique line parallel to ℓ,*

(ii) *let ℓ and ℓ' be two distinct parallel lines, let $P, Q \in \ell$ and let $P' \in \ell'$. If $R \in PP' \setminus \{P\}$, then the lines RQ and ℓ' have a common point,*

then $(\mathcal{P}, \mathcal{L})$ is either a Desarguesian affine space $\mathrm{AG}(d, \mathbb{F})$*, $d \geq 3$, for some (skew) field $\mathbb{F}$ or it is an affine plane.*

Definition 1.4.7. Let $\mathbb{P} = (\mathcal{P}, \mathcal{L})$ either a projective or an affine space. Let $m_1 < m_2 < \cdots < m_k$ be non-negative integers. A set $\mathcal{S}$ of points of $\mathbb{P}$ is of *type* $(m_1, m_2, \ldots, m_k)_h$ if for every $S_h \in \mathcal{S}_h$ it is $|S_h \cap \mathcal{S}| = m_i$ for some $i \in \{1, \ldots, k\}$ and $\forall\ i \in \{1, \ldots, k\}$ there is a subspace $S_h \in \mathcal{S}_h$ s.t. $|S_h \cap \mathcal{S}| = m_i$. Such a subspace is called an m_i-*secant* subspace w.r.t. $\mathcal{S}$. If $m_i = 0$, then S_h is also called an *external* subspace; if $m_i = 1$, then S_h is also called a *tangent* subspace.

1.5 The dual space of $\mathrm{PG}(V)$

Let V be a $(d+1)$-dimensional vector space over a field $\mathbb{F}$ and let V^* be its *dual* space, that is the vector space of the linear maps from V to $\mathbb{F}$. If $\mathcal{B} = (e_1, \ldots, e_{d+1})$ is an ordered basis of V, then $\mathcal{B}^* = (e_1^*, \ldots, e_{d+1}^*)$ defined by $e_i^*(e_j) = \delta_{ij}$ is the *dual* basis of $\mathcal{B}$. For every $v \in V$ such that $v = a_1e_1 + \cdots + a_{d+1}e_{d+1}$, it is $e_i^*(v) = a_i$. The projective space $\mathrm{PG}(V^*)$ is the *dual* space of $\mathrm{PG}(V)$ and it will be also denoted by $\mathrm{PG}(V)^*$.

Definition 1.5.1. If $\mathcal{R} = (\langle e_1 \rangle, \ldots, \langle e_{d+1} \rangle, \langle e_1 + \cdots + e_{d+1} \rangle)$ is a frame of $\mathrm{PG}(V)$, then $\mathcal{R}^* = (\langle e_1^* \rangle, \ldots, \langle e_{d+1}^* \rangle, \langle e_1^* + \cdots + e_{d+1}^* \rangle)$ is the *dual* frame of $\mathcal{R}$.

Let $\mathcal{R}$ be a fixed frame of $\mathrm{PG}(V)$ and let $\mathcal{R}^*$ be its dual frame. If π_a is a hyperplane of $\mathrm{PG}(V)$, then its points have coordinates, w.r.t. $\mathcal{R}$, satisfying

$$a_1x_1 + \cdots + a_{d+1}x_{d+1} = 0,$$

hence π_a determines a point π_a^* of $\mathrm{PG}(V)^*$ with coordinates $(a_1, \ldots, a_{d+1})_t$ w.r.t. $\mathcal{R}^*$. The map defined by $\pi_a \mapsto \pi_a^*$ sends hyperplanes of $\mathrm{PG}(V)$ into points of $\mathrm{PG}(V)^*$. It is an isomorphism between $\mathrm{PG}(V)$ and its dual $\mathrm{PG}(V)^*$. It gives a way to identify hyperplanes of $\mathrm{PG}(V)$ with points of $\mathrm{PG}(V)^*$. Hence, in the remaining part, we can think of the dual space $\mathrm{PG}(V)^*$ also as the projective space whose points are the hyperplanes of $\mathrm{PG}(V)$ and whose lines are either the pencils of hyperplanes through a common $(d-2)$-dimensional projective subspace of $\mathrm{PG}(V)$ or the $(d-2)$-dimensional subspaces themselves with the incidence $\supseteq$ instead of $\subseteq$. See e.g. [3],[8],[21].

1.6 Sesquilinear forms, correlations and polarities

Definition 1.6.1. Let V be an $\mathbb{F}$-vector space with finite dimension $d+1$. Let σ be an authomorphism of $\mathbb{F}$. A map

$$\langle\ ,\ \rangle : (v, v') \in V \times V \longrightarrow \langle v, v'\rangle \in \mathbb{F},$$

is either a *σ-sesquilinear form* or a *σ-semibilinear form* on V if it is a linear map on the first argument and it is a σ-linear map on the second argument. That is $\forall\ v, v', v'' \in V$, $\forall a \in \mathbb{F}$ it holds:

$$\langle v + v', v''\rangle = \langle v, v''\rangle + \langle v', v''\rangle,$$
$$\langle v, v' + v''\rangle = \langle v, v'\rangle + \langle v, v''\rangle,$$
$$\langle av, v'\rangle = a\langle v, v'\rangle, \quad \langle v, av'\rangle = a^\sigma\langle v, v'\rangle,$$

If σ is the identity map, then $\langle\ ,\ \rangle$ is an usual *bilinear form*.

If $\mathcal{B} = (e_1, e_2, \ldots, e_{d+1})$ is an ordered basis of V, then for $x, y \in V$ we have $\langle x, y\rangle = X_tAY^\sigma$, where $A = (\langle e_i, e_j\rangle)$ is the *associated* matrix to the σ-sesquilinear form w.r.t. $\mathcal{B}$, X and Y are the columns of coordinates of x, y w.r.t. $\mathcal{B}$. The term *sesqui* comes from the Latin and it means one and a half. For every subset S of V define its *left* and *right orthogonal* subspace, w.r.t. $\langle\ ,\ \rangle$ to be:

$$S^\perp := \{x \in V : \langle x, y\rangle = 0\ \ \forall y \in S\},$$
$$S^\top := \{y \in V : \langle x, y\rangle = 0\ \ \forall x \in S\}.$$

Both $S^\perp$ and $S^\top$ are subspaces of V.

Definition 1.6.2. The subspaces $V^{\perp}$ and $V^{\top}$ are called the *left* and the *right radical* of $\langle\ ,\ \rangle$, respectively.

Proposition 1.6.3. *For any pair of subspaces S and S' of a $(d+1)$-dimensional $\mathbb{F}$-vector space V it is:*

- $\dim S^{\perp} = \dim S^{\top}$,
- $\dim S + \dim S^{\perp} = d+1 = \dim S + \dim S^{\top}$,
- $S^{\perp} \cap S'^{\perp} = (S+S')^{\perp}, \quad S^{\top} \cap S'^{\top} = (S+S')^{\top}$.

Definition 1.6.4. A sesquilinear form is either *degenerate* or *non-degenerate* according to either $V^{\perp} = \{0\}$ or $V^{\perp} \neq \{0\}$.

Let $\langle\ ,\ \rangle$ be a sesquilinear form on V. A vector u is *isotropic* if $\langle u,u\rangle = 0$. A *totally isotropic subspace* S of V satisfies $\langle u,v\rangle = 0,\ \forall\, u,v \in S$. A *maximum totally isotropic subspace* is a totally isotropic subspace that is not contained in a larger totally isotropic subspace.

Theorem 1.6.5. *Let V be a $(d+1)$-dimensional $\mathbb{F}$-vector space. A totally isotropic subspace, w.r.t. a non-degenerate sesquilinear form has dimension at most $\lfloor \frac{d+1}{2} \rfloor$.*

Definition 1.6.6. A (*degenerate*) *duality* or (*degenerate*) *correlation* of $\mathrm{PG}(d,\mathbb{F})$ is a (degenerate) collineation between $\mathrm{PG}(d,\mathbb{F})$ and its dual space $\mathrm{PG}(d,\mathbb{F})^*$.

Remark 1.6.7. A duality of $\mathrm{PG}(d,\mathbb{F})$ can be seen as a bijective map of $\mathrm{PG}(d,\mathbb{F})$ reversing inclusion.

Theorem 1.6.8. *Any (possibly degenerate) duality of* $\mathrm{PG}(d,\mathbb{F})$*, $d>1$, is induced by a σ-sesquilinear form of the underlying vector space $\mathbb{F}^{d+1}$ and conversely.*

Proof. A (possibly degenerate) duality of $\mathrm{PG}(d,\mathbb{F})$, $d>1$, is induced by a σ-linear transformation f of $\mathbb{F}^{d+1}$ into its dual, since it is a (possibly degenerate) collineation. Define a map $\langle\ ,\ \rangle : \mathbb{F}^{d+1} \times \mathbb{F}^{d+1} \longrightarrow \mathbb{F}$ in the following way:

$$\langle u,v\rangle = f(v)(u),$$

that is the result of applying the element $f(v)$ of $(\mathbb{F}^{d+1})^*$ to u. It follows that $\langle\ ,\ \rangle$ is a σ-sesquilinear form. Indeed it is easy to see that $\langle\ ,\ \rangle$ is linear on the first argument and since

$$\langle u, v_1+v_1\rangle = f(v_1+v_2)(u) = f(v_1)(u) + f(v_2)(u) = \langle u,v_1\rangle + \langle u,v_2\rangle,$$

and

$$\langle u, av\rangle = f(av)(u) = a^{\sigma} f(v)(u) = a^{\sigma}\langle u,v\rangle,$$

it is semilinear on the second argument. Moreover $\langle\ ,\ \rangle$ is non-degenerate if and only if f is a bijection.
Conversely, any σ-sesquilinear form on $V = \mathbb{F}^{d+1}$ induces a (possibly degenerate) duality of $\mathrm{PG}(d, \mathbb{F})$ given by

$$\perp\colon P = \langle u \rangle \in \mathrm{PG}(d, \mathbb{F}) \setminus V^{\perp} \mapsto P^{\perp} = \{\langle v \rangle \mid \langle u, v \rangle = 0\} \in \mathrm{PG}(d, \mathbb{F})^{*}.$$

□

Remark 1.6.9. Every σ-sesquilinear form of $\mathbb{F}^{d+1}$ give rise to the following two (possibly degenerate) dualities of $\mathrm{PG}(d, \mathbb{F})$:

$$\perp\colon P = \langle u \rangle \in \mathrm{PG}(d, \mathbb{F}) \setminus V^{\perp} \mapsto P^{\perp} = \{\langle v \rangle \mid \langle u, v \rangle = 0\} \in \mathrm{PG}(d, \mathbb{F})^{*}.$$

and

$$\top : P = \langle v \rangle \in \mathrm{PG}(d, \mathbb{F}) \setminus V^{\top} \mapsto P^{\top} = \{\langle u \rangle \mid \langle u, v \rangle = 0\} \in \mathrm{PG}(d, \mathbb{F})^{*}.$$

Remark 1.6.10. Sometimes we will call *linear* a (degenerate) correlation whose associated form is a bilinear form ($\sigma = 1$).

Definition 1.6.11. Let $\langle\ ,\ \rangle$ be a sesquilinear form of $\mathbb{F}^{d+1}$. A point $P = \langle v \rangle$ of $\mathrm{PG}(d, \mathbb{F})$ is called either an *isotropic* point or an *absolute* point if $\langle v, v \rangle = 0$, i.e. v is an isotropic vector w.r.t. $\langle\ ,\ \rangle$.

Moreover, given a subspace U of $\mathrm{PG}(V)$, if $U \subseteq U^{\perp}$ or vice versa, then U is called *absolute*. If $U = U^{\perp}$, then U is called *totally isotropic.*

A duality of $\mathrm{PG}(d, \mathbb{F})$ applied twice gives a collineation of $\mathrm{PG}(d, \mathbb{F})$.

Definition 1.6.12. A *polarity* is a duality whose square is the identity.

Hence, if $\perp$ is a polarity, then for every pair of points P and R the following holds:

$$P \in R^{\perp} \iff R \in P^{\perp}.$$

Definition 1.6.13. A σ-sesquilinear form is *reflexive* if $\forall\ u, v \in V$ it is:

$$\langle u, v \rangle = 0 \iff \langle v, u \rangle = 0.$$

Proposition 1.6.14. *A duality is a polarity if and only if the induced non-degenerate sesquilinear form is reflexive.*

Proof. Let $\langle\ ,\ \rangle$ be a non-degenerate reflexive σ-sesquilinear form of $\mathbb{F}_q^{d+1}$. If $u \in \langle v \rangle^{\perp}$, then $v \in \langle u \rangle^{\perp}$. Hence the map $\langle u \rangle \mapsto \langle u \rangle^{\perp}$ defines a polarity. Conversely given a polarity $\perp$, if $v \in \langle u \rangle^{\perp}$, then $u \in \langle v \rangle^{\perp}$. So the induced sesquilinear form is reflexive. □

The non-degenerate, reflexive σ-sequilinear forms of a $(d+1)$-dimensional $\mathbb{F}$-vector space V have been classified (for a proof see e.g. Theorem 3.6 in [6] or Theorem 6.3 and Proposition 6.4 in [21]) in the following:

Theorem 1.6.15. *Let $\langle\ ,\ \rangle$ be a non-degenerate, reflexive σ-sesquilinear form of a $(d+1)$-dimensional $\mathbb{F}$-vector space. Then, up to a scalar factor, the form $\langle\ ,\ \rangle$ is one of the following:*

(i) a symmetric *form, i.e.*

$$\forall\ u, v \in V\ \ \langle u, v\rangle = \langle v, u\rangle\ \ (\mathit{char}(\mathbb{F}) = 2 \implies \exists\, v \in V : \langle v, v\rangle \neq 0),$$

(ii) an alternating *form, i.e.*

$$\forall\ v \in V\ \ \langle v, v\rangle = 0\quad (d \textit{ is necessarily odd}),$$

(iii) a hermitian *form, i.e.*

$$\forall\ u, v \in V\ \ \langle u, v\rangle = \langle v, u\rangle^{\sigma}\ \ (\sigma^2 = 1, \sigma \neq 1).$$

For the proofs of the results in this section see e.g. [6],[21].

1.7 Quadrics, Hermitian varieties, Symplectic geometries of $\mathrm{PG}(d, q)$

From the previous section, we have seen that polarities of $\mathrm{PG}(d, \mathbb{F})$ are in one to one correspondence with non-degenerate, reflexive σ-sesquilinear forms on $\mathbb{F}^{d+1}$. Hence, to every polarity of $\mathrm{PG}(d, \mathbb{F})$ there is an associated pair (A, σ), with A a non-singular matrix of order $d+1$ and σ an automorphism of $\mathbb{F}$. From the last theorem of the previous section, we have the following:

Corollary 1.7.1. *Let (A, σ) be a polarity of $\mathrm{PG}(d, q)$, one of the following holds:*

(i) $\sigma = 1$, A is a symmetric matrix. The polarity is called an orthogonal *polarity. If q is even, there is a non-absolute point.*

(ii) $\sigma = 1$, A is a skew-symmetric matrix, d is odd. Every point is an absolute point and the polarity is called a symplectic *polarity.*

(iii) *$\sigma^2 = 1$, so $\sigma : x \mapsto x^{\sqrt{q}}$, q is a square, A is a Hermitian matrix. The polarity is called a* Hermitian *or* unitary *polarity.*

Recall that a square matrix A is either *symmetric* if $A = A_t$, or *skew-symmetric* if $A = -A_t$ or *Hermitian* if $A = A_t^\sigma, \sigma^2 = 1, \sigma \neq 1$. Each of the above polarities of $\mathrm{PG}(d, q)$ determines a set $\Gamma : X_t A X^\sigma = 0$, as set of absolute points. The three type of polarities give rise to the following, well known, subsets of $\mathrm{PG}(d, q)$:

Definition 1.7.2. If (A, σ) is a polarity of $\mathrm{PG}(d, q)$, then one of the following holds:

(i) Γ is called a *quadric* of $\mathrm{PG}(d, q)$ (q odd, orthogonal polarity).
Γ is a hyperplane of $\mathrm{PG}(d, q)$ (q even, orthogonal polarity).

(ii) Γ is the full pointset of $\mathrm{PG}(d, q)$ (d odd, symplectic polarity) and the geometry determined is a *symplectic polar space*.

(iii) Γ is a *Hermitian* variety of $\mathrm{PG}(d, q)$ (q a square, $\sigma^2 = 1, \sigma \neq 1$, unitary polarity).

Remark 1.7.3. If q is even, $\sigma = 1$ and we have an orthogonal polarity, so A is a symmetrix matrix, then the set Γ of its absolute points is a hyperplane. Note that in many books (but not in the book of P. Dembowski [33]) this kind of polarity is called a *pseudo polarity*.

In all the cases of the previous definition, the set Γ is often called also *non-degenerate* since the associated σ-sesquilinear form is non-degenerate. All the above sets have been classified and for each of them it is possible to give a canonical equation.

Theorem 1.7.4. *If (A, σ) is a polarity of* $\mathrm{PG}(d, q)$*, then let $\Gamma : X_t A X^\sigma = 0$ be the set of its absolute points. The following holds:*

(i) If Γ is a quadric, so q is odd, then we have:

1) If d is even, then

$$\Gamma = \mathrm{Q}(d, q) : x_1 x_2 + \cdots + x_{d-1} x_d + x_{d+1}^2 = 0, \qquad (\textit{parabolic quadric}).$$

2) If d is odd, then either

$$\Gamma = \mathrm{Q}^-(d, q) : x_1 x_2 + \cdots + \alpha x_d^2 + \beta x_d x_{d+1} + \gamma x_{d+1}^2 = 0, with$$

$\alpha x_d^2 + \beta x_d x_{d+1} + \gamma x_{d+1}^2$ *irreducible polynomial over $\mathbb{F}_q$ (elliptic quadric) or*

$$\Gamma = \mathrm{Q}^+(d, q) : x_1 x_2 + \cdots + x_d x_{d+1} = 0 \qquad (\textit{hyperbolic quadric}).$$

If Γ is a hyperplane, so q is even, then $\Gamma : x_1 = 0$.

(ii) If Γ is a symplectic polar space, then Γ is the full pointset of $\mathrm{PG}(d, q)$, d odd. The geometry determined will be denoted by $W(d, q)$. A canonical form for the associated bilinear form is

$$\langle x, y\rangle = x_1y_2 - x_2y_1 + x_1y_3 - x_3y_1 + \cdots + x_dy_{d+1} - x_{d+1}y_d.$$

(iii) If Γ is a Hermitian variety, then

$$\Gamma = \mathrm{H}(d, q) : x_1^{\sqrt{q}+1} + x_2^{\sqrt{q}+1} + \cdots + x_{d+1}^{\sqrt{q}+1} = 0.$$

Remark 1.7.5. Regarding degenerate, reflexive σ-sesquilinear forms on $V = \mathbb{F}_q^{d+1}$, it is possible to prove that if dim $V^\perp = r + 1$, $r \geq 0$, then the set Γ of absolute points in $\mathrm{PG}(d, q)$ of the associated degenerate correlation is, in all the possible cases, a cone $\Gamma(\mathcal{V}_r, Q_{d-1-r})$ with vertex a subspace $\mathcal{V}_r$, of dimension r, projecting the set Q_{d-1-r} of absolute points of a polarity in a subspace S_{d-1-r}, of dimension $d-1-r$, skew with $\mathcal{V}_r$. The set Q_{d-1-r} can be either a quadric or the full pointset of $\mathrm{PG}(d-1-r, q)$ (a symplectic geometry) or a Hermitian variety (if q is a square). If Q_{d-1-r} is the full pointset of $\mathrm{PG}(d - 1 - r)$, then d and r must have the same parity and the cone $\Gamma(\mathcal{V}_r, \mathrm{PG}(d - 1 - r, q))$ is a quotient geometry $\mathrm{PG}(d, q)/\mathcal{V}_r$. In these cases we call the set of the absolute points a *degenerate quadric*, a *degenerate symplectic geometry* or a *degenerate Hermitian variety*, respectively. The knowledge of the set of the absolute points of a polarity of S_{d-1-r} determines also the knowledge of the set of the absolute points of a degenerate, reflexive correlation.

Sometimes we will call non-degenerate quadrics, non-degenerate symplectic geometries and non-degenerate Hermitian varieties the set of the absolute points associated to a non-degenerate reflexive σ-sesquilinear form. The following proposition characterizes these sets.

Proposition 1.7.6. *Let Γ be either a non-degenerate quadric or a non-degenerate symplectic polar space or a non-degenerate Hermitian variety of $\mathrm{PG}(d, q)$ and denote by $\perp$ the associated polarity. For any point Y of Γ, the set $Y^\perp$ is a hyperplane meeting Γ in a cone $\Gamma(Y, Q_{d-2})$, where Q_{d-2} is either a non-degenerate quadric or a non-degenerate symplectic polar space or a non-degenerate Hermitian variety, respectively and vice versa.*

We see, from the previous results, that we have missed quadrics in the q even case. In order to include quadrics for the q even case, another possible definition of quadric, independent of the characteristic of the field $\mathbb{F}$, is the following:

Definition 1.7.7. Let V be an $\mathbb{F}$-vector space. A *(degenerate) quadratic form* of V is a map $f : V \longrightarrow \mathbb{F}$ such that

$$f(av) = a^2 f(v) \ \ \forall a \in \mathbb{F}, v \in V,$$

$$\langle u, v\rangle = f(u+v) - f(u) - f(v) \ \forall u, v \in \mathrm{V}$$

is a (degenerate) symmetric bilinear form.

Definition 1.7.8. A *(degenerate) quadric* of $\mathrm{PG}(V)$ is any set $\mathrm{Q} = \{\langle v\rangle \in \mathrm{PG}(V) | f(v) = 0\}$, for some (degenerate) quadratic form f on V. A point $P = \langle v\rangle$ of Q is also called a *singular* point, w.r.t. the quadratic form f. A subspace U s.t. all its points are singular is a *totally singular* subspace. A *maximum totally singular* subspace is a totally singular subspace that is not contained in a larger totally singular subspace. The quadrics of a projective plane $\mathrm{PG}(2, \mathbb{F})$ are called *conics*.

Remarks 1.7.9.

1) If char $\mathbb{F} \neq 2$, then Q is a *non-degenerate* quadric if the associated form $\langle\ ,\ \rangle$ is a non-degenerate symmetric bilinear form. In this case, every (possibly degenerate) symmetric bilinear form gives a (possibly degenerate) quadratic form and vice versa, hence the two definitions of quadrics coincide.

2) If char $\mathbb{F} = 2$, then $\langle x, x\rangle = 0 \ \forall\ x \in V$ and the form $\langle\ ,\ \rangle$ cannot be non-degenerate, unless d is odd.

- If d is odd, then Q is a *non-degenerate* quadric if the associated form (a symplectic form) is a non-degenerate bilinear form.
- If d is even, then Q is a *non-degenerate* quadric if $f(x) \neq 0 \ \forall\ x \in V^{\perp}$, where $\perp$ denotes the degenerate correlation associated to $\langle\ ,\ \rangle$, that is a degenerate symplectic form with dim $V^{\perp} = 1$.

In what follows we will often omit the term non-degenerate.

Remark 1.7.10. Another possible definition of quadric, equivalent to that in 1.7.8, is the following. A *(possibly degenerate) quadric* of $\mathrm{PG}(V)$ is any set of points whose projective coordinates, w.r.t. a fixed frame $\mathcal{R}$ of $\mathrm{PG}(V)$, satisfy a second degree homogeneous equation in the unknowns x_i, $i = 1, \ldots, d{+}1$. Such an equation can always be written in the form $\mathcal{Q} : X_t A X = 0$, for some (non-skew-symmetric) matrix A. The bilinear form associated to $\mathcal{Q}$ being defined by $\langle u, v\rangle = X_t(A + A_t)Y$, where X and Y denotes the columns of coordinates of the points $\langle u\rangle$ and $\langle v\rangle$, rispectively, w.r.t. $\mathcal{R}$.

If char$(\mathbb{F}) \neq 2$, then $\mathcal{Q}$ is non-degenerate if and only if $|A + A_t| \neq 0$.

If char$(\mathbb{F}) = 2$, then we distinguish two cases:

- if d is odd, then $\mathcal{Q}$ is non-degenerate if and only if $|A + A_t| \neq 0$,

- if d is even, then $\mathcal{Q}$ is non-degenerate if and only if $\mathrm{rank}(A + A_t) = d$ and $N = V^{\perp} \notin \mathcal{Q}$.

The point N appearing in the case char$(\mathbb{F}) = 2$, d even, is called the *nucleus* of the quadric $\mathcal{Q}$.

Remark 1.7.11. It is possible to prove that the non-degenerate quadrics of $\mathrm{PG}(d, q)$, q even, can be divided into the same three families as for the q odd case, with the same canonical equations.

For the proofs of the results in this section see e.g. [49].

1.8 Classical polar spaces

Definition 1.8.1. A *partial linear space* $(\mathcal{P}, \mathcal{L})$ is an incidence structure of points and lines s.t.:

- any two distinct points are contained in at most one line,
- any line contains at least two points,
- there are at least two distinct lines.

Two points P, P' of a partial linear space are *collinear* points if there is a line containing them, denoted by PP', otherwise they are *non-collinear* points.

Definition 1.8.2. A *Polar space* is a partial linear space $\mathbb{P} = (\mathcal{P}, \mathcal{L})$ s.t.:

- for every point P and for every line ℓ with $P \notin \ell$, the set of points of ℓ collinear with P is either a singleton or the whole line ℓ,
- lines have at least three distinct points,
- through every point there are at least three distinct lines.

A *singular subspace* of a polar space $\mathbb{P}$ is any subset of pairwise collinear points of $\mathbb{P}$ (so a point, a line, etc.). A *degenerate* polar space has some points that are collinear with all the points. A polar space $\mathbb{P}$ is *finite* if it has a finite number of points.

Definition 1.8.3. A *generalized quadrangle* is a partial linear space $\mathbb{P} = (\mathcal{P}, \mathcal{L})$ s.t.:

- for every point P and for every line ℓ, with $P \notin \ell$, the set of points of ℓ collinear with P is a singleton,
- lines have at least three distinct points,
- through every point there are at least three distinct lines.

Hence a generalized quadrangle is a polar space with lines as maximal subspaces.

Let $\mathrm{PG}(d, q)$ be the projective space of dimension d over $\mathbb{F}_q$ and let f be either a reflexive, sesquilinear form or a quadratic form on the underlying vector space $\mathbb{F}_q^{d+1}$. The points, the lines and the subspaces of the finite classical polar space associated with this form consist either of the totally isotropic points, lines and subspaces (when f is a sesquilinear form) or the totally singular points, lines and subspaces (when f is a quadratic form) with respect to f.

The *Witt index* of the form f is the largest vector space dimension of the subspaces contained in the polar space, and it is called the *rank* of the polar space. A subspace of a polar space of maximum dimension is called a *generator* of the polar space. Finite classical polar spaces are those summarized in Theorem 1.7.4 plus the non-degenerate quadrics, q even. They are listed in the table below, where r is the rank of the polar space and $\theta_k(q)$ denotes the number of points of a $\mathrm{PG}(k, q)$, so it is equal to $q^k + q^{k-1} + \cdots + q + 1$.

Name	Notation	Number of points	Collineation Group
Symplectic	$\mathrm{W}(2r-1, q)$	$(q^r + 1)\theta_{r-1}(q)$	$\mathrm{P\Gamma Sp}(2r, q)$
Hermitian	$\mathrm{H}(2r-1, q)$	$(q^{r-1/2} + 1)\theta_{r-1}(q)$	$\mathrm{P\Gamma U(2r, q)}$
Hermitian	$\mathrm{H}(2r, q)$	$(q^{r+1/2} + 1)\theta_{r-1}(q)$	$\mathrm{P\Gamma U(2r+1, q)}$
Hyperbolic	$\mathrm{Q}^+(2r-1, q)$	$(q^{r-1} + 1)\theta_{r-1}(q)$	$\mathrm{P\Gamma O}^+(2r, q)$
Parabolic	$\mathrm{Q}(2r, q)$	$(q^r + 1)\theta_{r-1}(q)$	$\mathrm{P\Gamma O}(2r+1, q)$
Elliptic	$\mathrm{Q}^-(2r+1, q)$	$(q^{r+1} + 1)\theta_{r-1}(q)$	$\mathrm{P\Gamma O}^-(2r+2, q)$

Table 1.1: Finite classical polar spaces

Remark 1.8.4. There are no other finite polar spaces of rank at least three than those in the previous table. So every finite polar space of rank at least three is classical.

Remark 1.8.5. There are examples of non-classical finite generalised quadrangles. (See e.g. [17],[21],[82]).

For the proof of the results in this section see e.g. [6],[18],[19],[20],[21],[47],[101],[103].

1.9 Hyperovals of $\mathrm{PG}(2, 2^n)$

Definition 1.9.1. In $\mathrm{PG}(2,q)$ any set $\mathcal{K}$, of size k, with no three collinear points is a *k-arc* of $\mathrm{PG}(2,q)$.

It is easy to see that for any k-arc of $\mathrm{PG}(2,q)$, if q is odd, then $k \leq q+1$ and if q is even, then $k \leq q+2$.

Definition 1.9.2. If $\mathcal{K}$ is a $(q+1)$-arc of $\mathrm{PG}(2,q)$, then it is called an *oval*. If q is even and $\mathcal{K}$ is a $(q+2)$-arc of $\mathrm{PG}(2,q)$, then it is called a *hyperoval*.

Every non-degenerate conic of $\mathrm{PG}(2,q)$ is an oval and the property of being an oval characterises non-degenerate conics, for q odd, with the following remarkable result:

Theorem 1.9.3 (B. Segre [88]). *If q is odd, then every oval of $\mathrm{PG}(2,q)$ is a non-degenerate conic.*

The situation is different for q even. Indeed, if q is even, then for every non-degenerate conic Γ, the tangent lines to Γ meet at a common point N, the nucleus of Γ, with $N \notin \Gamma$. The set $\Gamma \cup \{N\}$ is a hyperoval. By removing a point M of Γ we have, for $q > 4$, an oval $\Gamma \cup \{N\} \setminus \{M\}$ that cannot be a conic since it has q points in common with Γ, while two distinct non-degenerate conics can have at most 4 points in common.

Definition 1.9.4. A hyperoval obtained by the union of a non-degenerate conic Γ with its nucleus N is called either a *regular* hyperoval or a *hyperconic*.

The following theorem, again due to B. Segre, characterizes hyperovals of $\mathrm{PG}(2,q)$ in terms of a class of permutation polynomials of $\mathbb{F}_q[x]$.

Theorem 1.9.5 (B. Segre [89]). *Let $q = 2^n$, $n > 1$ and let $f \in \mathbb{F}_q[x]$ satisfying the following properties:*

(i) *f is a permutation, reduced polynomial, $f(0) = 0, f(1) = 1$.*

(ii) $\forall\, \alpha \in \mathbb{F}_q\ g_\alpha(x) = \frac{f(x+\alpha)+f(\alpha)}{x}$ *is a permutation polynomial with $g_\alpha(0) = 0$.*

The set $\Omega(f) = \{(f(t), t, 1)\}_{t \in \mathbb{F}_q} \cup \{(1,0,0), (0,1,0)\}$ is a hyperoval of $\mathrm{PG}(2,q)$. Vice versa if Ω is a hyperoval of $\mathrm{PG}(2,q)$, there are a frame of $\mathrm{PG}(2,q)$ and a polynomial $f \in \mathbb{F}_q[x]$ with properties $(i), (ii)$ s.t. $\Omega = \Omega(f)$.

Definition 1.9.6. Polynomials satisfying (i), (ii) of the previous theorem are called *o-polynomials.*

The following table summarizes all but two infinite classes of o-polynomials of $\mathbb{F}_q$, $q = 2^n$, known and the names of the associated hyperovals:

Name	o-polynomial	Restrictions
regular	x^2	none
translation	x^{2^m}	$m > 1$, $(m, n) = 1$
Segre	x^6	n odd
Glynn I	$x^{3\sigma+4}$	$\sigma = 2^{\frac{n+1}{2}}$, n odd
Glynn II	$x^{\sigma+\lambda}$	$\sigma = 2^{\frac{n+1}{2}}, \lambda = 2^r$ if $n = 4r - 1$ $\sigma = 2^{\frac{n+1}{2}}, \lambda = 2^{3r+1}$ if $n = 4r + 1$
Payne	$x^{1/6} + x^{3/6} + x^{5/6}$	n odd
Cherowitzo	$x^\sigma + x^{\sigma+2} + x^{3\sigma+4}$	n odd

Table 1.2: Infinite classes of hyperovals

There are other two infinite classes of hyperovals:

- *Subiaco*:

$$f(x) = \frac{d^2(x^4 + x) + d^2(1 + d + d^2)(x^3 + x^2)}{(x^2 + dx + 1)^2} + x^{1/2},$$

  $Tr(1/d) = 1, d^2 + d + 1 \neq 0$ (or equivalently $d \notin \mathbb{F}_4$ if $n \equiv 2(\text{mod}4)$). It is a unique class of hyperovals if $n \not\equiv 2(\text{mod}4)$, two classes of inequivalent hyperovals if $n \equiv 2(\text{mod}4), n > 2$.

- *Adelaide*: Let $b \in \mathbb{F}_q$ such that $N(b) = 1, b \neq 1$,

  $$f(x) = tr(b)^{-1}tr(b^m)(x+1)+(tr(b)^{-1}tr((bx+b^{\sqrt{q}})^m)(x+tr(b)\sqrt{x}+1)^{1-m}+\sqrt{x},$$

  where $tr = tr_{\mathbb{F}_q/\mathbb{F}_{\sqrt{q}}}$ and n is even.

For more on hyperovals see e.g. [22],[23],[24],[25],[26],[45],[80],[81],[87],[88],[89],[91].

1.10 Blocking sets of $\mathrm{PG}(2, q^n)$

Let π_n be a finite projective plane of order n.

Definition 1.10.1. Let B be a set of points of π_n. The set B is a *blocking set* if it does not contain lines and for every line ℓ of π_n it is $\ell \cap B \neq \emptyset$. The blocking set B is *minimal* if there is no proper subset of B that is again a blocking set.

Proposition 1.10.2. *Let B be a blocking set of π_n and let ℓ be a line. Then*

$$|B \cap \ell| \leq |B| - n.$$

If $|B| = n + k$, then every line meets B in at most k points.

Definition 1.10.3. Let B be a blocking set of π_n with $|B| = n + k$. A line ℓ meeting B in exactly k points is a *Rédei* line. If for a blocking set B there exists a Rédei line, then B is a *Rédei* blocking set.

Examples 1.10.4. Let π_n be a projective plane of square order n.

- *Baer subplanes*. A subplane of order $\sqrt{n}$ of π_n is a minimal Rédei blocking set of size $n + \sqrt{n} + 1$. In the Desarguesian projective plane $\mathrm{PG}(2, q^2)$ a Baer subplane is isomorphic to $\mathrm{PG}(2, q)$.

- *Unitals*. A unital of order n of π_n is a set of $n\sqrt{n} + 1$ points meeting every line either in 1 or $\sqrt{n} + 1$ points. It is a minimal blocking set of π_n. In the Desarguesian projective plane $\mathrm{PG}(2, q^2)$ an important example of unital is given by the Hermitian curve or *classical unital* $H(2, q^2) : x_1^{q+1} + x_2^{q+1} + x_3^{q+1} = 0$.

In [14] A.A. Bruen characterizes Baer subplanes as blocking sets of minimum size.

Proposition 1.10.5 (A. A. Bruen [14]). *If B is a blocking set of π_n, then $|B| \geq n + \sqrt{n} + 1$. Equality holds if and only if n is a square and B is a Baer subplane of π_n.*

A blocking set is *small* if it has size at most $\frac{3(n+1)}{2}$. Therefore the Baer subplanes are examples of small blocking sets. In [15] A.A. Bruen and J.A. Thas characterize unitals as minimal blocking sets of maximum size.

Proposition 1.10.6 (A.A. Bruen - J.A. Thas [15]). *If B is a minimal blocking set of π_n, then $|B| \leq n\sqrt{n} + 1$. Equality holds if and only if n is a square and B is an unital of π_n.*

For more details on unital see e.g. [7].

1.11 Spreads of $\mathrm{PG}(d, q)$ and field reduction

Definition 1.11.1. Let r be a positive integer. An *r-spread* of $\mathrm{PG}(d, q)$ (resp. of $\mathbb{F}_q^n$) is a partition of $\mathrm{PG}(d, q)$ (resp. of $\mathbb{F}_q^n \setminus \{0\}$) in r-dimensional projective subspaces (resp. vector subspaces minus $\{0\}$). Instead of r–spread we can also say *spread* in *r-dimensional subspaces.*

Proposition 1.11.2. *An r-spread of* $\mathrm{PG}(d, q)$ *contains exactly*

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

elements. Hence if such a spread exists, then $q^{r+1}-1$ divides $q^{d+1}-1$ i.e. $r+1$ divides $d+1$.

Example 1.11.3 (*Linear spreads).* Let $d + 1 = (r + 1)(s + 1)$. Let α be a root of an irreducible polynomial of degree $r + 1$ over $\mathbb{F}_q$. Every element $x \in \mathbb{F}_{q^{r+1}}$ can be written as

$$x = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_r\alpha^r.$$

Let $(x_0, x_1, \ldots, x_s) \in \mathbb{F}_{q^{r+1}}^{s+1}$ and put

$$x_j = x_{j0} + x_{j1}\alpha + \cdots + x_{jr}\alpha^r, \ \forall \ j = 0, 1, \ldots, s.$$

Let $\phi : \mathbb{F}_{q^{r+1}}^{s+1} \longrightarrow \mathbb{F}_q^{d+1}$ be the $\mathbb{F}_q$-linear map defined by:

$$\phi(x_0, x_1, \ldots, x_s) = (x_{00}, x_{01}, \ldots, x_{0r}, x_{10}, \ldots, x_{1r}, \ldots, x_{s0}, \ldots, x_{sr}).$$

If S is an h-dimensional subspace of $\mathbb{F}_{q^{r+1}}^{s+1}$, then $\phi(S)$ is an $h(r + 1)$-dimensional subspace of $\mathbb{F}_q^{d+1}$. In particular if H is a 1-dimensional subspace, then $\phi(H)$ is an $(r + 1)$-dimensional subspace. The set of all 1-dimensional subspaces of $\mathbb{F}_{q^{r+1}}^{s+1}$, minus $\{0\}$, is a 1-spread of $\mathbb{F}_{q^{r+1}}^{s+1}$ to which there corresponds an $(r + 1)$-spread of $\mathbb{F}_q^{d+1}$. Such a spread is called a *linear* spread of $\mathbb{F}_q^{d+1}$.

It follows that:

Proposition 1.11.4. *Let r and d be two positive integers. If $r + 1$ divides $d + 1$, then there exists an r-spread $\mathcal{F}$ of* $\mathrm{PG}(d, q)$.

The map ϕ induces a map $\mathrm{PG}(s, q^{r+1}) \longrightarrow \mathrm{PG}(d, q)$ known as *field reduction*. Note that the points of $\mathrm{PG}(s, q^{r+1})$ are mapped into the *linear* r-spread of $\mathrm{PG}(d, q)$ and $(h - 1)$-dimensional projective subspaces of $\mathrm{PG}(s, q^{r+1})$ are mapped into $(h(r + 1) - 1)$-dimensional projective subspaces of $\mathrm{PG}(d, q)$.

Definition 1.11.5. A *regulus* in a projective space $\mathrm{PG}(rt-1,q)$, or $(t-1)$-*regulus*, is a set $\mathcal{R}$ of $(t-1)$-dimensional pairwise disjoint subspace, with $|\mathcal{R}| = q+1$, s.t. each line meeting three distinct elements of $\mathcal{R}$ meets all the elements of $\mathcal{R}$. If S_1, S_2, S_3 are three pairwise disjoint $(t-1)$-dimensional subspaces with $\dim\langle S_1, S_2, S_3\rangle = 2t-1$, then there is a unique regulus containing them, denoted by $\mathcal{R}(S_1, S_2, S_3)$. A *regular* spread $\mathcal{S}$ contains the regulus $\mathcal{R}(S_1, S_2, S_3)$ for any three different elements S_1, S_2, S_3 of $\mathcal{S}$.

For more on spreads and field reduction see e.g. [1],[6],[13],[67],[71],[79],[90].

1.12 $\mathbb{F}_q$-linear sets of $\mathrm{PG}(d, q^n)$

Definition 1.12.1. Let $\Omega = \mathrm{PG}(r-1, q^n), q = p^h$, p a prime. A set L is said an $\mathbb{F}_q$-*linear set* of Ω of rank t if it is defined by the non-zero vectors of an $\mathbb{F}_q$-vector subspace U of $V = \mathbb{F}_{q^n}^r$ of dimension t, that is

$$L = L_U = \{\langle u\rangle_{q^n} : u \in U \setminus \{0\}\}.$$

Let $\Lambda = \mathrm{PG}(W, \mathbb{F}_{q^n})$ be a subspace of Ω of dimension s, we say that Λ has *weight* i with respect to L_U if $\dim_{\mathbb{F}_q}(W \cap U) = i$. An $\mathbb{F}_q$-linear set L_U of Ω of rank t is said *scattered* if each point of L_U has weight 1, with respect to L_U.

In [10] it is proved that $t \leq rn/2$. In [86] it is proved that L_U is a scattered $\mathbb{F}_q$-linear set of rank t if and only if $|L_U| = q^{t-1} + q^{t-2} + \cdots + q + 1$. If L is a scattered linear set of $\mathrm{PG}(r-1, q^n)$ of rank $rn/2$ it is called a *maximum* scattered linear set.

If $\dim_{\mathbb{F}_q} U = \dim_{\mathbb{F}_{q^n}} V = r$ and $\langle U\rangle_{\mathbb{F}_{q^n}} = V$, then $L_U \cong \mathrm{PG}(U, \mathbb{F}_q)$ is a subgeometry of Ω. In such a case each point has weight 1, and hence $|L_U| = q^{r-1} + q^{r-2} + \cdots + q + 1$. Let $\Sigma = \mathrm{PG}(t, q)$ be a subgeometry of $\Sigma' = \mathrm{PG}(t, q^n)$ and suppose that there exists a $(t-r)$-dimensional subspace Ω' of Σ' disjoint from Σ. Let $\Omega = \mathrm{PG}(r-1, q^n)$ be an $(r-1)$-dimensional subspace of Σ' disjoint from Ω' and let Γ be the projection of Σ from Ω' to Ω i.e. $\Gamma = \{\langle \Omega', x\rangle \cap \Omega : x \in \Sigma\}$. Let $p_{\Omega',\Omega}$ be the map from $\Sigma \setminus \Omega'$ to Ω defined by $x \mapsto \langle \Omega', x\rangle \cap \Omega$. We call Ω' the *center* and Ω the *axis* of $p_{\Omega',\Omega}$. In [76] the following characterization of $\mathbb{F}_q$-linear sets is given:

Theorem 1.12.2. *If L is a projection of $\mathrm{PG}(t, q)$ into $\Omega = \mathrm{PG}(r-1, q^n)$, then L is an $\mathbb{F}_q$-linear set of Ω of rank $t+1$ and $\langle L\rangle = \Omega$. Conversely, if L is an $\mathbb{F}_q$-linear set of Ω of rank $t+1$ and $\langle L\rangle = \Omega$, then either L is a subgeometry of Ω or there are a $(t-r)$-dimensional subspace Ω' of $\Sigma' = \mathrm{PG}(t, q^n)$ disjoint from Ω and a subgeometry Σ of Σ' disjoint from Ω' such that $L = p_{\Omega',\Omega}(\Sigma)$.*

A family of maximum scattered linear sets to which a geometric structure, called pseudoregulus, can be associated has been defined in [74].

Definition 1.12.3. Let $L = L_U$ be a scattered $\mathbb{F}_q$-linear set of $\Gamma = \mathrm{PG}(2n-1, q^t)$ of rank $tn, t, n \geq 2$. We say that L is of *pseudoregulus type* if:

(i) there exist $m = \frac{q^{nt}-1}{q^t-1}$ pairwise disjoint lines of Γ, say $s_1, s_2, \ldots, s_m$, such that $w_L(s_i) = t, i.e. |L \cap s_i| = q^{t-1} + q^{t-2} + \cdots + q + 1 \;\; \forall\, i = 1, \ldots, m$,

(ii) there exist exactly two $(n-1)$-dimensional subspaces T_1 and T_2 of Γ disjoint from L such that $T_j \cap s_i \neq \emptyset \quad \forall\, i = 1, \ldots, m$ and $j = 1, 2$.

We call the set of lines $\mathcal{P}_L = \{s_i : i = 1, \ldots, m\}$ the $\mathbb{F}_q$*-pseudoregulus* (or simply the *pseudoregulus*) of Γ associated with L and we refer to T_1 and T_2 as *transversal spaces* of $\mathcal{P}_L$ (or transversal spaces of L). When $t = n = 2$, these objects already appeared first in [42], where the term pseudoregulus was introduced for the first time. See also [36].

In [38] and in [74] the following class of maximum scattered $\mathbb{F}_q$-linear sets of the projective line $\Gamma = \mathrm{PG}(1, q^t)$ with a structure resembling that of an $\mathbb{F}_q$-linear set of $\mathrm{PG}(2n-1, q^t), n, t \geq 2$, of pseudoregulus type has been studied. Let $P_1 = \langle w \rangle_{q^t}$ and $P_2 = \langle v \rangle_{q^t}$ be two distinct points of Γ and let τ be an automorphism of $\mathbb{F}_{q^t}$ such that $Fix(\tau) = \mathbb{F}_q$. For each $\rho \in \mathbb{F}_{q^t}^*$ the set $W_{\rho,\tau} = \{\lambda w + \rho \lambda^\tau v : \lambda \in \mathbb{F}_{q^t}\}$, is an $\mathbb{F}_q$-vector subspace of $V = \mathbb{F}_{q^t}^2$ of dimension t and $L_{\rho,\tau} = L_{W_{\rho,\tau}}$ is a scattered $\mathbb{F}_q$-linear set of Γ.

Definition 1.12.4. In [74] the linear sets $L_{\rho,\tau}$ have been called of *pseudoregulus type* and the points P_1 and P_2 the *transversal points* of $L_{\rho,\tau}$. If $L_{\rho,\tau} \cap L_{\rho',\tau} \neq \emptyset$, then $L_{\rho,\tau} = L_{\rho',\tau}$. Note that $L_{\rho,\tau} = L_{\rho',\tau}$ if and only if $N(\rho) = N(\rho')$ (where N denotes the Norm of $\mathbb{F}_{q^t}$ over $\mathbb{F}_q$); so P_1, P_2 and the automorphism τ define a set of $q-1$ mutually disjoint maximum scattered linear sets of pseudoregulus type admitting the same transversal points. Such maximal scattered linear sets, together with P_1 and P_2, cover the pointset of $\mathrm{PG}(1, q^t)$. All the $\mathbb{F}_q$-linear sets of pseudoregulus type in $\Gamma = \mathrm{PG}(1, q^t), t \geq 2$, are equivalent to the linear set L_{1,σ_1} under the action of the collineation group $\mathrm{P\Gamma L}(2, q^t)$.

Remark 1.12.5. We observe that the pseudoregulus is the same as the Norm surface (or sphere) of R.H. Bruck, introduced and studied, in the seventies, by R.H. Bruck (see [11],[12]) in the setting of circle geometries.

For more on $\mathbb{F}_q$-linear sets in finite projective spaces see e.g. [86].

1.13 Semifield flocks of a quadratic cone of $\mathrm{PG}(3, q^n)$

In this section q will be odd.

Definition 1.13.1. Let $\mathcal{K}$ be a quadratic cone of $\mathrm{PG}(3, q^n)$ with vertex the point $V = (0, 0, 0, 1)$ and base the conic with equations $x_1x_2 = x_3^2, x_4 = 0$. A *flock* $\mathcal{F}$ of $\mathcal{K}$ is a partition of the points of the cone, different from the vertex, into q^n conics. The planes containing the conics of the flock $\mathcal{F}$ are called the *planes of the flock* $\mathcal{F}$.

Example 1.13.2. The classical example of a flock is constructed by taking the set of planes, not through the vertex V, on a fixed line disjoint from the cone.

Definition 1.13.3. Given a flock $\mathcal{F}$ of $\mathcal{K}$, the planes of the flock are given by π_t : $tx_1 - f(t)x_2 + g(t)x_3 + x_4 = 0$, for some functions f, $g : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}$. We denote this flock by $\mathcal{F}(f, g)$. If f and g are $\mathbb{F}_q$-linear maps, then the flock is a *semifield* flock. We assume that $\mathbb{F}_q$ is the maximum subfield of $\mathbb{F}_{q^n}$ on which f and g are linear. In this case $\mathbb{F}_q$ is called the *kernel* of the flock.

Consider the dual space of $\mathrm{PG}(3, q^n)$. The lines of the cone $\mathcal{K}$ become lines of $\mathrm{PG}(3, q^n)$ all contained in the plane $\pi : x_4 = 0$ corresponding with the vertex of $\mathcal{K}$. They had the property that no three of them were contained in a plane, so now they form a dual oval of π. Since q is odd, this dual oval is a dual conic, i.e., the set of the tangent lines to the a conic $\mathcal{C}' : 4x_1x_2 - x_3^2 = 0, x_4 = 0$. Two planes π_t and π_s of the flock $\mathcal{F}$ correspond to the points $P_t = (t, f(t), g(t), 1)$ and $P_s = (s, f(s), g(s), 1)$. Since π_t and π_s do not intersect on the cone $\mathcal{K}$, the line P_sP_t intersects π in an internal point of $\mathcal{C}'$. If $\mathcal{F}(f, g)$ is a semifield flock, then f and g are $\mathbb{F}_q$-linear maps, so we obtain a set $\{(t, f(t), g(t), 0)\}_{t \in \mathbb{F}_{q^n}^*}$ of internal points to $\mathcal{C}'$, that is an $\mathbb{F}_q$-linear set of rank n of internal points to the conic $\mathcal{C}'$. We recall the known examples of semifield flocks of a quadratic cone of $\mathrm{PG}(3, q^n)$, q odd.

- *Linear*. All the planes of the flock share a common line. In this case we can take the linear functions $f(t) = t$ and $g(t) = 0$. The set of internal points to the conic $\mathcal{C}'$ is a single point.

- *Kantor-Knuth semifield*. Let m be a non-square of $\mathbb{F}_{q^n}$ and let $\sigma \neq 1$ be an automorphism of $\mathbb{F}_{q^n}$. The functions $f(t) = mt^\sigma, g(t) = 0$ define a semifield flock called the *Kantor-Knuth* semifield flock (see e.g. [44],[97]). The planes of the flock $\pi_t : tx_1 - mt^\sigma x_2 + x_4 = 0$, $t \in \mathbb{F}_{q^n}$ share a common point $(0, 0, 1, 0)$ but not a common line. The set of internal points to the conic $\mathcal{C}'$ is contained on a secant line ℓ to $\mathcal{C}'$.

- *Cohen-Ganley* ($q = 3$). If m is a non-square in $\mathbb{F}_{3^n}$, then the functions $f(t) = m^{-1}t + mt^9$ and $g(t) = t^3$ give a semifield flock. The planes of the flock are

$\pi_t : tx_1 - (m^{-1}t + mt^9)x_2 + t^3x_3 + x_4 = 0, t \in \mathbb{F}_{3^n}$. The corresponding set of internal points to $\mathcal{C}'$ is $\{(t, m^{-1}t + mt^9, t^3, 0)\}_{t\in\mathbb{F}^*_{q^n}}$. See [83].

- *Sporadic semifield flock.* T. Penttila and B. Williams in [84] proved, with a mix of theory and computer assistance, that the functions $f(t) = t^9$ $g(t) = t^{27}$ yield a translation ovoid of $Q(4, 3^5)$ (see Section 1.15 for the definition). By using the connection given by J.A. Thas in [98], L. Bader, G. Lunardon and I. Pinneri in [2] calculated the corresponding semifield flock, sometimes called a *sporadic* semifield flock. The planes of the flock are $\pi_t : tx_1 - t^9x_2 + t^{27}x_3 + x_4 = 0, t \in \mathbb{F}_{3^5}$. The corresponding set of internal points to the conic $\mathcal{C}'$ is given by $\{(t, t^9, t^{27}, 0)\}_{t\in\mathbb{F}^*_{3^5}}$.

1.14 Plücker coordinates

Let $\mathbb{F}$ be a field and let $u = (u_1, u_2, u_3, u_4), v = (v_1, v_2, v_3, v_4)$ be two independent vectors of $V = \mathbb{F}^4$. The *Plücker* coordinates of (u, v) are $p_{ij} = u_iv_j - u_jv_i$ for every $i \neq j$. Let τ be the map from pairs of linearly independent vectors of V to points of $\mathrm{PG}(5, \mathbb{F})$ defined by

$$\tau(u, v) = \langle(p_{12}, p_{13}, p_{14}, p_{23}, p_{24}, p_{34})\rangle.$$

Proposition 1.14.1. *The map τ is a well defined map from the lines of* $\mathrm{PG}(3, \mathbb{F})$ *into the points of* $\mathrm{Q}^+(5, \mathbb{F})$.

Remark 1.14.2. The map τ is also called the *Klein correspondence* and therefore the quadric $\mathrm{Q}^+(5, \mathbb{F})$ is also called the *Klein* quadric of $\mathrm{PG}(5, \mathbb{F})$. It gives the following correspondence between objects of $\mathrm{PG}(3, q)$ and $\mathrm{Q}^+(5, q)$.

$\mathrm{PG}(3, q)$	$\mathrm{Q}^+(5, q)$
intersecting lines	collinear points
skew lines	non-collinear points
lines of $\mathrm{W}(3, q)$	points of $\mathrm{Q}(4, q)$
star of lines	a plane
lines of a plane	a plane
pencil of lines in a plane	a line
a regulus	a non-degenerate conic
a spread	an ovoid
a regular spread	$\mathrm{Q}^-(3, q)$
a symplectic spread	an ovoid of $\mathrm{Q}(4, q)$

Table 1.3: Klein correspondence

For the proofs of the results in this section see e.g. [6],[8].

1.15 Translation ovoids of orthogonal polar spaces

Denote by $\mathbb{P}$ either the polar space associated with a non-degenerate quadric of $\mathrm{PG}(2n, q^t), n \geq 2,\ t \geq 1$ or the polar space associated with a non-degenerate quadric of $\mathrm{PG}(2n+1, q^t), n \geq 1, t \geq 1$.

Definition 1.15.1. An *ovoid* of $\mathbb{P}$ is a set of $q^{tn}+1$ points, no two collinear in $\mathbb{P}$. An ovoid $\mathcal{O}$ of $\mathbb{P}$ is a *translation* ovoid with respect to a point P of $\mathcal{O}$ if there is a collineation group of $\mathbb{P}$ fixing P linewise (i.e. stabilizing all lines through P) and acting sharply transitively on the points of $\mathcal{O} \setminus \{P\}$.

Examples of translation ovoids of $\mathrm{Q}^+(3, q^t)$ are the conics contained in it or also the image of a pseudoregulus of $\mathrm{PG}(3, q^t)$ under the Klein correspondence. (See Section 3.4). The ovoids of the Klein quadric $\mathrm{Q}^+(5, q^t)$ correspond to line spreads of $\mathrm{PG}(3, q^t)$ and translation ovoids are equivalent to semifield spreads. Hence, $\mathrm{Q}^+(5, q^t)$ has ovoids and translation ovoids for all values of q. If $\mathrm{Q}(4, q^t) = H \cap \mathrm{Q}^+(5, q^t)$ is a non-degenerate quadric, where H is a hyperplane of $\mathrm{PG}(5, q^t)$, then ovoids of $\mathrm{Q}(4, q^t)$ are equivalent to symplectic spreads of $\mathrm{PG}(3, q^t)$ and translation ovoids are equivalent to symplectic semifield spreads of $\mathrm{PG}(3, q^t)$. In [75] the following result, regarding translation ovoids of $\mathbb{P}$, has been achieved, by using a connection between translation ovoids of $\mathbb{P}$ and $\mathbb{F}_q$-linear sets.

Theorem 1.15.2. *Translation ovoids of $\mathbb{P}$ exist if and only if $\mathbb{P}$ is one of the following: $\mathrm{Q}^+(3, q^t), \mathrm{Q}(4, q^t), \mathrm{Q}^+(5, q^t)$.*

Consequently, the most important open problems are related to the existence and to the classification of translation ovoids of $Q(4, q^t)$ and $Q^+(5, q^t)$. For more results on (not necessarily translation) ovoids of finite (not necessarily orthogonal) polar spaces see e.g. [31].

We now recall the known ovoids of $\mathrm{Q}(4, q)$. Let $\mathrm{Q}(4, q) : x_1x_5 + x_2x_4 + x_3^2 = 0$ and note that an ovoid containing the point $(0, 0, 0, 0, 1)$ may be written in the form

$$\mathcal{O}(f) = \{(0, 0, 0, 0, 1)\} \cup \{(1, x, y, f(x, y), -y^2 - xf(x, y)) : x, y \in \mathbb{F}_q\}.$$

The only known ovoids in $\mathrm{Q}(4, q)$ are listed in Table 1.4. In the table n is a non-square of $\mathbb{F}_q$, $q = p^h$, and $\sigma \neq 1$ is an automorphism of $\mathbb{F}_q$.

All, but last two examples of ovoids in this table, are translation ovoids of $\mathrm{Q}(4, q)$. Let $\mathrm{Q}(4, q^n) : x_1x_2 - x_3^2 + x_4x_5 = 0$ in $\mathrm{PG}(4, q^n)$. The correspondence between semifield flocks and translation ovoids of $\mathrm{Q}(4, q^n)$ was first explained by J.A. Thas

Name	$f(x,y)$	Restrictions
Elliptic quadric	$-nx$	none
Kantor	$-nx^{\sigma}$	q odd, $h > 1$
Penttila-Williams	$-x^9 - y^{81}$	$p = 3$, $h = 5$
Thas-Payne	$-nx - (n^{-1}x)^{1/9} - y^{1/3}$	$p = 3, h > 2$
Ree-Tits slice	$-x^{2\sigma+3} - y^{\sigma}$	$p = 3, h > 1$, h odd, $\sigma = \sqrt{3q}$
Tits	$x^{\sigma+1} + y^{\sigma}$	$p = 2, h > 1$, h odd, $\sigma = \sqrt{2q}$

Table 1.4: Known ovoids of $\mathrm{Q}(4,q)$

in [97], and later by G. Lunardon [71] with more details. Let f and g be two $\mathbb{F}_q$-linear maps such that

$$\mathcal{F}(f,g) = \{\pi_t : tx_1 - f(t)x_2 + g(t)x_3 + x_4 = 0, t \in \mathbb{F}_{q^n}\}$$

is a semifield flock of $\mathcal{K}$ with $g(t) = \sum_i b_i t^{q^i}$ and $f(t) = \sum_i c_i t^{q^i}$. The corresponding translation ovoid $\mathcal{O}(f,g)$ of $\mathrm{Q}(4,q^n)$ is given by the set of points

$$\{(u, F(u,v), v, 1, v^2 - uF(u,v)) : (u,v) \in \mathbb{F}_{q^n}^2\} \cup \{(0,0,0,0,1)\},$$

with $F(u,v) = \sum_i (c_i u + b_i v)^{1/q^i}$.

For the proofs of the results in this section see e.g. [4],[6],[51],[65],[72],[84],[99],[100].

1.16 Spreads of $\mathrm{PG}(3,q^n)$ and affine set of a spread

In 1965, H. Lüneburg proved that if $q^n = 2^{2h+1}$, $h \geq 1$, then the set of absolute lines of a polarity of $\mathrm{W}(3,q^n)$ is a symplectic spread, now called the *Lüneburg spread* of $\mathrm{PG}(3,q^n)$ (see [78]).
Let Σ_∞ be a hyperplane of $\mathrm{PG}(4,q^n)$ and let $\mathrm{Q}^+(3,q^n)$ be a hyperbolic quadric of Σ_∞. A set $\mathcal{A}$ of q^{2n} points of $\mathrm{PG}(4,q^n) \setminus \Sigma_\infty$ s.t. the line joining any two of them is disjoint from $\mathrm{Q}^+(3,q^n)$ is called an *affine set* of $\mathrm{PG}(4,q^n) \setminus \Sigma_\infty$. In what follows we will denote by $\perp$ the polarity of $\mathrm{Q}^+(5,q^n)$. In [68] and also in [75] the following result has been proved.

Theorem 1.16.1. *Let $\mathcal{O}$ be an ovoid of $\mathrm{Q}^+(5,q^n)$, let P be a point of $\mathcal{O}$ and let Ω be a hyperplane of $\mathrm{PG}(5,q^n)$ not containing P. The set $\mathcal{A}_P(\mathcal{O})$ obtained by projecting $\mathcal{O}$ from the point P into Ω is an affine set of $\Omega \setminus P^\perp$. Conversely, if $\mathcal{A}$ is an affine set of $\Omega \setminus P^\perp$, then the set $\mathcal{O} = \{PR \cap \mathrm{Q}^+(5,q^n) : R \in \mathcal{A}\}$ is an ovoid of $\mathrm{Q}^+(5,q^n)$.*

If $\mathcal{S}$ is a spread of $\mathrm{PG}(3,q^n)$ and ℓ is a line of $\mathcal{S}$, then we will denote by $\mathcal{A}_\ell(\mathcal{S})$ the affine set arising from $\mathcal{S}$ with respect to ℓ.
If $\mathcal{S}$ is a symplectic spread, then $\mathcal{A}_\ell(\mathcal{S})$ is a set of q^{2n} points of an affine space $\mathrm{PG}(3,q^n)\setminus\pi_\infty$ such that the line joining any two of them is disjoint from a given non-degenerate conic $\mathcal{C}$ of π_∞.

1.17 The Segre variety

Let $\mathrm{PG}(l-1,q)$ and let $\mathrm{PG}(k-1,q)$ be two projective spaces over $\mathbb{F}_q$. We give the following:

Definition 1.17.1. The *Segre map*

$$\sigma_{l-1,k-1}:\mathrm{PG}(l-1,q)\times\mathrm{PG}(k-1,q)\longrightarrow\mathrm{PG}(lk-1,q)$$

is defined by:

$$\sigma_{l,k}((x_1,\ldots,x_l),(y_1,\ldots,y_k))=(x_1y_1,\ldots,x_1y_k,\ldots,x_ly_1,\ldots,x_ly_k).$$

$Im(\sigma_{l-1,k-1})$ is the *Segre variety* $\mathcal{S}_{l-1,k-1}$. If points of $\mathrm{PG}(lk-1,q)$ have coordinates $(x_{11},x_{12},\ldots,x_{1k},x_{21},\ldots,x_{2k},\ldots,x_{l1},\ldots,x_{lk})$, then the points of the Segre variety $\mathcal{S}_{l-1k-1}$ are the points whose corresponding matrix (x_{ij}), $i=1,\ldots,l$, $j=1,\ldots,k$ has rank 1.

By fixing a point of $\mathrm{PG}(l-1,q)$ and varying the point of $\mathrm{PG}(k-1,q)$, we obtain a $(k-1)$-dimensional subspace on $\mathcal{S}_{l-1k-1}$. The set of these subspaces is a *system of maximal subspaces* of $\mathcal{S}_{l-1k-1}$. Similarly, by fixing a point of $\mathrm{PG}(k-1,q)$ we obtain an l-dimensional subspace of $\mathcal{S}_{l-1k-1}$, by varying the point of $\mathrm{PG}(l-1,q)$. The set of these subspaces form the other *system of maximal subspaces* of $\mathcal{S}_{l-1k-1}$. Subspaces of different systems intersect each other in exactly one point, subspaces of the same system are pairwise disjoint. Moreover each subspace contained in $\mathcal{S}_{l-1k-1}$ is contained in an element of one of the two systems.

Proposition 1.17.2. *Let* $\Sigma=\mathrm{PG}(r,q)$ *be a subgeometry of* $\mathrm{PG}(r,q^n)$*. The image of the points of* Σ*, under the field reduction, is projectively equivalent to the system of* $(n-1)$*-dimensional subspaces of the Segre variety* $\mathcal{S}_{r,n-1}$*.*

Definition 1.17.3. Let $\mathcal{S}_{l-1,k-1}$ be the Segre variety of $\mathrm{PG}(lk-1,q)$, i.e. the set of points $(x_{11},\ldots,x_{1k},x_{21},\ldots,x_{2k},\ldots,x_{l1},\ldots,x_{lk})$ such that the matrix (x_{ij}), $i=1,\ldots,l$, $j=1,\ldots,k$ has rank 1. For every $r=1,\ldots,\min\{l-1,k-1\}$ the *r-th secant variety* to $\mathcal{S}_{l-1,k-1}$, denoted by $\Omega_r(\mathcal{S}_{l-1k-1})$, is the set of points of $\mathrm{PG}(lk-1,q)$ s.t. the matrix (x_{ij}) has rank r.

Proposition 1.17.4. *Let $\Sigma = \mathrm{PG}(r, q)$ be a subgeometry of $\mathrm{PG}(r, q^n)$. The image of the points on the r-dimensional subspaces spanned by $r + 1$ independent points of Σ, under the field reduction, is projectively equivalent to the set of points of the r-th secant variety $\Omega_r(\mathcal{S}_{r,n-1})$ to the Segre variety $\mathcal{S}_{r,n-1}$.*

See e.g. [49],[66],[67],[74].

1.18 Maximum rank distance codes

Let $M_{m,n}(\mathbb{F}_q)$, with $m \leq n$, be the vector space of all the $m \times n$ matrices with entries in $\mathbb{F}_q$. The *distance* between two matrices is the rank of their difference. An $(m \times n, q, s)$*-rank distance code* is a subset $\mathcal{X}$ of $M_{m,n}(\mathbb{F}_q)$ such that the minimum distance between any two of its distinct elements is s. An $\mathbb{F}_q$*-linear* $(m \times n, q, s)$-rank distance code is a subspace of $M_{m,n}(\mathbb{F}_q)$.

It is known (see e.g. [32]) that the size of an $(m \times n, q; s)$-rank distance code $\mathcal{X}$ satisfies the *Singleton-like bound*:

$$|\mathcal{X}| \leq q^{n(m-s)}.$$

When this bound is achieved, $\mathcal{X}$ is called an $(m \times n, q, s)$*-maximum rank distance code*, or $(m \times n, q, s)$*-MRD code*, for short.

In finite geometry $(m \times m, q, m)$-MRD codes are known as *spread sets* (see e.g. [33]) and there are examples for both cases $\mathbb{F}_q$-linear and non-linear.

In [32], P. Delsarte constructed linear MRD codes for all possible values of the parameters m, n, q and s. These codes were also constructed, independently, by E. M. Gabidulin in [43] and generalized by E. M. Gabidulin and A. Kshevetskiy in [63]. These codes are now known as *Generalized Gabidulin codes*.

In the case $n = m$, a different construction of Delsarte's MRD codes was given by B. N. Cooperstein in [27]. Recently, J. Sheekey in [93] and G. Lunardon, R. Trombetti and Y. Zhou in [77] provide some new linear MRD codes by using linearized polynomials over $\mathbb{F}_{q^n}$. For more details on the relation between linear sets and MRD codes see [71]. The first class of non-linear MRD codes have been constructed by A. Cossidente, G. Marino and F. Pavese [28] and later generalized first by N. Durante and A. Siciliano in [41] and finally by G. Donati and N. Durante in [39].

For more results on MRD codes we refer to the recent preprint [94].

Chapter 2

C_F^m-sets and σ-conics in $\mathrm{PG}(2, q^n)$

2.1 Steiner's construction of conics in $\mathrm{PG}(2, \mathbb{F})$

J. Steiner (1796-1863) was a swiss mathematician. He did not learn to read and write until he was 14 and only went to school at the age of 18, against the wishes of his parents. He studied at the Universities of Heidelberg and Berlin, supporting himself with a very modest income from tutoring. He was an early contributor to Crelle's Journal, the first journal devoted entirely to mathematics founded in 1826. He was appointed to a chair at the University of Berlin in 1834, a position he held until his death. He was one of the greatest contributors to projective geometry. He discovered the Steiner surface which has a double infinity of conic sections on it. He disliked algebra and analysis and believed that calculations replace thinking while geometry stimulates thinking.

The usual definition of a conic uses a quadratic form. An alternative definition of a conic uses an orthogonal polarity and it is due to K.G.C. von Staudt. The disadvantage of von Staudt's definition is that it only works when the underlying field has characteristic different from 2. In 1832, J. Steiner constructed conics by using projectivities between pencils of lines. His approach is independent of the characteristic of the underlying field. We recall his construction. In what follows if A is a point of $\mathrm{PG}(2, \mathbb{F})$, then we will denote by $\mathcal{P}_A$ the pencil of lines with center A.

Theorem 2.1.1 (J. Steiner [96]). *Let R and L be two different points of $\mathrm{PG}(2, \mathbb{F}), \mathbb{F}$ a field and let $\Phi : \mathcal{P}_R \longrightarrow \mathcal{P}_L$ be a projectivity. The set of points of intersection of corresponding lines under Φ is one of the following:*

- *a degenerate conic, if* $\Phi(RL) = RL$,
- *a non-degenerate conic, if* $\Phi(RL) \neq RL$.

Proof. Let $R = (1,0,0)$ and $L = (0,0,1)$, $\mathcal{P}_R = \{\ell_{a,b} : ax_2 + bx_3 = 0\}_{(a,b)\in \mathrm{PG}(1,q^n)}$ and $\mathcal{P}_L = \{\ell'_{a,b} : ax_1 + bx_2 = 0\}_{(a,b)\in \mathrm{PG}(1,q^n)}$. We distinguish two cases:

1) $\Phi(RL) \neq RL$.

We may suppose w.l.o.g. that:

$$\Phi(\ell_{1,0}) = \ell'_{1,0}, \Phi(\ell_{0,1}) = \ell'_{0,1} \text{ and } \Phi(\ell_{1,1}) = \ell'_{1,1}.$$

Hence $\Phi(\ell_{a,b}) = \ell'_{a,b}$. The set Γ of points of intersection of corresponding lines under Φ is given by the non-trivial solutions of the linear system

$$\begin{cases} ax_2 + bx_3 &= 0 \\ ax_1 + bx_2 &= 0. \end{cases}$$

This linear system has non-trivial solutions, in the unknowns a, b, if and only if $x_1x_3 - x_2^2 = 0$, that is the equation Γ.

2) $\Phi(RL) = RL$.

We may assume w.l.o.g. that

$$\Phi(\ell_{0,1}) = \ell'_{1,0} \text{ and } \Phi(\ell_{1,1}) = \ell'_{1,1}.$$

Hence $\Phi(\ell_{a,b}) = \ell'_{b,a}$. The set Γ of points of intersection of corresponding lines under Φ is given by the non-trivial solutions of the linear system

$$\begin{cases} ax_2 + bx_3 &= 0 \\ bx_1 + ax_2 &= 0. \end{cases}$$

This linear system has non-trivial solutions in the unknowns a, b if and only if $x_2(x_1 - x_3) = 0$, that is the equation of Γ. □

In Steiner's construction of conics if we assume that the points R and L coincide we get the following:

Proposition 2.1.2. *Let R be a point of* $\mathrm{PG}(2,\mathbb{F}), \mathbb{F}$ *a field and let* $\Phi : \mathcal{P}_R \longrightarrow \mathcal{P}_R$ *be a projectivity. The set of points of intersection of corresponding lines under* Φ *is one of the following:*

- *the point R, a line through R, two distinct lines through R,*

- *the pencil of lines through R, $\mathcal{P}_R$.*

Proof. Let R be a point and consider a projectivity Φ of $\mathcal{P}_R$ into itself. If Φ is not the identity it can have $0,1,2$ fixed elements giving as set of points of intersection of corresponding lines under Φ either just the point R, or a single line through R or a pair of lines through R. If $\Phi = 1$, then as set of points of intersection of corresponding lines under Φ we obtain the full pointset of $\mathrm{PG}(2,\mathbb{F})$ and, as geometry, we get the degenerate symplectic geometry of $\mathrm{PG}(2,\mathbb{F})$ having as lines the lines of $\mathcal{P}_R$. □

Remark 2.1.3. In this way, if $\mathbb{F}$ is a finite field or any algebraically closed field, then we get all the possible conics of $\mathrm{PG}(2,\mathbb{F})$. If $\mathbb{F}$ is $\mathbb{R}$, the field of real numbers, the only missing conic, up to projectivities, has equation $x_1^2 + x_2^2 + x_3^2 = 0$, that is the conic giving as locus in $\mathrm{PG}(2,\mathbb{R})$ the empty set.

Note that, since we obtained all, but the empty conic, and also the degenerate symplectic geometry, also the converse is true:

Proposition 2.1.4. *Let Γ be either a non-empty conic or a degenerate symplectic geometry of* $\mathrm{PG}(2,\mathbb{F})$*, $\mathbb{F}$ being a field. There are two points R and L of Γ and a projectivity $\Phi : \mathcal{P}_R \longrightarrow \mathcal{P}_L$ s.t. Γ is the set of points of intersection of corresponding lines under Φ.*

In the next section we will generalize Steiner's construction in a finite projective plane $\mathrm{PG}(2,q^n)$ by considering collineations instead of projectivities.

2.2 C_F^m-sets of $\mathrm{PG}(2,q^n)$

Let R and L be two distinct points of a projective plane $\mathrm{PG}(2,q^n)$ over the Galois field $\mathbb{F}_{q^n}$, $q = p^h$, p a prime number and let $\mathcal{P}_R$ and $\mathcal{P}_L$ be the pencils of lines with vertices R and L, respectively. Let σ be the Frobenius automorphism of $\mathbb{F}_{q^n}$ given by $\sigma : x \in \mathbb{F}_{q^n} \longrightarrow x^{q^m} \in \mathbb{F}_{q^n}$, with $(m,n) = 1$, and let $\Phi : \mathcal{P}_L \longrightarrow \mathcal{P}_R$ be a σ-collineation. We give the following

Definition 2.2.1. A *C_F^m-set* of $\mathrm{PG}(2,q^n)$ with *vertices R, L* is the set of points of intersection of corresponding lines under Φ, with $\Phi(RL) \neq RL$.

In this section we assume throughout that $\Phi(RL) \neq RL$.

Proposition 2.2.2. *A C_F^m-set with vertices $R = (1,0,0)$ and $L = (0,0,1)$ has canonical equation $x_1 x_3^\sigma - x_2^{\sigma+1} = 0$.*

Proof. It is $\mathcal{P}_R = \{\ell_{a,b} : ax_2 + bx_3 = 0\}_{(a,b)\in \mathrm{PG}(1,q^n)}$ and $\mathcal{P}_L = \{\ell'_{a',b'} : a'x_1 + b'x_2 = 0\}_{(a',b')\in \mathrm{PG}(1,q^n)}$. We may assume w.l.o.g. that

$$\Phi(\ell_{1,0}) = \ell'_{1,0}, \Phi(\ell_{0,1}) = \ell'_{0,1} \text{ and } \Phi(\ell_{1,1}) = \ell'_{1,1}.$$

Hence $\Phi(\ell_{a,b}) = \ell'_{a^\sigma,b^\sigma}$. The set of points of intersection of corresponding lines under Φ is given by the non-trivial solutions of the system

$$\begin{cases} ax_2 + bx_3 &= 0 \\ a^\sigma x_1 + b^\sigma x_2 &= 0. \end{cases}$$

This system is equivalent to the linear system in the unknowns a, b

$$\begin{cases} ax_2 + bx_3 &= 0 \\ ax_1^{\sigma^{-1}} + bx_2^{\sigma^{-1}} &= 0. \end{cases}$$

It has non-trivial solutions if and only if $x_1^{\sigma^{-1}}x_3 - x_2^{\sigma^{-1}+1} = 0$, that is the same as $x_1x_3^\sigma - x_2^{\sigma+1} = 0$, the *canonical equation* of a C_F^m-set. □

Every line through R (respectively through L) is a 2-secant line except the line $\Phi^{-1}(RL)$ (respectively the line $\Phi(LR)$) that is a tangent line, so every C_F^m-set has $q^n + 1$ points. The point of intersection of the tangent lines at R and at L, is called the *center* of the C_F^m-set.

Proposition 2.2.3. *Every line of* $\mathrm{PG}(2, q^n)$ *intersects a C_F^m-set in* $0, 1, 2$ *or* $q+1$ *points. In the last case these points form a subline over* $\mathbb{F}_q$*.*

Proof. Exercise. □

In what follows we will denote by N the norm $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ of elements of $\mathbb{F}_{q^n}$ w.r.t. $\mathbb{F}_q$ and for $a \in \mathbb{F}_q^*$ we will denote by $N_a = \{\alpha \in \mathbb{F}_{q^n} : N(\alpha) = a\}$.

Proposition 2.2.4. *Every C_F^m-set of* $\mathrm{PG}(2, q^n)$ *with vertices R and L is the union of $\{R, L\}$ with $q - 1$ pairwise disjoint subsets, each of which is a scattered $\mathbb{F}_q$-linear set of rank n.*

Proof. Let $\mathcal{C}$ be the C_F^m-set of $\mathrm{PG}(2, q^n)$ given by

$$\mathcal{C} = \{(t^{q^m+1}, t, 1) : t \in GF(q^n)\} \cup \{R\}.$$

The set $\mathcal{C} \setminus \{R, L\}$ is the union of the sets $\mathcal{C}_a = \{(t^{q^m+1}, t, 1) : t \in N_a\}$, with $a \in \mathbb{F}_q^*$. All these subsets are projectively equivalent. Indeed, let a be an element of $\mathbb{F}_q^*$ and let α be an element of $\mathbb{F}_{q^n}$ with $N(\alpha) = a$. The projectivity induced by the diagonal matrix Diag$(\alpha^{q^m+1}, \alpha, 1)$ maps the set $\mathcal{C}_1$ into the set $\mathcal{C}_a$. Since $(m, n) = 1$, it follows that $N_1 = \{x^{q^m-1} : x \in \mathbb{F}_{q^n}^*\}$ and hence $\mathcal{C}_1 = \{(x^{q^{2m}}, x^{q^m}, x) : x \in \mathbb{F}_{q^n}^*\}$. As $|\mathcal{C}_1| = |N_1| = \frac{q^n-1}{q-1}$, we have that $\mathcal{C}_1$ is a scattered $\mathbb{F}_q$-linear set of rank n. □

Remark 2.2.5. W.l.o.g. we may assume $m \leq n/2$. Indeed if $m > n/2$, then from $x_1 {x_3}^{q^m} - {x_2}^{q^m+1} = 0$ it follows that $x_1^{q^{n-m}} x_3 - {x_2}^{q^{n-m}+1} = 0$, that is a C_F^{n-m}-set.

Consider $\sigma : x \mapsto x^{q^m}$, $(m,n) = 1$ and $\sigma' : x \mapsto x^{q^{m'}}$, $(m',n) = 1$.

Proposition 2.2.6. *Let $\mathcal{C}$ be a C_F^m-set and let $\mathcal{C}'$ be a $C_F^{m'}$-set of* $\mathrm{PG}(2,q^n)$*. The sets $\mathcal{C}$ and $\mathcal{C}'$ are $P\Gamma L$-equivalent if and only if $m' = m$.*

Proof. W.l.o.g. we may assume that $\mathcal{C}$ and $\mathcal{C}'$ have the same vertices, say R and L. Denote by Φ and Φ' the collineations between $\mathcal{P}_R$ and $\mathcal{P}_L$ generating $\mathcal{C}$ and $\mathcal{C}'$ respectively. We may also assume that:

$$\Phi^{-1}(RL) = \Phi'^{-1}(RL) \text{ and } \Phi(RL) = \Phi'(RL).$$

Let f be a collineation of $\mathrm{PG}(2,q^n)$ mapping $\mathcal{C}$ to $\mathcal{C}'$. Since R and L are the unique points of both $\mathcal{C}$ and $\mathcal{C}'$ through which do not pass $(q+1)$-secant lines, it follows that f stabilizes the set $\{R, L\}$. First assume that $f(R) = L$. For every line ℓ in $\mathcal{P}_R$ we have that $f(\Phi(\ell)) = \Phi'^{-1}(f(\ell))$. As Φ and Φ'^{-1} are collineations with accompanying automorphisms $x \mapsto x^{q^m}$ and $x \mapsto x^{q^{n-m'}}$, respectively, we have that $m = n - m'$, and so $m = m' = \frac{n}{2}$ hence $n = 2, m' = m = 1$.

Next suppose that $f(R) = R, f(L) = L$. For every line $\ell \in \mathcal{P}_R$ we have that $f(\Phi(\ell)) = \Phi'(f(\ell))$, hence $m = m'$. □

Remarks 2.2.7.

1. Let f be a collineation of $\mathrm{PG}(2,q^n)$ with accompanying automorphism $x \mapsto x^{p^i}$ stabilizing the C_F^m-set $\mathcal{C}$ with equation $x_1 x_3^{q^m} - x_2^{q^m+1} = 0$. From the proof of the previous proposition we have that f fixes $\{L, R\}$ and it fixes the center C. First assume that f fixes pointwise $\{R, L\}$. There exist two elements $a, b \in \mathbb{F}_{q^n}^*$ such that $a = b^{q^m+1}$ and
$$f(x_1,x_2,x_3) = (a x_1^{p^i}, b x_2^{p^i}, x_3^{p^i}),$$
for some $i, 1 \leq i \leq n-1$. Hence if $n > 2$, then the collineation group G stabilizing $\mathcal{C}$ is the semidirect product of the cyclic linear collineation group H of order $q^n - 1$ whose elements are the projectivities
$$(x_1,x_2,x_3) \mapsto (a x_1, b x_2, x_3),$$
where $a = b^{q^m+1}$, with the cyclic group K of order nh generated by the collineation
$$(x_1,x_2,x_3) \mapsto (x_1^p, x_2^p, x_3^p).$$

So $G = H \rtimes K$ and $|G| = nh(q^n - 1)$.
Next assume that $f(L) = R$ and $f(R) = L$, hence $n = 2$. It follows that there exist $a, b \in \mathbb{F}_{q^2}^*$ s.t. $a = b^{q+1}$ and

$$f(x_1, x_2, x_3) = (ax_3^{p^i}, bx_2^{p^i}, x_1^{p^i}).$$

Let S be the subset of the following projectivities:

$$f(x_1, x_2, x_3) = (ax_3, bx_2, x_1).$$

The collineation group G stabilising a C_F^1-set $\mathcal{C}$ of $\mathrm{PG}(2, q^2)$ is the semidirect product of $S \cup H$ with K. So in this case $G = (S \cup H) \rtimes K$. It has order $4h(q^2 - 1)$.

2. Let $\mathcal{C}$ be a C_F^m-set of $\mathrm{PG}(2, q^n)$ with vertices R and L and centre C, generated by a σ-collineation Φ between $\mathcal{P}_R$ and $\mathcal{P}_L$. Let $\mathcal{T}$ be a scattered linear set of pseudoregulus type of the pencil $\mathcal{P}_R$ with transversal lines RL and LC. A *component* of $\mathcal{C}$ is the set of points of intersection of the lines of $\mathcal{T}$ with corresponding lines under Φ. It is easy to see that for a C_F^m-set $\mathcal{C}$ of $\mathrm{PG}(2, q^n)$ with equation $x_1x_3^{q^m} - x_2^{q^m+1} = 0$ the $q - 1$ components of $\mathcal{C}$ are the sets $\mathcal{C}_a$ defined in the proof of the previous proposition. Since $\mathcal{C}$ is the union of its $q - 1$ components with $\{R, L\}$ it follows easily that every $(q + 1)$-secant line to $\mathcal{C}$ is a $(q + 1)$-secant line to one of its components.

3. Consider the incidence structure $(\mathcal{C}_1, \mathcal{L})$ where $\mathcal{L}$ is the set of $(q + 1)$-secant lines to $\mathcal{C}_1$. Let us embed $\Omega = \mathrm{PG}(2, q^n)$ in $\Sigma' = \mathrm{PG}(n - 1, q^n)$ and let Ω' be an $(n - 4)$-dimensional subspace of Σ' disjoint from Ω. Consider a subgeometry $\Sigma = \mathrm{PG}(n - 1, q)$ of Σ' disjoint from Ω'. From Theorem 1.12.2 it follows that $\mathcal{C}_1$ is obtained via the projection $p_{\Omega',\Omega}$ from Ω' into Ω of the set Σ. As $\mathcal{C}_1$ is an $\mathbb{F}_q$-linear set contained in a set of type $(0, 1, 2, q+1)_1$, we have that $\mathcal{C}_1$ is of type $(0, 1, q+1)_1$. Via the projection $p_{\Omega',\Omega}$ it follows that Veblen-Young's axiom holds in $(\mathcal{C}_1, \mathcal{L})$ since it holds in Σ. Hence $(\mathcal{C}_1, \mathcal{L})$ is a projective geometry $\mathrm{PG}(n - 1, q)$ s.t. every three non-collinear points of $\mathcal{C}_1$ are also non-collinear points of $\mathrm{PG}(2, q^n)$.

4. Let $\mathcal{C}$ be a C_F^m-set of $\mathrm{PG}(2, q^n)$ with vertices R and L and center C and let G be the projective group stabilizing $\mathcal{C}$. As previously shown, G contains a cyclic subgroup H of order $q^n - 1$. The orbit of a point P, not on the edges of the triangle RLC, under the group H, is the unique C_F^m-set of $\mathrm{PG}(2, q^n)$ with vertices R and L and center C containing P. Let T be the unique subgroup of H of order $\frac{q^n-1}{q-1}$. The orbit of a point P, not on the edges of the triangle RLC, under the group T, is isomorphic to a projective geometry $\mathrm{PG}(n - 1, q)$ embedded in $\mathrm{PG}(2, q^n)$, so a component $\mathcal{C}_i$ of $\mathcal{C}$. The orbit of a point P on the edges of the triangle RLC, but different from R, L and C, is again isomorphic to a projective geometry $\mathrm{PG}(n - 1, q)$, but this time all of its points are on the same side of the triangle as the point

P. Hence it is an $\mathbb{F}_q$-linear set of pseudoregulus type with transversal points the two vertices of the triangle on the side containing P.

The definitions, the results and the proofs of this section have been originally given by G. Donati and N. Durante in [34] and [38].

2.3 Degenerate C_F^m-sets in $\mathrm{PG}(2,q^n)$

Let $\mathcal{P}_R$ and $\mathcal{P}_L$ be the pencils of lines with vertices two distinct points R and L of a projective plane $\mathrm{PG}(2,q^n)$ over the Galois field $\mathbb{F}_{q^n}$, $q = p^h$, p a prime number. Let $\Phi : \mathcal{P}_R \longrightarrow \mathcal{P}_L$ be a σ_m-collineation with $(m,n) = 1$.

Definition 2.3.1. A *degenerate C_F^m-set* of $\mathrm{PG}(2,q^n)$ with *vertices* R, L is the set of points of intersection of corresponding lines under Φ, with $\Phi(RL) = RL$.

In this section we will often denote by σ the authomorphism σ_m and we assume throught that $\Phi(RL) = RL$.

Proposition 2.3.2. *A degenerate C_F^m-set with vertices $R = (1,0,0)$ and $L = (0,1,0)$ has canonical equation $x_3(x_1x_3^{\sigma-1} - x_2^\sigma) = 0$.*

Proof. It is $\mathcal{P}_R = \{\ell_{a,b} : ax_2 + bx_3 = 0\}_{(a,b)\in \mathrm{PG}(1,q^n)}$ and
$\mathcal{P}_L = \{\ell'_{a,b} : ax_1 + bx_3 = 0\}_{(a,b')\in \mathrm{PG}(1,q^n)}$. We may assume w.l.o.g. that

$$\Phi(\ell_{1,0}) = \ell'_{1,0} \text{ and } \Phi(\ell_{1,1}) = \ell'_{1,1}.$$

Hence $\Phi(\ell_{a,b}) = \ell'_{a^\sigma,b^\sigma}$. The set of points of intersection of corresponding lines under Φ is giving by the non-trivial solutions to the system

$$\begin{cases} ax_2 + bx_3 & = & 0 \\ a^\sigma x_1 + b^\sigma x_3 & = & 0. \end{cases}$$

This system is equivalent of the linear system in the unknowns a, b

$$\begin{cases} ax_2 + bx_3 & = & 0 \\ ax_1^{\sigma^{-1}} + bx_3^{\sigma^{-1}} & = & 0. \end{cases}$$

It has non-trivial solutions if and only if $x_2x_3^{\sigma^{-1}} - x_1^{\sigma^{-1}}x_3 = 0$, that is if and only if $x_3(x_1x_3^{\sigma-1} - x_2^\sigma) = 0$, the *canonical equation* of a degenerate C_F^m-set with vertices R and L. □

Every degenerate C_F^m-set of $\mathrm{PG}(2,q^n)$ has $2q^n+1$ points, q^n+1 of them are the points of the line RL. We can assume, in the remaining part, that $m \leq n/2$ holds. Indeed, if $m > n/2$, then from $x_1x_3^{q^m} - x_3x_2^{q^m} = 0$ it follows that $x_1^{q^{n-m}}x_3 - x_3^{q^{n-m}}x_2 = 0$, that is a degenerate C_F^{n-m}-set. Now let $m, m' \leq n/2$, with $(m,n) = (m',n) = 1$.

Proposition 2.3.3. *Let $\mathcal{C}$ be a degenerate C_F^m-set and let $\mathcal{C}'$ be a degenerate $C_F^{m'}$-set of* $\mathrm{PG}(2,q^n)$*. The sets $\mathcal{C}$ and $\mathcal{C}'$ are $P\Gamma L$-equivalent if and only if $m' = m$.*

Proof. Let Φ (resp. Φ') be a σ-collineation (resp. σ'-collineation) defining $\mathcal{C}$ (resp. $\mathcal{C}'$). We may assume that both $\mathcal{C}$ and $\mathcal{C}'$ have the same vertices R and L. Observe that if $\mathcal{C}$ is a degenerate C_F^m-set of $\mathrm{PG}(2,q^n)$ with vertices R and L defined by a σ-collineation Φ, then $\mathcal{C}$ is also a degenerate C_F^{n-m}-set with vertices L and R, generated by the σ^{-1}-collineation Φ^{-1}.
Let f be a collineation of $\mathrm{PG}(2,q^n)$ mapping $\mathcal{C}$ into $\mathcal{C}'$. Since R and L are the unique points of both $\mathcal{C}$ and $\mathcal{C}'$ not incident with $(q+1)$-secant lines, it follows that f stabilizes the set $\{R, L\}$. First assume that $f(R) = L$. For every line ℓ through the point R, we have that $f(\Phi(\ell)) = (\Phi')^{-1}(f(\ell))$. As Φ and $(\Phi')^{-1}$ are collineations with accompanying automorphism σ and σ'^{-1}, respectively, we have that $m = n - m'$, and so $m = m' = \frac{n}{2}$. Since $(m,n) = (m',n) = 1$, it follows that $n = 2, m' = m = 1$. Next suppose that $f(L) = L, f(R) = R$. For every line ℓ through R we have that $f(\Phi(\ell)) = \Phi'(f(\ell))$, hence $\sigma = \sigma'$ so $m = m'$. □

Remark 2.3.4. Let f be a collineation of $\mathrm{PG}(2,q^n)$ with accompanying automorphism $x \mapsto x^{p^i}$ stabilizing the degenerate C_F^m-set with equation

$$x_3(x_1x_3^{q^{m-1}} - x_2^{q^m}) = 0.$$

From the proof of previous proposition, we have that f fixes $\{R, L\}$. If f fixes $\{R, L\}$ pointwise, then there exist four elements a, b, c, d of $\mathbb{F}_{q^n}$ with $ac \neq 0$, $a = c^{q^m}$, $b = d^{q^m}$ such that

$$f(x_1,x_2,x_3) = (ax_1^{p^i} + bx_3^{p^i}, cx_2^{p^i} + dx_3^{p^i}, x_3^{p^i}).$$

Hence the collineation group stabilizing a degenerate C_F^m-set of $\mathrm{PG}(2,q^n)$ is the semidirect product of the linear collineation group H of order $q^n(q^n-1)$ whose elements are the projectivities

$$(x_1,x_2,x_3) \mapsto (ax_1 + bx_3, cx_2 + dx_3, x_3),$$

where $ac \neq 0, a = c^\sigma, b = d^\sigma$ with the cyclic group K of order nh generated by the collineation

$$(x_1,x_2,x_3) \mapsto (x_1^p, x_2^p, x_3^p).$$

Hence $G = H \rtimes K$ and $|G| = nhq^n(q^n-1)$.
If $f(L) = R$ and $f(R) = L$, then $n = 2$. It follows that there exist four elements $a, b, c, d \in \mathbb{F}_{q^n}$ with $ac \neq 0, c = a^q, d = b^q$ such that

$$f(x_1, x_2, x_3) = (a^q x_2^{p^i} + b^q x_3^{p^i}, a x_1^{p^i} + b x_3^{p^i}, x_3^{p^i}).$$

Hence in this case, let S be the set of the following projectivities:

$$f(x_1, x_2, x_3) = (a^q x_2 + b^q x_3, a x_1 + b x_3, x_3).$$

It follows that the collineation group stabilizing a degenerate C_F^1-set of $\mathrm{PG}(2,q^2)$ is the semidirect product of $S \cup H$ with K. Hence $G = (S \cup H) \rtimes K$ and so $|G| = 4hq^n(q^n-1)$ in this case.

Proposition 2.3.5. *Every line of* $\mathrm{PG}(2,q^n)$*, different from the line RL, intersects a degenerate C_F^m-set either in $1, 2$ or $q+1$ points. In the last case these points form a subline over $\mathbb{F}_q$.*

Proof. Exercise. □

Proposition 2.3.6. *Every degenerate C_F^m-set $\mathcal{C}$ of* $\mathrm{PG}(2,q^n)$ *with vertices R and L is the union of the line RL with a scattered $\mathbb{F}_q$-linear set $\mathcal{S}$ of rank $n+1$, such that $\mathcal{S} \cap RL$ is an $\mathbb{F}_q$-linear set of pseudoregulus type with transversal points R and L and vice versa.*

Proof. Let $\mathcal{C}$ be a degenerate C_F^m-set of $\mathrm{PG}(2,q^n)$ with vertices R and L with equation $x_3(x_1 x_3^{\sigma-1} - x_2^\sigma) = 0$ and let $\mathcal{A} = \mathcal{C} \setminus RL$. We first prove that the union of the set $\mathcal{A}$ with the set of the directions of $\mathcal{A}$ on the line RL is a scattered $\mathbb{F}_q$-linear set of $\mathrm{PG}(2,q^n)$ of rank $n+1$. Let $X = (x^\sigma, x, 1)$ and $Y = (y^\sigma, y, 1)$ be any two distinct points of $\mathcal{A}$. The line XY meets the line RL in the point $((y-x)^\sigma, y-x, 0)$, hence the union of the set $\mathcal{A}$ with its directions on the line RL is given by $\mathcal{S} = \{(z^\sigma, z, a) : z \in \mathbb{F}_{q^n}, a \in \mathbb{F}_q, (z,a) \neq (0,0)\}$.
It is clear that $\mathcal{S}$ is an $\mathbb{F}_q$-linear set. Since $\mathcal{S}$ has size $q^n + q^{n-1} + \cdots + q + 1$, it follows that it is a scattered $\mathbb{F}_q$-linear set of $\mathrm{PG}(2,q^n)$ of rank $n+1$. Embed $\Omega = \mathrm{PG}(2,q^n)$ in $\Sigma' = \mathrm{PG}(n,q^n)$ and let Ω' be an $(n-3)$-dimensional subspace of Σ' disjoint from Ω. Consider a subgeometry $\Sigma = \mathrm{PG}(n,q)$ of Σ' disjoint from Ω'. Let H be the hyperplane of Σ' spanned by Ω' and the line RL. From Theorem 1.12.2 it follows that $\mathcal{S}$ (resp. $\mathcal{A}$) is obtained via the projection $p_{\Omega',\Omega}$ from Ω' into Ω of the set Σ (resp. $\mathrm{AG}(n,q) = \Sigma \setminus H$). As $\mathcal{C}$ is a set of type $(1,2,q+1)_1$ we have that $\mathcal{A}$ is of type $(0,1,q)_1$. Consider the incidence structure $(\mathcal{A}, \mathcal{L})$ where $\mathcal{L}$ is the set of q-secant lines to $\mathcal{A}$. Via the projection $p_{\Omega',\Omega}$ it follows that axioms in Theorem 1.4.6 are satisfied in $(\mathcal{A}, \mathcal{L})$ since they hold in $\Sigma \setminus H$. So $(\mathcal{A}, \mathcal{L})$ is an affine geometry $\mathrm{AG}(n,q)$. Since $\mathcal{S} \cap RL = \{(z^\sigma, z, 0) : z \in \mathbb{F}_{q^n}^*\}$ it follows that $\mathcal{S} \cap LR$ is an $\mathbb{F}_q$-linear set of pseudoregulus type with transversal points R and L.

Vice versa, let $\mathcal{C}$ be the union of the line RL with a scattered $\mathbb{F}_q$-linear set $\mathcal{S}$ of rank $n+1$, such that $\mathcal{S} \cap RL$ is an $\mathbb{F}_q$-linear set of pseudoregulus type with transversal points R and L. We may assume that $\mathcal{S} \cap RL = \{(z^{\sigma_m}, z, 0) : z \in \mathbb{F}_{q^n}^*\}$ for some $m \in \{1, \ldots, n-1\}$ with $(m, n) = 1$ (see [74]) and from the first part of this proof the set $\mathcal{S}$ is the projection of Σ from Ω' to Ω. Let Ψ be the collineation of Σ' of order n with accompanying automorphism $x \mapsto x^q$ such that $\Sigma = Fix(\Psi)$. As in [74], we may assume that $\Omega' = \langle R^{\Psi^i} : i \neq 0, m\rangle$ where L and $R = L^{\Psi^m}$ are the transversal points of $\mathcal{S} \cap RL$. Consider the following collineation with accompanying automorphism $x \mapsto x^{q^m}$

$$\Phi : \ell \in \mathcal{P}_R \to \langle \ell, \Omega' \rangle^{\Psi^m} \cap \Omega \in \mathcal{P}_L.$$

Since the collineation Ψ fixes the hyperplane $\langle \Omega', RL \rangle$, the collineation Φ maps the line RL into itself. For every line $\ell \in \mathcal{P}_R$ with ℓ different from RL, the hyperplane $\langle \ell, \Omega' \rangle$ meets Σ in a unique point P that is also the unique point of Σ in $\langle \ell^{\Phi}, \Omega' \rangle$ hence $\ell \cap \ell^{\Phi}$ is the projection of P from Ω' to Ω. It follows that $\mathcal{C}$ is a degenerate C_F^m-set of Ω. □

Remarks 2.3.7.

1. From the proof of the previous proposition it follows that every degenerate C_F^m-set of $\mathrm{PG}(2, q^n)$ is the union of the line RL with a set $\mathcal{A}$ of q^n points isomorphic to an affine geometry $\mathrm{AG}(n, q)$ such that every three non-collinear points of $\mathcal{A}$ are also non-collinear points of $\mathrm{PG}(2, q^n)$.

2. The set $\mathcal{S}$, defined in the proof of Proposition 2.3.6, is a small minimal $\mathbb{F}_q$-linear blocking set of Rédei type.

3. Let $\mathcal{C}$ be a degenerate C_F^m-set of $\mathrm{PG}(2, q^n)$ and let T be the linear collineation group of order q^n stabilizing $\mathcal{C}$, whose elements are the projectivities

$$(x_1, x_2, x_3) \mapsto (x_1 + a^{\sigma} x_3, x_2 + a x_3, x_3) \quad \text{for any } a \in \mathbb{F}_{q^n}.$$

The orbit of a point P, not on the line LR, under the action of T, is an affine geometry $\mathrm{AG}(n, q)$ embedded in $\mathrm{PG}(2, q^n)$. Hence it is the affine part of $\mathcal{C}$.

4. Let G be the collineation group stabilizing a degenerate C_F^m-set $\mathcal{C}$ of $\mathrm{PG}(2, q^n)$ calculated in Remark 2.3.4. Every element of G stabilizes the scattered $\mathbb{F}_q$-linear set $\mathcal{S}$, contained in $\mathcal{C}$, of rank $n+1$ of $\mathrm{PG}(2, q^n)$ such that $\mathcal{S} \cap LR$ is an $\mathbb{F}_q$-linear set of pseudoregulus type and vice versa. Thus the collineation group stabilizing $\mathcal{S}$ coincides with G.

The definitions, the results and the proofs of this section have been originally given by G. Donati and N. Durante in [35] and [38].

2.4 Characterizing $\Gamma : X_tAX = 0$ in $\mathrm{PG}(d, q^n)$

Let Γ be a proper subset of points of $\mathrm{PG}(d, \mathbb{F})$ with equation $X_tAX = 0$. The matrix A cannot be a skew-symmetric matrix and Γ is a (possibly degenerate) quadric and vice versa. Note that the previous holds, independently of the characteristic of the field $\mathbb{F}$, but in case of characteristic 2 there is no relation between $|A|$ and degeneracy or not of the quadric. Observe also that, not assuming A a symmetric matrix, also for characteristic of $\mathbb{F}$ either odd or 0, this relation is lost and, a bit surprisingly, also the following holds:

Proposition 2.4.1. *If $\Gamma : X_tAX = 0$ is a proper subset of points of $\mathrm{PG}(d, \mathbb{F})$, with $|A| = 0$, then Γ is a (possibly degenerate) quadric. Vice versa, if Γ is a non-empty (possibly degenerate) quadric of $\mathrm{PG}(d, \mathbb{F})$, then there exists a matrix A, with $|A| = 0$, s.t. Γ is projectively equivalent to the set of points with equation $X_tAX = 0$.*

Proof. Exercise.

Hence in the Desarguesian projective plane $\mathrm{PG}(2, q)$, since all conics are non-empty, we have the following:

Proposition 2.4.2. *If $\Gamma : X_tAX = 0$, with $|A| = 0$, is a set of points of $\mathrm{PG}(2, q^n)$, then Γ is either a degenerate symplectic geometry or a (possibly) degenerate conic. Vice versa if Γ is either a degenerate symplectic geometry or a (possibly degenerate) conic of $\mathrm{PG}(2, q^n)$, then there is a matrix A with $|A| = 0$ s.t. Γ is projectively equivalent to the set of points with equation $X_tAX = 0$.*

2.5 C_F^m-sets of $\mathrm{PG}(2, q^n)$ and sesquilinear forms

In what follows let $\sigma : x \mapsto x^{q^m}$, $(m, n) = 1$. If Γ is a (possibly degenerate) C_F^m-set of $\mathrm{PG}(2, q^n)$, then Γ has an equation of the following type $X_tAX^\sigma = 0$. Note also that the canonical equations of both a degenerate C_F^m-set and a C_F^m-set of $\mathrm{PG}(2, q^n)$ have $|A| = 0$.

In September 2018 Jozefien D′ haeseleer visited the University of Naples Federico II for two weeks and I had to look for a research problem to share with her. My proposal was to try to answer to the following question.

Problem. *Is it true that every set Γ of points of $\mathrm{PG}(2,q^n)$ satisfying an equation $X_tAX^\sigma = 0$, with $\sigma \neq 1$, $|A| = 0$ and spanning the plane $\mathrm{PG}(2,q^n)$, is one of the following:*

- *a pair of distinct lines,*
- *a degenerate Hermitian curve ($\sigma^2 = 1$),*
- *a (possibly degenerate) C_F^m-set.*

At a first look, my proposal seemed (also to me) impossible to be true. We started to look at all possible cases, a bit a la J.W.P. Hirschfeld w.r.t. conics, and we could see that, surprisingly, the answer was affermative in a lot of cases. Nevertheless we left a pair of "more difficult" open cases that did not enable us to answer affermatively to the previous question. Since then, specially preparing these notes, I decided, at a certain point, to give up with those difficult calculations (following J. Steiner's suggestion) and to try to see the problem from a different point of view. It was at this stage that degenerate, non-reflexive sesquilinear forms came in.

In this section we will see that there is a connection between (possibly degenerate) C_F^m-sets and degenerate, non-reflexive sesquilinear forms. As we have seen in the first chapter (degenerate or not) reflexive sesquilinear forms are classified and make rise to well studied classical objects in projective spaces. Actually, the knowledge of non-degenerate, reflexive, sesquilinear forms and hence non-degenerate quadrics, Hermitian varieties, symplectic geometries is enough to classify also the degenerate ones. Regarding non-degenerate, non-reflexive sesquilinear forms of $\mathbb{F}_{q^n}^3$ they, and their related sets of absolute points in $\mathrm{PG}(2,q^n)$, have been classified in ten different papers by B. Kestenband from 1990 to 2014. We will recall some of B. Kestenband's result in the next section. Up to our knowledge nothing is known on degenerate, non-reflexive sesquilinear forms of $V = \mathbb{F}_{q^n}^{d+1}$. We will see that degenerate and non-degenerate ones are not related to each other, opposite to the reflexive case, and the knowledge of one class does not imply the knowledge of the other class. In this section we will focus on degenerate, non-reflexive sesquilinear forms.

Remark 2.5.1. Let $\langle\ ,\ \rangle$ be a non-reflexive σ-sesquilinear form of $V = \mathbb{F}_{q^n}^{d+1}$. The set Γ of its absolute points is the set of points $X \in \mathrm{PG}(d,q^n)$ such that $X \in X^\perp$ (or equivalently $X \in X^\top$). Let $u, v \in V$ with coordinates X and Y, respectively. If $\langle u,v\rangle = X_tAY^\sigma$, then $\Gamma : X_tAX^\sigma = 0$.

Throughout we can assume $\sigma \neq 1$, since we have seen that if $\sigma = 1$, then Γ :

$X_tAX = 0$ is either a (possibly degenerate) quadric or Γ is the full point set of $\mathrm{PG}(d, q^n)$ and the geometry determined in a (possibly degenerate) symplectic geometry.

Definition 2.5.2. A *σ-quadric* of $\mathrm{PG}(d, q^n)$ is the set of the absolute points of a σ-sesquilinear form, $\sigma \neq 1$, of $\mathbb{F}_{q^n}^{d+1}$. A σ-quadric of $\mathrm{PG}(2, q^n)$ will be called a *σ-conic*.

Remark 2.5.3. Let $n = 2$, $m = 1$ so that we are in $\mathrm{PG}(d, q^2)$ and $\sigma : x \mapsto x^q$. Let $\Gamma : X_tAX^\sigma = 0$ be the set of absolute points of a (degenerate) reflexive σ-sesquilinear form. In this case the set Γ is a (degenerate) Hermitian variety of $\mathrm{PG}(d, q^2)$. We have included (degenerate) Hermitian varieties in our definition in order to have no exceptions everywhere. Indeed, we will see that (degenerate) Hermitian varieties appear as intersection of σ-quadrics of $\mathrm{PG}(d, q^2)$ with subspaces.

We can now start with the study of σ-quadrics. First we determine the set Γ in $\mathrm{PG}(1, q^n)$. In the proof of the next proposition it is $V = \mathbb{F}_{q^n}^2$.

Proposition 2.5.4. *Let Γ be a σ-quadric of $\mathrm{PG}(1, q^n)$. Then it is one the following:*

- *the empty set, a point, two points,*
- *an $\mathbb{F}_q$-subline.*

Proof. Let $\Gamma : X_tAX^\sigma = 0$. We divide two cases:

Case 1. $|A| = 0$.
In this case $\mathrm{rank}(A) = 1$. Hence we have that dim $V^\perp =$ dim $V^\top = 1$. First assume that $V^\perp \neq V^\top$. We may assume, w.l.o.g., that $V^\perp$ is the point $L = (0, 1)$ and $V^\top$ is the point $R = (1, 0)$ in $\mathrm{PG}(1, q^n)$. This gives $\Gamma : x_1{x_2}^\sigma = 0$, hence $\Gamma = \{L, R\}$. Next $V^\perp = V^\top$ and we may assume that it is the point $R = (1, 0)$ in $\mathrm{PG}(1, q^n)$. Hence $\Gamma : {x_2}^{\sigma+1} = 0$ so that $\Gamma = \{R\}$.

Case 2. $|A| \neq 0$.
In this case $\Gamma : a{x_1}^{\sigma+1} + bx_1{x_2}^\sigma + cx_2{x_1}^\sigma + d{x_2}^{\sigma+1} = 0$. If $\Gamma \neq \emptyset$ we may assume that $|\Gamma| > 2$ and hence that $(1, 0), (0, 1), (1, 1) \in \Gamma$ giving $a = d = 0$, $c = -b$ and hence $\Gamma : x_1x_2({x_1}^{\sigma-1} - {x_2}^{\sigma-1}) = 0$. This implies that $\Gamma = \mathrm{PG}(1, q)$. Finally, assume $\Gamma = \emptyset$. Hence certainly $ad \neq 0$ in the equation of Γ. Put $b = c = 0$, $a = 1$, it follows that $\Gamma : {x_1}^{\sigma+1} + d{x_2}^{\sigma+1} = 0$. We distinguish several cases.

- If q is odd, then let $-d$ be a non-square in $\mathbb{F}_{q^n}$. It follows that Γ has no points in $\mathrm{PG}(1, q^n)$ since $x^{\sigma+1} = -d$ has no solutions in $\mathbb{F}_{q^n}$.

- If q is even and n is even, then let $r = (q^n - 1, q^m + 1)$ and let d be an element of $\mathbb{F}_{q^n}$ such that $d^{\frac{q^n-1}{r}} \neq 1$. Again Γ has no points in $\mathrm{PG}(1, q^n)$ since $x^{\sigma+1} = d$ has no solutions in $\mathbb{F}_{q^n}$.
- if q is even and n is odd, then let $a = 1, c = 0$, so that the equation of Γ becomes ${x_1}^{\sigma+1} + bx_1{x_2}^{\sigma} + d{x_2}^{\sigma+1} = 0$. There exist values of b and d such that Γ has no points in $\mathrm{PG}(1, q^n)$, since there exist values of b and d such that $x^{\sigma+1} + bx + d = 0$ has no solutions in $\mathbb{F}_{q^n}$. (See e.g. [9],[48]).

□

Remarks 2.5.5.

1. Observe that in case $n = 2$ and $\sigma^2 = 1$, then a σ-quadric of $\mathrm{PG}(1, q^2)$ is a Baer subline $\mathrm{PG}(1, q)$ and also a Hermitian variety $H(1, q)$.

2. Observe that if $\langle\ ,\ \rangle$ is non-degenerate sesquilinear form of $\mathbb{F}_{q^n}^2$, then there are two induced maps
$$\perp\colon Y \in \mathrm{PG}(1, q^n) \mapsto Y_t A X^{\sigma} = 0 \in \mathrm{PG}(1, q^n)$$
and
$$\top : Y \in \mathrm{PG}(1, q^n) \mapsto X_t A Y^{\sigma} = 0 \in \mathrm{PG}(1, q^n).$$
Both are collineations of $\mathrm{PG}(1, q^n)$. The set Γ coincides with the set of fixed points of both $\perp$ and $\top$.

3. From the last theorem it follows that the number of solutions in $\mathbb{F}_{q^n}$ of equations of the following type:
$$ax^{\sigma+1} + bx^{\sigma} + cx + d = 0$$
is: $0, 1, 2, q + 1$.

Before studying σ-quadrics in $\mathrm{PG}(2, q^n)$ we determine the possible intersection configurations of a subspace of $\mathrm{PG}(d, q^n)$ and a σ-quadric.

Proposition 2.5.6. *Let Γ be a σ-quadric of $\mathrm{PG}(d, q^n)$. Every subspace S of $\mathrm{PG}(d, q^n)$ intersects Γ either a σ-quadric of S or it is contained in Γ.*

Proof. Let $\Gamma : X_t A X^{\sigma} = 0$ be a σ-quadric of $\mathrm{PG}(d, q^n)$ and let S be a subspace of $\mathrm{PG}(d, q^n)$ of dimension h, $0 \leq h \leq d - 1$. By choosing an appropriate frame of $\mathrm{PG}(d, q^n)$ we can always assume that $S : x_{h+2} = \cdots = x_{d+1} = 0$. Let A' be the submatrix of A obtained by deleting the last $d - h$ rows and columns; if $A' \neq 0$, then $S \cap \Gamma$ is a σ-quadric of S, otherwise $S \subset \Gamma$. □

Proposition 2.5.7. *Let* $\Gamma : X_tAX^\sigma = 0$, $|A| = 0$, *be a* σ*-conic of* $\mathrm{PG}(2,q^n)$ *with an associated degenerate* σ*-sesquilinear form. Then* Γ *is one of the following:*

- *a cone with vertex a point* R *projecting a* σ*-quadric on a line not on* R *(hence either the point* R *or a line, or two lines, or* $q+1$ *lines through* R*),*
- *a (possibly degenerate)* C_F^m*-set.*

Proof. Since $\langle\ ,\ \rangle$ is degenerate, we have that $|A| = 0$. We divide several cases.

- First assume $\mathrm{rk}(A) = 2$ and $V^\perp \neq V^\top$.
  In this case $V^\perp$ and $V^\top$ are one-dimensional subspaces of V, so points of $\mathrm{PG}(2,q^n)$. Since $V^\perp \neq V^\top$ we may assume w.l.o.g. that the point $R = (1,0,0)$ is the right radical and the point $L = (0,0,1)$ is the left radical. It follows that

$$A = \begin{pmatrix} 0 & a & b \\ 0 & c & d \\ 0 & 0 & 0 \end{pmatrix}$$

  and

$$\Gamma : X_tAX^\sigma = (ax_1 + cx_2)x_2^\sigma + (bx_1 + dx_2)x_3^\sigma = 0.$$

  The sesquilinear form induces two degenerate correlations in $\mathrm{PG}(2,q^n)$ given by:

$$\perp : Y \in \mathrm{PG}(2,q^n) \setminus L \mapsto Y_tAX^\sigma = 0 \in \mathrm{PG}(2,q^n)^*$$

  and

$$\top : Y \in \mathrm{PG}(2,q^n) \setminus R \mapsto X_tAY^\sigma = 0 \in \mathrm{PG}(2,q^n)^*.$$

  The second map $\top$ sends points into lines through the point L and points collinear with R are mapped into the same line through L. Hence, it induces a collineation Φ between the pencil of lines through R

$$\mathcal{P}_R = \{\ell_{\alpha,\beta} : (\alpha,\beta) \in \mathrm{PG}(1,q^n)\}, \text{ where}$$

$$\ell_{\alpha,\beta} : \begin{cases} x_1 &= \lambda \\ x_2 &= \mu\alpha \\ x_3 &= \mu\beta \end{cases}, (\lambda,\mu) \in \mathrm{PG}(1,q^n)$$

  and the pencil of lines through L

$$\mathcal{P}_R = \{\ell'_{\alpha',\beta'} : (\alpha',\beta') \in \mathrm{PG}(1,q^n)\}, \quad \text{where} \quad \ell'_{\alpha',\beta'} : \alpha' x_1 + \beta' x_2 = 0$$

given by $\Phi(\ell_{\alpha,\beta}) = \ell'_{\alpha',\beta'}$, where

$$(\alpha',\beta')_t = A'(\alpha,\beta)_t^\sigma$$

and A' is the matrix

$$A' = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Note that $|A'| \neq 0$ since $\mathrm{rank}(A) = 2$. Of course Γ is the set of points of intersection of corresponding lines under the collineation Φ and hence it is either a degenerate C_F^m-set or a C_F^m-set according to $\Phi(RL) = RL$ or $\Phi(RL) \neq RL$.

- Next we assume $\mathrm{rank}(A) = 2$ and $V^\perp = V^\top$.
In this case we may assume w.l.o.g. that $R = L = (1,0,0)$ is both the left and right radical of $\langle\ ,\ \rangle$. For the set $\Gamma : X_tAX^\sigma = 0$ we have

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix}$$

so

$$\Gamma : (ax_2 + bx_3)x_2^\sigma + (cx_2 + dx_3)x_3^\sigma = 0.$$

Note that in this case the degenerate collineation $\top$ induces a collineation Φ of $\mathcal{P}_R$ and again Γ is the set of points of intersection of corresponding lines under Φ. It follows that Γ is the set of points of a cone with vertex R over either the empty set, or a point, or two points, or $q+1$ points of an $\mathbb{F}_q$-subline of a line not through the point R.

- Finally, $\mathrm{rank}(A) = 1$.
In this case dim $V^\perp =$ dim $V^\top = 2$, so in $\mathrm{PG}(2,q^n)$ the left and right radical are given by two lines ℓ and r. First assume $\ell \neq r$, so we may put $\ell : x_1 = 0$, $r : x_3 = 0$, then $\Gamma : x_1x_3^\sigma = 0$, that is the union of the two lines r and ℓ. Finally, assume that $\ell = r$, e.g. $\ell = r : x_3 = 0$, then Γ has equation ${x_3}^{\sigma+1} = 0$, hence it is the line ℓ.

□

Remarks 2.5.8.

1. Note that we can now answer to the question posed in the previous Problem. Beside (possibly degenerate) C_F^m-sets, a pair of distinct lines and a degenerate Hermitian curve (if n is even and $\sigma^2 = 1$), there is a unique another possible set of points of $\mathrm{PG}(2,q^n)$ with equation $X_tAX^\sigma = 0$, $\sigma \neq 1$, generating the plane and

it is a cone with vertex a point V projecting an $\mathbb{F}_q$-subline on a line not through V (that is a degenerate Hermitian curve if n is even and $\sigma^2=1$).

2. With the previous proposition we have also completely determined the possible sets of absolute points of $\mathrm{PG}(2,q^n)$ of a degenerate, non-reflexive sesquilinear form of $\mathbb{F}_{q^n}^3$.

3. Observe that we have said nothing on absolute points of a non-degenerate, non-reflexive σ-sesquilinear form of $\mathbb{F}_{q^n}^3$. See last section of this chapter.

4. We observe that conics of $\mathrm{PG}(2,q)$ can be obtained also from degenerate non-reflexive bilinear forms exactly in the same way we obtained σ-conics. If q is even, we can obtain a non-degenerate conic in two ways:

   - as set of absolute points of a degenerate, non-reflexive bilinear form (this is equivalent to the Steiner's construction with $\Phi(RL)\neq RL$),
   - as the affine part, plus the point L, of the set of absolute points of a degenerate σ-sesquilinear form, with $\sigma: x\mapsto x^2$ (i.e. the affine part, plus the point L, of a degenerate C_F^1-set of $\mathrm{PG}(2,2^n)$).

2.6 Exercises

In this and in the following sections we will determine some of the possible applications for a (degenerate) C_F^m-sets of $\mathrm{PG}(2,q^n)$. In what follows let $\mathcal{C}'$: $4x_1x_2-x_3^2=0$ be a conic of $\mathrm{PG}(2,q^n)$.

1. Give a proof of Proposition 2.2.3.
2. Give a proof of Proposition 2.3.5.
3. Prove that the union of the affine part of a degenerate C_F^m-set of $\mathrm{PG}(2,2^n)$ with its vertices is either a regular hyperoval or a translation hyperoval according to $m=1$ or $(m,n)=1, m>1$.
4. Prove that the internal points to the conic $\mathcal{C}'$ of $\mathrm{PG}(2,q^n)$, q odd, corresponding to the Kantor-Knuth flock form a maximum scattered linear set of a line ℓ secant to $\mathcal{C}'$ with $\ell\cap\mathcal{C}'$ as trasversal points.
5. Determine a C_F^m-set Γ of $\mathrm{PG}(2,3^n)$ such that both components of Γ give a set of internal points to the conic $\mathcal{C}'$ of $\mathrm{PG}(2,3^n)$ corresponding to a Ganley flock.

6. Does there exist a C_F^m-set of $\mathrm{PG}(2,3^5)$ such that one of its components is projectively equivalent to the set of internal points to the conic $\mathcal{C}'$ corresponding to the sporadic flock? If such a C_F^m-set exists, is it true that also in this case both components correspond to the sporadic flock?

7. Give a simple proof that the Ganley flock and the sporadic flock are not isomorphic.

Open Problem: *Let $\mathcal{F}$ be a semifield flock of a quadratic cone of* $\mathrm{PG}(3,q^n)$, *q odd and let $\mathcal{I}(\mathcal{F})$ be its corresponding set of internal points to the conic $\mathcal{C}'$ of* $\mathrm{PG}(2,q^n)$. *Is it true that if $\mathcal{I}(\mathcal{F})$ spans* $\mathrm{PG}(2,q^n)$, *then $\mathcal{I}(\mathcal{F})$ is a component of a C_F^m-set?*

2.7 Intersection of two scattered $\mathbb{F}_q$-linear sets of rank $n+1$ in $\mathrm{PG}(2,q^n)$

In this section we study the possible intersection configurations of a degenerate C_F^m-set, say $\mathcal{C}$, with a degenerate $C_F^{m'}$-set, say $\mathcal{C}'$, both of $\mathrm{PG}(2,q^n)$ without the restriction $(n,m)=(n,m')=1$ and with $m \geq m'$. We assume that both $\mathcal{C}$ and $\mathcal{C}'$ have the same vertices R and L. In the meantime we also study the possible intersection configurations of two scattered $\mathbb{F}_q$-linear sets of rank $n+1$ such that both meet RL in an $\mathbb{F}_q$-linear set of pseudoregulus type with transversal points R and L.

Proposition 2.7.1. *Let $\mathcal{C}$ be a degenerate C_F^m-set of* $\mathrm{PG}(2,q^n)$ *defined by the collineation Φ and let $\mathcal{C}'$ be a degenerate $C_F^{m'}$-set of* $\mathrm{PG}(2,q^n)$ *defined by the collineation Φ'. If both $\mathcal{C}$ and $\mathcal{C}'$ have the same vertices R and L and $\mathcal{C} \neq \mathcal{C}'$, then $\mathcal{C} \cap \mathcal{C}' \setminus RL$ is one of the following:*

i) the empty set;

ii) one point;

iii) a degenerate $C_F^{n-m+m'}$-set of a subgeometry $\mathrm{PG}(2,q^t)$ *of* $\mathrm{PG}(2,q^n)$ *minus the line RL, where $t=(n,n-m+m')$, $m \neq m'$.*

Proof. If P is a point of $\mathcal{C} \cap \mathcal{C}' \setminus RL$, then $(RP)^{\Phi} = (RP)^{\Phi'}$ hence the points of $\mathcal{C} \cap \mathcal{C}' \setminus RL$ are in one-to-one correspondence with the lines of $\mathcal{P}_R \setminus \{RL\}$ fixed by the collineation $\Phi^{-1} \circ \Phi'$ with accompanying automorphism $\tau : x \mapsto x^{q^{n-m+m'}}$. The set of fixed lines of $\Phi^{-1} \circ \Phi'$, different from RL, is one of the following: the empty set, a line, a subpencil of $\mathcal{P}_R$ coordinatized over the subfield $\mathrm{Fix}(\tau) = \mathrm{GF}(q^t)$, where $t = (n, n-m+m')$. In this last case, by considering Φ and Φ' restricted to the subpencil $Fix(\Phi^{-1} \circ \Phi')$, we have that $\mathcal{C} \cap \mathcal{C}'$ is a degenerate $C_F^{n-m+m'}$-set of a subgeometry $\mathrm{PG}(2,q^t)$ of $\mathrm{PG}(2,q^n)$. Observe that if $m = m'$, then τ is the identity, $\Phi^{-1} \circ \Phi'$ is a projectivity and so case $iii)$ cannot occur. □

Next we study the intersections of two scattered $\mathbb{F}_q$-linear sets. We note that the intersection problem for two $\mathbb{F}_q$-linear sets generalizes the intersection problem for two subgeometries. Very little is known on the intersection of two $\mathbb{F}_q$-linear sets (see [66], [85]) while the intersection problem for two subgeometries was completely solved in [37].

Proposition 2.7.2. *Let $\mathcal{S}$ and $\mathcal{S}'$ be two scattered $\mathbb{F}_q$-linear sets of rank $n+1$ of $\mathrm{PG}(2,q^n)$ such that both meet the line RL in an $\mathbb{F}_q$-linear set of pseudoregulus type with transversal points R and L. If $\mathcal{S} \neq \mathcal{S}'$, then $\mathcal{S} \cap \mathcal{S}'$ is one of the following:*

- *the empty set;*
- *one point;*
- *a degenerate $C_F^{n-m+m'}$-set of a subgeometry $\mathrm{PG}(2,q^t)$ of $\mathrm{PG}(2,q^n)$ minus the line RL, where $t = (n, n-m+m')$, $m \neq m'$;*
- *the $\mathbb{F}_q$-linear set of pseudoregulus type $\mathcal{S} \cap RL$ with transversal points R and L;*
- *the union of a point with the set $\mathcal{S} \cap RL$;*
- *the union of a degenerate $C_F^{n-m+m'}$-set of a subgeometry $\mathrm{PG}(2,q^t)$ of $\mathrm{PG}(2,q^n)$ minus the line RL, where $t = (n, n-m+m')$, $m \neq m'$ with the set $\mathcal{S} \cap RL$.*

Proof. Exercise (Hint: use the previous proposition). □

2.8 C_F^m-sets and non-linear MRD-codes

MRD-codes have been another application of C_F^m-sets of $\mathrm{PG}(2,q^n)$. The first class of non-linear MRD-codes, different from spread sets, have been constructed by A. Cossidente, G. Marino and F. Pavese in [28]. They use C_F^1-sets of $\mathrm{PG}(2,q^3)$ in order to construct non-linear $(3 \times 3, q, 1)$-MRD codes

Starting with a C_F^1-set $\mathcal{C}$ of $\mathrm{PG}(2,q^3)$ in [28], they construct a set $\mathcal{E}$ of q^3+1 points that is an *exterior* set to the component $\mathcal{C}_1$ of $\mathcal{C}$. By using field reduction from

$\mathrm{PG}(2,q^3)$ to $\mathrm{PG}(8,q) = \mathrm{PG}(M_{3,3}(q))$, there corresponds to $\mathcal{C}_1 \cong \mathrm{PG}(2,q)$ the Segre variety $\mathcal{S}_{1,1}$, that is the matrices with rank 1 and there corresponds to $\mathcal{E}$ an exterior set to the Segre variety $\mathcal{S}_{1,1}$ of $\mathrm{PG}(8,q)$ and hence a set of q^6 matrices s.t. the difference between any two has rank at least two, i.e. a $(3\times 3, q, 2)$-MRD code. In this section, it is shown that, starting from a C_F^m-set of $\mathrm{PG}(2,q^n)$, infinite families of non-linear $(3\times n, q, 2)$-MRD codes can be constructed.
Let $R=(1,0,0)$ and $L=(0,0,1)$ be two points of $\mathrm{PG}(2,q^n)$ with $n \geq 3$ and let $\mathcal{C}$ be the C_F^m-set with vertices R and L given by

$$\mathcal{C} = \{P_t = (t^{q^m+1}, t, 1) : t \in \mathbb{F}_{q^n}\} \cup \{R\}.$$

It follows that

$$\mathcal{C} = \bigcup\nolimits_{a\in\mathbb{F}_q^*} \pi_a \cup \{R, L\},$$

with $\pi_a = \{P_t : t \in N_a\}$ and $N_a = \{x \in \mathbb{F}_{q^n} : N(x) = a\}$. For every $a \in \mathbb{F}_q^*$, consider the partition of the points of the line RL, different from R and L, into subsets $J_a = \{(-t,0,1) : t \in N_a\}$ and let $\pi_1' \cong \mathrm{PG}(2,q)$ be a subgeometry of π_1.

Theorem 2.8.1. *For every subset T of $\mathbb{F}_q^*$ containing 1, the set*

$$\mathcal{X} = (\mathcal{C} \setminus \bigcup\nolimits_{a\in T}\pi_a) \cup \bigcup\nolimits_{a\in T} J_a$$

is an exterior set with respect to π_1'.

Proof. The lines RP and LP, with $P \in \mathcal{C} \setminus (\bigcup_{a\in T}\pi_a \cup \{R,L\})$, meeting $\mathcal{C}$ exactly in two points, are external lines w.r.t. π_1'.
Similarly, for every $P \in \pi_b$ and $P' \in \pi_{b'}$ with $b, b' \in \mathbb{F}_q^* \setminus T$ the line PP' is external to π_1'.
Finally, for every point $P \in \pi_b$ with $b \in \mathbb{F}_q^* \setminus T$ and $P' \in J_a$ with $a \in T$, the line PP' is external to π_1'.
Indeed suppose, by way of contradiction, that the line PP' meets π_1' in a point S with coordinates $(x^{q^{2m}}, x^{q^m}, x)$. Let $P = (\alpha^{q^m+1}, \alpha, 1)$ with $N(\alpha) = b$ and let $P' = (-t, 0, 1)$ with $N(t) = a$. By calculating the determinant of the matrix M whose rows are the coordinates of the points S, P, P', we have that $|M| = -tM_1 + \alpha M_1^{q^m}$, where M_1 is the cofactor of the element $m_{3,1}$ of M. Since S, P are distinct points, so $M_1 \neq 0$, hence $|M| = 0$ if and only if $t = \alpha M_1^{q^m-1}$, that is a contradiction since $N(\alpha) = b$ while $N(t) = a$ with $a \neq b$. □

From the previous theorem we have the following result.

Corollary 2.8.2. *For all $n \geq 3, q > 2$, the vectors $\rho v \in M_{3,n}(q)$, $\rho \in \mathbb{F}_q^*$, whose corresponding points are in $\mathcal{X}$, plus the zero vector, give a $(3\times n, q, 2)$ non-linear MRD code.*

Remark 2.8.3. These codes have been generalized, first in the case of square matrices, by using bilinear forms and the cyclic representation of $\mathrm{PG}(n-1, q^n)$ by N. Durante and A. Siciliano [41] to non-linear $(n \times n, q, n-1)$ MRD codes and later by G. Donati and N. Durante with σ-normal rational curves, a generalization of normal rational curves in $\mathrm{PG}(d, q^n)$ [39] to non-linear $((d+1) \times n, q, d)$ MRD codes, where $d \leq n-1$.

2.9 Kestenband σ-conics of $\mathrm{PG}(2, q^n)$

Regarding absolute points in $\mathrm{PG}(2, q^n)$ of a non-degenerate, non-reflexive σ-sequilinear form, $\sigma \neq 1$, of $\mathbb{F}_{q^n}^3$ we mention here that these sets have been completely determined by the huge work of B.C. Kestenband. There are lots of different classes of such sets. Actually B.C. Kestenband has classified the non-degenerate correlations of finite Desarguesian planes in general. The interested reader can find all of them in 11 different papers by B.C. Kestenband from 1990 to 2014 covering 400 pages of mathematics.
(See [52], [53], [54], [55], [56], [57], [58], [59], [60], [61], [62]).
In what follows we will use the following definition.

Definition 2.9.1. A *Kestenband σ-conic* is the set of absolute points of a non-degenerate, non-reflexive σ-sesquilinear form, $\sigma \neq 1$, of $\mathbb{F}_{q^n}^3$.

Remark 2.9.2. Let Γ be a Kestenband σ-conic of $\mathrm{PG}(2, q^n)$. The associated form is a non-degenerate sesquilinear form $\langle\ ,\ \rangle$, hence Γ cannot contain lines. It follows that Γ has equation $X_t A X^\sigma = 0$, for some non-singular matrix A. Hence $|\Gamma \cap \ell| \in \{0, 1, 2, q{+}1\}$, for every line ℓ. The sesquilinear form has both left and right radical equal to $\{0\}$, hence it cannot be obtained by considering a collineation between pencils of lines in $\mathrm{PG}(2, q^n)$, opposite to all the previously studied degenerate or not σ-conics.

Let Γ be a Kestenband σ-conic of $\mathrm{PG}(2, q^{2n+1})$, then it is:

- $|\Gamma| \in \{q^{2n+1} + aq^{n+1} + 1\}$, where $a \in \{-1, 0, 1\}$.

Let Γ be a Kestenband σ-conic of $\mathrm{PG}(2, q^{2n})$, then it is:

- If n is odd, then $|\Gamma| \in \{q^{2n} - q^{n+1} + 1, q^{2n} + q^n + 1, q^{2n} + 1\}$.
- If n is even, then $|\Gamma| \in \{q^{2n} + q^{n+1} + 1, q^{2n} - q^n + 1, q^{2n} + 1\}$.

A remarkable example of Kestenband σ-conic is given by the set Γ of points of $\mathrm{PG}(2,q^n)$ satisfying the following equation:

$$x_1^{\sigma+1}+x_2^{\sigma+1}+x_3^{\sigma+1}=0$$

It has q^n+1 points and it intersects the subplane $\mathrm{PG}(2,q)$ in the conic with equation:

$$x_1^2+x_2^2+x_3^2=0.$$

If n is even, then Γ intersects also the subplane $\mathrm{PG}(2,q^2)$ in the non-degenerate Hermitian curve with equation

$$x_1^{q+1}+x_2^{q+1}+x_3^{q+1}=0.$$

.

Chapter 3

σ-quadrics of $\mathrm{PG}(3, q^n)$

3.1 Seydewitz's and Steiner's constructions of quadrics in $\mathrm{PG}(3, \mathbb{F})$

In this section we recall the constructions of F. Seydewitz and J. Steiner of quadrics of $\mathrm{PG}(3, \mathbb{F})$, $\mathbb{F}$ a field. We start with F. Seydewitz's construction. In what follows if P is a point of $\mathrm{PG}(3, \mathbb{F})$ we will denote with $\mathcal{S}_P$ the star of lines with center P and with $\mathcal{S}_P^*$ the star of planes with center P.

Theorem 3.1.1 (F. Seydewitz [92]). *Let R and L be two distinct points of $\mathrm{PG}(3, \mathbb{F})$ and let $\Phi : \mathcal{S}_R \longrightarrow \mathcal{S}_L^*$ be a projectivity. The set Γ of points of intersection of corresponding elements under Φ is one of the following:*

- *If $\Phi(RL)$ is a plane through the line RL, then Γ is either a quadratic cone or a hyperbolic quadric $\mathrm{Q}^+(3, \mathbb{F})$,*
- *If $\Phi(RL)$ is a plane not through the line RL, then Γ is a non-empty, non-degenerate quadric i.e. either an elliptic quadric $\mathrm{Q}^-(3, \mathbb{F})$ or an hyperbolic quadric $\mathrm{Q}^+(3, \mathbb{F})$.*

Proof. Exercise.

Next consider J. Steiner's construction. In what follows if s is a line of $\mathrm{PG}(3, \mathbb{F})$ we will denote by $\mathcal{P}_s$ the pencil of planes through s.

Theorem 3.1.2 (J. Steiner [96]). *Let r and ℓ be two skew lines of $\mathrm{PG}(3, \mathbb{F})$. Let $\Phi : \mathcal{P}_r \longrightarrow \mathcal{P}_\ell$ be a projectivity. The set of points of intersection of corresponding planes under Φ is a hyperbolic quadric $\mathrm{Q}^+(3, \mathbb{F})$ of $\mathrm{PG}(3, \mathbb{F})$.*

Proof. Exercise.

Proposition 3.1.3. *In* $\mathrm{PG}(2, \mathbb{F})$ *the set of absolute points of a linear correlation satisfies an equation* $X_t AX = 0$*, for some matrix* A*. Therefore it is one of the followings:*

- *the empty set (e.g.* $\mathbb{F} = \mathbb{R}$*)*
- *a point, a line, two lines,*
- *a non-degenerate conic,*
- *a degenerate symplectic geometry* $\mathcal{P}_R$*, for some point* R*.*

Proof. It follows immediately from Proposition 2.19. □.

In F. Seydewitz's construction if we assume the points R and L coincide, then we get the following:

Proposition 3.1.4. *Let* R *be a point of* $\mathrm{PG}(3, \mathbb{F})$*. Let* $\Phi : \mathcal{S}_R \longrightarrow \mathcal{S}_R^*$ *be a projectivity. The set* Γ *of points of intersection of corresponding elements under* Φ *is one of the following:*

- *the point* R *(e.g.* $\mathbb{F} = \mathbb{R}$*),*
- *a line through* R*, a plane through* R*, two distinct planes through* R*,*
- *a quadratic cone.*
- *a degenerate symplectic geometry* $\mathcal{P}_r$*, for some line* r *thorugh* R*.*

Proof. The set of points of intersection of corresponding elements under Φ is a cone with vertex the point R projecting the set of absolute points of a linear correlation in a plane π not through the point R. Hence the assertion follows from previous proposition. □

In J. Steiner's construction if the lines r and ℓ either intersect in a point V or coincide, then we get the following:

Proposition 3.1.5. *Let* r *and* ℓ *be two lines s.t.* $r \cap \ell = \{V\}$*. Let* $\Phi : \mathcal{P}_r \longrightarrow \mathcal{P}_\ell$ *be a projectivity. The set of points of intersection of corresponding planes under* Φ *is one of the following:*

- *a pair of distinct planes,*

- *a quadratic cone,*

Proposition 3.1.6. *Let $\Phi : \mathcal{P}_r \longrightarrow \mathcal{P}_r$ be a projectivity. The set of points of intersection of corresponding planes under Φ is one of the following:*

- *the line r,*
- *a plane, a pair of distinct planes,*
- *the degenerate symplectic geometry $\mathcal{P}_r$.*

Remark 3.1.7. With Seydewitz's construction in $\mathrm{PG}(3, \mathbb{F})$ we get all possible quadrics of $\mathrm{PG}(3, \mathbb{F})$ and a degenerate symplectic geometry $\mathcal{P}_r$, for some line r, if $\mathbb{F}$ is any algebraically closed field or a finite field If $\mathbb{F} = \mathbb{R}$ is the field of real numbers, then the only missing quadric, up to projectivities, is the quadric with equation $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 0$, that gives as set of points in $\mathrm{PG}(3, \mathbb{F})$, the empty set. With Steiner's construcion in $\mathrm{PG}(3, \mathbb{F})$ we miss also the elliptic quadric.

Note that also the converse holds:

Proposition 3.1.8. *Let Γ be either a, non-empty, quadric or a degenerate symplectic geometry of $\mathrm{PG}(3, \mathbb{F})$, $\mathbb{F}$ being a field. There exists two point R and L of Γ and a projectivity $\Phi : \mathcal{S}_R \longrightarrow \mathcal{S}_L^*$ s.t. Γ is the set of points of intersection of corresponding elements under Φ.*

3.2 Non-degenerate σ-quadrics in $\mathrm{PG}(d, q^n)$

For the remaining part of this chapter we can assume $\sigma \neq 1$. Let $V = \mathbb{F}_{q^n}^{d+1}$, let $\langle , \rangle$ be a degenerate σ-sesquilinear form with associated (degenerate) correlations $\perp$, $\top$ and let $\Gamma : X_t A X^\sigma = 0$ be the set of absolute points w.r.t $\langle , \rangle$, hence a σ-quadric. We will denote by $L = V^\perp$ and $R = V^\top$, the left and right radicals, respectively, seen as subspaces of $\mathrm{PG}(d, q^n)$. Before giving the definition of a σ-quadric, we prove the following:

Proposition 3.2.1. *Let $\Gamma : X_t A X^\sigma = 0$ be a σ-quadric of $\mathrm{PG}(d, q^n)$ and let $L = V^\perp$. For every point $Y \in L$, the set $Y^\top \cap \Gamma$ is union of lines through Y.*

Proof. Let Y be a point of L, then $Y_t A = 0$. Consider the intersection of the set $Y^\top : X_t A Y^\sigma = 0$ with Γ. Let Z be a point of $Y^\top$, the line YZ has equations: $X = \lambda Y + \mu Z, (\lambda, \mu) \in \mathrm{PG}(1, q^n)$, hence $Y^\top : X_t A Y^\sigma = 0$ is determined by the solutions in (λ, μ) of the following equation:

$$Y_t A Y^\sigma \lambda^{\sigma+1} + Y_t A Z^\sigma \lambda \mu^\sigma + Z_t A Y^\sigma \lambda^\sigma \mu + Z_t A Z^\sigma \mu^{\sigma+1} = 0. \tag{3.1}$$

In the previous equation it is $Y_tAY^\sigma = 0$, since $Y \in \Gamma$, $Z_tAY^\sigma = 0$, since $Z \in Y^\top$, $Y_tAZ^\sigma = 0$, since $Y \in L$. Hence the Equation 3.1 becomes $Z_tAZ^\sigma\mu^{\sigma+1} = 0$, it follows that the solutions in (λ, μ) of the Equation 3.1 can be either all the possible $(\lambda, \mu) \in \mathrm{PG}(1, q^n)$, if $Z \in \Gamma$, and in this case the line YZ is contained in Γ or $\mu = 0$, that is $(\lambda, 0)$, $\lambda \in \mathbb{F}_{q^n}$ and in this case the line YZ intersects Γ exactly in the point Y. □

Inspired by the characterization of non-degenerate quadrics, non-degenerate symplectic polar spaces and non-degenerate Hermitian varieties of $\mathrm{PG}(d, q^n)$ (see Proposition 1.7.6), we give the following definitions:

Definition 3.2.2. We define a non-degenerate σ-quadric of $\mathrm{PG}(d, q^n)$ by induction on the dimension d of the projective space. Let Γ be a σ-quadric of $\mathrm{PG}(d, q^n)$, denote by L and R the left and right radicals of the associated sesquilinear form.

i) Γ is a *non-degenerate* σ-quadric of $\mathrm{PG}(1, q^n)$ if $|\Gamma| \in \{0, 2, q + 1\}$.

ii) Γ is a *non-degenerate* σ-conic of $\mathrm{PG}(2, q^n)$, if it satisfies the following properties:

- $L \cap R = \emptyset$,
- the tangent line $L^\top$ to Γ intersects Γ exactly at the point L.

iii) Γ is *non-degenerate* σ-quadric of $\mathrm{PG}(d, q^n), d \geq 3$, if it satisfies the following properties:

- $L \cap R = \emptyset$,
- $\forall\ Y \in L$, the set $Y^\top \cap \Gamma$ is a cone $\Gamma(Y, Q)$, where Q is a non-degenerate σ-quadric in a subspace S, of dimension $d - 2$, not through Y.

Remark 3.2.3. Because of the previous definition we can divide σ-conics in two families:

- the degenerate σ-conics: a cone with vertex a point V projecting either the empty set or a point or two points or $q + 1$ points on a line ℓ not through the point V, and also the degenerate C_F^m-sets,
- the non-degenerate σ-conics: the Kestenband σ-conics and the C_F^m-sets.

In the remaining part of this chapter we will determine the canonical equations and some properties for the σ-quadrics of $\mathrm{PG}(3, q^n)$ whose associated non-reflexive sesquilinear form of $\mathbb{F}_{q^n}^4$ is degenerate; hence if Γ denotes such a σ-quadric it will have equation $X_tAX^\sigma = 0$ with A a singular matrix. We consider three separate cases according to $\mathrm{rank}(A) \in \{1,2,3\}$.

3.3 σ-quadrics of rank 3 in $\mathrm{PG}(3,q^n)$

Let $\Gamma : X_tAX^\sigma = 0$ be a σ-quadric of $\mathrm{PG}(3,q^n)$. In this section we assume throughout that $\mathrm{rank}(A) = 3$. Therefore the radicals $V^\perp$ and $V^\top$ are one-dimensional vector subspace spaces of V, so they are points of $\mathrm{PG}(3,q^n)$. We distinguish several cases:

1) $V^\perp \neq V^\top$.

We may assume w.l.o.g. that the point $R = (1,0,0,0)$ is the right radical and the point $L = (0,0,0,1)$ is the left radical. It follows that

$$A = \begin{pmatrix} 0 & a_{12} & a_{13} & a_{14} \\ 0 & a_{22} & a_{23} & a_{24} \\ 0 & a_{32} & a_{33} & a_{34} \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

and

$$\Gamma : (a_{12}x_1+a_{22}x_2+a_{32}x_3)x_2^\sigma+(a_{13}x_1+a_{23}x_2+a_{33}x_3)x_3^\sigma+(a_{14}x_1+a_{24}x_2+a_{34}x_3)x_4^\sigma = 0.$$

The sesquilinear form induces a degenerate collineation

$$\top : Y \in \mathrm{PG}(3,q^n) \setminus R \mapsto X_tAY^\sigma = 0 \in \mathrm{PG}(3,q^n)^*$$

that maps points into planes through the point L. Points that are on a common line through R are mapped into the same plane through L. Therefore $\top$ induces a collineation $\Phi : \mathcal{S}_R \longrightarrow \mathcal{S}_L^*$. Let

$$\mathcal{S}_R = \{\ell_{\alpha,\beta,\gamma} : (\alpha,\beta,\gamma) \in \mathrm{PG}(2,q^n)\}, \text{where}$$

$$\ell_{\alpha,\beta,\gamma} : \begin{cases} x_1 &= \lambda \\ x_2 &= \mu\alpha \\ x_3 &= \mu\beta \\ x_4 &= \mu\gamma \end{cases}, (\lambda,\mu) \in \mathrm{PG}(1,q^n)$$

and

$$\mathcal{S}_L^* = \{\pi_{\alpha',\beta',\gamma'} : (\alpha',\beta',\gamma') \in \mathrm{PG}(2,q^n)\}, \text{where } \pi_{\alpha',\beta',\gamma'} : \alpha' x_1 + \beta' x_2 + \gamma' x_3 = 0.$$

The collineation Φ is given by $\Phi(\ell_{\alpha,\beta,\gamma}) = \pi_{\alpha',\beta',\gamma'}$, with

$$(\alpha', \beta', \gamma')_t = A'(\alpha, \beta, \gamma)_t^\sigma,$$

where A' is the matrix obtained by A by deleting the last row and the first column. Note that $|A'| \neq 0$ since $\mathrm{rank}(A) = 3$. It is easy to see that Γ is the set of points of intersection of corresponding elements under the collineation Φ.
Let $Y = (y_1, y_2, y_3, y_4)$ be a point of $\Gamma \setminus \{R\}$, then the tangent plane π_Y to Γ at the point Y is the plane $\pi_Y = Y^\top$ with equation $X_t A Y^\sigma = 0$. It follows that, for every point Y of $\Gamma \setminus \{R\}$ the plane π_Y contains the point $L = (0, 0, 0, 1)$. The tangent plane $\pi_L = L^\top$ to Γ at the point L is the plane with equation $X_t A L^\sigma = 0$, that is:

$$\pi_L : a_{14}x_1 + a_{24}x_2 + a_{34}x_3 = 0.$$

We again distinguish some cases.

- First assume that π_L contains the line RL.
It follows that, w.l.o.g., we may put $\pi_L : x_3 = 0$. Then $a_{14} = a_{24} = 0$ and we can put $a_{34} = 1$ obtaining

$$\Gamma : (a_{12}x_1 + a_{22}x_2 + a_{32}x_3)x_2^\sigma + (a_{13}x_1 + a_{23}x_2 + a_{33}x_3)x_3^\sigma + x_3x_4^\sigma = 0.$$

With this assumption, the collineation Φ maps the line LR into the plane π_L. Consider now the pencil $\mathcal{P}_{R,\pi_L}$ of lines through R in π_L. We distinguish two cases.

i) Φ maps the lines of $\mathcal{P}_{R,\pi_L}$ into the planes through the line RL.
In this case, we can assume that Φ maps the line $x_3 = x_4 = 0$ into the plane $x_2 = 0$ and the line $x_2 = x_4 = 0$ into the plane $x_1 = 0$ obtaining

$$\Gamma : ax_1x_3^\sigma + bx_2^{\sigma+1} + x_3x_4^\sigma = 0.$$

We can assume that Γ contains the points $(0, 1, -1, 1)$ and $(1, 0, 1 - 1)$ obtaining $a = b = 1$ and hence a canonical equation in this case is given by

$$\Gamma : x_1x_3^\sigma + x_2^{\sigma+1} + x_3x_4^\sigma = 0.$$

Note that in this case Γ is the set of points studied in [40], where Γ has been called a σ-cone. In this paper we call this set a degenerate *parabolic σ-quadric* with *collinear vertex points* R and L.
In [40] it has been proved that the following holds:

Theorem 3.3.1. *Let Γ be a degenerate parabolic σ-quadric Γ of $\mathrm{PG}(3, q^n)$ with collinear vertex points R and L. Then $|\Gamma| = q^{2n} + q^n + 1$, RL is the unique line contained in Γ and π_L is the unique plane that meets Γ exactly in RL.*

ii) Φ does not map the lines of $\mathcal{P}_{R,\pi_L}$ into the planes through the line RL.
In this case, there exists a plane π containing RL such that the lines of the pencil $\mathcal{P}_{R,\pi}$ are mapped, under Φ into the planes through RL. Hence there is a unique line through R (beside RL) contained in Γ. In this case we may assume that Φ maps the line $x_3 = x_4 = 0$ into the plane $x_1 = 0$ and the line $x_2 = x_4 = 0$ into the plane $x_2 = 0$. Hence:

$$\Gamma : ax_1x_2^\sigma + bx_2x_3^\sigma + x_3x_4^\sigma = 0.$$

Assuming that Γ contains the points $(0, 1, 1, -1)$ and $(1, 1, -1, 0)$ we get $a = b = 1$ and hence a canonical equation in this case is given by

$$\Gamma : x_1x_2^\sigma + x_2x_3^\sigma + x_3x_4^\sigma = 0.$$

We will call this set a *hyperbolic σ-quadric* with *collinear vertex points R* and L.

Theorem 3.3.2. *Let Γ be a hyperbolic σ-quadric of $\mathrm{PG}(3, q^n)$ with collinear vertex points R and L. Then $|\Gamma| = (q^n + 1)^2$ and Γ contains exactly three lines: the line RL, a unique other line through R and a unique other line through L.*

- π_L does not contain the lines RL (or equivalently that Φ does not map the line RL into a plane through the line RL).
W.l.o.g. we may put $\pi_L : x_1 = 0$. In this case there is a plane through R (not containing L), say π_R, such that the pencil of lines through R in π_R is mapped, under Φ, into the pencil of planes through RL. We may assume that $\pi_R : x_4 = 0$. Hence Φ maps the lines $\ell_{\alpha,\beta,0}$ into the planes $\pi_{0,\beta',\gamma'}$ so we may assume that Φ maps the line $\ell_{1,0,0}$ into the plane $\pi_{0,1,0}$ and the line $\ell_{0,1,0}$ into the plane $\pi_{0,0,1}$. Hence the points of Γ satisfy the equation

$$ax_2^{\sigma+1} - bx_3^{\sigma+1} + x_1x_4^\sigma = 0.$$

Assuming, w.l.o.g., that the point $(1, 1, 0, -1)$ belongs to Γ we obtain $a = 1$. The number of lines through R contained in Γ depends on the number of solutions of the equation $x^{\sigma+1} = b$ and hence it is either $0, 1, 2$ or $q + 1$ depending upon q even or odd and n even or odd. We distinguish several case:

  - If q is even and n is even, then there are either 0 or 1 or $q + 1$ solutions giving either 0 or 1 or $q + 1$ lines through R (and hence through L) contained in Γ.
  - If q is even and n is odd, then there is a unique solution of the equation giving one line through R and one line through L contained in Γ.
  - If q is odd and n is even, then there are either 0 or $q + 1$ solutions of the equation giving either 0 or $q + 1$ lines through R (and through L) contained in Γ.

- If q is odd and n is odd, then there are either 0 or 2 solutions of the equation giving either 0 or 2 lines through R (and through L) contained in Γ.

In these cases we will call the set Γ either an *elliptic* or a *parabolic* or a *hyperbolic* or a $(q+1)$-*hyperbolic* σ-quadric with vertex points R and L according to the number of lines through R contained in Γ is either 0 or 1 or 2 or $q+1$. If q is even and n is even put $r=(q^n-1,q^m+1)$.

Theorem 3.3.3. *Let Γ be an elliptic σ-quadric of $\mathrm{PG}(3,q^n)$ with vertex points R and L. Then Γ has canonical equation $x_2^{\sigma+1}-bx_3^{\sigma+1}+x_1x_4^{\sigma}=0$, with b a non-square if q is odd and $b^{(q^n-1)/r}\neq 1$ if q is even and n is even. $|\Gamma|=q^{2n}+1$ and Γ contains no line.*

Theorem 3.3.4. *Let Γ be a parabolic σ-quadric of $\mathrm{PG}(3,q^n)$ with vertex points R and L. Then q is even and Γ has canonical equation $x_2^{\sigma+1}-bx_3^{\sigma+1}+x_1x_4^{\sigma}=0$, where the equation $x^{\sigma+1}=b$ has a unique solution. Moreover $|\Gamma|=q^{2n}+q^n+1$ and Γ contains a unique line through R and a unique line through L.*

Theorem 3.3.5. *Let Γ be a hyperbolic σ-quadric of $\mathrm{PG}(3,q^n)$ with vertex points R and L. Then q and n are odd and Γ has canonical equation $x_2^{\sigma+1}-bx_3^{\sigma+1}+x_1x_4^{\sigma}=0$, where $x^{\sigma+1}=b$ has exactly two solutions. Moreover $|\Gamma|=q^{2n}+2q^n+1$ and Γ contains exactly two lines through R and exactly two lines through L.*

Theorem 3.3.6. *Let Γ be a $(q+1)$-hyperbolic σ-quadric of $\mathrm{PG}(3,q^n)$ with vertex points R and L. Then n is even and Γ has canonical equiation $x_2^{\sigma+1}-bx_3^{\sigma+1}+x_1x_4^{\sigma}=0$, $x^{\sigma+1}=b$ has exactly $q+1$ solutions. Moreover $|\Gamma|=q^{2n}+(q+1)q^n+1$ and Γ contains exactly $q+1$ lines through R and exactly $q+1$ lines through L.*

2) $V^{\perp}=V^{\top}$.
We may assume w.l.o.g. that the point $R=L=(1,0,0,0)$ is both the left radical and the right radical. It follows that, in this case, Γ is a cone with vertex the point R. Since the matrix A has rank three with first column and first row equal to 0, by choosing a plane not through the point R, e.g. $\pi : x_1=0$, we get that the set $\Gamma\cap\pi$ is a σ-conic of the plane π with associated matrix of rank 3. Hence it is a Kestenband σ-conic of π. It follows that Γ is a cone with vertex the point R projecting a Kestenband σ-conic in a plane not through R. In particular if $n=2$ and $\sigma^2=1$, then Γ is a Hermitian cone with vertex the point R.

3.4 σ-quadrics of rank 2 in $\mathrm{PG}(3,q^n)$

In this section a σ-quadric Γ of $\mathrm{PG}(3,q^n)$ will have equation $X_tAX^{\sigma}=0$ with $\mathrm{rank}(A)=2$. It follows that the left and right radicals are two lines r and ℓ of $\mathrm{PG}(3,q^n)$. We distinguish three cases.

1) $r \cap \ell = \emptyset$.
We may assume w.l.o.g. that $r : x_3 = x_4 = 0$ and $\ell : x_1 = x_2 = 0$. Then:

$$\Gamma : (a_{13}x_1 + a_{23}x_2)x_3^\sigma + (a_{14}x_1 + a_{24}x_2)x_4^\sigma = 0,$$

that is the set of points of $\mathrm{PG}(3,q^n)$ of intersection of corresponding planes under a collineation $\Phi : \mathcal{P}_r \longrightarrow \mathcal{P}_\ell$, where

$$\mathcal{P}_r = \{\pi_{a,b} : ax_3{+}bx_4 = 0\}_{\{(a,b)\in\mathrm{PG}(1,q^n)\}}, \mathcal{P}_\ell = \{\pi'_{a,b} : ax_1{+}bx_2 = 0\}_{\{(a,b)\in\mathrm{PG}(1,q^n)\}}.$$

The set Γ contains the q^n+1 lines of a pseudoregulus with transversal lines r and ℓ. We call this set a *σ-quadric of pseudoregulus type with skew vertex lines* r and ℓ. Note that if $n = 2$, $\sigma^2 = 1$, σ-quadrics of pseudoregulus type with skew vertex line have been introduced and studied in [36] where they were called Q_F-sets.
Let $r : x_1 = 0, x_2 = 0$, $\ell : x_3 = 0, x_4 = 0$ and let $\Phi : \mathcal{P}_r \longrightarrow \mathcal{P}_s$ be a collineation with accompanying authomorphism $\sigma : x \mapsto x^{q^m}$, with $(m,n) = 1$.
Suppose that :

$$\Phi(\pi_{1,0}) = \pi'_{1,0}, \Phi(\pi_{0,1}) = \pi'_{0,1}, \Phi(\pi_{1,1}) = \pi'_{1,1},$$

then $\Phi(\pi_{a,b}) = \pi'_{a^\sigma,b^\sigma}$.
Hence the set $\mathcal{Q}$ of points of intersection of corresponding planes under Φ is given by the points whose homogeneous coordinates are solutions of the linear system

$$\begin{cases} ax_3 + bx_4 & = & 0 \\ a^\sigma x_1 + b^\sigma x_2 & = & 0, \end{cases}$$

where $(a,b) \in \mathrm{PG}(1,q^n)$. This system is equivalent to the linear system

$$\begin{cases} ax_3 + bx_4 & = & 0 \\ ax_1^{\sigma^{-1}} + bx_2^{\sigma^{-1}} & = & 0. \end{cases}$$

A point $P = (x_1,x_2,x_3,x_4)$ belongs to $\mathcal{Q}$ if and only if the previous linear system in the unknowns a and b has non-trivial solutions, hence if and only if $x_1^{\sigma^{-1}}x_4 - x_2^{\sigma^{-1}}x_3 = 0$, that is the same as $x_1x_4^\sigma - x_2x_3^\sigma = 0$, that can be seen as a canonical equation of a σ-quadric of pseudoregulus type with skew vertex lines. Let $c \in \mathbb{F}_q^*$ and let $\gamma \in \mathbb{F}_{q^n}^*$ be such that $N(\gamma) = c$. Put

$$\mathcal{Q}_c = \{(\gamma x^\sigma, \gamma y^\sigma, x, y)\}_{(x,y)\in\mathrm{PG}(1,q^n)}.$$

The set $\mathcal{Q}_c$ is a maximum scattered linear set of rank $2n$ of $\mathrm{PG}(3,q^n)$ of pseudoregulus type with transversal lines r and ℓ. Hence the set $\mathcal{Q}$ is the union of the skew lines r, ℓ and the $q-1$ linear sets of pseudoregulus type $\mathcal{Q}_c$, $c \in \mathbb{F}_{q^n}^*$.

The following hold.

Proposition 3.4.1. *let Γ be a σ-quadric of pseudoregulus type of $\mathrm{PG}(3, q^n)$ with skew transversal lines r and ℓ. The only lines contained in Γ are r, ℓ and the $q^n + 1$ lines of the pseudoregulus associated to Γ.*

Proposition 3.4.2. *Let a, b and c be three pairwise skew lines and let ℓ and s be two skew lines meeting a, b and c. There is a unique σ-quadric of pseudoregulus type of $\mathrm{PG}(3, q^n)$ with skew vertex lines r and ℓ containing a, b and c.*

Proposition 3.4.3. *Let Γ be a σ-quadric of pseudoregulus type of $\mathrm{PG}(3, q^n)$ with skew vertex lines r and ℓ. The set Γ is mapped, via the Klein correspondence, to the union of a translation ovoid of a hyperbolic quadric $\mathrm{Q}^+(3, q^n)$ with two points R and S.*

Proof. Let $r : x_1 = x_2 = 0$ and $\ell : x_3 = x_4 = 0$ and Γ be the σ-quadric with vertex lines ℓ and r with equation $x_1^\sigma x_4 - x_2^\sigma x_3 = 0$. The lines of the associated pseudoregulus are spanned by the points $(0, 0, \alpha, \beta)$ and $(c\alpha^\sigma, c\beta^\sigma, 0, 0)$, $(\alpha, \beta) \in \mathrm{PG}(1, q^n)$, $c \in \mathbb{F}_q^*$. Via the Klein correspondence the lines of the pseudoregulus are mapped to the set of points $\{(0, \alpha^{\sigma+1}, \alpha^\sigma\beta, \alpha\beta^\sigma, \beta^{\sigma+1}, 0)\}_{\{(\alpha,\beta)\in\mathrm{PG}(1,q^n)\}}$, i.e. the set of points of the ovoid

$$\mathcal{O} = \{(0, \alpha^{\sigma+1}, \alpha^\sigma, \alpha, 1, 0)\} \cup \{P_\infty = (0, 0, 0, 0, 1, 0)\}$$

of the hyperbolic quadric $\mathrm{Q}^+(3, q)$ with equations $x_1 = x_6 = 0, x_2x_5 - x_3x_4 = 0$ contained in the Klein quadric with equation $x_1x_6 - x_2x_5 + x_3x_4 = 0$. The two vertex lines r and ℓ are mapped, via the Klein correspondence, to the two points $(0, 0, 0, 0, 0, 1)$ and $(1, 0, 0, 0, 0, 0)$ on the line $x_2 = x_3 = x_4 = x_5 = 0$ that is the polar lines w.r.t. the three dimensional subspace with equations $x_1 = x_6 = 0$ containing the ovoid $\mathcal{O}$ under the polarity defined by the Klein quadric.
The ovoid $\mathcal{O}$ is a translation ovoid w.r.t. the point P_∞ of the hyperbolic quadric $\mathrm{Q}^+(3, q)$ since the group of projectivities of $\mathrm{PG}(5, q^n)$ induced by the matrices

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & b & 1 & 0 & 0 & 0 \\ 0 & b^\sigma & 0 & 1 & 0 & 0 \\ 0 & b^{\sigma+1} & b^\sigma & b & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$b \in \mathbb{F}_{q^n}$, stabilizes P_∞ and acts sharply transitively on the points of $\mathcal{O} \setminus \{P_\infty\}$. □

2) $r \cap \ell = V$ is a point. We may assume w.l.o.g. that $r : x_3 = x_4 = 0, \ell : x_2 = x_3 = 0$. In this case the σ-quadric Γ is a cone with vertex a point $V = r \cap \ell$ projecting a (degenerate or not) C_F^m-set in a plane not through V. Indeed let π be a plane not through the point V and let $R = r \cap \pi$, $L = \ell \cap \pi$. It follows that $\Gamma \cap \pi$ is a set of points of π generated by a collineation between the pencils of lines of π with center the points R and L induced by the collineation between the pencil of planes $\mathcal{P}_r$ and $\mathcal{P}_\ell$ that is associated to Γ.

3) $r = \ell$.
We may assume w.l.o.g. that $r = \ell : x_3 = x_4 = 0$. In this case the σ-quadric is a cone with vertex the line r over a σ-quadric of a line skew with r. That is Γ is either just the line r or a plane through r or a pair of distinct planes through r or $q + 1$ planes through r forming an $\mathbb{F}_q$-subpencil of planes through r.

3.5 σ-quadrics of rank 1 in $\mathrm{PG}(3, q^n)$

In this section the σ-quadric Γ has equation $X_t A X^\sigma = 0$ with $\mathrm{rank}(A) = 1$. Hence $\mathrm{dim} V^\perp = \mathrm{dim}\ V^\top = 3$ so left and righ-radicals in $\mathrm{PG}(3, q^n)$ are planes. We distinguish two cases:

- $V^\perp \neq V^\top$.
  We may assume that $r : x_4 = 0$ is the right-radical and $\ell : x_1 = 0$ is the left-radical. Hence $\Gamma : x_1 x_4^\sigma = 0$, that is the union of two different planes.

- $V^\perp = V^\top$.
  We may assume $r = \ell : x_4 = 0$ is both the left- and right- radical. Hence $\Gamma : x_4^{\sigma+1} = 0$, that it is a plane of $\mathrm{PG}(3, q^n)$.

3.6 σ-quadrics of $\mathrm{PG}(3, q^n)$ with $|A| = 0$

In this section we summarize the results obtained in the previous sections of this chapter.

Proposition 3.6.1. *Let $\Gamma : X_t A X^\sigma = 0$ be a σ-quadric of $\mathrm{PG}(3, q^n)$, whose associated sesquilinear form is degenerate, then Γ is one of the following:*

- *a cone with vertex a line v projecting a σ-quadric of a line ℓ skew with v (hence either just the line v or one, two or $q + 1$ planes through v),*

- *a cone with vertex a point V projecting either a a Kestenband σ-conic or a (possibly degenerate) C_F^m-set of a plane π, with $V \notin \pi$,*

- *a degenerate either parabolic or hyperbolic σ-quadric with two collinear vertex points R and L,*

- *a non-degenerate either elliptic or parabolic or hyperbolic or $(q + 1)$-hyperbolic σ-quadric with two vertex points R and L,*

- *a non-degenerate σ-quadric with two skew vertex lines (i.e. a σ-quadric of pseudoregulus type).*

Remark 3.6.2. Note that if $n=2$ and $\sigma^2=1$, then σ-quadrics of $\mathrm{PG}(3,q^2)$ in the first and second point of the list in the previous proposition are respectively a cone with vertex a line projecting an $\mathbb{F}_q$-subline and a cone with vertex a point projecting a Hermitian curve.

Let $\sigma : x \mapsto x^{q^m}$, $\sigma' : x \mapsto x^{q^{m'}}$, $(m,n)=(m',n)=1, m, m' \leq n/2$.

Proposition 3.6.3. *Let $\Gamma : X_tAX^\sigma = 0$ be a σ-quadric and let $\Gamma' : X_tA'X^{\sigma'}$ be a σ'-quadric of $\mathrm{PG}(3,q^n)$. Then Γ and Γ' are projectively equivalent if and only if $m=m'$ and Γ, Γ' are of the same type.*

3.7 σ-quadrics of rank 4 of $\mathrm{PG}(3,q^n)$

Remark 3.7.1. Opposite to the case of $\mathrm{PG}(2,q^n)$, nothing is known for the sets of absolute points in $\mathrm{PG}(3,q^n)$ of a non-degenerate, non-reflexive sesquilinear form of $\mathbb{F}_{q^n}^4$. Of course the set of points with equation

$$\Gamma : x_1^{\sigma+1} + x_2^{\sigma+1} + x_3^{\sigma+1} + x_4^{\sigma+1} = 0$$

is a remarkable example of such a set giving as intersection in a subgeometry $\mathrm{PG}(3,q)$ the quadric with equation

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = 0$$

and, if n is even as intersection in a subgeometry $\mathrm{PG}(3,q^2)$ the non-degenerate Hermitian curve with equation

$$x_1^{q+1} + x_2^{q+1} + x_3^{q+1} + x_4^{q+1} = 0$$

.

3.8 Degenerate σ-quadrics and Lüneburg spread of $\mathrm{PG}(3,2^n)$.

The affine set arising from the Lüneburg spread has been studied by A. Cossidente, G. Marino and O. Polverino in [29], where the following result has been obtained:

Theorem 3.8.1. *The affine set $\mathcal{A}$ of the Lüneburg spread of* $\mathrm{PG}(3,2^{2h+1})$*, is the union* 2^{2h+1}*-arcs, each of them can be completed to a translation hyperoval. The directions of $\mathcal{A}$ on π_∞ are the complement of a regular hyperoval.*

With the following theorem we observe that the affine set of a Lüneburg spread of $\mathrm{PG}(3,2^{2h+1})$ is the affine part of a degenerate elliptic σ-quadric of $\mathrm{PG}(3,2^{2h+1})$ with two vertex points.

Theorem 3.8.2. *Let Γ be a degenerate parabolic σ-quadric of* $\mathrm{PG}(3,2^n)$ *with collinear vertex points R and L. The lines joining any two points of $\Gamma \setminus RL$ are disjoint from a translation hyperoval $\mathcal{O}_\infty$ of the plane π_L, projectively equivalent to the set $\{(0,t,t^{\sigma^{-2}},1) : t \in \mathbb{F}_{2^n}\} \cup \{R,L\}$.*
If $n = 2h+1$ and σ is the automorphism of $\mathbb{F}_{2^n}$ given by $\sigma : x \mapsto x^{2^h}$, then $\mathcal{O}_\infty$ is a regular hyperoval. Hence the set $\Gamma \setminus RL$ is the affine set of the Lüneburg spread of $\mathrm{PG}(3,q^n)$.

Proof. Let Γ be a degenerate parabolic σ-quadric with collinear vertex points $R = (0,0,1,0)$ and $L = (0,1,0,0)$ with equation

$$x_4{}^{\sigma+1} + x_1 x_2^{\sigma} - x_3 x_1{}^{\sigma} = 0.$$

It follows that the plane π_{RL} has equation $x_1 = 0$. The set $\mathcal{A} = \mathcal{K} \setminus \pi_{RL}$ is given by $\mathcal{A} = \{(1,x,x^{\sigma}+y^{\sigma+1},y) : x,y \in \mathbb{F}_{q^n}\}$. Arguing as in Proposition 5.2 in [29], we obtain that the set of directions determined by $\mathcal{A}$ into the plane π_{RL} covers all the points of π_{RL} except to the points of a hyperoval $\mathcal{C}$ given by $\mathcal{C} = \{(0,x,x^{\sigma^{-2}},1) : x \in \mathbb{F}_{q^n}^*\}$. Note that if $q = 2^{2h+1}$ and $\sigma : x \mapsto x^{2^h}$, then the hyperoval $\mathcal{C}$ is a hyperconic. The assertion follows (see Section 3.8). □

3.9 Problems

- Is there any other interesting subset $\mathcal{S}$ of $\mathrm{PG}(3,q^n)$ s.t. $\mathcal{S}$ is either a σ-quadric or a remarkable subset of a σ-quadric?
- Is there any interesting subset $\mathcal{S}$ of $\mathrm{PG}(d,q^n)$, $d \geq 4$, s.t. $\mathcal{S}$ is either a σ-quadric or a remarkable subset of a σ-quadric?

  [Hint: There is at least another examples in the these notes.]

References

[1] J. André, Uber nich-Desarguessche Ebenen mit transitiver Translationsgruppe. *Math. Z.* 60, (1954) 156-186.

[2] L. Bader, G. Lunardon, I. Pinneri, A new semifield flock. *J. Combin. Theory Ser. A* 86 (1999) 49-62.

[3] R. Baer, Linear Algebra and Projective Geometry. (2005) [first published 1952].

[4] B. Bagchi, N.S. Narasimha Sastry, Even order inversive planes, generalized quadrangles and codes. *Geom. Dedicata* 22 (1987), 137–147.

[5] S. Ball, On ovoids of $O(5, q)$. *Adv. Geom.* 4 (2004), no. 1, 1–7.

[6] S. Ball, Simeon, Finite Geometry and Combinatorial Applications. London Mathematical Society Student Texts, Cambridge University Press, 2015.

[7] S. Barwick, G. Ebert, Unitals in Projective Planes. New York, Springer, 2008.

[8] A. Beutelspacher, U.Rosenbaum, Projective geometry: from foundations to applications. Cambridge University Press, 1998.

[9] A.W. Bluher, On $x^{q+1} + ax + b$. *Finite Fields and Their Applications* 10 (2004) 285-305.

[10] A. Blokhuis, M. Lavraw, Scattered spaces with respect to a spread in $\mathrm{PG}(n, q)$. *Geom. Dedicata* 81 (1– 3), (2000) 231–243.

[11] R.H. Bruck, Circle geometry in higher dimensions. In A Survey of Combinatorial Theory, J. N. Srivastava, et al, Eds., Chap. 6, pp. 69–77, North Holland, Amsterdam, 1973.

[12] R.H. Bruck, Circle geometry in higher dimensions II. *Geom. Dedicata* 2 (1973) 133–188.

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

[14] A.A. Bruen, Baer subplanes and blocking sets. *Bull. Amer. Math. Soc.* 76 (2), (1970) 342-344.

[15] A.A. Bruen, J.A. Thas, Blocking sets. *Geom. Dedicata* 6 (2), (1977) 193–203.

[16] F. Buekenhout, Ensembles Quadratiques des Espace Projective. *Math. Teitschr.* 110 (1969) 306-318.

[17] F. Buekenhout, ed., Handbook of incidence geometry, Buildings and foundations, North-Holland, Amsterdam, 1995.

[18] F. Buekenhout, Prehistory and History of Polar Spaces and of Generalized Polygons, Socrates Intensive Course Finite Geometry and its Applications Gent,. April 3-14 2000.

[19] F. Buekenhout, A.M. Cohen, Diagram Geometry (Related to classical groups and buildings), A Series of Modern Surveys in Mathematics, part 3, 57, Heidelberg: Springer, (2013).

[20] F. Buekenhout, Francis. E. Shult, On the foundations of polar geometry. *Geom. Dedicata* 3 (1974), 155–170.

[21] P.J. Cameron, Projective and polar spaces, University of London. *Queen Mary and Westfield College*, 1992.

[22] W. Cherowitzo, Hyperovals in Desarguesian planes of even order. *Ann. Discrete Math.*, 37 (1988) 87–94.

[23] W. Cherowitzo, Hyperovals in Desarguesian planes: an update. *Discrete Math.*, 155 (1–3) (1996) 31–38.

[24] W. Cherowitzo, α-flocks and hyperovals. *Geom. Dedicata*, 72 (3) (1998) 221–246.

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

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

[27] B.N. Cooperstein, External flats to varieties in $\mathrm{PG}(M_{n,n}(\mathrm{GF}(q)))$. *Linear Algebra Appl.* 267 (1997), 175–186.

[28] A. Cossidente, G. Marino, F. Pavese, Non-linear maximum rank distance codes. *Des. Codes Cryptogr.*, 79 (3) (2016), 597-609.

[29] A. Cossidente, G. Marino, O. Polverino, Affine sets arising from spreads.*Innov. Incidence Geom*. 6-7 (1), (2007) 127-138.

[30] H.S.M. Coxeter, Projective geometry, Toronto, Ont. *University of Toronto Press*, 1969.

[31] J. De Beule, A. Klein, K. Metsch, Substructures of finite classical polar spaces, In book: Current research topics in Galois geometry, NOVA Sci. Publ. Editors: Jan De Beule, Leo Storme, 2012.

[32] Ph. Delsarte, Bilinear forms over a finite field, with applications to coding theory. *J. Combin. Theory Ser. A* 25 (1978), 226–241.

[33] P. Dembowki, Finite geometries, Berlin, Heidelberg, New York: Springer-Verlag, 1997 (reprint of the 1968 edition).

[34] G. Donati, N. Durante, Some subsets of the Hermitian curve. *European J. of Combinatorics* 24, no. 2, (2003) 211–218.

[35] G. Donati, N. Durante, Baer subplanes generated by collineations between pencils of lines. *Rendiconti del Circolo Matematico di Palermo*. Serie II. Tomo LIV, (2005) 93–100.

[36] G. Donati, N. Durante, A subset of the Hermitian surface. *Innovations in Incidence Geometry* 3,(2006) 13–23.

[37] G. Donati, N. Durante, On the intersection of two subgeometries of $\mathrm{PG}(n, q)$. *Designs, Codes and Cryptography* 46 (3), (2008) 261–267.

[38] G. Donati, N. Durante, Scattered linear sets generated by collineations between pencils of lines. *J. Algebraic Combin.* 40 (4), (2014) 1121–1134.

[39] G. Donati, N. Durante, A generalization of the normal rational curve in $\mathrm{PG}(d, q^n)$ and its associated non-linear MRD codes. *Des. Codes Cryptogr.* 86 (2018), no. 6, 1175–1184.

[40] G. Donati, N. Durante, A generalization of the quadratic cone of $\mathrm{PG}(3, q^n)$ and its relation with the affine set of the Lüneburg spread, *J. of Algebraic Combinatorics*, 49 (2), (2019) 169–177.

[41] N. Durante, A. Siciliano, Non-linear maximum rank distance codes in the cyclic model fro the field reduction of finite geometries. *Electron. J. Combin.* 24 no. 2 (2017), Paper 2.33, 18 pp.

[42] J.W. Freeman, Reguli and pseudo-reguli in $\mathrm{PG}(3, s^2)$. *Geom. Dedic.* 9, (1980) 267–280.

[43] E.M. Gabidulin, Theory of codes with maximum rank distance. *Problemy Peredachi Informatsii* 21 (1985), no. 1, 3–16.

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

[45] D.G. Glynn, Two new sequences of ovals in finite Desarguesian planes of even order. (Combinatorial mathematics, X) Lecture Notes in Math., 1036, Berlin: Springer, pp. 217–229, 1983.

[46] K.W.Gruenberg, A.J. Weir, Linear Geometry. Graduate Texts in Mathematics, 49 (1st ed.), Springer-Verlag New York, 1977.

[47] G. Hanssens, A characterization of buildings of a spherical type. *European J. Combin.* 7 (1986), no. 4, 333–347.

[48] T. Helleseth, A. Kholosha, $x^{2^l+1} + x + a$ and related affine polynomials over $\mathrm{GF}(2^k)$. *Cryptogr. Commun.* 2 (2010), 85-109.

[49] J.W.P. Hirschfeld, J.A. Thas, General Galois geometries. Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, 1991. Oxford Science Publications.

[50] D.R. Hughes, F.C. Piper, Projective planes. Graduate Texts in Mathematics, Vol. 6. Springer-Verlag, New York-Berlin, 1973.

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

[52] B.C. Kestenband, Correlations whose squares are perspectivities. *Geom. Dedicata* 33 (1990), no. 3, 289–315.

[53] B.C. Kestenband, The correlations with identity companion automorphism, of finite Desarguesian planes. *Linear Algebra Appl.* 304 (2000), no. 1-3, 1–31.

[54] B.C. Kestenband, The correlations of finite Desarguesian planes. I. Generalities. *J. Geom.* 77 (2003), no. 1-2, 61–101.

[55] B.C. Kestenband, The correlations of finite Desarguesian planes of even nonsquare order. *JP J. Geom. Topol.* 5 (2005), no. 1, 1–62.

[56] B.C. Kestenband, The correlations of finite Desarguesian planes. II. The classification (I). *J. Geom.* 82 (2005), no. 1-2, 91–134.

[57] B.C. Kestenband, The correlations of finite Desarguesian planes. III. The classification (II). *J. Geom.* 83 (2005), no. 1-2, 88–120.

[58] B.C. Kestenband, The correlations of finite Desarguesian planes. IV. The classification (III). *J. Geom.* 86 (2006), no. 1-2, 98–139 (2007).

[59] B.C. Kestenband, The correlations of finite Desarguesian planes of square order defined by diagonal matrices. *Linear Algebra App*l. 423 (2007), no. 2-3, 366–385.

[60] B.C. Kestenband, Embedding finite projective geometries into finite projective planes. *Int. Electron. J. Geom.* 2 (2009), no. 2, 27–33.

[61] B.C. Kestenband, The correlations of finite Desarguesian planes of odd square order defined by upper triangular matrices with four nonzero entries. *JP J. Geom. Topol.* 10 (2010), no. 2, 113–170.

[62] B.C. Kestenband, The correlations of finite Desarguesian planes of even square order defined by upper triangular matrices with four nonzero entries. *JP J. Geom. Topol.* 16 (2014), no. 2, 127–152.

[63] A. Kshevetskiy, E. M. Gabidulin, The new construction of rank codes, Proc. IEEE Int. Symp. on Information Theory, pp. 2105-2108, 2005.

[64] T.Y. Lam, A first course in noncommutative rings, Graduate Texts in Mathematics. 131 (2 ed.) Springer. Springer, 2001.

[65] M. Lavrauw, Semifield flocks, eggs, and ovoids of $Q(4, q)$. *Adv. Geom.* 5 (2005), no. 3, 333–345.

[66] M. Lavrauw, G. Van de Voorde , On linear sets on a projective line. *Designs, Codes and Cryptography* 56 (2–3), (2010) 89–104.

[67] M. Lavrauw, G. Van de Voorde , Field reduction and linear sets in finite geometry, *Contemporary Mathematics. In Contemporary Mathematics* 632, (2015)271-293.

[68] M. Law, T. Penttila, Flocks, ovals and generalised quadrangles (Four Lectures in Napoli, June 2000), preprint n. 40 (2000), Dipartimento di Matematica e Applicazioni R. Caccioppoli – Universitá degli Studi di Napoli Federico II.

[69] H. Lenz, Zur Begründung der analytischen Geometrie. *Bayer. Akad. Wiss., math.-naturw. Klasse*, (1954) 17–72.

[70] R. Lidl, H. Niederreiter Finite Fields (2nd ed.), Cambridge University Press, 1997.

[71] G. Lunardon, Normal spreads. *Geom. Dedicata* 75 (3), (1999) 245-261.

[72] G. Lunardon, Flocks, ovoids of $Q(4, q)$ and designs. *Geom. Dedicata* 66 no. 2, (1997) 163–173.

[73] G. Lunardon, MRD-codes and linear sets. *J. Combin. Theory Ser. A* 149 (2017), 1–20.

[74] G. Lunardon, G. Marino, O. Polverino, R. Trombetti, Maximum scattered linear sets of pseudoregulus type and the Segre Variety $\mathcal{S}_{n,n}$. *J. Algebr. Comb.* 39, 807–831, 2014.

[75] G. Lunardon, O. Polverino, Translation ovoids of orthogonal polar spaces. *Forum-Math.* 16 (2004) 663–669.

[76] G. Lunardon, P. Polito, O. Polverino, A geometric characterization of linear k-blocking sets. J. of Geometry, 74 (1–2), (2002) 120–122.

[77] G. Lunardon, R. Trombetti, Y Zhou, Generalized Twisted Gabidulin Codes. *Journal of Combinatorial Theory Series A* 159 (2015) 79-106.

[78] H. Lüneburg: Die Suzukigruppen und ihre Geometrien. Springer-Verlag Berlin-New York (1965).

[79] F. Mazzocca, Note di Geometria Combinatoria, 2013.

[80] C.M. O'Keefe, T. Penttila, A new hyperoval in $\mathrm{PG}(2, 32)$. J. Geom., 44 (1–2), (1992) 117–139.

[81] S.E. Payne, A new infinite family of generalized quadrangles. *Congressus Numerantium* 49: (1985) 115–128.

[82] S.E. Payne, J.A. Thas, Finite generalized quadrangles. *Research Notes in Mathematics*, 110. Pitman (Advanced Publishing Program), Boston, MA, 1984.

[83] S.E. Payne, An essay on skew translation generalized quadrangles. *Geom. Dedicata* 32 (1989) 93–118.

[84] T. Penttila, B. Williams, Ovoids of parabolic spaces. *Geom. Dedicata* 82 (2000) 1–19.

[85] V. Pepe, On the agebraic variety $\mathcal{V}_{r,t}$. *Finite Fields and Their Applications* 17 (2011) 343–349.

[86] O. Polverino, Linear sets in finite projective spaces. *Discrete Math.* 310, (2010) 3096-3107.

[87] B. Qvist, Some remarks concerning curves of the second degree in a finite plane. *Ann. Acad. Sci. Fennicae. Ser. A. I. Math.-Phys.*, (134): 27, (1952).

[88] B. Segre, Ovals in a finite projective plane. *Canadian Journal of Mathematics*, 7 (10): (1995) 414–416.

[89] B. Segre, Ovali e curve σ nei piani di Galois di caratteristica due. *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat.* (8), 1962.

[90] B. Segre, Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane. *Ann. Mat. Pura Appl.* 64, (1964) 1-76.

[91] B. Segre, U. Bartocci, Ovali ed altre curve nei piani di Galois di caratteristica due. *Acta Arithmetica*, 18: (1971) 423–449.

[92] F. Seydewitz F, Lineäre Konstruktion einer Kurve doppelter Krümmung. *Arch. Math. Phys.* 10, (1847) 203–214.

[93] J. Sheekey, A new family of linear maximum rank distance codes. *Advances in Mathematics of Communications*, 10 (3) (2016) 475-488.

[94] J. Sheekey, MRD Codes: Constructions and Connections. Preprint arXiv:1904-05813v1 [math.CO] 11 Apr 2019.

[95] E.E. Shult, Points and lines. Characterizing the classical geometries. Universitext. Springer, Heidelberg, 2011.

[96] J. Steiner, Systematische Entwichlung der Abhä ngigkeit Geometrische Gestalten von einander. Reimer, Berlin (1832).

[97] J.A. Thas, Generalized quadrangles and flocks of cones. *European J. Combin.* 8 (1987) 441-452.

[98] Generalized quadrangles of order (s, s^2), II. *J. Combin. Theory Ser.* A, 79 (1997), pp. 223–254.

[99] J.A. Thas, S.E. Payne, Spreads and ovoids in finite generalized quadrangles. *Geom. Dedicata* 52 (1994), 227–253.

[100] J. Tits, Ovo´ides et groupes de Suzuki. *Arch. Math.* 13 (1962), 187–198.

[101] J. Tits, Buildings of spherical type and finite BN-pairs. Lecture Notes in Mathematics, Vol. 386. Springer-Verlag, Berlin-New York, 1974. x+299 pp.

[102] O. Veblen, J.W. Young, Projective Geometry, 2. vol., Ginn & Co. Boston, 1916.

[103] F.D. Veldkamp, Polar geometry. I, II, III, IV, V. Nederl. Akad. Wetensch. Proc. Ser. A 62; 63 = Indag. Math. 21 (1959), 512-551 22 (1959) 207–212. 50.30

Part III

Groups of finite projective spaces and their geometries

Francesco Pavese

Department of Mechanics, Mathematics and Management,
Polytechnic University of Bari,
Via Orabona 4, I-70125 Bari, Italy.

email: francesco.pavese@poliba.it

Contents

Preface

These lecture notes provide an introduction to the fascinating interplay between the theory of finite groups and their representations and the study of substructures of finite projective spaces. We will mainly be concerned with the investigation of certain subgroups of projectivities and the geometric objects that are left invariant by them.

In Chapter 1 the basic concepts and the geometric tools are outlined.

In Chapter 2, q–analogs of constant weight codes in the Johnson space are considered. The interest in these codes, known as *constant–dimension subspace codes*, has been increased in the last few years as a consequence of their new application in error–correction for random network coding. In this context, the main problem is to determine the largest possible size of constant–dimension codes with a given minimum distance. Here, we deal with the smallest open case; from a geometric point of view, it asks for the maximum number of planes in $\mathrm{PG}(5, q)$ mutually intersecting in at most one point.

In Chapter 3, we discuss *symmetric tactical decompositions* and *Cameron–Liebler line classes of* $\mathrm{PG}(3, q)$. These objects arose from the study of collineation groups of $\mathrm{PG}(3, q)$ having equally many orbits on points and lines of $\mathrm{PG}(3, q)$. The current status of research in this area is described.

Chapter 1

Basic concepts

In this section, we collect the definitions of the objects of study for the convenience of the reader, along with several standard results. Most of them will be stated without proof and we refer to [13, 19, 20, 21, 22, 26, 36] for more details.

1.1 Groups acting on sets

Let G be a finite group and let $\mathcal{X}$ be a non–empty set. An *action of G on $\mathcal{X}$* is a function

$$F : G \times \mathcal{X} \longrightarrow \mathcal{X},$$

where we write $F(g, x) = g(x)$ or $F(g, x) = x^g$, satisfying:

1) For all $g_1, g_2 \in G$ and $x \in X$, $g_1(g_2(x)) = (g_1g_2)(x)$ or equivalently $(x^{g_2})^{g_1} = x^{g_1g_2}$

2) For all $x \in X$, $1(x) = x$ or equivalently $x^1 = x$.

When the action F is understood, then the set $\mathcal{X}$ is said to be a G–set or G–invariant. It is also said that *G acts on $\mathcal{X}$*. Let $\mathcal{X}$ be a G–set and let $\mathcal{Y} \subseteq \mathcal{X}$. For an element $g \in G$, define

$$\mathcal{Y}^g = \{y^g \mid y \in \mathcal{Y}\}.$$

Note that if G acts on $\mathcal{X}$, then the map

$$F : (g, \mathcal{Y}) \in G \times 2^{|\mathcal{X}|} \longmapsto \mathcal{Y}^g \in 2^{|\mathcal{X}|}$$

canonically defines an action of G on the set of all subsets of $\mathcal{X}$.

The *stabilizer of $\mathcal{Y}$ in G* is the subgroup of G given by $\{g \in G \mid \mathcal{Y}^g = \mathcal{Y}\}$. It is denoted with $Stab_G(\mathcal{Y})$ or $G_{\mathcal{Y}}$. The *pointwise stabilizer of $\mathcal{Y}$ in G* is the subgroup of G given by $\{g \in G \mid y^g = y, \text{ for all } y \in \mathcal{Y}\}$.

The *orbit of $\mathcal{Y}$ under G* or the *G–orbit of $\mathcal{Y}$* is the set $\{\mathcal{Y}^g \mid \text{ for all } g \in G\}$ and it is denoted with $\mathcal{Y}^G$ or $Orb_G(\mathcal{Y})$. Thus $\mathcal{Y}^G \subseteq \mathcal{X}$.

Let $\mathcal{Y}_1, \mathcal{Y}_2 \subseteq \mathcal{X}$ and consider the following relation:

$$\mathcal{Y}_1 \sim \mathcal{Y}_2 \text{ if and only if } \mathcal{Y}_2 = \mathcal{Y}_1^g, \text{ for some } g \in G.$$

It can be seen that $\sim$ is an equivalence relation and hence two G–orbits are either disjoint or identical.

Theorem 1.1.1 (Orbit–Stabilizer Theorem). *Let $\mathcal{X}$ be a G–set and let $\mathcal{Y} \subseteq \mathcal{X}$. Then $|G| = |G_{\mathcal{Y}}||\mathcal{Y}^G|$.*

Proof. It is enough to prove that $|\mathcal{Y}^G| = |G : G_{\mathcal{Y}}|$. Indeed, we claim that

$$\mu : \mathcal{Y}^g \in \mathcal{Y}^G \longmapsto gG_{\mathcal{Y}} \in G/G_{\mathcal{Y}}$$

is a bijection between the elements of $\mathcal{Y}^G$ and the left cosets of $G_{\mathcal{Y}}$ in G. To see this fact let $\mathcal{Z}_1, \mathcal{Z}_2 \in \mathcal{Y}^G$. Then there exist two elements $g_1, g_2 \in G$ such that $\mathcal{Z}_1 = \mathcal{Y}_1^g$ and $\mathcal{Z}_2 = \mathcal{Y}^{g_2}$. Note that $\mathcal{Z}_1 = \mathcal{Z}_2$ if and only if $\mathcal{Y}^{g_1} = \mathcal{Y}^{g_2}$ if and only if $\mathcal{Y} = (\mathcal{Y}^{g_2})^{g_1^{-1}} = \mathcal{Y}^{g_1^{-1}g_2}$ if and only if $g_1^{-1}g_2 \in G_{\mathcal{Y}}$ if and only if $g_2 \in g_1G_{\mathcal{Y}}$ if and only if $g_1G_{\mathcal{Y}} = g_2G_{\mathcal{Y}}$. Therefore μ is an injective map. On the other hand, it is easily seen that μ is surjective. □

If G acts on $\mathcal{X}$ and $x^G = \mathcal{X}$ for some $x \in \mathcal{X}$, then we say that *G acts transitively on $\mathcal{X}$* or that *G is transitive on $\mathcal{X}$*.

1.2 Tactical configurations

Let $\mathcal{V}$ be a non–empty set of *points* and let $\mathcal{B}$ be a set of (equal size, proper) subsets of $\mathcal{V}$, called *blocks*. The triple $(\mathcal{V}, \mathcal{B}, \in)$ is called an *incidence structure*.

Definition 1.2.1. An incidence structure such that every block is incident with a constant number of points and every point is incident with a constant number of blocks is said to be a *tactical configuration*.

Let $\mathcal{S} = (\mathcal{V}, \mathcal{B})$ be a tactical configuration such that $|\mathcal{V}| = v$, $|\mathcal{B}| = b$, every block is incident with k points and every point is incident with r blocks. A standard double counting argument on couples (P, ℓ), where $P \in \mathcal{V}$, $\ell \in \mathcal{B}$ and $P \in \ell$ gives

$$vr = bk.$$

An *automorphism* of $\mathcal{S}$ is a bijection on the points and the blocks of $\mathcal{S}$ which preserves incidence, i.e., the bijection α is an automorphism of $\mathcal{S}$ if for any point $P \in \mathcal{V}$ and any block $\ell \in \mathcal{B}$, $P \in \ell$ implies $\alpha(P) \in \alpha(\ell)$. The set of all automorphisms of $\mathcal{S}$ forms a group, denoted with $Aut(\mathcal{S})$ and called *automorphisms group of* $\mathcal{S}$. Clearly every subgroup of $Aut(\mathcal{S})$ acts on $\mathcal{V}$.

A *tactical decomposition* of an incidence structure $\mathcal{S}$ is a partition of $\mathcal{V}$ into disjoint point sets $\mathcal{V}_1, \ldots, \mathcal{V}_m$ (called the *point classes*), together with a partition of $\mathcal{B}$ into disjoint block sets $\mathcal{B}_1, \ldots, \mathcal{B}_n$ (*block classes*), such that for any i, j, the incidence structure $(\mathcal{V}_i, \mathcal{B}_j, \in)$ is a tactical configuration. In other words: for any point class $\mathcal{V}_i$ and any block class $\mathcal{B}_j$, the number of points of $\mathcal{V}_i$ on a block of $\mathcal{B}_j$ depends only on i, j, and can hence be denoted by k_{ij}; dually, the number of blocks of $\mathcal{B}_j$ through a point of $\mathcal{V}_i$ depends only on i, j, and can hence be denoted by r_{ij}. It follows that

$$v_i r_{ij} = b_j k_{ij},$$

where $|\mathcal{V}_i| = v_i$ and $|\mathcal{B}_j| = b_j$.

Definition 1.2.2. A tactical decomposition is said to be *symmetric* if it has the same number of point as block classes, that is if $n = m$.

Lemma 1.2.3. *Let $\mathcal{S} = (\mathcal{V}, \mathcal{B})$ be an incidence structure and let G be a group acting on $\mathcal{V}$. Then the point–orbits and block–orbits of G form a tactical decomposition of $\mathcal{S}$.*

Proof. Let $\mathcal{V}_1, \ldots, \mathcal{V}_m$ and $\mathcal{B}_1, \ldots, \mathcal{B}_n$ be the point–orbits and block–orbits under the action of G, respectively. Let P be a point of $\mathcal{V}_i$ and assume that there are x blocks of $\mathcal{B}_j$ through P. Let Q be any other point of $\mathcal{V}_i$. Since $\mathcal{V}_i = P^G$, there exists $g \in G$ such that $Q = P^g$. Note that $\ell_1, \ldots, \ell_x$ are the blocks of $\mathcal{B}_j$ incident with P if and only if $\ell_1^g, \ldots, \ell_x^g$ are the blocks of $\mathcal{B}_j$ incident with Q. Similarly, if ℓ is a block of $\mathcal{B}_j$, ℓ is incident with y points of $\mathcal{V}_i$ and $r = \ell^g$ is any other block of $\mathcal{B}_j$, then $P_1, \ldots, P_y$ are the points of $\mathcal{V}_i$ incident with ℓ if and only if $P_1^g, \ldots, P_y^g$ are the points of $\mathcal{V}_i$ incident with r. □

1.2.1 Block's lemma

Definition 1.2.4. An incidence structure $(\mathcal{V}, \mathcal{B})$ such that every two distinct points of $\mathcal{V}$ are both incident with exactly λ blocks of $\mathcal{B}$ is called $2 - (v, k, \lambda)$ *design* or simply 2–*design*.

Counting in two ways the triples $(Q, \ell; P)$, where $Q \in \mathcal{V} \setminus \{P\}$ and $P, Q \in \ell \in \mathcal{B}$, for a fixed $P \in \mathcal{V}$, we obtain

$$(v-1)\lambda = r(k-1). \tag{1.1}$$

In particular, a 2–design is a tactical configuration. Moreover $v > k$ implies that $r > \lambda$.

Suppose that $\mathcal{V} = \{P_1, \dots, P_v\}$ and $\mathcal{B} = \{\ell_1, \dots, \ell_b\}$, then the v by b matrix $A = (a_{ij})$, where

$$a_{ij} = \begin{cases} 1 & \text{if } P_i \in \ell_j \\ 0 & \text{if } P_i \notin \ell_j \end{cases}$$

is an *incidence matrix* of $\mathcal{S}$.

Lemma 1.2.5. *If A is the incidence matrix of a 2–design, then* $\det(A) \neq 0$.

Proof. First of all observe that $\mathrm{rank}(AA^t) = v$. Indeed, $a_{is}a_{sj} = 1$ if and only if the points P_i and P_j are both incident with the block ℓ_s. Hence,

$$\sum_{s=1}^{b} a_{is}a_{sj} = \begin{cases} \lambda & \text{if } i \neq j \\ r & \text{if } i = j \end{cases} \quad \text{and} \quad AA^t = (r-\lambda)\mathcal{I} + \lambda\mathcal{J},$$

where $\mathcal{J}$ denotes all one matrix. Then subtract the first column of AA^t from every other column and in the so obtained matrix add to the first row every other row. This gives

$$\det(AA^t) = \det \left(\begin{array}{c|c} r+(v-1)\lambda & 0 \ \dots \ 0 \\ \hline \lambda & \\ \vdots & (r-\lambda)\mathcal{I} \\ \lambda & \end{array} \right) = (r+(v-1)\lambda)(r-\lambda)^{v-1}.$$

Taking into account (1.1), it follows that $\det(AA^t) = rk(r-\lambda)^{v-1} \neq 0$ and $\mathrm{rank}(AA^t) = v$. Since $v = \mathrm{rank}(AA^t) \leq \mathrm{rank}(A) \leq v$ the result follows. □

Corollary 1.2.6 (Fisher's Inequality)**.** *If $\mathcal{S}$ is a $2-(v,k,\lambda)$ designs, then $b \geq v$.*

Proof. From the proof of Lemma 1.2.5, we have that $v = \mathrm{rank}(AA^t) \leq \mathrm{rank}(A) \leq b$. □

Let $\mathcal{S} = (\mathcal{V}, \mathcal{B})$ be a 2–design and let $\mathcal{V}_1, \dots, \mathcal{V}_m$, $\mathcal{B}_1, \dots, \mathcal{B}_n$ be a tactical decomposition of $\mathcal{S}$. Consider the m by n matrices $K = (k_{ij})$ and $R = (r_{ij})$.

Theorem 1.2.7 (Block's Lemma). *Let $\mathcal{S} = (\mathcal{V}, \mathcal{B})$ be a 2–design and let $\mathcal{V}_1, \ldots, \mathcal{V}_m$, $\mathcal{B}_1, \ldots, \mathcal{B}_n$ be a tactical decomposition of $\mathcal{S}$. Then $0 \leq n - m \leq b - v$.*

Proof. We claim that $\operatorname{rank}(K) \geq m$. Note that r_{ij} is the sum of the entries in any column of the submatrix of A whose rows correspond to the points of $\mathcal{P}_i$ and whose columns correspond to the blocks of $\mathcal{B}_j$. Since $\operatorname{rank}(A) = v$, the v rows of A are linearly independent. Hence the m point classes are such that their union is represented by the linearly independent set of rows of A. It follows that the m rows of K must be linearly independent, otherwise it is possible to see that a dependence relation among them would give rise to a dependence relation among the rows of A. Therefore $\operatorname{rank}(K) \geq m$. On the other $\operatorname{rank}(K) \leq \min\{m, n\}$ and hence $0 \leq n - m$. By using a dual argument it can be shown that $\operatorname{rank}(K) \geq n - b + v$ and hence $n - m \leq b - v$. □

Corollary 1.2.8. $\operatorname{rank}(K) = \operatorname{rank}(R) = m$.

1.3 Finite Projective Spaces

Let q be a power of a prime, n a positive integer and let $\mathrm{GF}(q)$ denote the finite field with q elements. The n–dimensional projective space over $\mathrm{GF}(q)$, which we will denote by $\mathrm{PG}(n, q)$ or by $\mathrm{PG}(\mathrm{V})$ is defined as the $(n+1)$–dimensional vector space $\mathrm{V} = \mathrm{V}(n+1, q)$ over $\mathrm{GF}(q)$, modulo non–zero scalar equivalence of vectors; that is, we regard two $(n+1)$–tuples $\boldsymbol{x} = (x_1, \ldots, x_{n+1})$ and $\boldsymbol{y} = (y_1, \ldots, y_{n+1})$ to be equal if there exists a non–zero scalar $\lambda \in \mathrm{GF}(q)$ such that $\boldsymbol{x} = \lambda \boldsymbol{y}$. The elements of $\mathrm{PG}(n, q)$ are called *points*; these correspond to the one–dimensional subspaces of V. In general, a k–dimensional projective subspace of $\mathrm{PG}(n, q)$ (k–space for short) is defined to be the set of equivalence classes corresponding to a $(k+1)$–dimensional subspace of V. In order to avoid confusion we will take the word "dimension" and the symbol "dim" to mean vector space dimension except when otherwise stated. A 1–space of $\mathrm{PG}(n, q)$ is called a *line*, a 2–space a *plane*, a 3–space a *solid* and an $(n-1)$–space, a *hyperplane*. The number of k–spaces in $\mathrm{PG}(n, q)$ equals

$$\begin{bmatrix} n+1 \\ k+1 \end{bmatrix}_q = \prod_{i=0}^{k} \frac{q^{n+1} - q^i}{q^{k+1} - q^i}.$$

A *collineation* of $\mathrm{PG}(n, q)$ is a bijection on the points of the space which preserves incidence, i.e., the bijection α is a collineation of $\mathrm{PG}(n, q)$ if for any two subspaces S, S' of $\mathrm{PG}(n, q)$, $S \subseteq S'$ implies $\alpha(S) \subseteq \alpha(S')$. The set of all collineations of $\mathrm{PG}(n, q)$ forms a group, denoted by $\mathrm{P\Gamma L}(n+1, q)$ and called *automorphisms group of* $\mathrm{PG}(n, q)$. From the definition of $\mathrm{PG}(n, q)$, one can see that any non–singular linear transformation of V induces a collineation of $\mathrm{PG}(n, q)$, called *projectivity*. Note that two linear transformations induce the same projectivity if and only if they differ by multiplication by a scalar matrix. The set of all projectivities of $\mathrm{PG}(n, q)$ form the *projective linear group* $\mathrm{PGL}(n+1, q)$, where

$$\mathrm{PGL}(n+1, q) = \mathrm{GL}(n+1, q)/\{\lambda\mathcal{I} \mid \lambda \in \mathrm{GF}(q) \setminus \{0\}\}.$$

Here and elsewhere, $\mathcal{I}$ represents the identity transformation. Hence $\mathrm{PGL}(n+1, q)$ is a subgroup of $\mathrm{P\Gamma L}(n+1, q)$ and

$$|\,\mathrm{PGL}(n+1, q)| = q^{\frac{n(n+1)}{2}} \prod_{i=2}^{n+1} (q^i - 1).$$

Also, any automorphism of $\mathrm{GF}(q)$ induces a collineation of $\mathrm{PG}(n, q)$. The *Fundamental Theorem of Projective Geometry* asserts that $\mathrm{P\Gamma L}(n+1, q)$ is the semidirect product $\mathrm{PGL}(n+1, q) \rtimes Aut(\mathrm{GF}(q))$ induced by the natural action of $Aut(\mathrm{GF}(q))$ on $\mathrm{PGL}(n+1, \mathrm{GF}(q))$. In other words, it states that any collineation of $\mathrm{PG}(n, q)$ is induced by a semi–linear transformation of V. **We will be mainly concerned with projectivities of finite projective space; we shall find it helpful to work with the elements of** $\mathrm{PGL}(n+1, q)$ **as matrices in** $\mathrm{GL}(n+1, q)$ **and the points of** $\mathrm{PG}(n, q)$ **as column vectors, with matrices acting on the left.**

1.4 Finite Classical Polar Spaces

A map ρ sending the points of $\mathrm{PG}(n, q)$ to the hyperplanes of $\mathrm{PG}(n, q)$ is called a *correlation* if for any two subspaces S, S' of $\mathrm{PG}(n, q)$, $S \subseteq S'$ implies $\rho(S') \subseteq \rho(S)$. If the map ρ has order two, then it is called a *polarity*. If σ is an automorphism of $\mathrm{GF}(q)$, a *σ–sesquilinear form* on V is a map

$$\beta : \mathrm{V} \times \mathrm{V} \longrightarrow \mathrm{GF}(q)$$

such that

i) $\beta(\boldsymbol{x} + \boldsymbol{y}, \boldsymbol{z}) = \beta(\boldsymbol{x}, \boldsymbol{z}) + \beta(\boldsymbol{y}, \boldsymbol{z})$,

ii) $\beta(\boldsymbol{x}, \boldsymbol{y} + \boldsymbol{z}) = \beta(\boldsymbol{x}, \boldsymbol{y}) + \beta(\boldsymbol{x}, \boldsymbol{z})$,

iii) $\beta(a\boldsymbol{x}, b\boldsymbol{y}) = a\sigma(b)\beta(\boldsymbol{x}, \boldsymbol{y})$,

for all $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in \mathrm{V}$ and for all $a, b \in \mathrm{GF}(q)$. If $\sigma = 1$, then β is said to be *bilinear*. The σ–sesquilinear form β is *non–degenerate* if $\beta(\boldsymbol{x}, \boldsymbol{y}) = 0$, for all $\boldsymbol{y} \in \mathrm{V}$ implies that $\boldsymbol{x} = \mathbf{0}$ and similarly if $\beta(\boldsymbol{x}, \boldsymbol{y}) = 0$, for all $\boldsymbol{x} \in \mathrm{V}$ implies that $\boldsymbol{y} = \mathbf{0}$.

Any non–degenerate σ–sesquilinear form gives rise to a correlation ρ of $\mathrm{PG}(n, q)$ by the rule

$$\rho(S) = \{\boldsymbol{y} \in \mathrm{PG}(n, q) \mid \beta(\boldsymbol{x}, \boldsymbol{y}) = 0 \text{ for all } \boldsymbol{x} \in S\},$$

where S is a subspace of $\mathrm{PG}(n, q)$. The subspace $\rho(S)$ will also be denoted by S^ρ. Also, the Fundamental Theorem of Projective Geometry implies that any correlation of $\mathrm{PG}(n, q)$ is induced by a semi–linear transformation of V. Let g be a semi–linear transformation of V. Then g can be identified by a linear transformation f and a field automorphism σ. Define the function

$$\beta : (\boldsymbol{x}, \boldsymbol{y}) \in V \times V \longmapsto \boldsymbol{x}g(\boldsymbol{y})^t = \boldsymbol{x}f(\sigma(\boldsymbol{y}))^t \in \mathrm{GF}(q),$$

where t denotes transposition. Then it can be seen that β is a σ–sesquilinear form. Therefore correlations and non–degenerate σ–sesquilinear forms are equivalent. Let β be a non–degenerate σ–sesquilinear form of V and let ρ be the related correlation of $\mathrm{PG}(n, q)$. A subspace S of $\mathrm{PG}(n, q)$ is said to be *totally isotropic* with respect to β if $S \subseteq \rho(S)$.

A σ–sesquilinear form β is said to be *reflexive* if $\beta(\boldsymbol{x}, \boldsymbol{y}) = 0$ implies $\beta(\boldsymbol{y}, \boldsymbol{x}) = 0$, for all $\boldsymbol{x}, \boldsymbol{y} \in$ V. Moreover, β is reflexive if and only if the corresponding correlation is a polarity. If β is a non–degenerate reflexive σ–sesquilinear form of V, then β falls in one of the following types:

i) *Alternating*. In this case $\sigma = 1$ and $\beta(\boldsymbol{x}, \boldsymbol{x}) = 0$, for all $\boldsymbol{x} \in$ V.

ii) *Symmetric*. In this case $\sigma = 1$ and $\beta(\boldsymbol{x}, \boldsymbol{y}) = \beta(\boldsymbol{y}, \boldsymbol{x})$, for all $\boldsymbol{x}, \boldsymbol{y} \in$ V.

iii) *Hermitian*. In this case $\sigma^2 = 1$, $\sigma \neq 1$ and $\beta(\boldsymbol{x}, \boldsymbol{y}) = \sigma(\beta(\boldsymbol{x}, \boldsymbol{y}))$, for all $\boldsymbol{x}, \boldsymbol{y} \in$ V.

Note that if q is even, then any alternating form is also symmetric, but not conversely. Let β be a non–degenerate reflexive σ–sesquilinear form. Then according to the condition on β, we distinguish different types of polarity:

For q odd, we have three types of polarities.

1) If β is an alternating form and n is odd, the polarity is called *symplectic polarity*.
2) If β is a symmetric form, the polarity is called *orthogonal polarity*.
3) If β is a Hermitian form, the polarity is called *unitary polarity*.

For q even, there also exist three types of polarities.

1) If β is an alternating form and n is odd, the polarity is called *symplectic polarity*.

2) If β is a symmetric and not alternating form, the polarity is called *pseudo–polarity*.

3) If β is a Hermitian form, the polarity is called *unitary polarity*.

A *quadratic form* on V is a function

$$Q : \mathrm{V} \longrightarrow \mathrm{GF}(q)$$

such that

i) $Q(a\boldsymbol{x}) = a^2 Q(\boldsymbol{x})$ for all $\boldsymbol{x} \in \mathrm{V}$, $a \in \mathrm{GF}(q)$,

ii) $\beta(\boldsymbol{x}, \boldsymbol{y}) = Q(\boldsymbol{x} + \boldsymbol{y}) - Q(\boldsymbol{x}) - Q(\boldsymbol{y})$ is a bilinear form.

In this case β is called *the polar form of* Q. The quadratic form Q is *non–degenerate* if its polar form β has the property that $\beta(\boldsymbol{x}, \boldsymbol{y}) = Q(\boldsymbol{x}) = 0$ for all $\boldsymbol{y} \in \mathrm{V}$ implies $\boldsymbol{x} = 0$. When q is odd, then each of Q and β determines the other and β is a symmetric bilinear form. If q is even, then β is an alternating bilinear form, but Q cannot be recovered from β. Indeed, in this case, many different quadratic forms correspond to the same bilinear form. Let Q be a non–degenerate quadratic form of V. A subspace S of $\mathrm{PG}(n, q)$ is said to be *totally singular* with respect to Q if $Q(\boldsymbol{x}) = 0$ for all $\boldsymbol{x} \in S$.

Definition 1.4.1. Let β (resp. Q) be a non–degenerate reflexive σ–sesquilinear form (resp. non–degenerate quadratic form) of the vector space V. In PG(V), the set of totally isotropic subspaces with respect to β (resp. totally singular subspaces with respect to Q) is called a *finite classical polar space*, namely $\mathcal{P}$.

In particular $\mathcal{P}$ is said to be *symplectic*, *orthogonal*, *hermitian* or *pseudo–symplectic* according as the form is alternating, quadratic, hermitian or symmetric and not alternating, respectively. Let f be a linear transformation of V and let α be the projectivity of $\mathrm{PG}(n, q)$ induced by f. Then α is said to be a *similarity* of $\mathcal{P}$ if $\beta(f(\boldsymbol{x}), f(\boldsymbol{y})) = \lambda\beta(\boldsymbol{x}, \boldsymbol{y})$, or $Q(f(\boldsymbol{x})) = \lambda Q(\boldsymbol{x})$, for all $\boldsymbol{x}, \boldsymbol{y} \in \mathrm{V}$. The set of similarities of $\mathcal{P}$ forms a group that is the stabilizer of $\mathcal{P}$ in $\mathrm{PGL}(n + 1, q)$. Let q and n be not both even; observe that if $\perp$ denotes the polarity associated with $\mathcal{P}$ and S is a subspace of $\mathrm{PG}(n, q)$, then $\left(S^{\perp}\right)^{\alpha} = (S^{\alpha})^{\perp}$.

A projective subspace of maximal dimension contained in $\mathcal{P}$ is called a *generator* of $\mathcal{P}$ and one can prove that all generators of $\mathcal{P}$ have the same projective dimension. An orthogonal polar space is also called a *(non–degenerate) quadric*. Up to a change of the coordinate system the finite classical polar spaces can be described as follows:

- The *elliptic quadric* $\mathcal{Q}^-(2n+1, q)$, $n \geq 1$, with group of similarities denoted by $\mathrm{PGO}^-(2n+2, q)$ and formed by the points of $\mathrm{PG}(2n+1, q)$ satisfying the equation $X_1X_2 + \ldots + X_{2n-1}X_{2n} + f(X_{2n+1}X_{2n+2}) = 0$, where f is a homogeneous irreducible polynomial of degree two over $\mathrm{GF}(q)$.
- The *parabolic quadric* $\mathcal{Q}(2n, q)$, $n \geq 1$, with group of similarities denoted by $\mathrm{PGO}(2n+1, q)$ and formed by the points of $\mathrm{PG}(2n, q)$ satisfying the equation $X_1X_2 + \ldots + X_{2n-1}X_{2n} + X_{2n+1}^2 = 0$.
- The *hyperbolic quadric* $\mathcal{Q}^+(2n+1, q)$, $n \geq 0$, with group of similarities denoted by $\mathrm{PGO}^+(2n+2, q)$ and formed by the points of $\mathrm{PG}(2n+1, q)$ satisfying the equation $X_1X_2 + \ldots + X_{2n-1}X_{2n} + X_{2n+1}X_{2n+2} = 0$.
- The *symplectic polar space* $\mathcal{W}(2n+1, q)$, $n \geq 0$, with group of similarities denoted by $\mathrm{PSp}(2n+2, q)$ and formed by the subspaces of $\mathrm{PG}(2n, q)$ that are totally isotropic with respect to the alternating form $\beta(\boldsymbol{x}, \boldsymbol{y}) = x_1y_2 - x_2y_1 + \ldots + x_{2n+1}y_{2n+2} - x_{2n+2}y_{2n+1}$.
- The *hermitian polar space* $\mathcal{H}(n, q^2)$, $n \geq 1$, with group of similarities denoted by $\mathrm{PGU}(n+1, q^2)$ and formed by the points of $\mathrm{PG}(n, q^2)$ satisfying the equation $X_1^{q+1} + \ldots + X_{n+1}^{q+1} = 0$.

We remark that the projective linear group of the ambient projective space acts transitively on each of the polar space described above.

1.4.1 $\mathcal{Q}(2, q)$

A parabolic quadric $\mathcal{Q}(2, q)$ of $\mathrm{PG}(2, q)$ is also known as a *(non–degenerate) conic*, see [20, Section 7.2]. It consists of $q+1$ points of $\mathrm{PG}(2, q)$ no three on a line. The stabilizer of a conic in $\mathrm{PGL}(3, q)$, that is denoted by $\mathrm{PGO}(3, q)$, has order $q^3 - q$. Therefore, from the Orbit–Stabilizer Theorem it follows that there are

$$\frac{|\,\mathrm{PGL}(3, q)|}{|\,\mathrm{PGO}(3, q)|} = \frac{q^3(q^2-1)(q^3-1)}{q(q^2-1)} = q^5 - q^2$$

conics in $\mathrm{PG}(2, q)$. Let $\mathcal{Q}(2, q)$ be the conic of $\mathrm{PG}(2, q)$ given by

$$X_2^2 - X_1X_3 = 0.$$

Then a projectivity of $\mathrm{PGO}(3, q)$, the stabilizer of $\mathcal{Q}(2, q)$ in $\mathrm{PGL}(3, q)$, is associated with a matrix

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

for some $a, b, c, d \in \mathrm{GF}(q)$ with $ad - bc \neq 0$. In particular $\mathrm{PGO}(3, q) \simeq \mathrm{PGL}(2, q)$ and the isomorphism is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longleftrightarrow \begin{pmatrix} a^2 & 2ac & c^2 \\ ab & ad + bc & cd \\ b^2 & 2bd & d^2 \end{pmatrix},$$

with $a, b, c, d \in \mathrm{GF}(q)$, $ad - bc \neq 0$.

1.4.2 $\mathcal{Q}^+(3, q)$

A *regulus* of $\mathrm{PG}(3, q)$ is the set of lines intersecting three skew lines and has size $q + 1$.

Lemma 1.4.2. *Two distinct reguli of* $\mathrm{PG}(3, q)$ *have at most two lines in common.*

Proof. Use the Klein correspondence κ, see 1.5. □

A hyperbolic quadric $\mathcal{Q}^+(3, q)$ of $\mathrm{PG}(3, q)$ consists of $(q + 1)^2$ points of $\mathrm{PG}(3, q)$ and $2(q + 1)$ lines that are the union of two reguli $\mathcal{R}_1$, $\mathcal{R}_2$. Through a point of $\mathcal{Q}^+(3, q)$ there pass two lines belonging to different reguli. A plane π of $\mathrm{PG}(3, q)$ is either *secant to* $\mathcal{Q}^+(3, q)$ and $\pi \cap \mathcal{Q}^+(3, q)$ is a non–degenerate conic or it is *tangent to* $\mathcal{Q}^+(3, q)$ and meets $\mathcal{Q}^+(3, q)$ in a degenerate conic consisting of two distinct lines. The stabilizer of $\mathcal{Q}^+(3, q)$ in $\mathrm{PGL}(4, q)$ is denoted by $\mathrm{PGO}^+(4, q)$, has order $2(q^3 - q)^2$ and has a subgroup of index two isomorphic to $\mathrm{PGL}(2, q) \times \mathrm{PGL}(2, q)$. Therefore, from the Orbit–Stabilizer Theorem it follows that there are

$$\frac{|\,\mathrm{PGL}(4, q)|}{|\,\mathrm{PGO}^+(4, q)|} = \frac{q^6(q^2 - 1)(q^3 - 1)(q^4 - 1)}{2q^2(q^2 - 1)^2} = \frac{q^4(q^2 + 1)(q^3 - 1)}{2}$$

hyperbolic quadrics in $\mathrm{PG}(3, q)$. See [21, p. 23] for more details on $\mathcal{Q}^+(3, q)$. Let $\mathcal{Q}^+(3, q)$ be the hyperbolic quadric of $\mathrm{PG}(3, q)$ given by

$$X_1X_4 - X_2X_3 = 0.$$

If $P_i = (x_i, y_i) \in \mathrm{PG}(1, q)$, $1 \leq i \leq 2$, then $P_1 \otimes P_2 = (x_1, y_1) \otimes (x_2, y_2) = (x_1x_2, x_1y_2, y_1x_2, y_1y_2)$ is a point of $\mathcal{Q}^+(3, q)$ and

$$\mathcal{Q}^+(3, q) = \{P_1 \otimes P_2 \mid P_1, P_2 \in \mathrm{PG}(1, q)\}.$$

A projectivity of $\mathrm{PGL}(2, q) \times \mathrm{PGL}(2, q)$, the subgroup of index two of $\mathrm{PGO}^+(4, q)$, is associated with a matrix

$$M \otimes M' = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' & ab' & ba' & bb' \\ ac' & ad' & bc' & bd' \\ ca' & cb' & da' & db' \\ cc' & cd' & dc' & dd' \end{pmatrix}, \qquad (1.2)$$

where $a, b, c, d, a', b', c', d' \in \mathrm{GF}(q)$, with $ad - bc \neq 0$ and $a'd' - b'c' \neq 0$. In particular the group $\mathrm{PGL}(2, q) \times \mathrm{PGL}(2, q)$ fixes both reguli $\mathcal{R}_1$ and $\mathcal{R}_2$. The group $\mathrm{PGO}^+(4, q)$ can be described as the subgroup of $\mathrm{PGL}(4, q)$ generated by $\mathrm{PGL}(2, q) \times \mathrm{PGL}(2, q)$ and the involution τ, where τ is associated with the matrix

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

interchanges the reguli $\mathcal{R}_1$ and $\mathcal{R}_2$. More precisely

$$\mathrm{PGO}^+(4, q) = (\mathrm{PGL}(2, q) \times \mathrm{PGL}(2, q)) \rtimes \tau.$$

Lemma 1.4.3.

$$|Stab_{\mathrm{PGO}^+(4,q)}(P)| = \begin{cases} 2q^2(q-1)^2 & \textit{if } P \in \mathcal{Q}^+(3, q) \\ 2(q^3 - q) & \textit{if } P \notin \mathcal{Q}^+(3, q) \end{cases}$$

Proof. Let ξ be the projectivity of $\mathrm{PGL}(2, q) \times \mathrm{PGL}(2, q)$ associated with the matrix $M \otimes M'$ as indicated in (1.2).

Let $P = (1, 0, 0, 0) \in \mathcal{Q}^+(3, q)$. Then $P^\xi = P$ if and only if $ac' = ca' = cc' = 0$. First of all observe that both a and a' are not zero. Indeed, if $a = 0$, then necessarily $c \neq 0$, otherwise $ad - bc = 0$, a contradiction. Hence, since $ca' = cc' = 0$, we would obtain $a' = c' = 0$ and then $a'd' - b'c' = 0$, a contradiction. Similarly it can be seen that $a' \neq 0$. Therefore we have that $c = c' = 0$. Note that every projectivity associated with

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \otimes \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}, a, b, d, a', b', d' \in \mathrm{GF}(q), ad \neq 0, a'd' \neq 0,$$

fixes P. Finally note that τ stabilizes P as well.

Let $P = (0, 1, -1, 0) \in \mathrm{PG}(3, q) \setminus \mathcal{Q}^+(3, q)$. Then $P^\xi = P$ if and only if $ab' - ba' = cd' - dc' = 0$ and $ad' - bc' = da' - cb'$ if and only if

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d' & -b' \\ -c' & a' \end{pmatrix} = M \det(M') M'^{-1} = \lambda \mathcal{I},$$

where $\lambda = ad' - bc' = da' - cb'$. First of all note that $\lambda \neq 0$, otherwise $\det(M) = 0$, a contradiction. Hence, we have that $M' = \frac{\det(M')}{\lambda} M$. Since $\mu M \otimes M = M \otimes \mu M = \mu(M \otimes M)$, for all $\mu \in \mathrm{GF}(q) \setminus \{0\}$, it follows that ξ is induced by $M \otimes M$. On the other hand either τ or the projectivity associated with $M \otimes M$ stabilizes the point P. □

As a consequence we have the following result.

Corollary 1.4.4. *The group* $\mathrm{PGO}^+(4,q)$ *acts transitively on the points of* $\mathcal{Q}^+(3,q)$ *and on the points of* $\mathrm{PG}(3,q) \setminus \mathcal{Q}^+(3,q)$.

1.4.3 $\mathcal{W}(3,q)$

The set of all totally isotropic points and totally isotropic lines (i.e., generators) with respect to a (non–degenerate) symplectic polarity of $\mathrm{PG}(3,q)$ forms the symplectic polar space $\mathcal{W}(3,q)$. It consists of all the points of $\mathrm{PG}(3,q)$ and of $(q+1)(q^2+1)$ generators. Through every point $P \in \mathrm{PG}(3,q)$ there pass $q+1$ generators and these lines are coplanar. The plane containing these lines is the polar plane of P with respect to the symplectic polarity defining $\mathcal{W}(3,q)$. The lines in common to two distinct symplectic polar spaces of $\mathrm{PG}(3,q)$ form a so called *linear congruence* of $\mathrm{PG}(3,q)$, see [21, Section 15.2]. There are three types of linear congruences:

- the *elliptic congruence* consisting of q^2+1 pairwise disjoint lines of $\mathrm{PG}(3,q)$ forming a Desarguesian spread.
- the *hyperbolic congruence* consisting of the $(q+1)^2$ lines of $\mathrm{PG}(3,q)$ meeting two skew lines, that are the *axes* of the congruence.
- the *parabolic congruence* consisting of the q^2+q+1 lines of $\mathcal{W}(3,q)$ meeting a distinguished line of $\mathcal{W}(3,q)$, called the *axis* of the congruence.

Lemma 1.4.5. *Let* $\mathcal{L}$ *be a hyperbolic, parabolic or elliptic congruence, then every point of* $\mathrm{PG}(3,q)$ *(not on the axis or axes of* $\mathcal{L}$*) is contained in a unique line of* $\mathcal{L}$*.*

Proof. It is enough to show that through every point of $\mathrm{PG}(3,q)$ there pass at least a line of $\mathcal{L}$. Let $\mathcal{W}_1$ and $\mathcal{W}_2$ be two distinct symplectic polar spaces of $\mathrm{PG}(3,q)$ such that $\mathcal{W}_1 \cap \mathcal{W}_2 = \mathcal{L}$ and let $\perp_1$, $\perp_2$ be the symplectic polarities defining $\mathcal{W}_1$, $\mathcal{W}_2$, respectively. If P is a point of $\mathrm{PG}(3,q)$, then either $P^{\perp_1} \neq P^{\perp_2}$ and $\ell = P^{\perp_1} \cap P^{\perp_2}$ is a line belonging to both $\mathcal{W}_1$, $\mathcal{W}_2$ (hence $P \in \ell \in \mathcal{L}$), or $P^{\perp_1} = P^{\perp_2}$ and the $q+1$ lines through P contained in $P^{\perp_1}$ belong to $\mathcal{L}$. □

Lemma 1.4.6. *Let* $\mathcal{L}$ *be a hyperbolic, parabolic or elliptic congruence and let* $\mathcal{R}_1, \mathcal{R}_2$ *be two distinct reguli belonging to* $\mathcal{L}$*, i.e.* $\mathcal{R}_1, \mathcal{R}_2 \subseteq \mathcal{L}$*. Let* $\mathcal{Q}_i$ *be the hyperbolic quadric of* $\mathrm{PG}(3,q)$ *containing the regulus* $\mathcal{R}_i$*,* $1 \leq i \leq 2$*. Then* $\mathcal{Q}_1 \cap \mathcal{Q}_2$ *does not contain a non–degenerate conic.*

Proof. Assume by contradiction that $\mathcal{Q}_1 \cap \mathcal{Q}_2$ contains a non–degenerate conic, say $\mathcal{C}$. We consider several cases.

Let $\mathcal{L}$ be an elliptic congruence.

In this case through a point P of $\mathcal{C}$ there pass exactly a line of $\mathcal{R}_1$, say ℓ_1, and a line of $\mathcal{R}_2$, say ℓ_2. Since $\mathcal{R}_1, \mathcal{R}_2$ belong to $\mathcal{L}$, we have that both, ℓ_1 and ℓ_2 are lines of $\mathcal{L}$. From Lemma 1.4.5, we conclude that necessarily $\ell_1 = \ell_2$ and hence $\mathcal{R}_1 = \mathcal{R}_2$. This is a contradiction, since two distinct reguli share at most two lines.

Let $\mathcal{L}$ be a parabolic congruence having as axis the line r.

Each of the lines of both $\mathcal{R}_1$ and $\mathcal{R}_2$ intersects r in a point and hence r is a line of the opposite regulus of both $\mathcal{R}_1$ and $\mathcal{R}_2$. In particular $r \cap \mathcal{C}$ is a point. Let P be a point of $\mathcal{C} \setminus r$. By repeating the previous argument, we get that the reguli $\mathcal{R}_1$ and $\mathcal{R}_2$ have in common at least q lines. Therefore if $q \geq 3$, $\mathcal{R}_1 = \mathcal{R}_2$, a contradiction.

Let $\mathcal{L}$ be a hyperbolic congruence having as axes the lines r_1, r_2.

Each of the lines of both $\mathcal{R}_1$ and $\mathcal{R}_2$ intersects both r_1, r_2 in a point and hence r_1, r_2 are lines of the opposite regulus of both $\mathcal{R}_1$ and $\mathcal{R}_2$. In particular $r_i \cap \mathcal{C}$ is a point, $1 \leq i \leq 2$. Let P be a point of $\mathcal{C} \setminus (r_1 \cup r_2)$. By repeating the previous argument, we get that the reguli $\mathcal{R}_1$ and $\mathcal{R}_2$ have in common at least $q-1$ lines. Therefore if $q \geq 4$, $\mathcal{R}_1 = \mathcal{R}_2$, a contradiction. Some computations show that the result holds true in the remaining cases. □

1.5 The Klein Quadric

In this section we focus our attention on a specific polar space with rather remarkable properties, see [21, Chapter 15]. This is $\mathcal{Q}^+(5,q)$, the hyperbolic orthogonal space of $\mathrm{PG}(5,q)$, also known as the *Klein quadric*. Generators of $\mathcal{Q}^+(5,q)$ are planes and the points of $\mathcal{Q}^+(5,q)$ are in one–to–one correspondence with lines of $\mathrm{PG}(3,q)$ as we briefly explain in the next few lines. Let $\boldsymbol{x} = (x_1, x_2, x_3, x_4), \boldsymbol{y} = (y_1, y_2, y_3, y_4)$ be two distinct points of $\mathrm{PG}(3,q)$ and let ℓ be the line of $\mathrm{PG}(3,q)$ joining $\boldsymbol{x}$ and $\boldsymbol{y}$. For a line ℓ joining the points $\boldsymbol{x}$ and $\boldsymbol{y}$, define the *Plücker coordinates of ℓ* as

$$p_{ij} = \det \begin{pmatrix} x_i & x_j \\ y_i & y_j \end{pmatrix} = x_i y_j - x_j y_i, i < j,$$

Up to scalar multiples the *Plücker coordinates* $(p_{12}, p_{13}, p_{14}, p_{23}, p_{24}, p_{34})$ do not depend on the choice of the two distinct points $\boldsymbol{x}$ and $\boldsymbol{y}$ on ℓ and therefore to the line ℓ there corresponds a point $(p_{12}, p_{13}, p_{14}, p_{23}, p_{24}, p_{34})$ of $\mathrm{PG}(5, q)$. Furthermore, all such points satisfy the equation

$$p_{12}p_{34} - p_{13}p_{24} + p_{14}p_{23} = 0$$

and therefore lie on the hyperbolic quadric $\mathcal{Q}^+(5, q)$ given by

$$X_1X_6 - X_2X_5 + X_3X_4 = 0.$$

Since each of the points of $\mathcal{Q}^+(5, q)$ occurs as the Plücker coordinates of some line of $\mathrm{PG}(3, q)$, we have a bijection κ from the lines of $\mathrm{PG}(3, q)$ to the points of $\mathcal{Q}^+(5, q)$, called the *Klein correspondence*. Let $\perp$ be the polarity of $\mathrm{PG}(5, q)$ associated with $\mathcal{Q}^+(5, q)$.

Under the correspondence κ:

- the plane pencils of lines are mapped to the lines of $\mathcal{Q}^+(5, q)$;
- the set of all lines on a point or all lines in a plane is sent to the set of all points on a generator of $\mathcal{Q}^+(5, q)$. This gives a natural partition of the planes of $\mathcal{Q}^+(5, q)$ into two classes, called *Latin planes* and *Greek planes* respectively;
- the lines of a regulus $\mathcal{R}$ of a $\mathrm{PG}(3, q)$ are sent to the points of a non–degenerate conic $\kappa(\mathcal{R})$ of $\mathcal{Q}^+(5, q)$. In particular the plane $\langle\kappa(\mathcal{R})\rangle$, containing the conic $\kappa(\mathcal{R})$, meets the quadric $\mathcal{Q}^+(5, q)$ exactly in $\kappa(\mathcal{R})$;
- the two reguli of a hyperbolic quadric $\mathcal{Q}^+(3, q)$ are sent to two non–degenerate conics of $\mathcal{Q}^+(5, q)$ lying on two planes σ and $\sigma^\perp$, respectively;
- the lines of $\mathcal{W}(3, q)$ are mapped to the points of a parabolic quadric $\mathcal{Q}(4, q) \subset \mathcal{Q}^+(5, q)$;
- the lines of an elliptic congruence are mapped to the points of an elliptic quadric $\mathcal{Q}^-(3, q) \subset \mathcal{Q}^+(5, q)$;
- the lines of a hyperbolic congruence are mapped to the points of a hyperbolic quadric $\mathcal{Q}^+(3, q) \subset \mathcal{Q}^+(5, q)$;
- the lines of a parabolic congruence are mapped to the points of a quadratic cone of $\mathcal{Q}^+(5, q)$ having as vertex a point and as base a conic $\mathcal{Q}(2, q)$.

Chapter 2

Subspace codes

2.1 Introduction

Coding Theory studies techniques to correct errors arising during communications through noisy channels. Its distinguishing features are using discrete signals, which allows the description of signals in terms of abstract symbols and introducing the artificial redundancy, which gives the possibility to correct errors. Coding Theory uses a wide range of mathematical tools, from simple binary arithmetic to modern algebraic geometry, [28].

Let Λ be an alphabet of q elements. Let n be a positive integer and let Λ^n be the set of all n–tuples over Λ. Assume that Λ^n is a *metric space*, i.e., there exists a function

$$d : \Lambda^n \times \Lambda^n \longrightarrow \mathbb{Z},$$

called *distance*, such that $\forall \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in \Lambda^n$,

i) $d(\boldsymbol{x}, \boldsymbol{y}) \geq 0, d(\boldsymbol{x}, \boldsymbol{y}) = 0 \Longleftrightarrow \boldsymbol{x} = \boldsymbol{y}$,

ii) $d(\boldsymbol{x}, \boldsymbol{y}) = d(\boldsymbol{y}, \boldsymbol{x})$,

iii) $d(\boldsymbol{x}, \boldsymbol{z}) \leq d(\boldsymbol{x}, \boldsymbol{y}) + d(\boldsymbol{y}, \boldsymbol{z})$.

A *code* $\mathcal{C}$ of (Λ^n, d) of size $|\mathcal{C}| = M$ is defined as any set of M elements of Λ^n. The elements of $\mathcal{C}$ are called the *codewords*. The *minimum distance* of a code $\mathcal{C}$, denoted by $d(\mathcal{C})$, is the smallest of the distances between distinct codewords: $d(\mathcal{C}) = \min\{d(\boldsymbol{x}, \boldsymbol{y}) \mid \boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}, \boldsymbol{x} \neq \boldsymbol{y}\}$. The main problem in Coding Theory is to construct codes with given cardinality and having maximal pairwise distance as large as possible.

A *network* can be considered as a directed multigraph which consists of different nodes. In particular the source nodes transmit messages to the sink nodes through a channel of intermediate nodes. In contrast to traditional ways to operate a network that tries to avoid collisions of data streams as much as possible, a different approach, that allow the use of random mixing of data streams at intermediate nodes, has been proposed [1]. This approach, called *linear network coding*, aims to optimize the throughput by doing linear combinations on the intermediate nodes. In [27] the authors consider a channel that takes in a vector space and puts out another vector space, possibly with erasures, i.e. deletion of vectors from the transmitted space, or errors, i.e. addition of vectors to the transmitted space. Also, they define a suitable metric and show how to construct codes that correct combinations of errors and erasures for this channel. In what follows we give an overview of such a metric space. Let p be a prime, let $q = p^h$ any prime power and let V be an n–dimensional vector space over $\mathrm{GF}(q)$, the finite field with q elements. The set of all subspaces of V or subspaces of the projective space $\mathrm{PG}(n-1, q)$, forms a metric space with respect to the *subspace distance*, defined by

$$d(U, U') = \dim(U + U') - \dim(U \cap U').$$

Lemma 2.1.1. *$(\mathrm{PG}(n, q), d)$ is a metric space.*

Proof. Let U, U', U'' be projective subspaces of $\mathrm{PG}(n-1, q)$. Then it is easily seen that

i) $d(U, U') \geq 0, d(U, U') = 0 \Longleftrightarrow U = U'$,

ii) $d(U, U') = d(U', U)$,

Finally note that

$$d(U, U'') - d(U, U') - d(U', U'') = \dim(U) + \dim(U'') - 2\dim(U \cap U'')$$
$$- \dim(U) - \dim(U') + 2\dim(U \cap U') - \dim(U') - \dim(U'') + 2\dim(U' \cap U'') =$$
$$2\left(\dim(U \cap U') + \dim(U' \cap U'') - \dim(U \cap U'') - \dim(U')\right) =$$
$$2\left(\dim(U \cap U' \cap U'') + \dim((U \cap U') + (U' \cap U'')) - \dim(U \cap U'') - \dim(U')\right)$$
$$\leq 0.$$

Indeed,

$$(U \cap U') + (U' \cap U'') \subseteq U', \;\; U \cap U' \cap U'' \subseteq U \cap U''.$$

Hence

$$\dim((U \cap U') + (U' \cap U'')) \leq \dim(U'), \quad \dim(U \cap U' \cap U'') \leq \dim(U \cap U'').$$

□

Remark 2.1.2. The metric space $(\mathrm{PG}(n-1,q), d)$ can be considered as a q–analogue of the well–known Hamming space $(\mathrm{PG}(n-1,2), d_H)$. Here, if $\boldsymbol{x}, \boldsymbol{y}$ are points of $\mathrm{PG}(n-1,2)$, $d_H(\boldsymbol{x}, \boldsymbol{y})$ denotes the number of coordinates in which $\boldsymbol{x}$ and $\boldsymbol{y}$ differ. In particular, if $\mathrm{PG}(n-1,2)$ is identified with the set of subsets of $\{1, \dots, n\}$, we have that $d_H(\boldsymbol{x}, \boldsymbol{y}) = |\boldsymbol{x} \cup \boldsymbol{y}| - |\boldsymbol{x} \cap \boldsymbol{y}|, \forall \boldsymbol{x}, \boldsymbol{y} \in \mathrm{PG}(n-1,2)$.

We will consider codes in the space $\mathrm{PG}(n-1,q)$ endowed with the above defined subspace distance. In particular, we will restrict our attention to constant–dimension codes.

Definition 2.1.3. A *constant–dimension code* (or CDC) in $(\mathrm{PG}(n-1,q), d)$ is a code of which each codeword has the same dimension. A constant–dimension code $\mathcal{C}$ consisting of $(k-1)$–spaces, $2 \leq k \leq n-2$, such that $|\mathcal{C}| = M$ and $\forall U, U' \in \mathcal{C}$, $U \neq U'$, $d(U,U') = \dim(U+U') - \dim(U \cap U') = 2(k - \dim(U \cap U')) \geq 2\delta$ is denoted by $(n, M, 2\delta; k)_q$–code.

From a combinatorial point of view an $(n, M, 2\delta; k)_q$ constant–dimension subspace code, $\delta > 1$, is a collection $\mathcal{C}$ of $(k-1)$–spaces of $\mathrm{PG}(n-1,q)$ such that $|\mathcal{C}| = M$ and every $(k-\delta)$–space of $\mathrm{PG}(n-1,q)$ is contained in at most one member of $\mathcal{C}$. Equivalently, an $(n, M, 2\delta; k)_q$ constant–dimension subspace code, $\delta > 1$, is a collection $\mathcal{C}$ of $(k-1)$–spaces of $\mathrm{PG}(n-1,q)$ such that $|\mathcal{C}| = M$ and distinct members of $\mathcal{C}$ pairwise meet in at most a $(k-\delta-1)$–space of $\mathrm{PG}(n-1,q)$. (If $\delta = 1$, then every $(k-1)$–space can be considered as a member of an $(n, M, 2; k)_q$ constant–dimension code.)

The maximum number of codewords in an $(n, M, 2\delta; k)_q$–code is denoted by $\mathcal{A}_q(n, 2\delta, k)$.

As in classical coding theory, in the context of subspace coding theory, the main problem asks for the determination of the largest sizes of codes for a given dimension n and minimum distance and of course the classification of the corresponding optimal codes.

Let $\mathcal{C}$ be a constant–dimension code and let $\perp$ be a non–degenerate polarity of $\mathrm{PG}(n-1,q)$. Define $\mathcal{C}^\perp = \{U^\perp \mid U \in \mathcal{C}\}$.

Lemma 2.1.4. *If $\mathcal{C}$ is an $(n, M, 2\delta, k)_q$ constant–dimension code, then $\mathcal{C}^\perp$ is an $(n, M, 2\delta, n-k)_q$ constant–dimension code.*

Proof. Let $A, A' \in \mathcal{C}^{\perp}$, $A \neq A'$, and let $U, U' \in \mathcal{C}$ such that $A = U^{\perp}, A' = U'^{\perp}$. Then $d(A, A') = d(U^{\perp}, U'^{\perp}) = \dim(U^{\perp} + U'^{\perp}) - \dim(U^{\perp} \cap U'^{\perp}) = \dim((U \cap U')^{\perp}) - \dim((U + U')^{\perp}) = (n - \dim(U \cap U')) - (n - \dim(U + U')) = \dim(U + U') - \dim(U \cap U') = d(U, U')$. □

Corollary 2.1.5. $\mathcal{A}_q(n, 2\delta, k) = \mathcal{A}_q(n, 2\delta, n - k)$.

Definition 2.1.6. A *partial* $(k-1)$*–spread* $\mathcal{S}$ of $\mathrm{PG}(n-1, q)$ is a set of pairwise disjoint $(k-1)$–spaces of $\mathrm{PG}(n-1, q)$ for which any point of $\mathrm{PG}(n-1, q)$ is contained in at most one member of $\mathcal{S}$. If every point of $\mathrm{PG}(n-1, q)$ is contained in a member of $\mathcal{S}$, then $\mathcal{S}$ is called a $(k-1)$*–spread*.

Spreads and partial spreads are basic concepts which were very well studied in finite geometry. If $\delta = k$, then an $(n, M, 2k, k)_q$ constant–dimension code is nothing else than a (partial) $(k-1)$–spread of $\mathrm{PG}(n-1, q)$. Hence $\mathcal{A}_q(n, 2k, k)$ coincides with the size of the largest (partial) $(k-1)$–spread of $\mathrm{PG}(n-1, q)$. We recall some of the most significative known results regarding spreads and partial spreads in a finite projective space [24].

Theorem 2.1.7 ([33])**.** *A* $(k-1)$*–spread of* $\mathrm{PG}(n-1, q)$ *exists if and only if* $n \equiv 0 \pmod{k}$.

Theorem 2.1.8 ([4])**.** *If* $1 \equiv n \pmod{k}$ *and* $k \geq 2$*, then the largest partial* $(k-1)$*–spread of* $\mathrm{PG}(n-1, q)$ *has size* $\frac{q^n - q^k(q-1) - 1}{q^k - 1}$.

Theorem 2.1.9 ([30])**.** *Let* $r \equiv n \pmod{k}$*. If* $k > (q^r - 1)/(q - 1)$*, then the largest partial* $(k-1)$*–spread of* $\mathrm{PG}(n-1, q)$ *has size* $\frac{q^n - q^k(q^r - 1) - 1}{q^k - 1}$.

Note that from Theorem 2.1.8, the maximum size of a partial line–spread of $\mathrm{PG}(2m, q)$ equals $\frac{q^{2m+1} - q^3 + q^2 - 1}{q^2 - 1} = q^{2m-1} + q^{2m-3} + \ldots + q^5 + q^3 + 1$. As a consequence of the previous results, we obtain the exact values of the corresponding $\mathcal{A}_q(n, 2k, k)$. In particular:

- $\mathcal{A}_q(4, 4, 2) = q^2 + 1$,
- $\mathcal{A}_q(5, 4, 2) = \mathcal{A}_q(5, 4, 3) = q^3 + 1$,
- $\mathcal{A}_q(6, 4, 2) = \mathcal{A}_q(6, 4, 4) = q^4 + q^2 + 1$,
- $\mathcal{A}_q(6, 6, 3) = q^3 + 1$.

2.2 Planes of $\mathrm{PG}(5,q)$ pairwise intersecting in at most a point

The smallest open case for which the main problem of subspace coding theory has not yet an exact answer arises when $n = 6$, $k = 3$ and $\delta = 2$. It asks for the maximum size M that a $(6, M, 4; 3)_q$ constant–dimension code may have. Equivalently it asks for the maximum number of planes of $\mathrm{PG}(5,q)$ pairwise intersecting in at most a point. The following result provides un upper bound on $\mathcal{A}_q(6,4,3)$.

Lemma 2.2.1. $\mathcal{A}_q(6,4,3) \leq (q^3+1)^2$.

Proof. Let $\mathcal{C}$ be the largest set of planes of $\mathrm{PG}(5,q)$ such that two distinct planes of $\mathcal{C}$ meet in at most a point. Let P be a point of $\mathrm{PG}(5,q)$, let x_P be the number of planes of $\mathcal{C}$ through P and let Π be a hyperplane of $\mathrm{PG}(5,q)$ not containing P. Every plane π_i of $\mathcal{C}$ containing P meets Π in a line, say ℓ_i, $1 \leq i \leq x_P$. Note that, if $i \neq j$, then $|\ell_i \cap \ell_j| = 0$, otherwise π_i and π_j would share the line joining P and $\ell_i \cap \ell_j$, a contradiction. Hence ℓ_i, $1 \leq i \leq x_P$ is a partial 1–spread of Π and, from Theorem 2.1.8, we have that $x_P \leq q^3+1$. A standard double counting argument on couples (P,π), where P is a point of $\mathrm{PG}(5,q)$, π is a plane of $\mathcal{C}$ and $P \in \pi$, gives:

$$|\mathcal{C}|(q^2+q+1) \leq (q^5+q^4+q^3+q^2+q+1)(q^3+1).$$

The result follows. □

In the remaining part of this section we will give a constructive lower bound on $\mathcal{A}_q(6,4,3)$, see [8], [9]. We need the following definition, see also 4.1.

Definition 2.2.2. A *projective bundle* $\mathcal{B}$ of $\mathrm{PG}(2,q)$ is a collection of q^2+q+1 non–degenerate conics of $\mathrm{PG}(2,q)$ such that two distinct conics of $\mathcal{B}$ intersect in exactly one point.

Proposition 2.2.3. *The incidence structure whose points are the points of* $\mathrm{PG}(2,q)$ *and whose lines are the conics of a projective bundle* $\mathcal{B}$ *of* $\mathrm{PG}(2,q)$ *is a projective plane.*

Proof. Any two distinct points are on at most a conic of $\mathcal{B}$, otherwise we would have two distinct conics of $\mathcal{B}$ sharing two points, a contradiction. Also, every conic of $\mathcal{B}$ determines $q(q+1)/2$ couples of distinct points and hence there are $q(q+1)(q^2+q+1)/2$ couples of distinct points of $\mathrm{PG}(2,q)$ such that each of them is on a conic of $\mathcal{B}$. On the other hand, there are $q(q+1)(q^2+q+1)/2$ couples of distinct points in $\mathrm{PG}(2,q)$ and hence any two distinct points of $\mathrm{PG}(2,q)$ lie on a conic of $\mathcal{B}$. By definition two distinct conics of $\mathcal{B}$ meet in exactly a point and it is easily seen that there are four points, no three of them on a conic of $\mathcal{B}$. Hence the result follows from [25, p. 77]. □

Lemma 2.2.4. *Let $\mathcal{C}$ and $\mathcal{C}'$ be two distinct conics of $\mathcal{B}$ such that $\mathcal{C} \cap \mathcal{C}' = P$. Then, the tangent lines t and t' to $\mathcal{C}$ and $\mathcal{C}'$ at P, respectively, must be distinct.*

Proof. Assume by contradiction that t and t' coincide. Through P there are $q+1$ conics of $\mathcal{B}$ covering all the points of π. Each of the $q-1$ conics of $\mathcal{B}$ through P and distinct from $\mathcal{C}$ and $\mathcal{C}'$ meets t in at most one further point other than P. This means that on t there should be at least one uncovered point, a contradiction. □

Let $\mathrm{PG}(3,q)$ be the three–dimensional projective space over $\mathrm{GF}(q)$, equipped with homogeneous projective coordinates (X_1, X_2, X_3, X_4). Let π be a plane of $\mathrm{PG}(3,q)$ and let $\mathcal{B}$ be a projective bundle of π. Let G be the stabilizer of π in $\mathrm{PGL}(4,q)$. Then G is a group isomorphic to $q^3 : \mathrm{GL}(3,q)$. For instance, if π has equation $X_4 = 0$, then the elements of G are associated with the following matrices:

$$\left(\begin{array}{ccc|c} & & & a \\ & A & & b \\ & & & c \\ \hline 0 & 0 & 0 & 1 \end{array}\right),$$

where $a, b, c \in \mathrm{GF}(q)$ and $A \in \mathrm{GL}(3,q)$.

Lemma 2.2.5. *The group G has two orbits on hyperbolic quadrics of* $\mathrm{PG}(3,q)$*, according as π is a tangent or a secant plane.*

Proof. Let $\mathcal{Q}^+(3,q)$ be a hyperbolic quadric of $\mathrm{PG}(3,q)$ and let $\perp$ the polarity of $\mathrm{PG}(3,q)$ associated with $\mathcal{Q}^+(3,q)$. Let $G_{\mathcal{Q}^+}$ be the stabilizer of $\mathcal{Q}^+(3,q)$ in G. Then $G_{\mathcal{Q}^+}$ is the stabilizer of π in $\mathrm{PGO}^+(4,q)$, which in turn coincides with the stabilizer of P in $\mathrm{PGO}^+(4,q)$, where $P = \pi^\perp$. Therefore, either $P \in \mathcal{Q}^+(3,q)$, the plane π is tangent to $\mathcal{Q}^+(3,q)$ at P and $|G_{\mathcal{Q}^+}| = |G_P| = 2q^2(q-1)^2$, or $P \notin \mathcal{Q}^+(3,q)$, the plane π is secant to $\mathcal{Q}^+(3,q)$ and $|G_{\mathcal{Q}^+}| = |G_P| = 2(q^3-q)$. From the Orbit–Stabilizer Theorem, it follows that under the action of G, there are $q^4(q+1)(q^3-1)/2$ hyperbolic quadrics such that π is tangent and $q^5(q-1)(q^3-1)/2$ hyperbolic quadrics such that π is secant. On the other hand, $q^4(q+1)(q^3-1)/2 + q^5(q-1)(q^3-1)/2 = q^4(q^2+1)(q^3-1)/2$, which is the total number of hyperbolic quadrics of $\mathrm{PG}(3,q)$. □

Lemma 2.2.6. *Let $\mathcal{C}$ be a non–degenerate conic of π. Then there are $q^3(q-1)/2$ hyperbolic quadrics of* $\mathrm{PG}(3,q)$ *meeting π in $\mathcal{C}$ and they are permuted in a single orbit by the group $G_{\mathcal{C}}$.*

Proof. The number of non–degenerate conics of π equals $q^5 - q^2$ and they are permuted in a single orbit by the group G. Hence, $G_{\mathcal{C}}$ the stabilizer in G of a non–degenerate conic $\mathcal{C}$ of π has order $q^3(q^3-q)(q-1)$. Let $\mathcal{Q}^+(3,q)$ be a hyperbolic quadric of $\mathrm{PG}(3,q)$ such that $\mathcal{Q}^+(3,q) \cap \pi = \mathcal{C}$ and let $\perp$ the polarity of $\mathrm{PG}(3,q)$ associated with $\mathcal{Q}^+(3,q)$. The stabilizer of $\mathcal{Q}^+(3,q)$ in the group $G_{\mathcal{C}}$ is the stabilizer of π in $\mathrm{PGO}^+(4,q)$, which in turn coincides with the stabilizer of P in $\mathrm{PGO}^+(4,q)$, where $P = \pi^\perp$. Therefore it has order $2(q^3-q)$. From the Orbit–Stabilizer Theorem, we have that, under the action of $G_{\mathcal{C}}$, the number of hyperbolic quadrics through the conic $\mathcal{C}$ is $q^3(q-1)/2$. Finally, note that $(q^5-q^2)q^3(q-1)/2$ is the number of hyperbolic quadrics of $\mathrm{PG}(3,q)$ such that π is secant. □

Let $\mathcal{H}$ be the set of all hyperbolic quadrics of $\mathrm{PG}(3,q)$ meeting π in a conic of $\mathcal{B}$. Taking into account Lemma 2.2.6 and the fact that $|\mathcal{B}| = q^2+q+1$, we have that $|\mathcal{H}| = q^3(q-1)(q^2+q+1)/2 = (q^6-q^3)/2$.

Let κ be the Klein map between the lines of $\mathrm{PG}(3,q)$ and the points of a hyperbolic quadric $\mathcal{Q}^+(5,q)$ of $\mathrm{PG}(5,q)$. Let $\perp$ be the polarity of $\mathrm{PG}(5,q)$ associated with $\mathcal{Q}^+(5,q)$. The lines of the plane π are mapped by κ to the points of a Greek plane, say α, of $\mathcal{Q}^+(5,q)$. The lines of a regulus $\mathcal{R}$ of a $\mathcal{Q}^+(3,q)$ are sent by κ to the points of a non–degenerate conic $\kappa(\mathcal{R})$ of $\mathcal{Q}^+(5,q)$. In particular the plane $\langle\kappa(\mathcal{R})\rangle$, containing the conic $\kappa(\mathcal{R})$, meets the quadric $\mathcal{Q}^+(5,q)$ exactly in $\kappa(\mathcal{R})$. Therefore, by applying the Klein map to the q^6-q^3 reguli of the quadrics of $\mathcal{H}$, we get a set of q^6-q^3 non–degenerate conics of $\mathcal{Q}^+(5,q)$. Each of these conics is contained in a plane. Let $\mathcal{X}$ be the set consisting of these q^6-q^3 planes of $\mathrm{PG}(5,q)$.

$$\mathcal{X} = \{\langle\kappa(\mathcal{R})\rangle \mid \mathcal{R} \textit{ is a regulus of a quadric of } \mathcal{H}\}.$$

Lemma 2.2.7. *If $\mathcal{Q}_1, \mathcal{Q}_2 \in \mathcal{H}$ are not on the same conic of $\mathcal{B}$, i.e., $\mathcal{Q}_i \cap \pi = \mathcal{C}_i$, $\mathcal{C}_i \in \mathcal{B}$, $1 \le i \le 2$, $\mathcal{C}_1 \neq \mathcal{C}_2$. Then*

i) $|\mathcal{Q}_1 \cap \mathcal{Q}_2| \ge |\mathcal{C}_1 \cap \mathcal{C}_2| \ge 1$,

ii) *$\mathcal{Q}_1, \mathcal{Q}_2$ can share at most one line in a regulus.*

Proof. Assume that a regulus of $\mathcal{Q}_1$ shares two lines with a regulus of $\mathcal{Q}_2$, then $|\mathcal{C}_1 \cap \mathcal{C}_2| \ge 2$, a contradiction. On the other hand, $|\mathcal{Q}_1 \cap \mathcal{Q}_2| \ge |\mathcal{C}_1 \cap \mathcal{C}_2| \ge 1$. □

Lemma 2.2.8. *If $\sigma \in \mathcal{X}$, then $|\sigma \cap \alpha| = 0$.*

Proof. It is enough to observe that no line contained in a hyperbolic quadric of $\mathcal{H}$ lies on π. □

Proposition 2.2.9. *$\mathcal{X}$ consists of q^6-q^3 planes mutually intersecting in at most one point.*

Proof. Let σ_1 and σ_2 be two distinct planes of $\mathcal{X}$ and let $\mathcal{R}_1$ and $\mathcal{R}_2$ be the two reguli of quadrics of $\mathcal{H}$ such that $\kappa(\mathcal{R}_i) = \sigma_i \cap \mathcal{Q}^+(5,q)$, $1 \le i \le 2$. Let $\mathcal{Q}_i$ be the hyperbolic quadric of $\mathcal{H}$ containing the regulus $\mathcal{R}_i$, $1 \le i \le 2$. Assume by contradiction that $\sigma_1 \cap \sigma_2$ is a line, say ℓ. Then σ_1 and σ_2 generate a 3–space, say Σ. First of all observe that $\Sigma \cap \mathcal{Q}^+(5,q)$ cannot contain a plane γ of $\mathcal{Q}^+(5,q)$, otherwise $\gamma \cap \sigma_1$ would be a line contained in the non–degenerate conic $\sigma_1 \cap \mathcal{Q}^+(5,q)$, a contradiction. Therefore Σ meets $\mathcal{Q}^+(5,q)$ in either a hyperbolic quadric, or an elliptic quadric, or a quadratic cone.

We may assume that $\mathcal{Q}_1 \neq \mathcal{Q}_2$. Indeed, if $\mathcal{Q}_1 = \mathcal{Q}_2$, then $\mathcal{R}_1$ is the opposite regulus of $\mathcal{R}_2$ and hence $\sigma_2 = \sigma_1^\perp$. In this case σ_1 and σ_2 generate a 4–space if q is even and the whole 5–space if q is odd, a contradiction.

If $\mathcal{Q}_1$ and $\mathcal{Q}_2$ were on the same conic of $\mathcal{B}$, i.e., $\mathcal{Q}_1 \cap \pi = \mathcal{Q}_2 \cap \pi$, then $\mathcal{Q}_1 \cap \mathcal{Q}_2$ would contain a non–degenerate conic, contradicting Lemma 1.4.6.

Assume that $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are not on the same conic of $\mathcal{B}$, i.e., $\mathcal{Q}_i \cap \pi = \mathcal{C}_i$, $\mathcal{C}_i \in \mathcal{B}$, $1 \le i \le 2$, $\mathcal{C}_1 \neq \mathcal{C}_2$. We consider several cases.

$\boxed{\Sigma \cap \mathcal{Q}^+(5,q) \text{ is a hyperbolic quadric}}$

In this case $\mathcal{R}_1, \mathcal{R}_2$ belong to a hyperbolic congruence and $\sigma_1^\perp \cap \sigma_2^\perp = \Sigma^\perp$ is a line that is secant to $\mathcal{Q}^+(5,q)$. Hence the opposite regulus of $\mathcal{R}_1$ would share two lines with the opposite regulus of $\mathcal{R}_2$, contradicting Lemma 2.2.7 *ii)*.

$\boxed{\Sigma \cap \mathcal{Q}^+(5,q) \text{ is a quadratic cone}}$

In this case $\mathcal{R}_1, \mathcal{R}_2$ belong to a parabolic congruence with axis r. Each of the lines of both $\mathcal{R}_1$ and $\mathcal{R}_2$ intersects r in a point and hence r is a line of the opposite regulus of both $\mathcal{R}_1$ and $\mathcal{R}_2$. In particular $r \subseteq \mathcal{Q}_1 \cap \mathcal{Q}_2$ and $r \cap \pi \subseteq \mathcal{C}1 \cap \mathcal{C}_2$. Thus $r \cap \pi = \mathcal{C}_1 \cap \mathcal{C}_2 = P$. Let ℓ_i be the line of $\mathcal{R}_i$ through the point P, $1 \le i \le 2$. Recall that in a parabolic congruence with axis r there are $q+1$ planes on r and each of them contains (apart from r) other q lines of the congruence forming a pencil with center on r. This means that r, ℓ_1 and ℓ_2 are contained in a plane ξ. Note that ξ is tangent to both $\mathcal{Q}_1$ and $\mathcal{Q}_2$ at P. Therefore $\xi \cap \pi$ is a line that is tangent to both $\mathcal{C}_1$ and $\mathcal{C}_2$ at the point P, contradicting Lemma 2.2.4.

$\boxed{\Sigma \cap \mathcal{Q}^+(5,q) \text{ is an elliptic quadric}}$

In this case $\mathcal{R}_1, \mathcal{R}_2$ belong to an elliptic congruence $\mathcal{L}$ (i.e., a regular spread of $\mathrm{PG}(3,q)$). If ℓ is secant to $\mathcal{Q}^+(5,q)$, then the reguli $\mathcal{R}_1$ and $\mathcal{R}_2$ should share two lines, contradicting Lemma 2.2.7 *ii)*. If ℓ is external to $\mathcal{Q}^+(5,q)$, then $\mathcal{R}_1$ and $\mathcal{R}_2$

are disjoint reguli of $\mathcal{L}$. Then $|\mathcal{Q}_1 \cap \mathcal{Q}_2| = 0$, contradicting Lemma 2.2.7 *i)*. If ℓ is tangent to $\mathcal{Q}^+(5,q)$, then $\sigma_1^\perp \cap \sigma_2^\perp = \Sigma^\perp$ that is a line external to $\mathcal{Q}^+(5,q)$ and, since $\langle \sigma_1^\perp, \sigma_2^\perp \rangle = \ell^\perp$, the 3–space they generate meets $\mathcal{Q}^+(5,q)$ in a quadratic cone. This case has already been considered and the proof is now complete. □

Note that the set $\mathcal{X}$ is left invariant by a group of order $q^6(q-1)(q^2-1)(q^3-1)$ isomorphic to G. Let $\mathcal{Y}$ be the set of q^3+q^2+q Greek planes of $\mathcal{Q}^+(5,q)$ distinct from α.

Proposition 2.2.10. *$\mathcal{X} \cup \mathcal{Y}$ is a set of q^6+q^2+q planes mutually intersecting in at most one point.*

Proof. If $\sigma \in \mathcal{X}$, then $\sigma \cap \mathcal{Q}^+(5,q)$ is a non–degenerate conic. Let $\xi \in \mathcal{Y}$. Then $|\sigma \cap \xi| \leq 1$. Indeed, otherwise $\sigma \cap \xi$ should be a line contained in $\sigma \cap \mathcal{Q}^+(5,q)$, a contradiction. On the other hand, if $\xi_1, \xi_2 \in \mathcal{Y}$, $\xi_1 \neq \xi_2$, then $|\xi_1 \cap \xi_2| = 1$, since any two Greek planes share exactly a point. □

Proposition 2.2.11. *There exists a family $\mathcal{Z}$ of q^2+q+1 planes meeting α in a line and mutually intersecting in one point.*

Proof. Through a line ℓ of $\mathcal{Q}^+(5,q)$ there are $q-1$ planes of $\mathrm{PG}(5,q)$ meeting $\mathcal{Q}^+(5,q)$ exactly in ℓ. Let $\mathcal{T}_\ell$ be the set consisting of these $q-1$ planes. Varying the line ℓ over the plane α and choosing one of the planes in $\mathcal{T}_\ell$, for every line of α, we get a family $\mathcal{Z}$ of q^2+q+1 planes. Let $\xi_1 \in \mathcal{T}_{\ell_1}$ and $\xi_2 \in \mathcal{T}_{\ell_2}$ be planes of $\mathrm{PG}(5,q)$ meeting α in the lines ℓ_1 and ℓ_2, respectively, with $\ell_1 \neq \ell_2$. Assume by contradiction that the planes ξ_1 and ξ_2 share a line. Then they generate a projective 3–space containing α and therefore another plane α' contained in $\mathcal{Q}^+(5,q)$. In particular α' is a Latin plane. This means that α' meets ξ_1, ξ_2 in a line contained in $\mathcal{Q}^+(5,q)$ and distinct from ℓ_1 and ℓ_2, respectively, contradicting the fact that $\xi_i \cap \mathcal{Q}^+(5,q) = \ell_i$, $1 \leq i \leq 2$. □

Proposition 2.2.12. *$\mathcal{X} \cup \mathcal{Y} \cup \mathcal{Z}$ is a set of q^6+2q^2+2q+1 planes mutually intersecting in at most one point.*

Proof. Let $\eta \in \mathcal{X}$, $\gamma \in \mathcal{Y}$ and $\xi \in \mathcal{Z}$. We need to show that $\eta \cap \xi$ cannot be a line and $\gamma \cap \xi$ cannot be a line.

Assume, by contradiction, that $\eta \cap \xi$ is a line, say ℓ. If $\ell = \xi \cap \alpha$ then ℓ is contained in $\mathcal{Q}^+(5,q)$ and $\ell = \eta \cap \xi \cap \mathcal{Q}^+(5,q)$. In this case the non–degenerate conic $\eta \cap \mathcal{Q}^+(5,q)$ contains the line ℓ, a contradiction. If $\ell \neq \xi \cap \alpha$, then ℓ is a line tangent to $\mathcal{Q}^+(5,q)$ at a point $P \in \alpha$. Hence, in this case the non–degenerate conic $\eta \cap \mathcal{Q}^+(5,q)$ contains the point $P \in \alpha$, contradicting Lemma 2.2.8.

Assume, by contradiction, that $\xi \cap \gamma$ is a line, say r. Then r should be contained in $\mathcal{Q}^+(5,q)$. But the unique line of ξ contained in $\mathcal{Q}^+(5,q)$ is the line $\xi \cap \alpha$. Hence $r = \xi \cap \alpha = \xi \cap \gamma$. In particular $r = \gamma \cap \alpha$ and the two Greek planes, α and γ have the line r in common, a contradiction. □

We can summarize the previous results in the following theorem.

Theorem 2.2.13. *Any projective bundle of* $\mathrm{PG}(2,q)$ *gives rise to a* $(6, q^6 + 2q^2 + 2q + 1, 4; 3)_q$ *constant–dimension subspace code.*

Corollary 2.2.14. $\mathcal{A}_q(6,4,3) \geq q^6 + 2q^2 + 2q + 1$.

The exact value of $\mathcal{A}_q(6,4,3)$ is known only when $q = 2$: the maximum number of planes of $\mathrm{PG}(5,2)$ pairwise intersecting in at most a point is 77. In particular in [23], with the aid of a computer, it has been shown that there are 5 non–isomorphic examples of $(6,77,4;3)_2$ constant–dimension codes. The code arising from Proposition 2.2.12 falls in one of these 5 classes and it is optimal when $q = 2$.

Open Problems 2.2.15. *1)* Improve the lower and upper bounds on $\mathcal{A}_q(6,4,3)$.

2) Determine the exact value of $\mathcal{A}_q(6,4,3)$ for small q.

Chapter 3

Cameron–Liebler line classes of $\mathrm{PG}(3,q)$

Here we are concerned with Cameron–Liebler line classes of $\mathrm{PG}(3,q)$, see [6, 7].

3.1 Tactical decompositions of $\mathrm{PG}(3,q)$

Let $\mathcal{S}$ be the 2–design whose points are the points of $\mathrm{PG}(3,q)$ and whose blocks are the lines of $\mathrm{PG}(3,q)$. Let G be a collineation group of $\mathrm{PG}(3,q)$, i.e., $G \leq \mathrm{P\Gamma L}(4,q)$. From Lemma 1.2.3, the orbits of G on points and lines of $\mathrm{PG}(3,q)$ form a tactical decomposition $\mathcal{V}_1,\ldots,\mathcal{V}_m$, $\mathcal{B}_1,\ldots,\mathcal{B}_n$ of $\mathcal{S}$. To avoid obvious cases we suppose $1 < m < (q+1)(q^2+1)$ and $1 < n < (q^2+1)(q^2+q+1)$. Assume that there are k_{ij} points of $\mathcal{V}_i$ on a block of $\mathcal{B}_j$ and r_{ij} blocks of $\mathcal{B}_j$ through a point of $\mathcal{V}_i$, where $1 \leq i \leq m$ and $1 \leq j \leq n$. Recall that

$$v_i r_{ij} = b_j k_{ij}, \tag{3.1}$$

where $|\mathcal{V}_i| = v_i$ and $|\mathcal{B}_j| = b_j$, $1 \leq i \leq m$ and $1 \leq j \leq n$.

Definition 3.1.1. The m by n matrix $K = (k_{ij})$ is called *block tactical decomposition matrix* and the m by n matrix $R = (r_{ij})$ is called *point tactical decomposition matrix*.

Observe that

$$\sum_{i=1}^{m} k_{ij} = q+1, \text{ for all } 1 \leq j \leq n \text{ and } \sum_{j=1}^{n} r_{ij} = q^2+q+1, \text{ for all } 1 \leq i \leq m.$$

Hence

$$\mathcal{J}K = (q+1)\mathcal{J} \text{ and } R\mathcal{J} = (q^2+q+1)\mathcal{J}, \tag{3.2}$$

where $\mathcal{J}$ denotes the all one matrix. Moreover $\mathrm{rank}(K) = \mathrm{rank}(R) = m$.

From Block's Lemma (Lemma 1.2.7) $n \geq m$, i.e., the group G has at least as many orbits on lines as on points.

Assume that the group G as equally many orbits on lines and points of $\mathrm{PG}(3, q)$. Then the tactical decomposition induced by G is symmetric, that is $n = m$.

The following are trivial examples of subgroups of $\mathrm{P\Gamma L}(4, q)$ with equally many orbits on lines and points of $\mathrm{PG}(3, q)$.

Examples 3.1.2. Let P be a point of $\mathrm{PG}(3, q)$ and let π be a plane of $\mathrm{PG}(3, q)$ with $P \notin \pi$.

1. If $G = Stab_{\mathrm{P\Gamma L}(4,q)}(P)$. Then G has two orbits on points of $\mathrm{PG}(3, q)$, namely P and $\mathrm{PG}(3, q) \setminus \{P\}$, and two orbits on lines of $\mathrm{PG}(3, q)$, namely those containing P and the complement.
2. If $G = Stab_{\mathrm{P\Gamma L}(4,q)}(\pi)$. Then G has two orbits on points of $\mathrm{PG}(3, q)$, namely π and $\mathrm{PG}(3, q) \setminus \{\pi\}$, and two orbits on lines of $\mathrm{PG}(3, q)$, namely those contained in π and the complement.
3. If $G = Stab_{\mathrm{P\Gamma L}(4,q)}(\{P, \pi\})$. Then G has three orbits on points of $\mathrm{PG}(3, q)$, namely P, π and $\mathrm{PG}(3, q) \setminus (\{P\} \cup \pi)$, and three orbits on lines of $\mathrm{PG}(3, q)$, namely those through P, those contained in π and their complement.

Let A and B be the following n by n diagonal matrices

$$A = \mathrm{diag}(v_1, \ldots, v_n), B = \mathrm{diag}(b_1, \ldots, b_n).$$

From equations (3.1), we have that

$$AR = KB. \tag{3.3}$$

Theorem 3.1.3. *A line class $\mathcal{B}_i$ of a symmetric tactical decomposition of* $\mathrm{PG}(3, q)$ *has the following properties:*

i)

$$|\mathcal{B}_i| = b_i = x_i(q^2+q+1).$$

ii)

$$|\{\ell \in \mathcal{B}_i \ : \ |\ell \cap m| = 1\}| = \begin{cases} x_i(q+1) & \textit{if } m \notin \mathcal{B}_i \\ x_i(q+1) + q^2 - 1 & \textit{if } m \in \mathcal{B}_i \end{cases}.$$

Proof. Let Q be a fixed point of $\mathcal{V}_j$ and let us count the triples $(P,\ell;Q)$, where $P\in\mathcal{V}_i$ and $P,Q\in\ell\in\mathcal{B}_t$. Since through Q there pass r_{jt} lines of $\mathcal{B}_t$ and each of these lines contains k_{it} points of $\mathcal{V}_i$, we have that there are $k_{it}r_{jt}$ of such triples. Hence for a fixed $Q\in\mathcal{V}_j$ the following relation holds true:

$$\sum_{t=1}^{n} k_{it}r_{jt}=\sum_{t=1}^{n}|\{(P,\ell;Q)\mid P\in\mathcal{V}_i,P,Q\in\ell\in\mathcal{B}_t\}|=$$

$$=\begin{cases} v_i & \text{if } i\neq j\\ v_i-1+q^2+q+1 & \text{if } i=j\end{cases}.$$

Therefore

$$\left(KR^t\right)_{ij}=\sum_{t=1}^{n}k_{it}r_{jt}=\begin{cases} v_i & \text{if } i\neq j\\ v_i+q^2+q & \text{if } i=j\end{cases},$$

or, equivalently,

$$KR^t=(q^2+q)\mathcal{I}+A\mathcal{J}.$$

In particular taking into account (3.2), (3.3),

$$KR^tK=(q^2+q)\mathcal{I}K+A\mathcal{J}K=(q^2+q)K+(q+1)A\mathcal{J}=$$
$$=(q^2+q)K+\frac{q+1}{q^2+q+1}AR\mathcal{J}=(q^2+q)K+\frac{q+1}{q^2+q+1}KB\mathcal{J}.$$

Since $n=m$, the matrix K is invertible (see Corollary 1.2.8) and the previous equation becomes

$$R^tK=(q^2+q)\mathcal{I}+\frac{q+1}{q^2+q+1}B\mathcal{J}. \tag{3.4}$$

Since $gcd(q+1,q^2+q+1)=1$, a first consequence of (3.4) is that

$$|\mathcal{B}_i|=b_i=x_i(q^2+q+1),1\le i\le n,$$

which proves *i)*.

Moreover

$$\left(R^tK\right)_{ij}=\sum_{t=1}^{n}r_{ti}k_{tj}=\begin{cases}\frac{(q+1)b_i}{q^2+q+1} & \text{if } i\neq j\\ \frac{(q+1)b_1}{q^2+q+1}+q^2+q & \text{if } i=j\end{cases}.$$

Let m be a fixed line of $\mathcal{B}_j$ and let us count the triples $(\ell,P;m)$, where $\ell\in\mathcal{B}_i$ and $P\in\ell\cap m, P\in\mathcal{V}_t$. Since in m there are k_{tj} points of $\mathcal{V}_t$ and through each of these points there pass r_{ti} lines of $\mathcal{B}_i$, we have that there are $r_{ti}k_{tj}$ of such triples. Hence if $i\neq j$, then $\sum_{t=1}^{n}r_{ti}k_{tj}$ counts how many lines of $\mathcal{B}_i$ meet a given line of $\mathcal{B}_j$. If $i=j$ then $\sum_{t=1}^{n}r_{ti}k_{tj}-(q+1)$ counts how many lines of $\mathcal{B}_i$ meet a given line of $\mathcal{B}_i$ in a point. □

Theorem 3.2 motivates the following definition.

Definition 3.1.4. A line set $\mathcal{L}$ of $\mathrm{PG}(3,q)$ is said to be a *Cameron–Liebler line class of* $\mathrm{PG}(3,q)$ with parameter x if

$$|\{\ell\ :\ \ell \in \mathcal{L}, |\ell \cap m| > 0\}| = \begin{cases} x(q+1) & m \notin \mathcal{L} \\ x(q+1)+q^2 & m \in \mathcal{L} \end{cases}.$$

The complement of a Cameron–Liebler line class with parameter x is a Cameron–Liebler line class with parameter q^2+1-x and the union of two disjoint Cameron–Liebler line classes with parameters x and y, respectively, is a Cameron–Liebler line class with parameter $x+y$. From Examples 3.1.2 there are trivial examples of symmetric tactical decompositions of $\mathrm{PG}(3,q)$ with two or three point and line classes. Hence there are trivial examples of Cameron–Liebler line classes of $\mathrm{PG}(3,q)$ with parameter $1, 2, q^2, q^2-1$.

Remark 3.1.5. It can be seen that a Cameron–Liebler line class with parameter $x=1$ consists of either the set of lines through a point or of the set of lines in a plane. A Cameron–Liebler line class with parameter $x=2$ is the union of the two previous examples, if the point is not in the plane [7].

Proposition 3.1.6. *A Cameron–Liebler line class of* $\mathrm{PG}(3,q)$ *with parameter* 2 *is not a line class of a symmetric tactical decomposition of* $\mathrm{PG}(3,q)$.

Proof. Let P be a point of $\mathrm{PG}(3,q)$ and let π be a plane of $\mathrm{PG}(3,q)$ with $P \notin \pi$. Let $\mathcal{L}$ be the line set consisting of the lines through P or contained in π. Then $|\mathcal{L}| = 2(q^2+q+1)$. Moreover a line ℓ of $\mathrm{PG}(3,q)$ is incident either with $2(q+1)+q^2$ lines of $\mathcal{L}$ or with $2(q+1)$ lines of $\mathcal{L}$ according as $\ell \in \mathcal{L}$ or does not. Therefore $\mathcal{L}$ is a Cameron–Liebler line class of $\mathrm{PG}(3,q)$ with parameter 2.

Observe that $\mathcal{L}$ cannot arise as a line class of a symmetric tactical decomposition $\mathcal{T}$ of $\mathrm{PG}(3,q)$. Otherwise, since P is the unique point of $\mathrm{PG}(3,q)$ such that through P there pass q^2+q+1 lines of $\mathcal{L}$, then $\{P\}$ has to form a point class of $\mathcal{T}$. On the other hand, a line ℓ of $\mathcal{L}$ contains either one point of $\{P\}$ or none, according as $P \in \ell$ or $P \notin \ell$. Therefore $\mathcal{L}$ cannot be a line class of $\mathcal{T}$. □

In [6], the authors stated the following conjectures.

Conjecture 3.1.7. A collineation group of $\mathrm{PG}(3,q)$, which has the same number of point and line orbits either is line transitive, or it is listed in Examples 3.1.2.

Conjecture 3.1.8. Let $\mathcal{T}$ be a symmetric tactical decomposition of $\mathrm{PG}(3,q)$. Then $\mathcal{T}$ is one of those listed in Examples 3.1.2.

Conjecture 3.1.9. Let $\mathcal{L}$ be a Cameron–Liebler line classes of $\mathrm{PG}(3,q)$. Then $\mathcal{L}$ is one of those arising from Examples 3.1.2.

Conjecture 3.1.10 (Weaker Conjecture). In a symmetric tactical decomposition of $\mathrm{PG}(3, q)$ either one of the point classes consists of one point or one of the point classes is a hyperplane.

Recently Conjecture 3.1.7 has been proved [2], and [7].

Theorem 3.1.11. *A collineation group G of $\mathrm{PG}(d, q)$ having equally many orbits on points and lines either*

i) stabilizes a hyperplane π and acts line–transitively on it; or (dually)

ii) fixes a point P and acts line–transitively on the quotient space; or

iii) is line–transitive. In this case three possibilities occur:

a) G contains $\mathrm{PSL}(d+1, q)$;

b) $G = A_7 \leq \mathrm{PGL}(4, 2)$,

c) G is the normalizer in $\mathrm{PGL}(5, 2)$ of a Singer cyclic group of $\mathrm{PG}(4, 2)$.

Remark 3.1.12. Let $\mathcal{S}$ be the 2–design whose points are the points of $\mathrm{PG}(2, q)$ and whose blocks are the lines of $\mathrm{PG}(2, q)$. Then $v = b = q^2 + q + 1$ and hence $n = m$. Therefore in this case any tactical decomposition of $\mathcal{S}$ is symmetric. On the other hand, if $\mathcal{S}$ is the 2–design whose points are the points of $\mathrm{PG}(s, q)$ and whose blocks are the lines of $\mathrm{PG}(s, q)$, $s \geq 3$, and Σ is an s'–space of $\mathrm{PG}(s, q)$, $s' \geq 2$, then a symmetric tactical decomposition of $\mathcal{S}$ induces a symmetric tactical decomposition of Σ.

In [12], the authors provided the first counterexample to Conjecture 3.1.8, see Remark 3.2.10. Also Conjecture 3.1.9 has been disproved (see Section 3.2), while Conjecture 3.1.10 is still open.

We conclude this section with the following results on symmetric tactical decompositions of $\mathrm{PG}(3, q)$ having two or three classes [34] [35].

Theorem 3.1.13. *Let $\mathcal{T}$ be a symmetric tactical decomposition of $\mathrm{PG}(3, q)$ with two classes. Then either $\mathcal{T}$ is one of those listed in Examples 3.1.2 or q is an odd square and one of the two point classes of $\mathcal{T}$ has size either*

$$\frac{1 + (q^2 + q + 1)(q - \sqrt{q}) - q\sqrt{q}}{2} \text{ or } \frac{1 + (q^2 + q + 1)(q - \sqrt{q}) + q\sqrt{q}}{2}.$$

Theorem 3.1.14. *Let $\mathcal{T}$ be a symmetric tactical decomposition of $\mathrm{PG}(3, q)$ with three classes such that one point class and one line class consist of all the points and lines of a plane π. Then either $\mathcal{T}$ is one of those listed in Examples 3.1.2 or q is an odd square and one of the two point classes of $\mathcal{T}$ distinct from π has size*

$$\frac{q^3 - \sqrt{q}^3}{2}.$$

Using the same techniques the following result on symmetric tactical decomposition of $\mathrm{PG}(3, q)$ with four classes can be shown.

Theorem 3.1.15. *Let $\mathcal{T}$ be a symmetric tactical decomposition of $\mathrm{PG}(3, q)$ with four classes such that one point class and one line class consist of all the points and lines of a plane π and one point class and one line class of a point $P \notin \pi$ and all the lines through P. Then q is an odd square and one of the two point classes of $\mathcal{T}$ distinct from π and $\{P\}$ has size*

$$\frac{q^3 - 1}{2}.$$

Open Problems 3.1.16. *1)* Prove or disprove the Weaker Conjecture 3.1.10.

2) Provide an upper bound on the number of classes that a symmetric tactical decomposition may have.

3) Construct new non–trivial symmetric tactical decompositions of $\mathrm{PG}(3, q)$.

4) The existence of a structure as indicated in Theorem 3.1.13 would disprove the Weaker Conjecture. Prove or disprove that a non–trivial symmetric tactical decomposition of $\mathrm{PG}(3, q)$ with two classes as indicated in Theorem 3.1.13 exists.

5) Prove or disprove that a non–trivial symmetric tactical decomposition of $\mathrm{PG}(3, q)$ with three classes as indicated in Theorem 3.1.14 exists.

6) Classify the symmetric tactical decomposition of $\mathrm{PG}(3, q)$ with four classes as indicated in Theorem 3.1.15.

7) Investigate symmetric tactical decompositions in other structures, such as generalized quadrangles and polar spaces.

8) Classify the symmetric tactical decompositions of $\mathrm{PG}(3, q)$ for small q.

3.2 Cameron–Liebler line classes of $\mathrm{PG}(3, q)$

Let $\mathcal{L}$ be a Cameron–Liebler line class of $\mathrm{PG}(3, q)$. The numbers

$$|\{\ell \in \mathcal{L} \ : \ \ell \subset \pi\}|, \pi \text{ a plane, or } |\{\ell \in \mathcal{L} \ : \ P \in \ell\}|, P \text{ a point}$$

are the *characters of $\mathcal{L}$* with respect to line–sets in planes or line–stars of $\mathrm{PG}(3, q)$.

Lemma 3.2.1. *Let $\mathcal{L}$ be a Cameron–Liebler line class of $\mathrm{PG}(3, q)$ and let $\perp$ be a polarity of $\mathrm{PG}(3, q)$. Then $\mathcal{L}^\perp = \{\ell^\perp \mid \ell \in \mathcal{L}\}$ is a Cameron–Liebler line class with the same characters of $\mathcal{L}$.*

Proof. The result easily follows from the fact that two lines ℓ, ℓ' of $\mathrm{PG}(3,q)$ are incident if and only if $\ell^\perp, \ell'^\perp$ are incident. Moreover, since the lines through a point are mapped by $\perp$ to the lines in a plane, it follows that the characters of $\mathcal{L}$ with respect to line–sets in planes are the characters of $\mathcal{L}^\perp$ with respect to line–stars of $\mathrm{PG}(3,q)$ and viceversa. □

Definition 3.2.2. Two Cameron–Liebler line classes $\mathcal{L}, \mathcal{L}'$ of $\mathrm{PG}(3,q)$ are said to be *equivalent* or *isomorphic* if there exists a collineation α of $\mathrm{PG}(3,q)$ such that $\mathcal{L}^\alpha = \mathcal{L}'$ or $\mathcal{L}^\alpha = \mathcal{L}'^\perp$.

Note that isomorphic Cameron–Liebler line classes have the same characters. The next result mentions some of the characterizations of a Cameron–Liebler line class of $\mathrm{PG}(3,q)$ which have been proved by several authors, see [6, 31].

Theorem 3.2.3. *The following properties are equivalent:*

- *$\mathcal{L}$ is a Cameron–Liebler line class of* $\mathrm{PG}(3,q)$ *with parameter x.*
- $|\mathcal{R} \cap \mathcal{L}| = |R^o \cap \mathcal{L}|$ *for every regulus $\mathcal{R}$ and its opposite $\mathcal{R}^o$.*
- $|\mathcal{L} \cap \mathcal{S}| = x$ *for every line–spread $\mathcal{S}$.*
- $|\mathcal{L} \cap \mathcal{S}| = x$ *for every regular line–spread $\mathcal{S}$.*

Non–existence results have been proved in [29], [17].

Theorem 3.2.4. *Let $\mathcal{L}$ be a Cameron–Liebler line class of* $\mathrm{PG}(3,q)$ *with parameter x, then*

- *either $x \leq 2$ or $x > \left(\sqrt[3]{\frac{q}{2}} - \frac{2}{3}\right) q$;*
- *the following modular equation has to be satisfied:*

$$\binom{x}{2} + c(c-x) \equiv 0 \pmod{q+1},$$

where c is a character of $\mathcal{L}$.

3.2.1 The Bruen–Drudge's example

Let q be odd. An elliptic quadric $\mathcal{Q}^-(3,q)$ of $\mathrm{PG}(3,q)$ with orthogonal polarity $\perp$ consists of q^2+1 points no three on a line. Each point of $\mathcal{Q}^-(3,q)$ lies on q^2 secants to $\mathcal{Q}^-(3,q)$, and on $q+1$ tangent lines. The lines that are tangent to a point

$P \in \mathcal{Q}^-(3,q)$ are contained in the plane $P^\perp$ and pass through P. A plane $\pi = P^\perp$ of $\mathrm{PG}(3,q)$ is either *secant to* $\mathcal{Q}^-(3,q)$ and $\pi \cap \mathcal{Q}^-(3,q)$ is a non–degenerate conic (in this case $P \notin \pi$) or it is *tangent to* $\mathcal{Q}^-(3,q)$ and meets $\mathcal{Q}^-(3,q)$ in the point P. The stabilizer of $\mathcal{Q}^-(3,q)$ in $\mathrm{PGL}(4,q)$ is denoted by $\mathrm{PGO}^-(4,q)$ and has order $2(q^6-q^2)$. The group $\mathrm{PGO}^-(4,q)$ and has a subgroup of index two isomorphic to $\mathrm{PGL}(2,q^2)$, which in turn contains a subgroup of index two isomorphic to $\mathrm{PSL}(2,q^2)$.

In [5] Bruen and Drudge found an infinite family of Cameron–Liebler line classes with parameter $x = (q^2+1)/2$, q odd. Bruen–Drudge's example admits a group isomorphic to $\mathrm{PSL}(2,q^2)$, stabilizing an elliptic quadric $\mathcal{Q}^-(3,q)$ of $\mathrm{PG}(3,q)$, as an automorphism group.

Let $\mathcal{Q}^+(3,q^2)$ be the hyperbolic quadric of $\mathrm{PG}(3,q^2)$ having equation $X_1X_4 - X_2X_3 = 0$. Recall that if $P_i = (x_i,y_i) \in \mathrm{PG}(1,q^2)$, $1 \le i \le 2$, then $P_1 \otimes P_2 = (x_1,y_1)\otimes(x_2,y_2) = (x_1x_2, x_1y_2, y_1x_2, y_1y_2)$ is a point of $\mathcal{Q}^+(3,q^2)$ and

$$\mathcal{Q}^+(3,q^2) = \{P_1 \otimes P_2 \mid P_1, P_2 \in \mathrm{PG}(1,q^2)\}.$$

Consider the following subset of points of $\mathcal{Q}^+(3,q)$

$$\begin{aligned}\mathcal{E} = \{P \otimes P^q \mid P \in \mathrm{PG}(1,q^2)\} = \\ = \{(x^{q+1}, xy^q, x^qy, y^{q+1}) \mid x,y \in \mathrm{GF}(q^2), (x,y) \neq (0,0)\} = \\ = \{(1,z,z^q,z^{q+1}) \mid z \in \mathrm{GF}(q^2)\} \cup \{(0,0,0,1)\}.\end{aligned}$$

Then $\mathcal{E} \subset \Sigma = \{(u,z,z^q,v) \mid u,v \in \mathrm{GF}(q), z \in \mathrm{GF}(q^2), (u,v,z) \neq (0,0,0)\}$.

Proposition 3.2.5. *$\mathcal{E}$ is an elliptic quadric $\mathcal{Q}^-(3,q)$ of the Baer subgeometry $\Sigma \simeq \mathrm{PG}(3,q)$.*

Proof. Let $\alpha \in \mathrm{GF}(q)$ such that $X^2 + \alpha = 0$ is irreducible over $\mathrm{GF}(q)$. Let $\boldsymbol{i} \in \mathrm{GF}(q^2)$ such that $\boldsymbol{i}^2 + \alpha = 0$. Since $\boldsymbol{i}(\boldsymbol{i}^q + \boldsymbol{i}) = \boldsymbol{i}^{q+1} + \boldsymbol{i}^2 = \boldsymbol{i}^{q+1} - \alpha \in \mathrm{GF}(q)$, then necessarily $\boldsymbol{i}^q + \boldsymbol{i} = 0$. Let $\mathrm{GF}(q^2) = \mathrm{GF}(q)[\boldsymbol{i}]$. Hence if $z \in \mathrm{GF}(q^2)$, then $z = a + \boldsymbol{i}b$, $z^q = a - \boldsymbol{i}b$ and $z^{q+1} = a^2 + \alpha b^2$, where $a, b \in \mathrm{GF}(q)$. Let φ be the projectivity of $\mathrm{PG}(3,q^2)$ associated with the matrix

$$\begin{pmatrix} 0 & 1/2\boldsymbol{i} & -1/2\boldsymbol{i} & 0 \\ 0 & 1/2 & 1/2 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

If $P = (u,z,z^q,v)$ and $z = a + \boldsymbol{i}b$, then $P^\varphi = (b,a,v,u)$. Therefore

$$\Sigma^\varphi = \{(b,a,v,u) \mid a,b,u,v \in \mathrm{GF}(q), (b,a,v,u) \neq (0,0,0,0)\} = \mathrm{PG}(3,q)$$

and

$$\mathcal{E}^{\varphi} = \{(b, a, a^2 + \alpha b^2, 1) \mid a, b \in \mathrm{GF}(q^2)\} \cup \{(0,0,1,0)\},$$

that is the elliptic quadric $\mathcal{Q}^-(3,q)$ of $\mathrm{PG}(3,q)$ satisfying $\alpha X_1^2 + X_2^2 - X_3X_4 = 0$. □

Let G be the subgroup of index two of $\mathrm{PGO}^-(4,q)$, stabilizing $\mathcal{E}$. It is easily seen that a projectivity of G is associated with a matrix

$$M \otimes M^q = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} a^q & b^q \\ c^q & d^q \end{pmatrix} = \begin{pmatrix} a^{q+1} & ab^q & ba^q & b^{q+1} \\ ac^q & ad^q & bc^q & bd^q \\ ca^q & cb^q & da^q & db^q \\ c^{q+1} & cd^q & dc^q & d^{q+1} \end{pmatrix}, \tag{3.5}$$

where $a, b, c, d \in \mathrm{GF}(q^2)$, with $ad - bc \neq 0$.

Let K the subgroup of index two of G whose elements are associated with a matrix $M \otimes M^q$, where $M \in \mathrm{SL}(2,q^2)$, i.e., $\det(M) = 1$. Then $|K| = (q^6 - q^2)/2$.

Proposition 3.2.6. *The group K has three orbits on points of Σ: the points of $\mathcal{E}$ and other two orbits $\mathcal{O}_s$ and $\mathcal{O}_n$ of size $q^2(q^2+1)/2$.*

Proof. Let ξ be the projectivity of $K \simeq \mathrm{PSL}(2,q^2)$ associated with the matrix $M \otimes M^q$ as indicated in (3.5), where $\det(M) = 1$.

Let $U_1 = (1,0,0,0) \in \mathcal{Q}^-(3,q)$. Then $U_1^{\xi} = U_1$ if and only if $c = 0$. Indeed, every projectivity associated with

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \otimes \begin{pmatrix} a^q & b^q \\ 0 & d^q \end{pmatrix}, a, b, d \in \mathrm{GF}(q), ad = 1, \text{ i.e. } d = a^{-1}$$

fixes U_1. Since the couples (a,b) and $(-a,-b)$ determine the same projectivity ξ, we have that $|Stab_K(U_1)| = q^2(q^2-1)/2$. Hence $|U_1^K| = q^2 + 1 = |\mathcal{E}|$.

Let $v \in \mathrm{GF}(q) \setminus \{0\}$ and let $P = (1,0,0,v) \in \mathrm{PG}(3,q) \setminus \mathcal{Q}^-(3,q)$. Then $P^{\xi} = P$ if and only if $ac^q + vbd^q = 0$ and $a^{q+1} + vb^{q+1} = v^{-1}c^{q+1} + d^{q+1}$ if and only if

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a^q & c^q \\ vb^q & vd^q \end{pmatrix} = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda v \end{pmatrix},$$

where $\lambda = a^{q+1} + vb^{q+1}$. Taking the determinants in the previous equation we get $\lambda = \pm 1$. Then we have that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \lambda d^q & -\frac{\lambda}{v} c^q \\ -\lambda v b^q & \lambda a^q \end{pmatrix},$$

that is equivalent to $c = \lambda v b^q, d = \lambda a^q$. Hence ξ is induced by $M \otimes M^q$, where either

$$M = \begin{pmatrix} a & b \\ -vb^q & a^q \end{pmatrix}, a, b \in \mathrm{GF}(q^2), a^{q+1} - vb^{q+1} = 1,$$

or

$$M = \begin{pmatrix} a & b \\ vb^q & -a^q \end{pmatrix}, a, b \in \mathrm{GF}(q^2), a^{q+1} + vb^{q+1} = -1.$$

Since the couples (a,b) and $(-a,-b)$ determine the same projectivity ξ, it follows that ξ can be chosen in $q^3 - q$ ways. Hence $|Stab_K(P)| = q(q^2-1)$ and $|P^K| = (q^3+q)/2$. □

Remark 3.2.7. If $P = (1,0,0,v) \in \mathrm{PG}(3,q) \setminus \mathcal{Q}^-(3,q)$, $v \in \mathrm{GF}(q) \setminus \{0\}$, then $P^\xi = (a^{q+1} + vb^{q+1}, ac^q + vbd^q, ca^q + vdb^q, c^{q+1} + vd^{q+1})$. Let Q be the quadratic form associated to $\mathcal{E}$, note that $Q(P^\xi)$ is a square or a non–square in $\mathrm{GF}(q)$ according as $Q(P)$ is a square or a non–square in $\mathrm{GF}(q)$.

The two orbits $\mathcal{O}_s$, $\mathcal{O}_n$ correspond to points of $\mathrm{PG}(3,q)$ such that the evaluation of the quadratic form associated to $\mathcal{E}$ is a square or a non–square in $\mathrm{GF}(q)$, respectively.

Proposition 3.2.8. *i) The group K has four orbits on lines of Σ: two orbits, say $\mathcal{L}_1$ and $\mathcal{L}_2$, both of size $(q+1)(q^2+1)/2$, consisting of lines tangent to $\mathcal{E}$ and two orbits, say $\mathcal{L}_3$ and $\mathcal{L}_4$, both of size $q^2(q^2+1)/2$ consisting of lines secant and external to $\mathcal{E}$, respectively.*

ii) A line of $\mathcal{L}_1$ ($\mathcal{L}_2$) contains q points of $\mathcal{O}_s$ ($\mathcal{O}_n$), a secant line to $\mathcal{E}$ contains $(q-1)/2$ points of $\mathcal{O}_s$ and $(q-1)/2$ points of $\mathcal{O}_n$ and an external line to $\mathcal{E}$ contains $(q+1)/2$ points of $\mathcal{O}_s$ and $(q+1)/2$ points of $\mathcal{O}_n$.

Proof. Let ℓ be a line of Σ and let ξ be the projectivity of $K \simeq \mathrm{PSL}(2,q^2)$ associated with the matrix $M \otimes M^q$ as indicated in (3.5), where $\det(M) = 1$.

If ℓ is given by $zX_3 - z^qX_2 = 0$, for some $z \in \mathrm{GF}(q^2) \setminus \{0\}$, then ℓ is tangent to $\mathcal{E}$ at the point $U_1 = (1,0,0,0)$. Varying $u \in \mathrm{GF}(q)$, $T = (u, z, z^q, 0)$ is a point of ℓ distinct from U_1. In order to fix ℓ, the projectivity ξ has to fix $\ell \cap \mathcal{E} = U_1$. Hence $c = 0$ and $a = 1/d$. Straightforward calculations show that T^ξ belongs to ℓ if and only if $d^2 = d^{2q}$, that is $d^2 \in \mathrm{GF}(q) \setminus \{0\}$. There are $2(q-1)$ elements d in $\mathrm{GF}(q^2) \setminus \{0\}$ such that $d^2 \in \mathrm{GF}(q) \setminus \{0\}$. However if d has this property also $-d$ has this property but they determine the same projectivity ξ. On the other hand b can be chosen arbitrarily in $\mathrm{GF}(q^2)$ and ξ is induced by

$$\begin{pmatrix} 1/d & b \\ 0 & d \end{pmatrix} \otimes \begin{pmatrix} 1/d^q & b^q \\ 0 & d^q \end{pmatrix}, b, d \in \mathrm{GF}(q), d^2 \in \mathrm{GF}(q) \setminus \{0\}.$$

Therefore $|Stab_K(\ell)| = q^2(q-1)$ and $|\ell^K| = (q+1)(q^2+1)/2$. Note that $Q(T) = -z^{q+1}$ and hence $T \in \mathcal{O}_s$ or $T \in \mathcal{O}_n$ according as $-z^{q+1}$ is a square or a non–square in GF(q). Then either ℓ contains q points of $\mathcal{O}_s$ or q points of $\mathcal{O}_n$.

Let ℓ be the secant line to $\mathcal{E}$ given by $X_2 = X_3 = 0$. Here $\ell \cap \mathcal{E} = \{U_1 = (1,0,0,0), U_4 = (0,0,0,1)\}$. Varying $u,v \in$ GF(q), $(u,v) \neq (0,0)$, the point $T = (u,0,0,v)$ belongs to ℓ. Some calculations show that T^ξ belongs to ℓ if and only if $uac^q + vbd^q = 0$. Then two possibilities arise: either $c = 0$, which implies $b = 0$, $a,d \neq 0$, $a = 1/d$, or $c \neq 0$ and then $a = d = 0$, $b \neq 0$, $b = -1/c$. In the former case ξ is induced by

$$\begin{pmatrix} 1/d & 0 \\ 0 & d \end{pmatrix} \otimes \begin{pmatrix} 1/d^q & 0 \\ 0 & d^q \end{pmatrix}, d \in \mathrm{GF}(q^2) \setminus \{0\}.$$

Note that d and $-d$ determine the same projectivity and hence there are $(q^2-1)/2$ projectivities arising in this way. In the latter case ξ is induced by

$$\begin{pmatrix} 0 & -1/c \\ c & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & -1/c^q \\ c^q & 0 \end{pmatrix}, c \in \mathrm{GF}(q^2) \setminus \{0\}.$$

Again c and $-c$ determine the same projectivity and hence there are $(q^2-1)/2$ projectivities arising in this way. Hence $|Stab_K(\ell)| = q^2-1$ and $|\ell^K| = q^2(q^2+1)/2$ that is the total number of secant lines to $\mathcal{E}$. On the other hand $\ell^\perp$ is a line external to $\mathcal{E}$ and hence K has a unique orbit on external lines to $\mathcal{E}$ as well. Finally observe that if $T \in \ell \setminus \mathcal{E}$, then $Q(T) = uv \in$ GF$(q) \setminus \{0\}$. Therefore $\{Q(T) \mid T \in \ell \setminus \mathcal{E}\} =$ GF$(q) \setminus \{0\}$ and ℓ contains $(q-1)/2$ points of both $\mathcal{O}_s$ and $\mathcal{O}_n$. □

The block–tactical decomposition matrix for this orbit decomposition is

$$K = \left[\begin{array}{c|cccc} & \mathcal{L}_1 & \mathcal{L}_2 & \mathcal{L}_3 & \mathcal{L}_4 \\ \hline \mathcal{E} & 1 & 1 & 2 & 0 \\ \mathcal{O}_n & q & 0 & \frac{q-1}{2} & \frac{q+1}{2} \\ \mathcal{O}_s & 0 & q & \frac{q-1}{2} & \frac{q+1}{2} \end{array}\right], \tag{3.6}$$

and hence the point–tactical decomposition matrix is

$$R = \left[\begin{array}{c|cccc} & \mathcal{L}_1 & \mathcal{L}_2 & \mathcal{L}_3 & \mathcal{L}_4 \\ \hline \mathcal{E} & \frac{q+1}{2} & \frac{q+1}{2} & q^2 & 0 \\ \mathcal{O}_n & q+1 & 0 & \frac{q(q-1)}{2} & \frac{q(q+1)}{2} \\ \mathcal{O}_s & 0 & q+1 & \frac{q(q-1)}{2} & \frac{q(q+1)}{2} \end{array}\right]. \tag{3.7}$$

From the orbit–decompositions above it is an easy matter to prove that gluing together one set among $\mathcal{L}_1$, $\mathcal{L}_2$ and one set among $\mathcal{L}_3$, $\mathcal{L}_4$, an example of Cameron–

Liebler line class is obtained. This is the Cameron–Liebler line class constructed in [5].

Theorem 3.2.9. *Gluing together one set among $\mathcal{L}_1$, $\mathcal{L}_2$ and one set among $\mathcal{L}_3$, $\mathcal{L}_4$, a Cameron–Liebler line class of* $\mathrm{PG}(3,q)$ *is obtained.*

Proof. Consider the line–set $\mathcal{L}_1 \cup \mathcal{L}_3$. The other cases are similar. From the first and third column of the matrix 3.6, a line of $\mathcal{L}_1$ in incident with one point of $\mathcal{E}$ and q points of $\mathcal{O}_n$, whereas a line of $\mathcal{L}_3$ shares 2 points with $\mathcal{E}$ and $(q-1)/2$ points with both $\mathcal{O}_s$ and $\mathcal{O}_n$. On the other hand, from the first and third column of the matrix 3.7 there are $(q+1)/2$ lines of $\mathcal{L}_1$ though a point of $\mathcal{E}$ and $q+1$ lines of $\mathcal{L}_1$ through a point of $\mathcal{O}_n$, while there are q^2 lines of $\mathcal{L}_3$ through a point of $\mathcal{E}$ and $q(q-1)/2$ lines of $\mathcal{L}_3$ through a point of $\mathcal{O}_n$ or of $\mathcal{O}_s$. Hence there are $(q-1)/2+q^2+1$ lines of $\mathcal{L}_1$ meeting a given line of $\mathcal{L}_1$ and $q^2+q^2(q-1)/2$ lines of $\mathcal{L}_3$ incident with a given line of $\mathcal{L}_1$. Analogously there are $2(q+1)/2+(q-1)/2(q+1)$ lines of $\mathcal{L}_1$ incident with a given line of $\mathcal{L}_3$ and $2(q^2-1)+2(q-1)/2\,(q(q-1)/2-1)+1$ lines of $\mathcal{L}_3$ meeting a given line of $\mathcal{L}_3$. Therefore there are

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

lines of $\mathcal{L}_1 \cup \mathcal{L}_3$ incident with a line of $\mathcal{L}_1 \cup \mathcal{L}_3$.

Similarly, from the second and fourth column of the matrix 3.6 a line of $\mathcal{L}_2$ in incident with one point of $\mathcal{E}$ and q points of $\mathcal{O}_s$, whereas a line of $\mathcal{L}_4$ shares $(q+1)/2$ points with both $\mathcal{O}_s$ and $\mathcal{O}_n$. Hence there are $(q+1)/2$ lines of $\mathcal{L}_1$ meeting a given line of $\mathcal{L}_2$ and $q^2+q^2(q-1)/2$ lines of $\mathcal{L}_3$ incident with a given line of $\mathcal{L}_2$. Analogously there are $(q+1)/2(q+1)$ lines of $\mathcal{L}_1$ incident with a given line of $\mathcal{L}_4$ and $2(q+1)/2q(q-1)/2$ lines of $\mathcal{L}_3$ meeting a given line of $\mathcal{L}_4$. Therefore there are

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

lines of $\mathcal{L}_1 \cup \mathcal{L}_3$ incident with a line of $\mathcal{L}_2 \cup \mathcal{L}_4$ □

3.2.2 The known examples of Cameron–Liebler line classes of $\mathrm{PG}(3,q)$

Up to date, the following infinite families of Cameron–Liebler line classes with parameter x are known.

1) The Bruen–Drudge's family [5], admitting the group $K \simeq \mathrm{PSL}(2,q^2)$ stabilizing an elliptic quadric $\mathcal{Q}^-(3,q)$ of $\mathrm{PG}(3,q)$, q odd.

   In particular, if $\mathcal{L}^i = \mathcal{L}_2 \cup \mathcal{L}_4$, then $\mathcal{L}^i$ has the following three characters with respect to line–sets in planes of $\mathrm{PG}(3,q)$:

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

   and

   $$\frac{q+1}{2}, \frac{q^2+q}{2}, \frac{q^2+q}{2}+q+1,$$

   with respect to line–stars of $\mathrm{PG}(3,q)$.

2) The first family derived from Bruen–Drudge [8], [16], admitting the stabilizer K' of a point of $\mathcal{Q}^-(3,q)$ in K, $q \geq 5$ odd.

   Consider a point R of $\mathcal{Q}^-(3,q)$ and let ρ be the tangent plane to $\mathcal{Q}^-(3,q)$ at the point R. Let $\mathcal{L}^{ii}$ be the line–set of $\mathrm{PG}(3,q)$ obtained from $\mathcal{L}^i$, by replacing the q^2 lines of $\mathcal{L}_4$ contained in ρ with the q^2 lines of $\mathcal{L}_3$ passing through R. Then $\mathcal{L}^{ii}$ is again a Cameron–Liebler line class with parameter $(q^2+1)/2$. In particular, $\mathcal{L}^{ii}$ has the following five characters with respect to line–sets in planes of $\mathrm{PG}(3,q)$:

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

   and

   $$\frac{q+3}{2}, \frac{q^2+q}{2}-q, \frac{q^2+q}{2}+1, \frac{q^2+q}{2}+q+2, q^2+\frac{q+1}{2},$$

   with respect to line–stars of $\mathrm{PG}(3,q)$. It turns out that, if $q>3$, these characters are distinct from those of a Bruen–Drudge Cameron–Liebler line class.

3) The second family derived from Bruen–Drudge [10], say $\mathcal{L}^{iii}$, admitting a subgroup of K' of order $q^2(q+1)$, $q \geq 7$ odd.

   Here the existence of a pencil of elliptic quadrics fixed by a subgroup of K' of order $q^2(q+1)$ plays a crucial role and the derivation is similar to the previous example with a more restrictive selection of tangent lines to the elliptic quadrics of the pencil. The characters of the Cameron–Liebler line class $\mathcal{L}^{iii}$ with respect to line–sets in planes of $\mathrm{PG}(3,q)$ form a subset of:

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

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

and with respect to line–stars of $\mathrm{PG}(3,q)$ form a subset of:

$$\left\{\frac{q+1}{2}, \frac{5(q+1)}{2}, \frac{q^2+q}{2} - 2(q+1), \frac{q^2+q}{2} - (q+1),\right.$$

$$\left.\frac{q^2+q}{2}, \frac{q^2+q}{2} + q + 1, \frac{q^2+q}{2} + 2(q+1), \frac{q^2+q}{2} + 3(q+1)\right\}.$$

4) The third family derived from Bruen–Drudge [11], say $\mathcal{L}^{iv}$, admitting an automorphism group isomorphic to $\mathrm{PGL}(2,q)$, $q \equiv 1 \pmod 4$, $q \geq 9$ odd. The characters of $\mathcal{L}^{iv}$, with respect to line–stars of $\mathrm{PG}(3,q)$ are:

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

whereas the characters of $\mathcal{L}^{iv}$, with respect to line–sets in planes of $\mathrm{PG}(3,q)$ are:

$$\frac{3q+5}{2}, \frac{q^2+q}{2} - q, \frac{q^2+q}{2} + 1, \frac{q^2+q}{2} + q + 2, \frac{q^2+q}{2} + 2q + 3, q^2 + \frac{q+1}{2}.$$

5) The "cyclic" family [12], [14], admitting a group of order $3(q-1)(q^2+q+1)/2$, $q \equiv 5$ or $9 \pmod{12}$.

Infinite families of Cameron–Liebler line classes with parameter $(q^2-1)/2$ were found for $q \equiv 5$ or $9 \pmod{12}$ in [12], [14]. By construction, for a line class $\mathcal{X}$ of such a family there is a fixed plane Π and a fixed point $z \notin \Pi$ such that $\mathcal{X}$ never contains the lines $\mathcal{Y}$ of the plane Π and the lines $\mathcal{Z}$ through the point z. Therefore, $\mathcal{X} \cup \mathcal{Y}$ and $\mathcal{X} \cup \mathcal{Z}$ are both examples of Cameron–Liebler line classes with parameter $(q^2+1)/2$ and $\mathcal{X} \cup \mathcal{Y} \cup \mathcal{Z}$ is a Cameron–Liebler line class with parameter $(q^2+3)/2$. In particular the examples $\mathcal{X} \cup \mathcal{Y}$, $\mathcal{X} \cup \mathcal{Z}$ and $\mathcal{X} \cup \mathcal{Y} \cup \mathcal{Z}$ admit q^2+q+1 as a character.

It should be noted that there are other sporadic constructions of Cameron–Liebler line classes of $\mathrm{PG}(3,q)$:

- a Cameron–Liebler line class of $\mathrm{PG}(3,4)$ with parameter 7 [18];
- a Cameron–Liebler line class of $\mathrm{PG}(3,5)$ with parameter 10, [17];
- Cameron–Liebler line class of $\mathrm{PG}(3,q)$ with parameter $\frac{(q+1)^2}{3}$, $q \equiv 2 \pmod 3$, $q < 150$, [32].

Finally, Cameron–Liebler line classes have been classified in $\mathrm{PG}(3,q)$, $q = 2, 3, 4, 5$, see [15].

Remark 3.2.10. In [12], the authors studied the action of a group G of order $(q-1)(q^2+q+1)/4$ fixing a plane Π and a point $z \notin \Pi$. If $q \equiv 5$ or $9 \pmod{12}$, the group G in its action on lines stabilizes a partition into four disjoint Cameron–Liebler line classes consisting of $\mathcal{Y}$ the line set of Π, $\mathcal{Z}$ the lines through z, $\mathcal{L}_1$ and $\mathcal{L}_2$ both having parameter $(q^2-1)/2$; in its action on points of $\mathrm{PG}(3,q) \setminus (\{z\} \cup \Pi)$ the group G has 4 orbits. Moreover, if $q \equiv 9 \pmod{12}$, i.e. $q = 3^{2h}$, then through a point of $\mathrm{PG}(3,q) \setminus (\{z\} \cup \Pi)$ there pass either $(q+1)(q-\sqrt{q})$ or $(q+1)(q+\sqrt{q})$ lines of $\mathcal{L}_1$. Hence there exists a non–trivial tactical decomposition of $\mathrm{PG}(3,q)$ with four point and line classes.

Open Problems 3.2.11. *1)* Construct new examples of Cameron–Liebler line classes.

2) Determine new values of x for which a Cameron–Liebler line class of $\mathrm{PG}(3,q)$ with parameter x cannot exist.

Chapter 4

Appendix

4.1 The known bundles of $\mathrm{PG}(2,q)$

The *pencil* of quadrics of $\mathrm{PG}(n,q)$ generated by two quadrics with equations $F = 0$ and $F' = 0$, respectively, is the set of quadrics defined by $\lambda F + \mu F'$, where $\lambda, \mu \in \mathrm{GF}(q)$, $(\lambda, \mu) \neq (0,0)$. A *linear system* of quadrics of $\mathrm{PG}(n,q)$ is a collection $\mathcal{B}$ of quadrics of $\mathrm{PG}(n,q)$ such that the pencil generated by two quadrics of $\mathcal{B}$ is contained in $\mathcal{B}$.

A cyclic group of $\mathrm{PGL}(3,q)$ permuting points (lines) of $\mathrm{PG}(2,q)$ in a single orbit is called a *Singer cyclic group* of $\mathrm{PGL}(3,q)$. A generator of a Singer cyclic group is called a *Singer cycle*. See [20].

A *projective bundle* of $\mathrm{PG}(2,q)$ is a family of q^2+q+1 non–degenerate conics of $\mathrm{PG}(2,q)$ mutually intersecting in a point. In other words, the conics in a projective bundle play the role of lines in $\mathrm{PG}(2,q)$, i.e., it is a model of projective plane (see Proposition 2.2.3). Let π be the projective plane $\mathrm{PG}(2,q)$. Embed π into $\Pi = \mathrm{PG}(2,q^3)$, and let τ be the period 3 collineation of Π fixing pointwise π. Let us fix a triangle Δ of vertices P, P^τ, P^{τ^2} in Π. Up to date, the known types of projective bundles are as follows:

1. *circumscribed bundle* consisting of all conics of π that extended over $\mathrm{GF}(q^3)$ contain the vertices of Δ. This exists for all q;

2. *inscribed bundle* consisting of all conics of π that extended over $\mathrm{GF}(q^3)$ are tangent to the three sides of Δ. This exists for all odd q;

3. *self–polar bundle* consisting of all conics of π that extended over $\mathrm{GF}(q^3)$ admit Δ as a self–polar triangle. This exists for all odd q.

Since the triangle Δ is fixed by a Singer cyclic group of $\mathrm{PGL}(3,q)$, we may conclude that all these projective bundles are invariant under a Singer cyclic group of $\mathrm{PGL}(3,q)$. The first and third types are linear systems of conics, whereas the inscribed bundle is not a linear system. For more details on projective bundles, see [3] and references therein.

4.2 The circumscribed bundle of $\mathrm{PG}(2,q)$

In this section we describe in more details the circumscribed bundle of $\mathrm{PG}(2,q)$. Let π be a subplane isomorphic to $\mathrm{PG}(2,q)$. Embed π into $\Pi = \mathrm{PG}(2,q^3)$, and let τ be the period 3 collineation of Π fixing pointwise π.

Let G be the group of collineations of Π stabilizing π. The group G has three orbits on points of Π:

- $\mathcal{O}_1$ consisting of the q^2+q+1 points of π;
- $\mathcal{O}_2$ consisting of the $q(q^2-1)(q^2+q+1)$ points of $\Pi \setminus \pi$ lying on the lines of Π arising from sublines of π;
- $\mathcal{O}_3$ consisting of the $q^3(q^2-1)(q-1)$ points of their complement.

Hence line set of Π is partitioned into three G–orbits corresponding to sublines of π, lines meeting π in a point and lines external to π. Observe that $\tau \leq G$ fixes pointwise $\mathcal{O}_1$ and induces a partition of both $\mathcal{O}_2$ and $\mathcal{O}_3$ into subsets of points of size three. Each of these subsets has three collinear points or a triangle according as it is contained in $\mathcal{O}_2$ or in $\mathcal{O}_3$, respectively.

Lemma 4.2.1. *[20, Corollary 7.5] In a Desarguesian projective plane there exists a unique non–degenerate conic containing five points, no three of them are on a line.*

Lemma 4.2.2. *Let $\bar{\mathcal{C}}$ be a non–degenerate conic of Π. Then $\bar{\mathcal{C}} \cap \pi$ is a non–degenerate conic of π if and only if $\bar{\mathcal{C}}$ is fixed by τ.*

Proof. Let $\bar{\mathcal{C}}$ be a non–degenerate conic of Π and let $\mathcal{C} = \bar{\mathcal{C}} \cap \pi$. If $\mathcal{C}$ is a non–degenerate conic of π and $q \geq 4$, then τ has to fix $\bar{\mathcal{C}}$, otherwise $\mathcal{C} \subseteq \bar{\mathcal{C}}^{\tau} \cap \bar{\mathcal{C}}$ and $|\mathcal{C}| \geq 5$, contradicting Lemma 4.2.1. Some computations show that the result holds true also if $q = 2, 3$.

Viceversa, let $\pi = \mathrm{PG}(2,q)$. Then τ is the collineation of order 3 of Π given by

$$X_1' = X_1^q, X_2' = X_2^q, X_3' = X_3^q.$$

If $\bar{\mathcal{C}}$ is given by

$$\sum_{i,j=1,i\leq j}^{3} a_{ij}X_iX_j = 0,$$

where $a_{ij} \in \mathrm{GF}(q^3)$. Moreover $\bar{\mathcal{C}}^\tau$ is given by

$$\sum_{i,j=1,i\leq j}^{3} a_{ij}^q X_iX_j = 0.$$

Since $\bar{\mathcal{C}} = \bar{\mathcal{C}}^\tau$, we have that there exists $\lambda \in \mathrm{GF}(q^3) \setminus \{0\}$ such that $a_{ij} = \lambda a_{ij}^q$, for all i, j. Of course there exists at one among the a_{ij} which is not zero. Thus we may assume that such an a_{ij} equals 1 and hence $\lambda = 1$ and $a_{ij} \in \mathrm{GF}(q)$, for all i, j. This means that $\bar{\mathcal{C}} \cap \mathrm{PG}(2,q) = \mathcal{C}$ is a conic of $\mathrm{PG}(2,q)$. □

Let $\Delta = \{U_1, U_2, U_3\}$ be a triangle consisting of points of $\mathcal{O}_3$ left invariant by τ. Assume that $U_1^\tau = U_2$, $U_2^\tau = U_3$ and $U_3^\tau = U_1$. Note that a line ℓ joining two points of Δ has the property that $\ell \cap \ell^\tau \in \Delta$ and hence has to be disjoint from π, otherwise $\ell \cap \ell^\tau \in \pi$, a contradiction. Therefore, if P, T are two distinct points of π, then $\{U_1, U_2, U_3, P, T\}$ is a set of five points of Π no three of them on a line. From Lemma 4.2.1 there is a unique conic $\bar{\mathcal{C}}$ of Π containing these five points. We claim that $\bar{\mathcal{C}}$ is fixed by τ. Indeed, assume by contradiction that $\bar{\mathcal{C}}^\tau \neq \bar{\mathcal{C}}$, then $\{U_1, U_2, U_3, P, T\} \subseteq \bar{\mathcal{C}}^\tau \cap \bar{\mathcal{C}}$, contradicting Lemma 4.2.1.

For any two distinct points P, T of π consider the conic of Π containing $\{U_1, U_2, U_3, P, T\}$. Hence there are

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

conics of Π arising in this way. From Lemma 4.2.2, each of these $q^2 + q + 1$ conics of Π meets π in a non–degenerate conic of π. Let $\mathcal{B}$ denote the $q^2 + q + 1$ conics of π so obtained. For a fixed point $P \in \pi$, let us count in two ways the couples $(T, \mathcal{C})$ where $\mathcal{C}$ is a conic of $\mathcal{B}$ such that $P \in \mathcal{C}$ and T is a point of $\pi \setminus \{P\}$ such that $T \in \mathcal{C}$; then

$$q^2 + q = qr,$$

where x denotes the number of conics of $\mathcal{B}$ through P. Hence $r = q + 1$. As a consequence two distinct conics of $\mathcal{B}$ meet in exactly one point, i.e., $\mathcal{B}$ is a bundle of $\mathrm{PG}(2,q)$.

In terms of coordinates, in $\mathrm{PG}(2,q^3)$ let π be the set consisting of the points (x, x^q, x^{q^2}), where $x \in \mathrm{GF}(q^3) \setminus \{0\}$. If ω is a primitive element of $\mathrm{GF}(q^3)$, then the projectivity of $\mathrm{PG}(2,q^3)$ associated with the matrix

$$\begin{pmatrix} 1 & 1 & 1 \\ \omega & \omega^q & \omega^{q^2} \\ \omega^2 & \omega^{2q} & \omega^{2q^2} \end{pmatrix}$$

maps π to the canonical subplane of $\mathrm{PG}(2,q^3)$. Hence π is a subplane of $\mathrm{PG}(2,q^3)$ isomorphic to $\mathrm{PG}(2,q)$. Let τ be the collineation of order 3 of $\mathrm{PG}(2,q^3)$ given by

$$X_1' = X_3^q, X_2' = X_1^q, X_3' = X_2^q.$$

It is easily seen that a point P of $\mathrm{PG}(2,q^3)$ is fixed by τ if and only if P belongs to π. Let Δ denote the $\langle\tau\rangle$–orbit triangle consisting of $U_1 = (1,0,0), U_2 = (0,1,0), U_3 = (0,0,1)$.

Let $a \in \mathrm{GF}(q^3) \setminus \{0\}$ and let $\mathcal{Q}_a$ be the non–degenerate conic of $\mathrm{PG}(2,q^3)$ given by

$$aX_1X_2 + a^qX_1X_3 + a^{q^2}X_2X_3 = 0.$$

Straightforward computations show that $\mathcal{Q}_a$ is fixed by τ and that $\Delta \subset \mathcal{Q}_a$, for all $a \in \mathrm{GF}(q^3) \setminus \{0\}$. Therefore

$$\mathcal{B} = \{\mathcal{Q}_a \mid a \in \mathrm{GF}(q^3) \setminus \{0\}\}$$

is the circumscribed bundle of π.

References

[1] R. Ahlswede, N. Cai, S.Y.R. Li, R.W. Yeung, Network information flow, *IEEE Transactions on Information Theory*, 46 (4), 1204–1216, 2000.

[2] J. Bamberg, T. Penttila, Overgroups of cyclic Sylow subgroups of linear groups, *Comm. Algebra* 36 (2008), no. 7, 2503–2543.

[3] R.D. Baker, J.M.N. Brown, G.L. Ebert, J.C. Fisher, Projective bundles, *Bull. Belg. Math. Soc. Simon Stevin* 1 (1994), no. 3, 329–336.

[4] A. Beutelspacher, Partial spreads in finite projective spaces and partial designs, *Math. Z.* 145 (1975), no. 3, 211–229.

[5] A.A. Bruen, K. Drudge, The construction of Cameron–Liebler line classes in $\mathrm{PG}(3,q)$, *Finite Fields Appl.* 5 (1999), no. 1, 35–45.

[6] P.J. Cameron, R.A. Liebler, Tactical decompositions and orbits of projective groups, *Linear Algebra Appl.* 46 (1982), 91–102.

[7] P.J. Cameron, Four lectures on projective geometry, *Finite geometries (Winnipeg, Man., 1984)*, 27–63, Lecture Notes in Pure and Appl. Math., 103, Dekker, New York, 1985.

[8] A. Cossidente, F. Pavese, On subspace codes, *Des. Codes Cryptogr.* 78 (2016), no. 2, 527–531.

[9] A. Cossidente, F. Pavese, L. Storme, Geometrical aspects of subspace codes, *Network coding and subspace designs*, 107–129, Signals Commun. Technol., Springer, Cham, 2018.

[10] A. Cossidente, F. Pavese, New Cameron–Liebler line classes with parameter $\frac{q^2+1}{2}$, *J. Algebraic Combin.* 49 (2019), no. 2, 193–208.

[11] A. Cossidente, F. Pavese, Cameron–Liebler line classes of $\mathrm{PG}(3,q)$ admitting $\mathrm{PGL}(2,q)$, *J. Combin. Theory Ser. A* 167 (2019), 104–120.

[12] J. De Beule, J. Demeyer, K. Metsch, M. Rodgers, A new family of tight sets in $\mathcal{Q}^+(5,q)$, *Des. Codes Cryptogr*. 78 (2016), no. 3, 655–678.

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

[14] T. Feng, K. Momihara, Q. Xiang, Cameron–Liebler line classes with parameter $x = \frac{q^2-1}{2}$, *J. Combin. Theory Ser. A* 133 (2015), 307–338.

[15] A.L. Gavrilyuk, I. Matkin, Cameron–Liebler line classes in $\mathrm{PG}(3,5)$, *J. Combin. Des.* 26 (2018), no. 12, 563–580.

[16] A.L. Gavrilyuk, I. Matkin, T. Penttila, Derivation of Cameron–Liebler line classes, *Des. Codes Cryptogr.* 86 (2018), no. 1, 231–236.

[17] A.L. Gavrilyuk, K. Metsch, A modular equality for Cameron–Liebler line classes, *J. Combin. Theory Ser. A* 127 (2014), 224–242.

[18] P. Govaerts, T. Penttila, Cameron–Liebler line classes in $\mathrm{PG}(3,4)$, *Bull. Belg. Math. Soc. Simon Stevin* 12 (2005), no. 5, 793–804.

[19] Larry C. Grove, *Classical groups and geometric algebra*, Graduate Studies in Mathematics, 39. American Mathematical Society, Providence, RI, 2002.

[20] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford Mathematical Monographs, Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1998.

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

[22] J.W.P. Hirschfeld, J.A. Thas, *General Galois Geometries*, Springer Monographs in Mathematics, Springer, London, 2016.

[23] T. Honold, M. Kiermaier, S. Kurz, Optimal binary subspace codes of length 6, constant dimension 3 and minimum subspace distance 4, *Topics in finite fields*, 157–176, *Contemp. Math.*, 632, Amer. Math. Soc., Providence, RI, 2015.

[24] T. Honold, M. Kiermaier, S. Kurz, Partial spreads and vector space partitions, *Network coding and subspace designs*, 131–170, Signals Commun. Technol., Springer, Cham, 2018.

[25] D.R. Hughes, F.C. Piper, *Projective planes*, Graduate Texts in Mathematics, Vol. 6. Springer-Verlag, New York-Berlin, 1973.

[26] D.R. Hughes, F.C. Piper, *Design theory*, Second edition. Cambridge University Press, Cambridge, 1988.

[27] R. Kötter, F.R. Kschischang, Coding for errors and erasures in random network coding, *IEEE Transactions on Information Theory*, 54(8), 3579–3591, 2008.

[28] F.J. MacWilliams, N.J.A. Sloane, *The theory of error-correcting codes I, II*, North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.

[29] K. Metsch, An improved bound on the existence of Cameron–Liebler line classes, *J. Combin. Theory Ser. A* 121 (2014), 89–93.

[30] E. Nvastase, P. Sissokho, The maximum size of a partial spread in a finite projective space, *J. Combin. Theory Ser. A* 152 (2017), 353–362.

[31] T. Penttila, Cameron–Liebler line classes in $\mathrm{PG}(3, q)$, *Geom. Dedicata* 37 (1991), no. 3, 245–252.

[32] M. Rodgers, On some new examples of Cameron–Liebler line classes, *Ph.D. Thesis*, University of Colorado, Denver, 2012.

[33] B. Segre, Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane, *Ann. Mat. Pura Appl.* 64, 1–76 (1964).

[34] M. Tallini–Scafati, Calotte di tipo (m, n) in uno spazio di Galois $S_{r,q}$, *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur.* (8) 53 (1972), 71–81 (1973).

[35] M. Tallini–Scafati, On k–sets of kind (m, n) of a finite projective or affine space, *Combinatorial and geometric structures and their applications* (Trento, 1980), pp. 39–56, *Ann. Discrete Math.*, 14, North-Holland, Amsterdam-New York, 1982.

[36] D.E. Taylor, *The geometry of the classical groups*, Sigma Series in Pure Mathematics, 9. Heldermann Verlag, Berlin, 1992.

Part IV

Linear Sets

Geertrui Van de Voorde

School of Mathematics and Statistics
University of Canterbury
Private Bag 4800
Christchurch 8140
Zealand

email: geertrui.vandevoorde@canterbury.ac.nz

Contents

Preface

These lectures notes serve as an introduction to the theory of linear sets. Since their formal introduction almost 20 years ago, a large amount of material has been published either using linear sets or about linear sets themselves. The excellent survey on linear sets and their applications by O. Polverino [60] deserves a special mention here.

Most of these papers deal with the applications of linear sets to a variety of geometrical problems. Depending on the problem, a different point of view on linear sets may be used. In an attempt to unify these different approaches, these lecture notes mostly focus on the different definitions, points of view and notations that are in use. We hope that this helps students and researchers to feel more at ease when encountering linear sets. The material in these notes are only partly new. The majority has been taken from various sources, in particular [17, 18, 19, 45]. Of course, there is much more that can be said and done. Even though they provide (way) too much material to be covered in this summer school, these lecture notes are in no way complete!

In the first section, the concept of *field reduction* will be introduced. We will see how this way to think about Desarguesian spreads fits in with the more classical approach using indicator sets. In Section 2, we come to the definition of a linear set and navigate between different equivalent views, from a purely geometric one to a more algebraic one. In Section 3, we will continue down the algebraic path and link linear sets with linearised polynomials and the direction problem. In Section 4, we will see some applications of linear sets to blocking sets, hyperovals and KM-arcs.

The last section contains some open research problems for which all the necessary background is covered in these lecture notes. It would be great if the lectures are an incentive for participants to tackle some of these problems – I would love to see some of them solved in the near future!

Geertrui Van de Voorde, Christchurch, May 2019

Chapter 1

Field reduction and Desarguesian spreads

1.1 Some basics of (finite) fields

Let $q = p^h$, p prime, $h \geq 1$. Up to isomorphism, there is a unique finite field of order q, denoted by $\mathbb{F}_q$ (or $\mathrm{GF}(q)$). This field can be constructed as follows:

$$\mathbb{F}_q \cong \mathbb{Z}_p[X]/(f(X)),$$

where f is a monic irreducible polynomial of degree h.

Example 1.1.1. We can construct $\mathbb{F}_{16} = \mathbb{F}_{2^4}$ as

$$\mathbb{Z}_2[X]/(X^4 + X + 1).$$

Hence, the elements are cosets of polynomials and can be represented by their coset leaders

$$0, 1, X, X + 1, X^2, X^2 + 1, X^2 + X, X^2 + X + 1,$$

$$X^3, X^3+1, X^3+X, X^3+X+1, X^3+X^2, X^3+X^2+1, X^3+X^2+X, X^3+X^2+X+1.$$

Addition of two elements of $\mathbb{F}_{16}$ is executed in $\mathbb{Z}_2[X]$, e.g.

$$(X^3 + X^2 + X) + (X + 1) = X^3 + X^2 + 1.$$

Obviously, the symbol X may now be replaced by any other symbol. We see that $\mathbb{F}_{16}$ forms a 4-dimensional vector space over $\mathbb{Z}_2$.

Let ω be a root of the polynomial $X^4 + X + 1$, then we have that

$$\omega^0 = 1, \omega^1 = \omega, \omega^2 = \omega^2, \omega^3 = \omega^3, \omega^4 = \omega + 1, \omega^5 = \omega^2 + \omega,$$
$$\omega^6 = \omega^3 + \omega^2, \omega^7 = \omega^3 + \omega + 1, \omega^8 = \omega^2 + 1, \omega^9 = \omega^3 + \omega, \omega^{10} = \omega^2 + \omega + 1,$$
$$\omega^{11} = \omega^3 + \omega^2 + \omega, \omega^{12} = \omega^3 + \omega^2 + \omega + 1, \omega^{13} = \omega^3 + \omega^2 + 1, \omega^{14} = \omega^3 + 1,$$

We see that all elements of $\mathbb{F}_{16}^*$ are obtained by the first 15 powers of the element ω ($\omega^{15} = 1$). The elements of $\mathbb{F}_{16}^*$ thus form a cyclic group, generated by ω. Such an element ω is called a *primitive* element.

The behaviour seen in the previous example extends to general finite fields. The main properties are stated in the following result.

Result 1.1.2. Let $q = p^h$, p prime.

1. $\mathbb{F}_p \cong \mathbb{Z}_p$
2. $pa = 0$ for all $a \in \mathbb{F}_q$, where $pa = \underbrace{a + a + \ldots + a}_{p \text{ times}}$
3. The $q - 1$ non-zero elements of $\mathbb{F}_q$ satisfy
$$x^{q-1} = 1.$$
4. The multiplicative group of $\mathbb{F}_q$ is cyclic. Thus $\mathbb{F}_q$ contains an element ω, (called a *primitive element* or *generator* of $\mathbb{F}_q$), such that
$$\omega, \omega^2, \ldots, \omega^{q-1}$$
are the $q - 1$ non-zero elements of $\mathbb{F}_q$.
5. Every automorphism of $\mathbb{F}_q$ is of the form $x \mapsto x^{p^r}$ for some $0 \leq r \leq h - 1$. In particular,
$$(a + b)^p = a^p + b^p.$$
6. For each divisor r of h, $\mathbb{F}_{p^h}$ has a unique subfield of order p^r. Furthermore, these are the only subfields of $\mathbb{F}_{p^h}$.

We have seen that $\mathbb{F}_{16}$ is 4-dimensional over its *prime field* $\mathbb{Z}_2$ (the prime field of a field is the intersection of all its subfields). But it is not hard to see that a finite field is a vector space over all its subfields. More precisely, we have the following result.

Result 1.1.3. The field $\mathbb{F}_{q^t}$ is a t-dimensional vector space over $\mathbb{F}_q$. Moreover, there exists an element $\beta \in \mathbb{F}_{q^t}$ such that

$$S = \{\beta, \beta^q, \beta^{q^2}, \ldots, \beta^{q^{t-1}}\}$$

forms a basis for $\mathbb{F}_{q^t}$ over $\mathbb{F}_q$. Such an element β is called a *normal* element and the set S is called a *normal basis* of $\mathbb{F}_{q^t}$ over $\mathbb{F}_q$.

Exercise 1.1.4. Let $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$.

(i) Show that $\alpha^2 = \alpha + 1$.

(ii) Construct $\mathbb{F}_{2^4}$ as $\mathbb{F}_4[X]/(X^2 + 1)$ (write down the elements).

(iii) Find a normal basis for $\mathbb{F}_{16}$ over $\mathbb{F}_4$.

(iv) Find a normal basis for $\mathbb{F}_{16}$ over $\mathbb{F}_2$.

1.2 Field reduction

Consider the r-dimensional vector space over the finite field $\mathbb{F}_{q_0}$. This vector space is usually denoted by $\mathbb{F}_{q_0}^r$ and consists of all vectors of length r with entries in $\mathbb{F}_{q_0}$. The projective space $\mathrm{PG}(r-1, q_0)$ can be obtained as the quotient space

$$(\mathbb{F}_{q_0}^r)^* / \sim$$

where $(x_0, \dots, x_{r-1}) \sim (y_0, \dots, y_{r-1})$ if and only if

$$(x_0, \dots, x_{r-1}) = \alpha(y_0, \dots, y_{r-1})$$

for some $\alpha \in \mathbb{F}_{q_0}^*$.

A k-dimensional subspace of $\mathbb{F}_{q_0}^r$ corresponds to a (projective) subspace of $\mathrm{PG}(r-1, q_0)$ which has dimension $(k-1)$. Projective subspaces of dimension 0,1, and 2 are called *points, lines and planes* respectively. A projective subspace of dimension $(r-2)$ is called a *hyperplane*.

We see that a point P of $\mathrm{PG}(r-1, q_0)$ corresponds to a 1-dimensional subspace of $\mathbb{F}_{q_0}^r$, consisting of a set of vectors

$$S_v := \{\alpha v \mid \alpha \in \mathbb{F}_{q_0}\}.$$

We will often denote this as $P = \langle v \rangle_{q_0}$, indicating that P is defined by the vector v, and that all $\mathbb{F}_{q_0}$ multiples of v give rise to the same point in $\mathrm{PG}(r-1, q_0)$.

We will now take the field $\mathbb{F}_{q^t}$ for $\mathbb{F}_{q_0}$. We will consider $\mathbb{F}_{q^t}^r$ as a vector space V over $\mathbb{F}_q$, which can more formally be done as in the following lemma.

Lemma 1.2.1. *Let V be the set of vectors of $\mathbb{F}^r_{q^t}$. Consider the usual addition on V but define scalar multiplication of vectors in V* only with elements of $\mathbb{F}_q$. *Then V is a vector space over $\mathbb{F}_q$ of dimension rt. Moreover, the set of vectors in S_v forms a t-dimensional subspace of V.*

Proof. Since $(\mathbb{F}^r_{q^t}, +)$ is an abelian group, so is $V, +$. The axioms for associativity of scalar multiplication, distributivity of scalar sums and distributivity of vector sums follow directly from the fact that $\mathbb{F}^r_{q^t}$ is a vector space over $\mathbb{F}_{q^t}$ and these operations are internal in $\mathbb{F}_q$ (restricting the scalars to elements of $\mathbb{F}_q$ doesn't affect these properties). Finally, since 1 is contained in the subfield $\mathbb{F}_q$, we have an identity element for the scalar multiplication in $\mathbb{F}_q$. It follows that V is an $\mathbb{F}_q$-vector space. Since it contains $(q^t)^r = q^{rt}$ elements, V is rt-dimensional over $\mathbb{F}_q$.

The vectors in S_v are the vectors in V of the form αv, $\alpha \in \mathbb{F}_{q^t}$. Let $\alpha_1 v$ and $\alpha_2 v$ be elements of S_v , then for all $\lambda_1, \lambda_2 \in \mathbb{F}_q$, we have that $\lambda_1(\alpha_1 v) + \lambda_2(\alpha_2 v) = (\lambda_1\alpha_1 + \lambda_2\alpha_2)v \in S_v$. We conclude that S_v is a subspace of V (over $\mathbb{F}_q$). Since S_v contains q^t vectors, it is has dimension t. □

Let P be a point in $\mathrm{PG}(V) = \mathrm{PG}(r-1, q^t)$ then

$$P = (x_1, \ldots, x_r)_{q^t} = \langle v \rangle_{q^t}$$

where $v \in V$. The notation $(x_1, \ldots, x_r)_{q^t}$, or $\langle v \rangle_{q^t}$ explicitely indicates that all $\mathbb{F}_{q^t}$-multiples of the vector $v = (x_1, \ldots, x_r)$ of V define the same projective point, i.e.

$$(x_1, \ldots, x_r)_{q^t} = \langle v \rangle_{q^t} = \langle \alpha v \rangle_{q^t},$$

for $\alpha \in \mathbb{F}_{q^t}$. In the above case, V is an $\mathbb{F}_{q^t}$-vector space of dimension r. We have just seen that V is an $\mathbb{F}_q$-vector space of dimension rt, denote this vector space by W. We have that $\mathrm{PG}(W) = \mathrm{PG}(rt-1, q)$. A vector v in V is also a vector in W, so we can consider v as coordinates for a point in $\mathrm{PG}(W)$. We find points with coordinates

$$Q = \langle v \rangle_q,$$

where $v \in W$. Note that in $\mathrm{PG}(W)$, points are only defined up to an $\mathbb{F}_q$-multiple. So while $P = \langle v \rangle_{q^t} = \langle \alpha v \rangle_{q^t}$, the points $\langle v \rangle_q$ and $\langle \alpha v \rangle_q$ of $\mathrm{PG}(W)$ are different.

Remark 1.2.2. The set $\{\langle \alpha v \rangle_q | \alpha \in \mathbb{F}^*_{q^t}\}$ is precisely the $(t-1)$-dimensional space in $\mathrm{PG}(W)$ defined by S_v.

In this way, we see that with every point of $\mathrm{PG}(r-1, q^t)$, there is a $(t-1)$-subspace of $\mathrm{PG}(W)$ assiciated. This is the idea behind *field reduction*. We formalise this idea introducing the *field reduction map*.

Definition 1.2.3. The field reduction map $\mathcal{F}_{r,t,q}$ is a map from the points of $\mathrm{PG}(r-1,q^t)$ to (certain) subspaces of $\mathrm{PG}(rt-1,q)$ defined as:

$$\mathcal{F}_{r,t,q} : \mathrm{PG}(r-1,q^t) \to \mathrm{PG}(rt-1,q) : \langle v\rangle_{q^t} \mapsto \{\langle \alpha v\rangle_q | \alpha \in \mathbb{F}^*_{q^t}\}. \tag{1.1}$$

Lemma 1.2.4. *Let $\mathcal{P}$ be the point set of $\mathrm{PG}(r-1,q^t)$. The following properties hold.*
(i) The field reduction map $\mathcal{F}_{r,t,q}$ is injective.
(ii) Any two distinct elements of $\mathcal{F}_{r,t,q}(\mathcal{P})$ are disjoint.
(iii) Each point in $\mathrm{PG}(rt-1,q)$ is contained in an element of $\mathcal{F}_{r,t,q}(\mathcal{P})$.
(iv) $|\mathcal{F}_{r,t,q}(\mathcal{P})| = (q^{rt}-1)/(q^t-1)$.

Proof. (i)-(ii) Suppose that $\langle v\rangle_{q^t} \mapsto \{\langle \alpha v_1\rangle_q | \alpha \in \mathbb{F}^*_{q^t}\}$ and $\langle v\rangle_{q^t} \mapsto \{\langle \alpha v_2\rangle_q | \alpha \in \mathbb{F}^*_{q^t}\}$, have at least one point in common. Then we find $\alpha, \beta \in \mathbb{F}^*_{q^t}$ and $\lambda \in \mathbb{F}^*_q$ such that $\alpha v_1 = \lambda\beta v_2$. It follows that v_1 and v_2 are $\mathbb{F}_{q^t}$-multiples of each other, and hence, that $\langle v_1\rangle_{q^n} = \langle v_2\rangle_{q^n}$. This shows that $\mathcal{F}_{r,t,q}$ is injective and that any two distinct elements of $\mathcal{F}_{r,t,q}(\mathcal{P})$ are disjoint.
(iii) Let $Q = \langle v\rangle_q$ be a point of $\mathrm{PG}(rt-1,q)$, then $\langle v\rangle_q = \langle 1.v\rangle_q$ is contained in $\mathcal{F}_{r,t,q}(\langle v\rangle_{q^n})$.
(iv) The number of points in $\mathcal{P}$ is $(q^{rt}-1)/(q^t-1)$.

□

This field reduction map extends naturally to a map defined on sets of points or subspaces, so we may e.g. write $\mathcal{F}_{r,t,q}(\pi)$ when π is a subspace of $\mathrm{PG}(r-1,q^t)$.

Exercise 1.2.5. If π is a $(k-1)$-dimensional subspace of $\mathrm{PG}(r-1,q^t)$, then $\mathcal{F}_{r,t,q}(\pi)$ is a subspace of dimension $kt-1$, spanned by the images under $\mathcal{F}_{r,t,q}$ of the points of π.

1.3 Desarguesian spreads

1.3.1 Construction via field reduction

A $(t-1)$-*spread* in $\mathrm{PG}(n-1,q)$ is a set of $(t-1)$-spaces, partitioning the set of points in $\mathrm{PG}(n-1,q)$. Two spreads $\mathcal{S}_1$ and $\mathcal{S}_2$ in $\mathrm{PG}(n-1,q)$ are *equivalent* (or $\mathrm{P}\Gamma\mathrm{L}$-equivalent) if there exists a collineation of $\mathrm{PG}(n-1,q)$ mapping one to the other. The following theorem of Segre gives a necessary and sufficient condition for the existence of a $(t-1)$-spread in $\mathrm{PG}(n-1,q)$. We can use the field reduction map for the construction.

Theorem 1.3.1. *[64] There exists a $(t-1)$-spread in* $\mathrm{PG}(n-1,q)$ *if and only if t divides n.*

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

$$\mathcal{D}_{r,t,q} := \mathcal{F}_{r,t,q}(\mathcal{P}) \tag{1.2}$$

where $\mathcal{F}_{r,t,q}$ is defined as in (1.1) and $\mathcal{P}$ denotes the set of points of $\mathrm{PG}(r-1,q^t)$. Then Lemma 1.2.4 implies that $\mathcal{D}_{r,t,q}$ is a $(t-1)$-spread of $\mathrm{PG}(rt-1,q)$. □

A spread $\mathcal{S}$ in $\mathrm{PG}(n-1,q)$ is called *Desarguesian* if there exist natural numbers r and t such that $n = rt$ and $\mathcal{S}$ is equivalent to $\mathcal{D}_{r,t,q}$.

1.3.2 Construction via indicator spaces

1.3.3 Subgeometries

Recall that a $(k-1)$-dimensional *subspace* U of $\mathrm{PG}(n-1,q)$, corresponds to a k-dimensional vector space over $\mathbb{F}_q$ and is isomorphic to a projective space $\mathrm{PG}(k-1,q)$. A $(k-1)$-dimensional subgeometry B on the other hand is isomorphic to a projective space $\mathrm{PG}(k-1,q_0)$ for some subfield $\mathbb{F}_{q_0}$ of $\mathbb{F}_q$. We define a *subgeometry* B by the set of points of a projective space $\mathrm{PG}(k-1,q)$ whose coordinates with respect to some fixed frame take values from a subfield $\mathbb{F}_{q_0}$ of $\mathbb{F}_q$. In this case the subspaces of B correspond to the intersections of subspaces of $\mathrm{PG}(n-1,q)$ with B. We also say that B is a subgeometry *over* $\mathbb{F}_{q_0}$ or *of order* q_0. For instance, for $k = n$, we take in a projective space $\mathrm{PG}(n-1,q)$ the set of points B that have coordinates in a subfield $\mathbb{F}_{q_0}$ of $\mathbb{F}_q$, together with all the intersections of subspaces of $\mathrm{PG}(n-1,q)$ with B. In this way we obtain a subgeometry over $\mathbb{F}_{q_0}$ (*canonical* with respect to the frame to which these coordinates are defined). This subgeometry is isomorphic to a projective space $\mathrm{PG}(n-1,q_0)$. If $q = q_0^2$, then B is usually called a *Baer subgeometry*.

1.3.4 Desarguesian spreads and subgeometries

By [64] a $(t-1)$-spread in $\mathrm{PG}(n-1,q)$, where t is a divisor of n, can be also constructed as follows. Embed $\mathrm{PG}(rt-1,q)$ as a subgeometry of $\mathrm{PG}(rt-1,q^t)$

in the canonical way, i.e. by restricting the coordinates to $\mathbb{F}_q$. Let σ be the automorphic collineation of $\mathrm{PG}(rt-1,q^t)$ induced by the field automorphism $x \rightarrow x^q$ of $\mathbb{F}_{q^t}$, i.e., $\sigma : (x_0, x_1, \ldots, x_{rt-1}) \mapsto (x_0^q, x_1^q, \ldots, x_{rt-1}^q)$. Then σ fixes $\mathrm{PG}(rt-1,q)$ pointwise and one can prove that a subspace of $\mathrm{PG}(rt-1,q^t)$ of dimension d is fixed by σ if and only if it intersects the subgeometry $\mathrm{PG}(rt-1,q)$ in a subspace of dimension d and that there exists an $(r-1)$-space π skew to the subgeometry $\mathrm{PG}(rt-1,q)$ (see [15]). Let P be a point of π and let $L(P)$ denote the $(t-1)$-dimensional subspace generated by the conjugates of P, i.e., $L(P) = \langle P, P^\sigma, \ldots, P^{\sigma^{t-1}} \rangle$. Then $L(P)$ is fixed by σ and hence it intersects $\mathrm{PG}(rt-1,q)$ in a $(t-1)$-dimensional subspace over $\mathbb{F}_q$. Repeating this for every point of π, one obtains a set $\mathcal{S}$ of $(t-1)$-spaces of the subgeometry $\mathrm{PG}(rt-1,q)$ forming a spread. This spread is equivalent to $\mathcal{D}_{r,t,q}$.

Exercise 1.3.2. Consider the case $\mathrm{PG}(3,q^2)$: Let σ be the automorphic collineation of $\mathrm{PG}(3,q^2)$ induced by the field automorphism $x \rightarrow x^q$ of $\mathbb{F}_{q^2}$, i.e.,

$$\sigma : (x_0, x_1, x_2, x_3) \mapsto (x_0^q, x_1^q, x_2^q, x_3^q).$$

Let Σ be the set of points fixed by σ. Then Σ is a subgeometry $\cong \mathrm{PG}(3,q)$. Note that σ is an involution.

(i) Show that if a line L is disjoint from Σ, then L^σ is disjoint from Σ and disjoint from L.

(ii) Let P be a point of L. Show that the line PP^σ meets Σ in a line of Σ (that is, in $q+1$ collinear points).

(iii) Show that the lines obtained as $PP^\sigma \cap \Sigma$, where P ranges over L, are disjoint.

(iv) Show that the lines obtained as $PP^\sigma \cap \Sigma$, where P ranges over L, form a spread of Σ.

1.3.5 Regular and normal spreads

A *regulus* in a projective space, or $(t-1)$*-regulus* if we want to specify the dimension of the elements, is a set $\mathcal{R}$ of $q+1$ two by two disjoint $(t-1)$-spaces with the property that each line meeting three elements of $\mathcal{R}$ meets all elements of $\mathcal{R}$.

Exercise 1.3.3. Show that three disjoint lines l_1, l_2, l_3 in $\mathrm{PG}(3,q)$ determine a unique regulus. Show that the set of lines meeting l_1, l_2 and l_3 determine a regulus as well. The latter regulus is called the *opposite regulus*.

The property of the previous exercise can be shown to hold in general: if S_1, S_2, S_3 are mutually disjoint $(t-1)$-subspaces with $\dim\langle S_1, S_2, S_3\rangle = 2t-1$, then there is a unique regulus $\mathcal{R}(S_1, S_2, S_3)$ containing S_1, S_2, S_3. A spread $\mathcal{S}$ is called *regular* if the regulus $\mathcal{R}(S_1, S_2, S_3)$ is contained in $\mathcal{S}$ for each three different elements S_1, S_2, S_3 of $\mathcal{S}$.

Exercise 1.3.4. Let $t = 2$, $r = 3$. Use coordinates introduced in the previous section for the Desarguesian line spread $\mathcal{D}$ in $\mathrm{PG}(3, q)$ using field reduction. Let L_1, L_2 and L_3 be lines of $\mathcal{D}$. If M is a line meeting L_1, L_2, L_3 in points $P_1 = \langle v_1 \rangle_q, P_2 = \langle v_2 \rangle_q, P_3 = \langle v_3 \rangle_q$ respectively, then show that the unique transversal line to the regulus R through the point $\langle \alpha_0 v_1 \rangle_q$ meets L_2 and L_3 in $\langle \alpha_0 v_2 \rangle_q$ and $\langle \alpha_0 v_3 \rangle_q$. Write down the coordinates for the lines $L_4, \ldots, L_{q+1} \in \mathcal{D}$ of the regulus R through L_1, L_2, L_3 and deduce that $\mathcal{D}$ is regular.

It is not too hard to show that a general Desarguesian spread is regular. The following shows that the converse is true as well (provided that a regulus contains more than just 3 lines).

Theorem 1.3.5. *[14] If $q > 2$, a $(t-1)$-spread of $\mathrm{PG}(2t-1, q)$ is Desarguesian if and only if it is regular.*

Exercise 1.3.6. The spread constructed in Exercise 1.3.2 is regular (and hence, Desarguesian).

Note that a Desarguesian spread satisfies the property that each subspace spanned by spread elements is partitioned by spread elements (Exercise 1.2.5). Spreads satisfying this property are called *normal* or *geometric*. Clearly, a $(t-1)$-spread in $\mathrm{PG}(2t-1, q)$ is always normal.

Theorem 1.3.7. *[4] A $(t-1)$-spread $\mathcal{S}$ in $\mathrm{PG}(rt-1, q)$, with $r > 2$, is normal if and only if $\mathcal{S}$ is Desarguesian.*

For a survey and self-contained proofs of these characterisations of Desarguesian spreads, we refer to [2].

1.4 André/Bruck-Bose

To explain why the spread $\mathcal{D}_{r,t,q}$ is called 'Desarguesian', we need to consider the following incidence structure constructed from a spread. Let $\mathcal{S}$ be a $(t-1)$-spread in $\mathrm{PG}(2t-1, q)$. Embed $\mathrm{PG}(2t-1, q)$ as a hyperplane H in $\mathrm{PG}(2t, q)$. Consider the following incidence structure $\mathcal{P}(\mathcal{S}) = (\mathcal{P}, \mathcal{L}, \mathrm{I})$, where I is symmetric containment:

$\mathcal{P}$: points of $\mathrm{PG}(rt, q) \setminus H$ and elements of $\mathcal{S}$

$\mathcal{L}$: t-spaces of $\mathrm{PG}(rt, q)$ intersecting H exactly in an element of $\mathcal{S}$ and H itself.

Exercise 1.4.1. Show that $\mathcal{P}(\mathcal{S})$ is a projective plane, i.e., every two points determine a unique line and every two lines meet in a unique point.

The projective plane constructed above is a translation plane of order q^t, and in this construction is known as the *André/Bruck-Bose construction*. The spread $\mathcal{S}$ is Desarguesian if and only if $\mathcal{P}(\mathcal{S})$ is the Desarguesian projective plane.

Exercise 1.4.2. (Hall plane) The Hall plane of order q^2, $q \geq 3$ can be constructed as follows. Let $\mathcal{D}$ be the Desarguesian line spread of $\mathrm{PG}(3, q)$ and let $\mathcal{R}$ be a regulus contained in $\mathcal{D}$. Replace the lines of $\mathcal{R}$ in $\mathcal{D}$ by the lines of its opposite regulus and call $\mathcal{D}'$ the set of points obtained in that way. Show that $\mathcal{D}'$ is a non-Desarguesian spread. The projective plane defined by the André/Bruck-Bose construction starting with the spread $\mathcal{D}'$ is the *Hall plane* (see e.g. [32]).

1.4.1 Coordinates for André/Bruck-Bose

Consider $\Pi = \mathrm{PG}(2, q^t)$ where points have coordinates $(x, y, z)_{q^t}$, $x, y, z \in \mathbb{F}_{q^t}$. Let ℓ_∞ be the line with equation $z = 0$. The *affine* points of Π are the points, not on ℓ_∞. These can all be represented in a unique way by coordinates of the form $(x_0, y_0, 1)_{q^t}$.

Consider $\mathbb{F}_q^{2t+1}$, the $(2t + 1)$-dimensional vector space over $\mathbb{F}_q$. Think of $\mathbb{F}_q^{2t+1}$ as $S \oplus T \oplus U$, where S and T are t-dimensional vector spaces over $\mathbb{F}_q$ and U is 1-dimensional. Every vector $v \in \mathbb{F}_q^{2t+1}$ can be written in a unique way as (v_1, v_2, v_3), where $v = v_1 + v_2 + v_3$ and $v_1 \in S, v_2 \in T, v_3 \in U$.

Identify, as before, S and T with $\mathbb{F}_{q^t}$. Then we can represent every vector v as (v_1, v_2, v_3), where $v_1, v_2 \in \mathbb{F}_{q^t}$ and $v_3 \in \mathbb{F}_q$. Since $S \oplus T \oplus U$ is $(2t+1)$-dimensional over $\mathbb{F}_q$, $\mathrm{PG}(S \oplus T \oplus U) = \mathrm{PG}(2t, q)$ and every point of $\mathrm{PG}(2t, q)$ has coordinates of the form $(v_1, v_2, v_3)_q$, where $v_1, v_2 \in \mathbb{F}_{q^t}$ and $v_3 \in \mathbb{F}_q$.

Exercise 1.4.3. (see also [63]) Show the following:

(i) The set of points of the form $(v_1, v_2, 0)_q$ $v_1, v_2 \in \mathbb{F}_{q^t}$ forms a hyperplane H_∞ of $\mathrm{PG}(S \oplus T \oplus U)$.

(ii) The map ϕ that takes the affine point $(x, y, 1)_{q^t}$ of Π to $(x, y, 1)_q$ is a bijection between the affine points of Π and the affine points of $\mathrm{PG}(2t, q)$ (these are the points not on H_∞).

(iii) The map ϕ' that takes a point $(x,y,0)_{q^t}$ of Π to $\{(\alpha x, \alpha y, 0)_q | \alpha \in \mathbb{F}_{q^t}^*\}$ is a bijection between the points of ℓ_∞ and spread elements of a Desarguesian spread in $\mathrm{PG}(2t-1,q)$.

(iv) The maps ϕ and ϕ' determine the André/Bruck-Bose embedding of $\mathrm{PG}(2,q^t)$ in $\mathrm{PG}(2t,q)$. Show that it can also be obtained as the intersection of the images under the field reduction map with a fixed $2t$-space of $\mathrm{PG}(3t-1,q)$.

1.5 Desarguesian spreads and the Segre variety

We have seen in the previous subsection that applying the field reduction map $\mathcal{F}_{r,t,q}$ to all points of a projective space yields a Desarguesian spread $\mathcal{D}_{r,t,q}$. If we apply the field reduction map $\mathcal{F}_{r,t,q}$ to all points of a subgeometry $\mathrm{PG}(r-1,q)$ of $\mathrm{PG}(r-1,q^t)$, then we obtain a subset of $\mathcal{D}_{r,t,q}$ that forms one of the systems of a *Segre variety* $\mathcal{S}_{r-1,t-1}$.

Definition 1.5.1. The *Segre map* $\sigma_{l,k} : \mathrm{PG}(l,q) \times \mathrm{PG}(k,q) \to \mathrm{PG}((l+1)(k+1)-1,q)$ is defined by

$$\sigma_{l,k}((x_0,\dots,x_l),(y_0,\dots,y_k)) := (x_0y_0,\dots,x_0y_k,\dots,x_ly_0,\dots,x_ly_k).$$

The image of the Segre map $\sigma_{l,k}$ is called the *Segre variety* $\mathcal{S}_{l,k}$.

If we give the points of $\mathrm{PG}((l+1)(k+1)-1,q)$ coordinates in the form

$$(x_{00},x_{01},\dots,x_{0k};x_{10},\dots,x_{1k};\dots;x_{l0},\dots,x_{lk}),$$

then it is clear that the points of the Segre variety $\mathcal{S}_{l,k}$ are exactly the points that have coordinates such that the matrix (x_{ij}), $0 \le i \le l$, $0 \le j \le k$, has rank 1 (see also [31, Theorem 25.5.7]).

By fixing a point in $\mathrm{PG}(l,q)$ and varying the point of $\mathrm{PG}(k,q)$, we obtain a k-dimensional space on $\mathcal{S}_{l,k}$. For every point of $\mathrm{PG}(l,q)$ such a space exists, and the set of these subspaces, which are clearly disjoint, is called a *system* (*of maximal subspaces*). Similarly, by fixing a point in $\mathrm{PG}(k,q)$, we obtain an l-dimensional space on $\mathcal{S}_{l,k}$ by varying the point of $\mathrm{PG}(l,q)$; the set of these subspaces is again called a system (of maximal subspaces). Subspaces of different systems intersect each other in exactly one point, while subspaces within the same system intersect each other trivially. Moreover, each subspace lying on the variety $\mathcal{S}_{l,k}$ is contained in an element of one of these two systems.

Theorem 1.5.2. *(see e.g. [45, Theorem 2.6]) If $\mathcal{P}_\Sigma$ is the set of points of the canonical subgeometry $\Sigma \cong \mathrm{PG}(r-1,q)$ of $\mathrm{PG}(r-1,q^t)$ of order q, then $\mathcal{F}_{r,t,q}(\mathcal{P}_\Sigma)$ is projectively equivalent to a maximal system of $(t-1)$-spaces of a Segre variety $\mathcal{S}_{r-1,t-1}$.*

Corollary 1.5.3. *The system of $(t-1)$-spaces of a Segre variety $\mathcal{S}_{k-1,t-1}$ in $\mathrm{PG}(rt-1,q)$, $k \leq r$, is projectively equivalent to a subset of $\mathcal{D}_{r,t,q}$, whereas the system of $(r-1)$-spaces of a Segre variety $\mathcal{S}_{r-1,u-1}$ in $\mathrm{PG}(rt-1,q)$, $u \leq t$, is projectively equivalent to a subset of $\mathcal{D}_{t,r,q}$.*

Chapter 2

Linear sets

Linear sets generalise the concept of subgeometries in a projective space. They have many applications in finite geometry; linear sets have been intensively used in recent years in order to classify, construct or characterise various geometric structures, e.g. blocking sets (see Chapter 4), but also translation ovoids, KM-arcs, semifields, MRD codes,... For a further discussion of some of these applications, we refer to the survey of O. Polverino [60].

2.1 Definition

To obtain a linear set in a projective space, some kind of reverse field reduction is used. The field reduction map takes as input a subspace of $\mathrm{PG}(r-1, q^t)$ and returns a subspace of $\mathrm{PG}(rt-1, q)$. Or in other words from an $\mathbb{F}_{q^t}$-subspace we obtain an $\mathbb{F}_q$-subspace. A linear set, on the other hand, is defined by an $\mathbb{F}_q$-subspace and returns, not a subspace, but a subset of a projective $\mathbb{F}_{q^t}$-linear space, i.e. a subset of some $\mathrm{PG}(r-1, q^t)$.

More precisely, let $V = \mathbb{F}_{q^t}^r$. A set L of points in $\mathrm{PG}(V)$ is called an $\mathbb{F}_q$-*linear set* (*of rank* k) if there exists a subset U of V that forms a (k-dimensional) $\mathbb{F}_q$-subspace of V, such that $L = L_U$, where

$$L_U = \{\langle u \rangle_{q^t} : u \in U \setminus \{0\}\}.$$

The notation L_U is used to indicate the underlying subspace U. Obviously, if we say that the subset U forms an $\mathbb{F}_q$-subspace of V, then we mean a subspace of the rt-dimensional space that is obtained by considering V as vector space over $\mathbb{F}_q$. We make no distinction between the $\mathbb{F}_q$-vector subspace U and the subset U.

2.1.1 A geometric point of view

Recall that the field reduction map $\mathcal{F}_{r,t,q}$ gives us a one-to-one correspondence between the points of $\mathrm{PG}(r-1,q^t)$ and the elements of a Desarguesian spread $\mathcal{D}_{r,t,q}$. This will gives us a geometric interpretation of a linear set:

Theorem 2.1.1. *If L_U is an $\mathbb{F}_q$-linear set of rank k in $\mathrm{PG}(r-1,q^t)$, then there exists a $(k-1)$-dimensional subspace π in $\mathrm{PG}(rt-1,q)$ such that the points of L correspond to the elements of $\mathcal{D}_{r,t,q}$ that have a non-empty intersection with π. Vice versa, the set of spread elements of $\mathcal{D}_{r,t,q}$ that have a non-emtpty intersection with a $(k-1)$-dimensional subspace of $\mathrm{PG}(rt-1,q)$ correspond to the points of an $\mathbb{F}_q$-linear set.*

Proof. Let $L_U = \{\langle u\rangle_{q^t} : u \in U \setminus \{0\}\}$, where U is a subset of $V = \mathbb{F}_{q^t}^r$ that forms a k-dimensional $\mathbb{F}_q$-subspace. Let $P = \langle u_1\rangle_{q^t}$ be a point of L_U, then P corresponds to the spread element $\langle \alpha u_1\rangle_q$ which contains the point $\langle u_1\rangle$. Let π be the point set of $\mathrm{PG}(rt-1,q)$ consisting of the points $\{\langle u\rangle_q : u \in U \setminus \{0\}\}$, then π forms an $\mathbb{F}_q$-subspace since U is an $\mathbb{F}_q$-vector space. The dimension of π is clearly $(k-1)$, and we have just seen that every spread element corresponding to a point of L_U contains at least one point of π.

Vice versa, consider a $(k-1)$-dimensinal subspace μ in $\mathrm{PG}(rt-1,q)$, then $\mu = \{\langle u\rangle_q : u \in V \setminus \{0\}\}$ for some k-dimensional vector space V. As above, we see that L_V is the $\mathbb{F}_q$-linear set consisting of the points corresponding to the spread elements intersecting μ non-trivially. □

Remark 2.1.2. The notation $\mathcal{B}(\pi)$, where π is the projective space corresponding to U is frequently used to denote either the point set L_U or the set of spread elements intersecting the subspace π.

Exercise 2.1.3. Use this geometric point of view to determine the different possibilities for the size of a linear set of rank 1, 2, 3 in $\mathrm{PG}(1,q^t)$, $t \geq 3$. Show that an $\mathbb{F}_q$-linear set of rank $k > t$ in $\mathrm{PG}(1,q^t)$ is the set of all points of $\mathrm{PG}(1,q^t)$

If P is a point of $\mathcal{B}(\pi)$ in $\mathrm{PG}(r-1,q^t)$, where π is a subspace of $\mathrm{PG}(rt-1,q)$, then we define the *weight of* P as $wt(P) := \dim(\mathcal{F}_{r,t,q}(P) \cap \pi) + 1$. This makes a point to have weight 1 if its corresponding spread element intersects π in a point. It is clear that a point of an $\mathbb{F}_q$-linear set of rank k in $\mathrm{PG}(r-1,q^t)$ can have weight at most $\min\{k,t\}$.

Exercise 2.1.4. If $\pi = \langle U\rangle_q$, then we have seen that $L_U = \mathcal{B}(\pi)$. Show that the weight of a point $P = \langle v\rangle_{q^t}$ in L_U is the vector dimension of the $\mathbb{F}_q$ vector space $U \cap S_v$, where $S_V = \{\langle \alpha v\rangle_{q^t} | \alpha \in \mathbb{F}_{q^t}^*\}$.

Exercise 2.1.5. (see also [60, Proposition 2.2]) Let L_U be a linear set of rank $k > 0$ and denote by x_i the number of points of weight i, with $m = \min\{k,t\}$, then the

following relations hold:
(i) $|L_U| = x_1 + x_2 + \cdots + x_m$
(ii) $x_1 + (q+1)x_2 + \frac{q^3-1}{q-1}x_3 + \cdots + \frac{q^m-1}{q-1}x_m = \frac{q^k-1}{q-1}$
(iii) $|L_U| \leq \frac{q^k-1}{q-1}$
(iv) $|L_U| \equiv 1 \bmod q$.

2.1.2 Scattered linear sets

If π intersects the elements of $\mathcal{D}$ in at most a point, i.e. the size of $\mathcal{B}(\pi)$ is maximal, or equivalently every point of $\mathcal{B}\pi)$ has weight one, then we say that π is *scattered with respect to $\mathcal{D}$*; in this case $\mathcal{B}(\pi)$ is called a *scattered linear set*. The notion of scattered linear sets was introduced in [10], where the following bound on the rank of a scattered linear set was obtained.

Theorem 2.1.6. *[10, Theorem 4.3] A scattered $\mathbb{F}_q$-linear set in $\mathrm{PG}(r-1, q^t)$ has rank $\leq rt/2$.*

Scattered linear sets that meet this bound are called *maximum scattered*.

Example 2.1.7. The set

$$S = \{(x, x^q) | x \in \mathbb{F}_{q^t}^*\}$$

is a maximum scattered linear set in $\mathrm{PG}(1, q^t)$. Since $\mathbb{F}_{q^t}$ is a t-dimensional $\mathbb{F}_q$-vector space, the set S is an $\mathbb{F}_q$-linear set of rank t. To determine the number of points in S we notice that the points (x, x^q), $x \in \mathbb{F}_{q^t}$ and $(y, y^q), y \in \mathbb{F}_{q^t}$ are the same if and only if $x = \lambda y$ and $x^q = \lambda y^q$ for some $\lambda in \mathbb{F}_{q^t}^*$. This happens if and only if $(\frac{x}{y})^{q-1} = 1$ and hence if and only if x and y are $\mathbb{F}_q$-multiples. This shows that S has $\frac{q^t-1}{q-1}$ points, and hence, that S is scattered. Since $t = rt/2$ for $r = 2$, S is maximum scattered.

Maximum scattered linear sets are related to interesting geometric objects such as two-weight codes, two-intersection sets, strongly regular graphs, pseudoreguli and hyperovals (see [37], [54], [41], [19]). For a survey dedicated to these applications, see [40].

2.1.3 Different subspaces determining the same linear set

It is clear that, if $U = U'$, then $L_U = L_{U'}$. However, it is not because $L_U = L_{U'}$ that $U = U'$. It is not even necessary that both subspaces U and U' have the same dimension as seen in the folowing example. This means that the rank of a linear set is not defined if the underlying vector space is not specified!

Example 2.1.8. Consider the point set $S = \{(1,x)_{q^4} | x \in \mathbb{F}_{q^2}\} \cup \{(0,1)_{q^4}\}$ in $\mathrm{PG}(1,q^4)$. This point set S is an $\mathbb{F}_{q^2}$-subline of $\mathrm{PG}(1,q^4)$. We can rewrite this set as

$$S = \{(x,y)_{q^4} | x,y \in \mathbb{F}_{q^2}, (x,y) \neq (0,0)\} = \{\langle u\rangle_{q^4} | u \in U^*\},$$

where $U = \mathbb{F}_{q^2}^2$. Since U is a vector space of dimension 4, $S = L_U$ is a linear set of rank 4, and hence, is defined by the spread elements of the Desarguesian 3-spread in $\mathrm{PG}(7,q)$ obtained by field reduction intersecting the 3-dimensional subspace $\pi = \langle U\rangle_q$. Note that S has q^2+1 elements, and all spread elements intersecting $\langle U\rangle_q$, intersect it in a line: $\langle \alpha u\rangle_q \cap \langle U\rangle_q$, where $u \in U$ contains the $q+1$ points $\langle \beta u\rangle_q$, where $\beta \in \mathbb{F}_{q^2}$. Now consider a plane $\mu = \langle V\rangle$ contained in π, then V is a 3-dimensional vector space. As every element of $L_U = \mathcal{B}(\pi)$ intersects π in a line, it also intersects μ. We see that $L_U = L_V$, but L_U is a linear set of rank 4 and L_V is a linear set of rank 3.

Exercise 2.1.9. Every $\mathbb{F}_q$-linear set L_U can be written as an $\mathbb{F}_q$-linear set $L_{U'}$ that contains at least one point of weight one.

We might be tempted to think that if $L_U = L_V$ for U and V subspaces of the same dimension, we have that $U = V$. This is not true, as seen in the following exercise.

Exercise 2.1.10. Let $\mathcal{D}$ be the Desarguesian $(t-1)$-spread of $\mathrm{PG}(rt-1,q)$. Let $\mathcal{B}(\pi)$ be a linear set of rank $k+1$, where π is a k-dimensional space. Show that, for every point R in $\mathrm{PG}(rt-1,q)$, contained in a spread element meeting π, there is a k-dimensional space π', through R, such that $\mathcal{B}(\pi) = \mathcal{B}(\pi')$.

The previous exercise give rise to an important question: how many different subspaces π' of dimension $(k-1)$ are there through a fixed point R such that $\mathcal{B}(\pi') = \mathcal{B}(\pi)$? If $\mathcal{B}(\pi)$ is a regulus, this means π is a line, then it is clear that through every point of an element of $\mathcal{B}(\pi)$, there is exactly one line π' such that $\mathcal{B}(\pi') = \mathcal{B}(\pi)$, because through every point of a regulus, there exists a unique transversal line to this regulus. But the answer to this question is not always equal to one! In [16], a linear called is called *simple*, if the answer to this question is one. Some cases of this problem are well understood, but in general, this question remains open (see e.g. [16],[74]).

2.2 Linear sets and projections of subgeometries

It is clear from the definition (or from the link with Segre varieties described in Section 1.5) that a subgeometry is a linear set, but a linear set is not necessarily a subgeometry. However, the following theorem by Lunardon and Polverino shows that every linear set is a projection of a subgeometry. For the particular case of linear *blocking sets*, this was proven in [58], for the case of scattered linear sets, but not using this terminology, it was shown already in 1981 in [48].

Let $\Sigma = \mathrm{PG}(k-1,q)$ be a subgeometry of $\Sigma^* = \mathrm{PG}(k-1,q^t)$ and suppose there exists an $(k-r-1)$-dimensional subspace Ω^* of Σ^* disjoint from Σ. Let $\Omega = \mathrm{PG}(r-1,q^t)$ be an $(r-1)$-dimensional subspace of Σ^* disjoint from Ω^*. Let $p_{\Omega^*,\Omega}$ denote the projection map defined by $x \mapsto \langle \Omega^*, x\rangle \cap \Omega$ for each point $x \in \Sigma^* \setminus \Omega^*$. The point set $\Gamma = p_{\Omega^*,\Omega}(\Sigma)$, i.e., the image of Σ under the projection map $p_{\Omega^*,\Omega}$ is simply called the *projection* of Σ from Ω^* into Ω.

Theorem 2.2.1. *[53, Theorem 1 and 2] If Γ is a projection of $\mathrm{PG}(k-1,q)$ into $\Omega = \mathrm{PG}(r-1,q^t)$ with $k \geq r$, then Γ is an $\mathbb{F}_q$-linear set of rank k and $\langle\Gamma\rangle = \Omega$. Conversely, if L is an $\mathbb{F}_q$-linear set of Ω of rank k and $\langle L\rangle = \Omega = \mathrm{PG}(r-1,q^t)$, then either L is a canonical subgeometry of Ω or there are a $(k-r-1)$-dimensional subspace Ω^* of $\Sigma^* = \mathrm{PG}(k-1,q^t)$ disjoint from Ω and a canonical subgeometry Σ of Σ^* disjoint from Ω^* such that $L = p_{\Omega^*,\Omega}(\Sigma)$.*

Sketch of the proof: We will first recover the easy direction: if Γ is a projection of $\mathrm{PG}(k-1,q)$ into $\Omega = \mathrm{PG}(r-1,q^t)$ with $k \geq r$, then Γ is an $\mathbb{F}_q$-linear set of rank k and $\langle\Gamma\rangle = \Omega$.

The canonical subgeometry $\Sigma = \mathrm{PG}(k-1,q)$ of $\mathrm{PG}(k-1,q^t)$ is the linear set $L_U = \{\langle u\rangle_{q^t} | u \in U\}$, where $U = \mathbb{F}_q^k$. Consider U as an $\mathbb{F}_q$-vector space and let $\pi = \langle U\rangle_q$ be the corresponding $(k-1)$-dimensional subspace of $\mathrm{PG}(rt-1,q)$. The $(k-r-1)$-dimensional subspace Ω^* corresponds to a $((k-r)t-1)$-dimensional subspace μ^* of $\mathrm{PG}(rt-1,q)$ and $\Omega = \mathrm{PG}(r-1,q^t)$ corresponds to a $(rt-1)$-dimensional subspace μ^*. Both μ and μ^* are spanned by spread elements of $\mathcal{D}$, the Desarguesian spread. The points of Γ are obtained as the projection of the points of Σ from Ω^* onto Ω. It now follows that they correspond to the spread elements intersecting the subspace $\mu \cap \langle \mu^*, \pi\rangle$.

The proof of the other direction of the previous theorem is based on the following observation: if a linear set L_U of rank k spans an $r-1$-dimensional projective space Ω, then we can filter a $\mathbb{F}_q$-basis for U, say $a_1,\ldots,a_k$ to an $\mathbb{F}_{q^t}$ basis for the vector space defining Ω. Suppose that $a_{k-r+1},\ldots,a_k$ are an $\mathbb{F}_{q^t}$-independent. Let $b_1,\ldots,b_{k-r}$ be $\mathbb{F}_{q^t}$-independent, then they define a $(k-r-1)$-dimensional projective space Ω^*. Now let $v_i = a_i + b_i$ for $1 \leq i \leq k-r$ and $v_j = a_j$ for $k-r+1 \leq j \leq k$. Then it is not too hard to show that the set of points $\langle v_i\rangle_{q^t}$ forms a $(k-1)$-dimensional subgeometry Σ and the projection of Σ from Ω^* onto Ω is precisely L_U. □

When we apply field reduction to the spaces Ω^*, Σ^* and Σ of Theorem 2.2.1 and use Theorem 1.5.2, we obtain the following geometric characterisation of the spread elements defining a linear set.

Corollary 2.2.2. *The set $\mathcal{B}(\pi)$ of elements of $\mathcal{D}_{r,t,q}$, where π is a $(k-1)$-dimensional space in $\overline{\Omega} = \mathrm{PG}(rt-1, q)$ is the projection of one of the two systems of a Segre variety $\mathcal{S}_{k-1,t-1}$ from a $(kt-rt-1)$-dimensional space $\overline{\Omega^*}$ skew from $\mathcal{S}_{k-1,t-1}$ and $\overline{\Omega}$ and vice versa.*

Remark 2.2.3. In the previous corollary, we have seen that $\mathcal{B}(\pi)$ is a projection of a Segre variety (this projection is not necessarily injective). Projections of Segre varieties are studied by Zanella in [80], where he shows that every embedded *product space* is the injective projection of a Segre variety. In [43], the authors investigate the embedding of the product space $\mathrm{PG}(n-1,q) \times \mathrm{PG}(n-1,q)$ in $\mathrm{PG}(2n-1,q)$ and show that $\mathcal{B}(W)$, where W is a scattered subspace of rank n is an embedding of the product space $\mathrm{PG}(n-1,q) \times \mathrm{PG}(n-1,q)$. This embedding is of course covered by two systems of $(n-1)$-dimensional subspaces. However, they prove that $\mathcal{B}(W)$ contains n systems of $(n-1)$-dimensional subspaces, and hence for $n > 2$, contrary to what one might expect, there exist systems of maximum subspaces which are not the image of maximum subspaces of the Segre variety.

Chapter 3

Linear sets and directions determined by a point set

3.1 Directions determined by a point set

Consider $\mathrm{PG}(2,q)$ with the line $\ell_\infty : x = 0$ as line at infinity. The *affine points* of $\mathrm{PG}(2,q)$ are the points, not on ℓ_∞. An affine point of $\mathrm{PG}(2,q)$ has unique coordinates of the form $(1, x_i, y_i)$ for some $x_i, y_i \in \mathbb{F}_q$. The set of directions determined by an affine point set $\mathcal{A} = \{(1, x_i, y_i) \mid 1 \leq i \leq n\}$ in $\mathrm{PG}(2,q)$ is the set $\{(0, x_i - x_j, y_i - y_j) \mid 1 \leq i \neq j \leq n\}$. The study of the number of directions determined by an affine point set goes back to Rédei and many results, e.g., on blocking sets are going back to these techniques. In this section, we will see that a similar approach is useful for the study of linear sets as well.

The following theorem essentially determines the number of directions determined by a map defined on a finite field. The *graph* of a function f defined on $\mathbb{F}_q$ is the point set $\{(x, f(x))|x \in \mathbb{F}_q\}$ in the affine plane $\mathrm{AG}(2,q)$. This can be though of as the point set $\{(1, x, f(x)|x \in \mathbb{F}_q\}$ in $\mathrm{PG}(2,q)$.

Theorem 3.1.1 ([3]). *Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be a function. Let N be the number of directions determined by f. Let $s = p^e$ be maximal such that any line with a direction determined by f that is incident with a point of the graph of f is incident with a multiple of s points of the graph of f. Then one of the following holds:*

(i) $s = 1$ *and* $\frac{q+3}{2} \leq N \leq q+1$*;*
(ii) $\mathbb{F}_s$ *is a subfield of* $\mathbb{F}_q$ *and* $\frac{q}{s} + 1 \leq N \leq \frac{q-1}{s-1}$*;*
(iii) $s = q$ *and* $N = 1$.

Moreover, if $s > 2$, then the graph of f is $\mathbb{F}_s$-linear.

Theorem 3.1.1 completed two unresolved cases from [9, Theorem 1.1].

Remark 3.1.2. The previous theorem says that if $s > 2$, the point set of the graph is $\mathbb{F}_s$-linear, by which the author meant that f is an $\mathbb{F}_s$-linear map. In [67], the citation of the same theorem says 'U is a $\mathbb{F}_{p^e}$-linear subspace'.

A set of the form $\mathcal{A} = \{(1, x, f(x)) \mid x \in V\}$, where f is an $\mathbb{F}_q$-linear map and V is an $\mathbb{F}_q$-vector subspace of $\mathbb{F}_{q^t}$, is called an *affine $\mathbb{F}_q$-linear set* in [23]. We will see later that an affine linear set will be the affine part of an $\mathbb{F}_q$-linear set of $\mathrm{PG}(2, q^t)$ as defined by us.

In this subsection, we explore the connections between directions determined by an $\mathbb{F}_q$-linear map and $\mathbb{F}_q$-linear sets. We will restrict ourselves to linear sets on a line and in a plane. However, most of what follows can be easily generalised to linear sets in higher dimensions.

3.2 $\mathbb{F}_q$-linear maps of $\mathbb{F}_{q^t}$, linearised polynomials and linear sets

3.2.1 Linearised polynomials

Recall that an $\mathbb{F}_q$-linear $f : V \to W$ (where V and W are vector spaces over some extension field of $\mathbb{F}_q$) is a map satisfying the following properties for $u_1, u_2 \in V$ and $\lambda \in \mathbb{F}_q$

$$\begin{aligned} f(u_1 + u_2) &= f(u_1) + f(u_2) \\ f(\lambda u) &= \lambda f(u) \end{aligned}$$

A *linearised polynomial* (or q-polynomial) on $\mathbb{F}_{q^t}$ of *q-degree r* is a polynomial of the form $L(x)$ where

$$L(x) = a_0 x + a_1 x^q + a_2 x^{q^2} + \ldots + a_{n-1} x^{q^r},$$

where $a_i \in \mathbb{F}_{q^t}$.

Exercise 3.2.1. Show that the following hold:

(i) L is an $\mathbb{F}_q$-linear map.

(ii) Every $\mathbb{F}_q$-linear map on $\mathbb{F}_{q^t}$ can uniquely be represented by a linearised polynomial of q-degree at most $t-1$.

(iii) The roots of a linearised polynomial form an $\mathbb{F}_q$-vector space.

The vice versa part of Exercise 3.2.1(iii) also holds: every $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^t}$ can be represented as the roots of a linearised polynomial:

Theorem 3.2.2. *[47, Theorem 3.52] Let V be a $\mathbb{F}_q$-vector subspace of $\mathbb{F}_{q^t}$ of dimension k. Then the polynomial vanishing on the elements of V is a linearised polynomial, i.e.*

$$\prod_{\beta \in V}(X-\beta) = X^{q^k} + \alpha_1 X^{q^{k-1}} + \alpha_2 X^{q^{k-2}} + \ldots + \alpha_k X\,,$$

for some $\alpha_i \in \mathbb{F}_{q^t}$.

This information will be useful in the next subsection when we derive the shape of a Rédei polynomial of a linear set.

Exercise 3.2.3. The trace map of $\mathbb{F}_{q^t}$ is the map $x \to \mathrm{Tr}(x) = x + x^q + \ldots + x^{q^{t-1}}$. The *rank* of a polynomial is its rank as an $\mathbb{F}_q$-linear map. Show that all linearised polynomials of rank 1 are of the form $x \to \alpha\mathrm{Tr}(\beta x)$ for some $\alpha, \beta \in \mathbb{F}^*_{q^t}$ (see also [47, Theorem 2.24]).

Exercise 3.2.4. (Gabidulin codes) It is clear that the set of all linearised polynomials on $\mathbb{F}_{q^t}$ forms a vector space with usual addition and scalar multiplication with scalars in $\mathbb{F}_{q^t}$. Let $k \leq t-1$. Show that the set

$$\mathcal{G}_k = \{a_0 x + a_1 x^q + a_2 x^{q^2} + \ldots + a_{k-1} x^{q^{k-1}} | a_i \in \mathbb{F}_{q^t}\}$$

is an $\mathbb{F}_{q^t}$-vector space such that for all $f \neq g \in \mathcal{G}_k$,

$$\mathrm{rank}(f-g) \geq t-k+1.$$

This set of polynomials forms a *rank metric code* such that each non-zero codeword has rank at least $t-k+1$. The number of codewords is $(q^t)^k$ (why?) which ensures that this codes meets the *Singleton-like bound* and hence is an *MRD (maximum rank distance) code.* See e.g. [65]

Remark 3.2.5. 1. One of the main nice properties of linearised polynomials is that they allow a multiplication operation which is internal: the *symbolic* product of linearised polynomials. This is defined as their composition and denoted by $\circ$. More precisely, let $F(x)$ and $G(x)$ be two $\mathbb{F}_q$-linearised polynomials, then

$$(F \circ G)(x) := F(G(x)) \bmod x^{q^t} - x.$$

Unlike the ordinary product of two linearised polynomials, the composition of two linearised polynomials is again a linearised polynomial. The symbolic product of two $\mathbb{F}_q$-polynomials will correspond precisely to the composition of their corresponding linear maps.

2. We know that every $\mathbb{F}_q$-linear map of $\mathbb{F}_{q^t}$ (where we see $\mathbb{F}_{q^t}$ as an $\mathbb{F}_q$-vector space of dimension n) corresponds to an $(n \times n)$-matrix. To make an explicit correspondence between linearised polynomials and matrices, we can introduce the *Dickson* matrix: the linearised polynomial

$$L(x) = a_0x + a_1x^q + a_2x^{q^2} + \ldots + a_{t-1}x^{q^{t-1}}$$

then corresponds to the matrix

$$\begin{pmatrix} a_0 & a_1 & a_2 & \ldots & a_{t-1} \\ a_{t-1}^q & a_0^q & a_1^q & \ldots & a_{t-2}^q \\ \ldots & & & & \\ a_1^{q^{t-1}} & a_2^{q^{t-1}} & a_3^{q^{t-1}} & \ldots & a_0^{q^{t-1}} \end{pmatrix}$$

The *rank* of the linearised polynomial coincides with the rank of the associated Dickson matrix. For more information, see [47, 56], and [79] for a recent treatment.

3.2.2 Linear sets and linearised polynomials

We now show that we can represent every linear set in $\mathrm{PG}(1, q^t)$ through an $\mathbb{F}_q$-linear map. Many of the below ideas work for linear sets in arbitrary dimension as well. Note that the only $\mathbb{F}_q$-linear set of rank $k > t$ in $\mathrm{PG}(1, q^t)$ is the set of all points of $\mathrm{PG}(1, q^t)$ (see Exercise 2.1.3). For this reason, we restrict ourselves to $\mathbb{F}_q$-linear sets of rank $k \leq t$. The following lemma's are taken from [18].

Lemma 3.2.6. *Let L_U be an $\mathbb{F}_q$-linear set of rank k in $\mathrm{PG}(1, q^t)$, $k \leq n$, not containing the point $(0, 1)$, then $L = \{(x, f(x)) | x \in V^*\}$ for some vector subspace V of dimension k and some $\mathbb{F}_q$-linear map $f : V \to \mathbb{F}_{q^t}$.*

Proof. We have that $L_U = \{\langle u\rangle_{q^t} \mid u \in U^*\}$, where U is a subspace of dimension k of $\mathbb{F}_q^{2t}$. We consider $\mathbb{F}_q^{2t}$ as $\mathbb{F}_{q^t}^2$ and see that every element of U can be written as (α_i, β_i) for some α_i, β_i in $\mathbb{F}_{q^t}$, $i = 1, \ldots, q^k$. Put $\beta_i = f(\alpha_i)$. Suppose to the contrary that $\alpha_{i_0} = \alpha_{j_0}$ for some $i_0 \neq j_0$. The elements $(\alpha_{i_0}, f(\alpha_{i_0}))$ and $(\alpha_{j_0}, f(\alpha_{j_0}))$ are distinct elements of U, so if $\alpha_{i_0} = \alpha_{j_0}$, then $f(\alpha_{i_0}) \neq f(\alpha_{j_0})$. As U is a vector subspace, it follows that $(\alpha_{i_0}, f(\alpha_{i_0})) - (\alpha_{j_0}, f(\alpha_{j_0})) = (0, f(\alpha_{i_0}) - f(\alpha_{j_0})$ is an element of U. But L_U is skew from the point $(0, 1)$, a contradiction. We conclude that $V = \{\alpha_i \mid 1 \leq i \leq q^k\}$ has size q^k.

Since U is an $\mathbb{F}_q$ subspace, we have that for all $1 \leq i \leq q^k$, and $\lambda, \mu \in \mathbb{F}_q$ that $\lambda(\alpha_i, f(\alpha_i)) + \mu(\alpha_j, f(\alpha_j)) = (\lambda\alpha_i + \mu\alpha_j, \lambda f(\alpha_i) + \mu f(\alpha_j))$ has to be a vector of U. Hence, both the set $V = \{\alpha_i \mid 1 \leq i \leq q^k\}$ as the map f are closed under

$\mathbb{F}_q$-linear combinations. It follows that $V = \{\alpha_i \mid 1 \leq i \leq q^k\}$ is an $\mathbb{F}_q$-subspace of dimension k and that f is an $\mathbb{F}_q$-linear map.

□

Lemma 3.2.7. *The number of points of $L = \{(x, f(x))|x \in V^*\}$, where V is a vector subspace of $\mathbb{F}_{q^t}$ and $f : V \to \mathbb{F}_{q^t}$ is an $\mathbb{F}_q$-linear map, is equal to the number of directions determined by the affine pointset $\mathcal{A} = \{(1, x, f(x)) \mid x \in V\}$.*

Proof. The number of points of $\{(x, f(x))|x \in V^*\} = \{(1, f(x)/x)|x \in V^*\}$ is clearly equal to the size of the set $W = \{f(x)/x|x \in V^*\}$. The points $(1, x_1, f(x_1))$ and $(1, x_2, f(x_2))$ determine the direction $(0, x_1 - x_2, f(x_1) - f(x_2))$. Since f is $\mathbb{F}_q$-linear and V is a subspace, $(0, x_1 - x_2, f(x_1) - f(x_2))$ is the direction $(0, 1, f(x_3)/x_3)$, with $x_3 = x_1 - x_2$. This implies that every direction determined by $\mathcal{A}$ is an element of the set $\{(0, 1, w) \mid w \in W\}$. Vice versa, take a point $(0, 1, w_0)$, with $w_0 \in W$, then $w_0 = f(x_0)/x_0$ for some $x_0 \in V^*$. Then $(1, 0, 0)$ and $(1, x_0, f(x_0))$ are points of $\mathcal{A}$ that determine the direction $(0, 1, w_0)$. This proves that the number of directions determined by $\mathcal{A}$ is equal to the size of W. □

3.3 The Rédei polynomial of a linear set

3.3.1 Rédei polynomials

Let $S = \{(1, x_i, y_i) \mid 1 \leq i \leq |S|\}$ be a set of affine points in PG$(2, q^t)$. Define the Rédei polynomial of S as follows:

$$R(X, Y) = \prod_{i=1}^{|S|} (X - x_i Y + y_i).$$

As usual (see e.g. [9, 23]), we can consider the expansion of $R(X, Y)$ using elementary symmetric polynomials. Let $\sigma_i(Y)$ be the i-th elementary symmetric polynomial of the set $\{-x_i Y + y_i|1 \leq i \leq |S|\}$, then

$$R(X, Y) = X^{|S|} + \sum_{i=1}^{|S|} \sigma_i(Y) X^{|S|-i}.$$

Note that $\deg \sigma_i(Y) \leq i$. Substituting the variable Y in $R(X, Y)$ by slopes will provide particular information on the shape of the Rédei polynomial. In the language of direction problems, the next Lemma deals with substitution of a determined slope.

Lemma 3.3.1. *Let $P = (x_0, f(x_0))$ be a point of weight j in $L_U = \{(x, f(x)) \mid x \in V^*\}$, then $R(X, y_0)$ with $y_0 = f(x_0)/x_0$ is of the form*

$$R(X, y_0) = \prod_{i=1}^{q^{k-j}} (X - \alpha_i)^{q^j},$$

for distinct $\alpha_i \in \mathbb{F}_{q^t}$.

Proof. Let $P = (x_0, f(x_0))$ be a point of weight j in $L_U = \{(x, f(x))|x \in V^*\}$. By definition, P has weight j in L_U if there are q^j elements $\Lambda \in \mathbb{F}_{q^t}$ such that $(\Lambda x, \Lambda f(x))$ is contained in $U = \{(x, f(x))|x \in V\}$. This implies that

$$f(\Lambda x_0) = \Lambda f(x_0) \tag{3.1}$$

has q^j solutions for Λ.

Let $x_1 \in V$ and let $\mathcal{A} = \{(1, x, f(x)) \mid x \in V\}$. For any $\Lambda \in \mathbb{F}_{q^t}$, the point $(1, x_1 + \Lambda x_0, f(x_1) + \Lambda f(x_0)) \in \boldsymbol{A} \iff f(x_1 + \Lambda x_0) = f(x_1) + \Lambda f(x_0)$ and $x_1 + \Lambda x_0 \in V$. The condition $x_1 + \Lambda x_0 \in V$ is equivalent with $\Lambda x_0 \in V$, and so the condition $f(x_1 + \Lambda x_0) = f(x_1) + \Lambda f(x_0)$ is equivalent with $f(\Lambda x_0) = \Lambda f(x_0)$.

Hence, the number of points of $\mathcal{A}$ on the line through $(1, x_1, f(x_1)$ and $(0, x_0, f(x_0))$ equals precisely the number of solutions of Equation 3.1 (and $\Lambda = 0$ corresponds with the point $(1, x_1, f(x_1))$).

By definition, $R(X, y_0) = \prod_{x \in V}(X - xy_0 + f(x))$. Now $X - xy_0 + f(x) = X - x_1y_0 + f(x_1)$ if and only if the points $(1, x, f(x))$, $(1, x_1, f(x_1))$, and $(0, 1, y_0)$ are collinear. Hence, the factor $(X - x_1y_0 + f(x_1))$ appears exactly q^j times in $R(X, y_0)$. □

Remark 3.3.2. We can also deduce Lemma 3.3.1 from a more geometrical point of view. Let $L_U = \mathcal{B}(\pi)$, where π is a $(k-1)$-space in $\mathrm{PG}(2t-1, q)$, embed $\mathrm{PG}(2t-1, q)$ as the subspace consisting of all points of the form $\langle(0, y, z)\rangle_q$ in $\mathrm{PG}(3t-1, q)$ and consider L_U as a subset of $\mathrm{PG}(2, q^t)$, contained in the line $X_0 = 0$ (at infinity). Let μ be the subspace spanned by the point $\langle(1, 0, 0)\rangle_q$ of $\mathrm{PG}(3t-1, q)$ and π. Then $\mathcal{B}(\mu) \setminus \mathcal{B}(\pi)$ consists of the q^k points of $\{(1, x, f(x)) \mid x \in V\}$). If $P = (0, x_0, f(x_0))$, $x_0 \in V^*$ is a point of weight j in $L_U = \mathcal{B}(\pi)$, this means the spread element S (of the Desarguesian $(t-1)$-spead $\mathcal{S}$) corresponding to P meets π, and hence also μ, in a $(j-1)$-dimensional space. Every line through P in $\mathrm{PG}(2, q^t)$ containing a point $(1, x_0, f(x_0))$ of $\{(1, x, f(x)) \mid x \in V\}$ corresponds to a $(2t-1)$-dimensional subspace of $\mathrm{PG}(3t-1, q)$, spanned by spread elements of $\mathcal{S}$, meeting μ in a subspace ν of dimension j. As π is a hyperplane of μ, and $P = \mathcal{B}(\pi \cap \nu)$ this means that the line $\mathcal{B}(\nu)$ contains exactly q^j points of $\{(1, x, f(x)) \mid x \in V\}$.

Hence every line on a point of weight j of L_U that contains a point of $\mathcal{A}$, contains exactly q^j points of $\mathcal{A}$. From the definition of the Rédei polynomial $R(X,Y)$, this is saying exactly that every root of $R(X,y_0)$ has multiplicity exactly q^j, if y_0 is a slope corresponding with a point of weight j of L_U, in other words, every factor of $R(X,y_0)$ has multiplicity q^j.

We are now ready to deduce the shape of the Rédei polynomial of the set $\mathcal{A} = \{(1,x,f(x)) \mid x \in U\}$.

Lemma 3.3.3. *If $\mathcal{A} = \{(1,x,f(x)) \mid x \in V\}$, where V is an $\mathbb{F}_q$-vector subspace of $\mathbb{F}_{q^t}$ of dimension k and $f : V \to \mathbb{F}_{q^t}$ is an $\mathbb{F}_q$-linear map, then the Rédei polynomial of $\mathcal{A}$ is of the following shape:*

$$R(X,Y) = X^{q^k} + \sigma_{q^k-q^{k-1}}(Y)X^{q^{k-1}} + \sigma_{q^k-q^{k-2}}(Y)X^{q^{k-2}} + \ldots + \sigma_{q^k-1}(Y)X\ . \quad (3.2)$$

Proof. First consider an element $y_0 \notin \mathcal{D}_\mathcal{A}$, where $\mathcal{D}_\mathcal{A}$ is the set of directions determined by $\mathcal{A}$. Then the set $V_{y_0} = \{-xy_0 + f(x) | x \in V\}$ is an $\mathbb{F}_q$-vector subspace of $\mathbb{F}_{q^t}$ of dimension k. Hence, by Theorem 3.2.2,

$$R(X,y_0) = \prod_{\beta \in V_{y_0}} (X-\beta) = X^{q^k} + \alpha_1 X^{q^{k-1}} + \alpha_2 X^{q^{k-2}} + \ldots + \alpha_k X\ ,$$

with $\alpha_i \in \mathbb{F}_{q^t}$. Then consider an element $y_1 \in \mathcal{D}_\mathcal{A}$. By Lemma 3.3.1, we know that if $(1,y_1)$ is a point of weight j_1, then $R(X,y_1)$ contains q^{k-j_1} distinct factors, each of degree q^{j_1}. As before, the set $V_{y_1} = \{-xy_1 + f(x) | x \in V\}$ is an $\mathbb{F}_q$-vector subspace of $\mathbb{F}_{q^t}$, but the number of elements in V_{y_1} is q^{k-j_1}, and hence, the dimension of V_{y_1} is $k - j_1$. We now obtain that

$$R(X,y_1) = \prod_{\beta' \in V_{y_1}} (X-\beta')^{q^j} = (X^{q^{k-j_1}} + \alpha'_1 X^{q^{k-j_1-1}} + \alpha'_2 X^{q^{k-j_1-2}} + \ldots + \alpha'_{k-j_1-1} X)^{q^{j_1}},$$

We conclude that for all $y \in \mathbb{F}_{q^t}$, $\sigma_i(y) = 0$ if $i \notin \{q^k - q^j | j = 0 \ldots k-1\}$. Since $\deg \sigma_i(Y) \leq i$, each of the polynomials $\sigma_i(Y), i \notin \{q^k - q^j | j = 0 \ldots k-1\}$ has more roots than its degree, and so is identically zero. Also note that since $(1,0,0) \in \boldsymbol{A}$, $0 \in \{-x_i Y + y_i | 1 \leq i \leq |\boldsymbol{A}|\}$, hence $\sigma_{q^k}(Y)$ is identically zero. So $R(X,Y)$ has the shape of (3.2).

□

We see that if $R(X,Y)$ is the Rédei polynomial associated with $\{(1,x,f(x)) \mid x \in V\}$ then for every $y \in \mathbb{F}_{q^t}$, the map $R(X,y)$ is a linearised polynomial.

3.4 A lower bound on the size of a linear set

In the paper [18], a lower bound on the size of a linear set was derived by using the previous observations, together with some of the machinery of [23]. It is explained there that we can write

$$X^{q^t} - X = R(X,Y)Q(X,Y) - H(X,Y) - X\,. \tag{3.3}$$

for some polynomial H and deduce the following lemma:

Lemma 3.4.1. *Let $R(X,Y)$ be the Rédei polynomial of the point set $\mathcal{A} = \{(1, x, f(x)) \mid x \in V\}$, and $H(X,Y)$ the polynomial defined in Equation 3.3. Then the number of points in $L_U = \{(x, f(x)) \mid x \in V^*\}$ is at least $\deg_X H(X,Y)$.*

Theorem 3.4.2. *[18, Theorem 3.7] Let $L_U = \{(x, f(x)) \mid x \in V^*\}$, where V has dimension k, be an $\mathbb{F}_q$-linear set in $\mathrm{PG}(1, q^t)$ of rank k which contains at least one point of weight one, then the size of L_U is at least $q^{k-1} + 1$.*

Proof. With $R(X,Y)$ the Rédei-polynomial of $\mathcal{A} = \{(1, x, f(x)) \mid x \in V^*\}$, and $H(X,Y)$ defined as in (3.3), by Lemma 3.4.1, we know that the number of points in L_U is at least $\deg_X H(X,Y)$. Let $P = (x_0, f(x_0))$ be a point of weight one in L_U. By Lemma 3.3.1, $R(X, y_0)$ with $y_0 = f(x_0)/x_0$ splits in factors of degree q, and since $R(X, y_0)$ has degree q^k, there are q^{k-1} different factors, each of the form $(X - \alpha_i)^q$ for some $\alpha_i \in \mathbb{F}_{q^t}$, $i = 1, \ldots, q^{k-1}$. Since $X - \alpha_i$ divides $X^{q^t} - X$, it divides $H(X,y) - X$ as well. As we have found at least q^{k-1} different linear factors dividing $H(X,y) - X$, this implies that $\deg_X H(X,Y)$ is at least q^{k-1}. We conclude that the number of points in L_U is at least q^{k-1}, and hence, by Exercise 2.1.5, at least $q^{k-1} + 1$. □

In Theorem 3.4.2, we find that the number of points in an $\mathbb{F}_q$-linear set of rank k in $\mathrm{PG}(1, q^t)$, containing a point of weight one, is at least $q^{k-1} + 1$. This lower bound is sharp.

Exercise 3.4.3. Let $2 \leq k \leq t$. Show that there exists an $\mathbb{F}_q$-linear set of rank k in $\mathrm{PG}(1, q^t)$ with $q^{k-1} + 1$ elements.

Remark 3.4.4. An example of a set $\mathcal{B}(\pi)$ for Exercise 3.4.3 can be obtained using coordinates as follows: take $\alpha_0 = 1, \alpha_1, \ldots, \alpha_{t-k}$ to be $\mathbb{F}_q$-linearly independent elements of $\mathbb{F}_{q^t}$, let V be the vector space of $\mathbb{F}_{q^t}$ defined by $\mathrm{Tr}(\alpha_i x) = 0$, for $i = 1, \ldots, t-k$ and put $L_U = \{(x, \mathrm{Tr}(x)) \mid x \in V^*\}$.

However, not every $\mathbb{F}_q$-linear set of size $q^{k-1} + 1$ arises in this way. For example, in $\mathrm{PG}(1, q^4)$, it is possible to find two non-equivalent $\mathbb{F}_q$-linear sets of rank 4, each containing $q^3 + 1$ points (see Example B1 and C12 of [12]). The example of Proposition 3.4.3 arises as $\mathcal{B}(\pi)$, where π is a 3-space meeting one element of the

Desarguesian 3-spread $\mathcal{S}$ of $\mathrm{PG}(7, q)$ in a plane, and q^3 other elements in a point. The other example arises as $\mathcal{B}(\pi)$ where π meets $q + 1$ elements of a regulus of $\mathcal{S}$ in a line and $q^3 - q$ others in a point.

Chapter 4

Linear blocking sets, translation hyperovals and translation KM-arcs

4.1 Blocking sets

4.1.1 Introduction

Blocking sets are well-studied objects in finite geometry. Their theory goes back to the 1950's [62]. For a survey of planar blocking sets, see e.g. the set of lecture notes of Aart Blokhuis for the Socrates intensive course [8]. The more recent [11] provides a survey focussing on the higher-dimensional case. More background info can also be found in [75].

A *blocking set* in $\mathrm{PG}(n,q)$ *with respect to k-spaces* is a set B of points such that every k-dimensional space in $\mathrm{PG}(n,q)$ contains at least one point of B. If we are considering blocking sets with respect to hyperplanes, we simply say that B is a *blocking set*. A *minimal* blocking set B (w.r.t. k-spaces) is a blocking set such that no proper subset of B is a blocking set (w.r.t. k-spaces). A *small* blocking set in $\mathrm{PG}(n,q)$ with respect to k-spaces is a blocking set of size smaller then $3(q^{n-k}+1)/2$. A blocking set B in $\mathrm{PG}(n,q)$ with respect to k-spaces is *of Rédei-type* if there is a hyperplane containing $|B|-q^{n-k}$ points.

Linear blocking sets with respect to $(k-1)$-spaces in $\mathrm{PG}(n-1,q^t)$ were introduced by Lunardon [50]: he argues that an $\mathbb{F}_q$-linear set of rank $nt-kt+1$ is a blocking set with respect to $(k-1)$-spaces.

Exercise 4.1.1. Show that an $\mathbb{F}_q$-linear set of rank $nt-kt+1$ defines a blocking set respect to $(k-1)$-spaces in $\mathrm{PG}(n-1,q^t)$.

Polito and Polverino [58] showed that one can construct minimal linear blocking sets in $\mathrm{PG}(2,p^t)$, p prime, $t \geq 4$ that are not of Rédei-type. This contradicted a widespread belief (and even conjecture) saying that a small minimal blocking set in $\mathrm{PG}(2,q^t)$ would necessarily be of Rédei-type.

Remark 4.1.2. This false conjecture however has some truth hidden in it: it was shown in [67] that a small minimal blocking set of Rédei-type with respect to k-spaces is a linear set. Care should be taken when using this result, as the authors essentially prove that the affine part of the Rédei-type blocking set is an affine linear set. This however implies that the set itself is linear as well.

Exercise 4.1.3. Let B be a minimal blocking set of Rédei-type in $\mathrm{PG}(2,q)$ of size at most $2q$, and let ℓ_∞ be its Rédei-line (i.e., the line containing $|B|-q$ points). Show that B consists of the q affine points, together with their determined directions. Vice versa, show that a point set of size q together with its determined directions define a minimal blocking set of Rédei-type, provided that not all directions are determined.

Theorem 4.1.4. *Let f be an $\mathbb{F}_q$-linear map on $\mathbb{F}_{q^t}$. The set*

$$B = \{(1,x,f(x))|x \in \mathbb{F}_{q^t}\} \cup \{(0,x,f(x))\}$$

in $\mathrm{PG}(2,q^t)$ is a minimal blocking set of Rédei-type. Moreover, the set B is an $\mathbb{F}_q$-linear set of rank $t+1$.

Proof. The set B consists of q^t affine points, together with their directions. Since $f(x)/x$ takes on at most $\frac{q^t-1}{q-1}$ different values, not all directions are determined. Hence, by Exercise 4.1.3, B is a minimal blocking set of Rédei-type. Let $\mathrm{PG}(2,q^t) = \mathrm{PG}(V)$, where $V = W_1 \oplus W_2 \oplus W_3$. We see that he point set $U = \{(\lambda,x,f(x))|\lambda \in \mathbb{F}_q, x \in \mathbb{F}_{q^t}\}$ is an $\mathbb{F}_q$-subspace of V of dimension $t+1$. Furthermore, the point with coordinates $(\lambda,x,f(x))$ in $\mathrm{PG}(2,q^t)$, $\lambda \neq 0$ is the point $(1,x/\lambda,f(x)/\lambda) = (1,x',f(x'))$ since $\lambda \in \mathbb{F}_q$ and f is $\mathbb{F}_q$-linear. This implies that the points in B are precisely the points of L_U, so B is an $\mathbb{F}_q$-linear set of rank $t+1$. (Note that this again shows (by 4.1.1) that B is a blocking set.)

□

Soon after it was proven that there are small minimal linear blocking sets that are not of Rédei-type, people conjectured that all small minimal blocking sets should be linear sets. This conjecture was stated formally by Sziklai in 2008 [71]. Up to our knowledge, this is the complete list of cases in which the linearity conjecture for blocking sets in $\mathrm{PG}(n,p^s)$, p prime w.r.t. k-spaces has been proven.

- $s=1$ (for $n=2$, see [7]; for $n>2$, $k=n-1$, see [29]; for $n>2$, $k\neq n-1$, see [70])
- $s=2$ (for $n=2$, see [69]; for $n>2$, $k=n-1$, see [68]; for $n>2$, $k\neq n-1$, see [78])
- $s=3$ (for $n=2$, see [59]; for $n>2$, $k=n-1$, see [68]; for $n>2$, $k\neq n-1$, see [44, 28])
- $k=n-1$ and B is of Rédei-type (for $n=2$, see [3, 9]; for $n>2$, see [67])
- $k=n-1$ and $\dim\langle B\rangle=s-1$ (see [72])
- $k=n-1$ and $\dim\langle B\rangle=s$ (see [70]).

It is shown in [76] that, loosely speaking, if the linearity conjecture holds in $\mathrm{PG}(2,p^s)$, then it also holds for blocking sets with respect to k-spaces in $\mathrm{PG}(n,p^s)$, provided that p is large enough.

4.1.2 The size of an $\mathbb{F}_q$-linear (blocking) set in $\mathrm{PG}(2,q^t)$

The results of Theorem 3.4.2 can be used to derive a lower bound on the number of points in a linear sets in a plane. However, we have to impose a certain hypothesis, namely that there exists a $(q+1)$-secant to the set. Note that this hypothesis implies that the linear set is not contained in a line.

Theorem 4.1.5. *[18, Theorem 4.1] Let L be an $\mathbb{F}_q$-linear set of rank $k>2$ in $\mathrm{PG}(2,q^t)$ such that there is at least one line of $\mathrm{PG}(2,q^t)$ meeting L in exactly $q+1$ points, then L contains at least $q^{k-1}+q^{k-2}+1$ points.*

The bound in Theorem 4.1.5 is sharp:

Exercise 4.1.6. Let $3\leq k\leq n$. Show that there exists an $\mathbb{F}_q$-linear set S of rank k in $\mathrm{PG}(2,q^t)$ with $q^{k-1}+q^{k-2}+1$ elements such that there is a line meeting S in exactly $q+1$ points.

Recall that it is conjectured (see [71, Conjecture 3.1]) that all *small* minimal blocking sets in $\mathrm{PG}(2,q^t)$ are $\mathbb{F}_p$-linear sets where q is a power of the prime p. In the same paper, the author conjectures the following:

Conjecture 4.1.7. [71, p.1170] Let p be a prime. If $\mathbb{F}_{p^e}$ is the "maximum field of linearity" then a non-trivial blocking set in $\mathrm{PG}(2, p^s)$, with $s = en$, has at least $(p^e)^n + (p^e)^{n-1} + 1$ points.

The notion "maximum field of linearity" is used by Sziklai to indicate the following: the maximum field of linearity of a blocking set in $\mathrm{PG}(2, p^s)$ is $\mathbb{F}_{p^e}$ if and only if every line meets the blocking set in $1 \bmod p^e$ points, but not every line meets in $1 \bmod p^{e+1}$ points. The fact that e is a divisor of t, and hence, that there is a subfield $\mathbb{F}_{p^e}$ of $\mathbb{F}_{p^s}$ follows from his work on blocking sets, but it does not necessarily hold for linear sets in general (see [18, Remark 12]).

Remark 4.1.8. Theorem 4.1.5 shows that an $\mathbb{F}_q$-linear set of rank k that contains a $(q+1)$-secant, contains at least $q^{k-1} + q^{k-2} + 1$ points. It is clear if an $\mathbb{F}_q$-linear set contains a $(q+1)$-secant, then the maximum field of linearity is indeed $\mathbb{F}_q$. In [71, Corollary 5.2], the author also shows the converse for blocking sets with respect to k-spaces in $\mathrm{PG}(r-1, q^t)$: if the maximum field of linearity is $\mathbb{F}_{p^e}$, then there are (many) $(p^e + 1)$-secants to the set. This observation shows that assuming that there is $(q+1)$-secant in the case of an $\mathbb{F}_q$-linear blocking set in $\mathrm{PG}(2, q^t)$, is equivalent to assuming that the maximum field of linearity is $\mathbb{F}_q$. So we see that if the linearity conjecture for blocking sets holds, then Theorem 4.1.5 proves Conjecture 4.1.7.

4.2 Translation hyperovals and KM-arcs

4.2.1 KM-arcs

Point sets in $\mathrm{PG}(2, q)$, the Desarguesian projective plane of over the finite field $\mathbb{F}_q$ of order q, that have few different intersections sizes with lines have been a research subject throughout the last decades. A point set $\S$ of *type* $(i_1, \ldots, i_m)$ in $\mathrm{PG}(2, q)$ is a point set such that for every line in $\mathrm{PG}(2, q)$ the intersection size $\ell \cap \S$ equals i_j for some j and such that each value i_j occurs as intersection size for some line. In [55] point sets of type $(0, 2, q/2)$ of size $\frac{3q}{2}$ were studied. This led to the following generalisation by Korchmáros and Mazzocca in [36].

Definition 4.2.1. A *KM-arc of type s* in $\mathrm{PG}(2, q)$ is a point set of type $(0, 2, t)$ with size $q + s$. A line containing i of its points is called an i-secant.

Originally these KM-arcs were called $(q+s)$-arcs of type $(0, 2, s)$ [36] or '$(q+s, s)$-arcs of type $(0, 2, s)$' [25] but in honour of Korchmáros and Mazzocca we denote them by KM-arcs. The following results were obtained in [25] and [36].

Theorem 4.2.2. *[25, Theorem 2.5],[36, Proposition 2.1].*

If $\mathcal{A}$ is a KM-arc of type t in $\mathrm{PG}(2,q)$*,* $2 < s < q$*, then*

- *q is even;*
- *s is a divisor of q;*
- *there are $\frac{q}{s}+1$ different s-secants to $\mathcal{A}$, and they are concurrent.*

If $\boldsymbol{A}$ is a KM-arc of type s, then the point contained in all s-secants to $\boldsymbol{A}$ is called the *s-nucleus* of $\boldsymbol{A}$.

Definition 4.2.3. A point set § in $\mathrm{PG}(2,q)$ is a called a *translation set* with respect to the line ℓ if the group of elations with axis ℓ fixing § acts transitively on the points of $\S \setminus \ell$; the line ℓ is called the *translation line*. If a KM-arc is a translation set, then it is called a *translation KM-arc*.

Theorem 4.2.4 ([36, Proposition 6.2])**.** *If* $\S \subset \mathrm{PG}(2,q)$ *is a translation KM-arc of type s with respect to the line ℓ, then ℓ is a s-secant to* §*.*

Definition 4.2.5. An i-club in $\mathrm{PG}(1,q^t)$ is an $\mathbb{F}_q$-linear set such that there is exactly one point of weight i (called the *head* of the i-club) and all other points have weight one.

Exercise 4.2.6. Determine the number of points in an i-club of rank k in $\mathrm{PG}(1,q^t)$. Show that $\{(x,\mathrm{Tr}(x))|x \in \mathbb{F}_{q^t}\}$ is a $(t-1)$-club of rank t in $\mathrm{PG}(1,q^t)$.

The next two results show that i-clubs of rank h in $\mathrm{PG}(1,2^h)$ and KM-arcs of type 2^i are equivalent objects.

Let $\mathcal{D}$ be the Desarguesian $(h-1)$-spread in $\mathrm{PG}(3h-1,2)$ corresponding to $\mathrm{PG}(2,2^h)$, let ℓ_∞ be the line at infinity of $\mathrm{PG}(2,2^h)$ and let H be the $(2h-1)$-space such that $\mathcal{B}(H)=\ell_\infty$. The points of $\mathrm{PG}(2,2^h)$ that are not on ℓ_∞ are the affine points.

Theorem 4.2.7. *[17, Theorem 2.1] Let μ be an $(h-1)$-space in* $\mathrm{PG}(2h-1,2)$ *such that $\mathcal{B}(\mu)$ is an i-club $\mathcal{C}$ of rank h with head N in ℓ_∞, and let $\rho \in \mathcal{D}$ be the spread element such that $\mathcal{B}(\rho)=N$. Let π be an h-space meeting H exactly in μ. Then the point set $\mathcal{B}(\pi)\setminus\mathcal{C}$ together with the points of $\ell_\infty \setminus \mathcal{C}$ forms a translation KM-arc of type 2^i in* $\mathrm{PG}(2,2^h)$ *with axis ℓ_∞ and with 2^i-nucleus N.*

Proof. We denote $(\mathcal{B}(\pi)\setminus\mathcal{C})\cup(\ell_\infty\setminus\mathcal{C})$ by $\boldsymbol{A}$. As π is an h-space that meets H, which is spanned by spread elements, in an $(h-1)$-space, a spread element that meets $\pi\setminus\mu$ non-trivially, meets it in a point. Consequently, $\boldsymbol{A}$ has 2^h affine points. The size of $\mathcal{C}=\mathcal{B}(\mu)$ is $2^{h-1}+\cdots+2^i+1$, which implies that $\boldsymbol{A}$ contains $(2^h+1)-(2^{h-1}+\cdots+2^i+1)=2^i$ points of ℓ_∞. So in total, $\boldsymbol{A}$ has 2^h+2^i points.

Let ℓ be a line in $\mathrm{PG}(2,2^h)$ different from ℓ_∞, and let L be the $(2h-1)$-space in $\mathrm{PG}(3h-1,2)$ such that $\ell=\mathcal{B}(L)$. If $L\cap H=\rho$, then L contains the $(i-1)$-space $\mu\cap\rho$. Since L contains no other points of H than the points of ρ, either $L\cap\pi$ is an i-space, or else $L\cap\pi$ equals the $(i-1)$-space $\mu\cap\rho$. In the former case $|\boldsymbol{A}\cap\ell|=2^i$, in the latter case ℓ contains no points of $\mathcal{A}$.

If $L\cap H$ is a spread element different from ρ, then L meets μ in a point or $L\cap\mu=\emptyset$. In the former case ℓ has no point in common with $\ell_\infty\setminus\mathcal{C}$, and L meets meet π in a line or a point, so $\ell\cap(\mathcal{B}(\pi)\setminus\mathcal{C})$ equals 0 or 2. In the latter case ℓ has one point in common with $\ell_\infty\setminus\mathcal{C}$, and L meets meet π in a point by the Grassmann identity, so $|\ell\cap(\mathcal{B}(\pi)\setminus\mathcal{C})|$ equals 1. Consequently, all lines meet $\boldsymbol{A}$ in 0, 2 or 2^i points, and all lines that meet it in 2^i points, pass through N; $\boldsymbol{A}$ is a KM-arc of type 2^i with 2^i-nucleus N.

We now prove that $\boldsymbol{A}$ is a translation KM-arc with axis ℓ_∞. Let P_1 and P_2 be two points of $\mathcal{A}\setminus\ell_\infty$, and let $Q_1,Q_2\in(\pi\setminus\mu)$ be the points such that $\mathcal{B}(Q_1)=P_1$ and $\mathcal{B}(Q_2)=P_2$. We consider the elation γ in the $(2h)$-space $\langle H,\pi\rangle$ with axis H, that maps Q_1 on Q_2. This elation induces an elation $\overline{\gamma}$ of $\mathrm{PG}(2,2^h)$ with axis $\mathcal{B}(H)=\ell_\infty$. Note that π is fixed by γ, and hence $\mathcal{B}(\pi)$ is fixed by $\overline{\gamma}$. So $\mathcal{A}$ is fixed by $\overline{\gamma}$. Since $Q_1^\gamma=Q_2$, $P_1^{\overline{\gamma}}=P_2$. □

Theorem 4.2.8. *[17, Theorem 2.2] Every translation KM-arc of type 2^i in $\mathrm{PG}(2,2^h)$ can be constructed as in Theorem 4.2.7.*

Proof. From [36, Proposition 6.3], we know that if $\boldsymbol{A}$ is a translation KM-arc of type t in $\mathrm{PG}(2,q), q=2^h$ with translation line $Z=0$, and $(0,1,0)$ as t-nucleus, then the affine points of $\boldsymbol{A}$ can be written as $(f(t),t,1)$ where $f(z)=\sum_{i=0}^{h-1}\alpha_i z^{2^i}$ with $\alpha_i\in\mathbb{F}_2$.

Now let $\{\omega,\omega^2,\omega^{2^2},\ldots,\omega^{2^{h-1}}\}$ be a normal basis for $\mathbb{F}_{2^h}$ over $\mathbb{F}_2$ and consider field reduction with respect to this basis, i.e. we let the vector (u,v,w) of $\mathbb{F}_{2^h}^3$ correspond to the vector $(u_0,\ldots,u_{h-1};v_0,\ldots,v_{h-1};w_0,\ldots,w_{h-1})$ of $\mathbb{F}_2^{3h}$, where $u=\sum_{i=0}^{h-1}u_i\omega^{2^i}$, $v=\sum_{i=0}^{h-1}v_i\omega^{2^i}$ and $w=\sum_{i=0}^{h-1}w_i\omega^{2^i}$.

Write $1=\sum_{i=0}^{h-1}a_i\omega^{2^i}$, and let $k\in\{0,\ldots,h-1\}$ be an index for which $a_k=1$. Let $t\in\mathbb{F}_{2h}=\sum_{i=0}^{h-1}t_i\omega^{2^i}$, then $t^{2^j}=\sum_{i=0}^{h-1}t_{h-j+i}\omega^{2^i}$, where the indices are taken modulo h. We see that $f(t)=\sum_{j=0}^{h-1}(\sum_{i=0}^{h-1}\alpha_j t_{h-i+j}\omega^{2^i})$, again with the indices taken modulo h.

This implies that every point $(f(t),t,1)$, $t\in\mathbb{F}_{2^h}$ is defined by a vector of $\mathbb{F}_{2^{3h}}$ corresponding to a point of $\mathrm{PG}(3h-1,2)$ that belongs to the h-dimensional subspace

π defined by the $2h-1$ equations:

$$X_i = \sum_{j=i}^{h-1} \alpha_j X_{h-i+j} + \sum_{j=0}^{i-1} \alpha_j X_{2h-i+j}, i \in \{0,\dots,h-1\}$$
$$X_{2h+j} = a_j X_{2h+k}, j \in \{0,\dots,h-1\}, j \neq k.$$

The intersection of π with the $(2h-1)$-space H corresponding to the line $z=0$, defined by $X_{2h} = X_{2h+1} = \dots = X_{3h-1} = 0$ satisfies one extra equation, namely $X_{2h+k} = 0$, hence, π meets H in an $(h-1)$-dimensional space μ.

Since f is an $\mathbb{F}_2$-linear map, the set of directions determined by the set $\{(f(t),t,1) \mid t \in \mathbb{F}_{2^h}\}$ equals $\{(f(z),z,0)|z \in \mathbb{F}_{2^h}\}$.

If $\boldsymbol{A}$ is a KM-arc with affine part $\boldsymbol{A}'$ then it is clear that the set of points of the KM-arc of type 2^i on the line at infinity is exactly the set of non-determined directions by $\boldsymbol{A}'$. The size of this set is 2^i, which shows that the set $\boldsymbol{A}'$ determines $2^h - 2^i + 1$ directions and that $|\mathcal{B}(\mu)| = 2^h - 2^i + 1$. Since we know that the point $(0,1,0)$ lies on all 2^i-secants to the affine part of $\boldsymbol{A}$, determined by $\mathcal{B}(\pi) \setminus \mathcal{B}(\mu)$, we obtain that the spread element corresponding to $(0,1,0)$ meets μ in an $(i-1)$-space. Consequently, all other spread elements that meet μ, meet it in a point, and $\mathcal{B}(\mu)$ is an i-club. □

4.2.2 Translation hyperovals and scattered linear sets of pseudoregulus type

The construction of Theorem 4.2.7 also works for $i=1$. In this case, we start with a 1-club in $\mathrm{PG}(1,2^h)$, i.e. a *scattered linear set*. The obtained KM-arc is an arc of type 2, which means that it is simply a *hyperoval*, and since it is a translation set, we obtain a *translation hyperoval*. The correspondence between translation hyperovals and scattered linear sets was already established in [27, Theorem 2]. It is well-known that every translation hyperoval in $\mathrm{PG}(2,q)$ is PGL-equivalent to a point set $\{(1,t,t^{2^i})|t \in \mathbb{F}_q\} \cup \{(0,1,0),(0,0,1)\}$, where $q=2^h$ and $\gcd(i,h)=1$, see [30, Theorem 8.5.4].

Remark 4.2.9. In [5], the authors use maximum scattered $\mathbb{F}_2$-linear sets in $\mathrm{PG}(r-1,2^t)$ to construct translation *caps* in even order projective spaces, based on the same idea. The caps constructed in this way come close to the theoretical lowed bound of the size of a cap making them extremely interesting objects.

Let S be a scattered $\mathbb{F}_q$-linear set of $\mathrm{PG}(2k-1,q^t)$ of rank kt, $t,k \geq 2$. We say that S is of *pseudoregulus type* if

1. there exist $m = \frac{q^{kt}-1}{q^t-1}$ pairwise disjoint lines of $\mathrm{PG}(2k-1,q^t)$, say $s_1, s_2, \dots, s_m$, such that
$$|S \cap s_i| = \frac{q^t-1}{q-1} \quad \forall i = 1, \dots, m,$$
2. there exist exactly two $(k-1)$-dimensional subspaces T_1 and T_2 of $\mathrm{PG}(2k-1,q^t)$ disjoint from S such that $T_j \cap s_i \neq \emptyset$ for each $i = 1, \dots, m$ and $j = 1, 2$.

The set of lines s_i, $i = 1, \dots m$ is called the *pseudoregulus* of $\mathrm{PG}(2k-1,q^t)$ associated with the linear set S and we refer to T_1 and T_2 as *transversal spaces* to this pseudoregulus. Since a maximum scattered linear set spans the whole space, we find that the transversal spaces are disjoint. For more information we refer to [52].

Theorem 4.2.10 ([52, Theorem 3.12]). *Each $\mathbb{F}_q$-linear set of $\mathrm{PG}(2k-1,q^t)$ of pseudoregulus type is of the form $L_{\rho,f}$ with*

$$L_{\rho,f} = \{(u, \rho f(u))_{q^t} | u \in U_0\}$$

with $\rho \in \mathbb{F}_{q^t}^*$, U_0, U_1 the k-dimensional vector spaces corresponding to the transversal spaces T_0, T_1 and with $f : U_0 \to U_1$ an invertible semilinear map, with companion automorphism $\sigma \in Aut(\mathbb{F}_{q^t})$, $Fix(\sigma) = \mathbb{F}_q$.

Exercise 4.2.11. Find the transversal spaces T_0 and T_1 of $L_{\rho,f}$ as given in the previous result and find the lines meeting $L_{\rho,f}$ in exactly $\frac{q^t-1}{q-1}$ points.

Recently, in [19], the André/Bruck-Bose representation of translation hyperovals was studied and the following theorem was shown (this extends the work of [6]).

Theorem 4.2.12. *[19] Let $\mathcal{Q}$ be a set of q^k affine points in $\mathrm{PG}(2k,q)$, $q = 2^h$, $h \geq 4$, $k \geq 2$, determining a set D of $q^k - 1$ directions in the hyperplane at infinity $H_\infty = \mathrm{PG}(2k-1,q)$. Suppose that every line has 0, 1, 3 or $q-1$ points in common with the point set D. Then*

(1) D is an $\mathbb{F}_2$-linear set of pseudoregulus type.

(2) There exists a Desarguesian spread $\mathcal{S}$ in H_∞ such that, in the André/Bruck-Bose plane $\mathcal{P}(\mathcal{S}) \cong \mathrm{PG}(2,q^k)$, with H_∞ corresponding to the line l_∞, the points of $\mathcal{Q}$ together with 2 extra points on ℓ_∞, form a translation hyperoval in $\mathrm{PG}(2,q^k)$.

Vice versa, via the André/Bruck-Bose construction, the set of affine points of a translation hyperoval in $\mathrm{PG}(2,q^k)$, $q > 4, k \geq 2$, corresponds to a set $\mathcal{Q}$ of q^k affine points in $\mathrm{PG}(2k,q)$ whose set of determined directions D is an $\mathbb{F}_2$-linear set of pseudoregulus type. Consequently, every line meets D in $0, 1, 3$ or $q-1$ points.

Exercise 4.2.13. Use the representation of a translation hyperoval in $\mathrm{PG}(2,q)$ as $\{(1,t,t^{2^i})|t \in \mathbb{F}_q\} \cup \{(0,1,0),(0,0,1)\}$, where $q = 2^h$ and $\gcd(i,h) = 1$ and the coordinates of Exercise 1.4.3 to deduce the vice versa part of the previous theorem.

Chapter 5

Related research problems

The following research problems are related to the material of this course and vary in level of difficulty.

Problem 5.0.1. Prove or disprove the linearity conjecture in the plane which states that every minimal blocking set in $\mathrm{PG}(2, q)$ of size smaller than $3(q+1)/2$ is an $\mathbb{F}_p$-linear set, where $q = p^h$, p prime.

Problem 5.0.2. *(Probably somewhat easier than the previous problem.)* Show that a minimal blocking set cannot have smaller than the size of the smallest linear blocking set.

Problem 5.0.3. Find a lower bound on the size of an $\mathbb{F}_q$-linear set in $\mathrm{PG}(2, q^t)$, without imposing the existence of a $(q+1)$-secant.

Problem 5.0.4. Determine a condition for linear sets L_U to be simple. (see [16])

Problem 5.0.5. Deduce whether or not the following holds: if an $\mathbb{F}_q$-linear set L_U of rank k has only points of weight at least 2, is it then true that L_U is an $\mathbb{F}_{q^i}$-linear set for some $i > 1$? (It follows from [9] that this statement is true for $\mathbb{F}_q$-linear sets of rank t in $\mathrm{PG}(1, q^t)$.)

Problem 5.0.6. Determine exact conditions on k, h, t under which a k-club of rank h in $\mathrm{PG}(1, q^t)$ exists.

Problem 5.0.7. In particular, settle the (non-)existence problem for a 2-club of rank t in $\mathrm{PG}(1, 2^t)$ when $t > 5$. The equivalent non-existence of translation KM-arcs of type 4 was conjectured by Limbupasiriporn [49], see Section 4.2.

Problem 5.0.8. Let $L_1, \ldots, L_{\frac{q^k-1}{q-1}}$ be a set of $\frac{q^k-1}{q-1}$ mutually disjoint lines in $\mathrm{PG}(2k-1, q)$, q even, such that every line meets the point set of these lines in $0, 1, 3$ or $q+1$ points. Do the lines of $L_1, \ldots, L_{\frac{q^k-1}{q-1}}$ define a regulus or a pseudoregulus?

(Compare with Theorem 24 of [46], where this a similar theorem is shown to hold in $\mathrm{PG}(3, q^3)$ where $q > 2$.)

References

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

[2] L. Bader and G. Lunardon. Desarguesian spreads. *Ricerche mat.* **60 (1)** (2011), 15–37.

[3] S. Ball. The number of directions determined by a function over a finite field. *J. Combin. Theory Ser. A* **104 (2)** (2003), 341–350.

[4] A. Barlotti and J. Cofman. Finite Sperner spaces constructed from projective and affine spaces. *Abh. Math. Semin. Univ. Hamb.* **40** (1974), 231–241.

[5] D. Bartoli, M.Giuletti, G. Marino, and O. Polverino. Maximum Scattered Linear Sets and Complete Caps in Galois Spaces. *Cobinatorica* **38 (2)**, 255–278.

[6] S.G. Barwick, W-A Jackson, A characterization of translation ovals in finite even order planes. *Finite fields Appl.* 33 (2015), 37–52.

[7] A. Blokhuis. On the size of a blocking set in $\mathrm{PG}(2,p)$. *Combinatorica* **14 (1)** (1994), 111–114.

[8] A Blokhuis. *Blocking Sets in Projective and Affine Planes*. lecture notes available from `http://cage.ugent.be/geometry/links.php`

[9] A. Blokhuis, S. Ball, A.E. Brouwer, L. Storme, and T. Szőnyi. On the number of slopes of the graph of a function defined on a finite field. *J. Combin. Theory Ser. A* **86 (1)** (1999), 187–196.

[10] A. Blokhuis and M. Lavrauw. Scattered spaces with respect to a spread in $\mathrm{PG}(n,q)$. *Geom. Dedicata* **81 (1-3)** (2000), 231–243.

[11] A. Blokhuis, T. Szőnyi and P. Sziklai. *Blocking sets in projective spaces*. Chapter in: De Beule J., Storme L. (eds.) Current Research Topics in Galois Geometry. NOVA Academic Publishers, 2011.

[12] G. Bonoli and O. Polverino. $\mathbb{F}_q$-linear blocking sets in $\mathrm{PG}(2,q^4)$. *Innov. Incidence Geom.* **2** (2005), 35–56.

[13] R.C. Bose, J.W. Freeman, and D.G. Glynn. On the intersection of two Baer subplanes in a finite projective plane. *Utilitas Math.* **17** (1980), 65–77.

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

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

[16] B. Csajbók and C. Zanella. On the equivalence of linear sets. *Des. Codes Cryptogr.* **81 (2)** (2016), 269–281.

[17] M. De Boeck and G. Van de Voorde. A linear set view on KM-arcs.*J. Algebraic Combin.* **44(1)** (2016), 131–164.

[18] J. De Beule and G. Van de Voorde. The minimum size of a linear set. *J. Combin. Theory Ser. A* **164** (2019), 109–124.

[19] J. D'haeseleer and G. Van de Voorde. Translation hyperovals and $\mathbb{F}_2$-linear sets of pseudoregulus type. Preprint.

[20] G. Donati and N. Durante. On the intersection of two subgeometries of $\mathrm{PG}(n, q)$. *Des. Codes Cryptogr.* **46 (3)** (2008), 261–267.

[21] Sz.L. Fancsali and P. Sziklai. About maximal partial 2-spreads in $\mathrm{PG}(3m - 1, q)$. *Innov. Incidence Geom.* **4** (2006), 89–102.

[22] Sz.L. Fancsali and P. Sziklai. Description of the clubs. *Ann. Univ. Sci. Budapest. Eötvös Sect. Math.* **51** (2009), 141–146.

[23] Sz. L. Fancsali, P. Sziklai, and M. Takáts. The number of directions determined by less than q points. *J. Algebraic Combin.*, 37(1):27–37, 2013.

[24] J.W. Freeman. Reguli and pseudo-reguli in $\mathrm{PG}(3, q^2)$. *Geom. Dedicata* **9** (1980), 267–280.

[25] A. Gács and Zs. Weiner. On $(q + t)$-arcs of type $(0, 2, t)$. *Des. Codes Cryptogr.*, **29 (1-3)** (2003), 131–139.

[26] N. Gill. Polar spaces and embeddings of classical groups. *New Zealand J. Math.* **36** (2007), 175–184.

[27] D. Glynn and G. Steinke. Laguerre planes of even order and translation ovals. *Geom. Dedicata* **51** (1994), 105–112.

[28] N.V. Harrach, K. Metsch, T. Szőnyi, and Zs. Weiner. Small point sets of $\mathrm{PG}(n, p^{3h})$ intersecting each line in 1 mod p^h points. *J. Geom.* **98 (1–2)** (2010), 59–78.

[29] U. Heim. Proper blocking sets in projective spaces. *Discrete Math.* **174 (1–3)** (1997), 167–176.

[30] J. W. P. Hirschfeld, Projective Geometries over Finite Fields. *Oxford University Press*, Oxford (1979).

[31] J.W.P. Hirschfeld and J.A. Thas. *General Galois Geometries*. Oxford University Press, Oxford, 1991.

[32] D. R. Hughes and F. C. Piper, Projective Planes, Springer-Verlag New York Inc., 1973.

[33] I. Jagos, G. Kiss, and A. Pór. On the intersection of Baer subgeometries of $\mathrm{PG}(n, q^2)$. *Acta Sci. Math.* **69 (1–2)** (2003), 419–429.

[34] S. Kelly. Constructions of intriguing sets of polar spaces from field reduction and derivation. *Des. Codes Cryptogr.* **43 (1)** (2007), 1–8.

[35] P. Kleidman and M. Liebeck. *The Subgroup Structure of the Finite Classical Groups.* Cambridge University Press, Cambridge, 1990.

[36] G. Korchmáros and F. Mazzocca. On $(q + t)$-arcs of type $(0, 2, t)$ in a desarguesian plane of order q. *Math. Proc. Cambridge Philos. Soc.*, **108 (3)** (1990), 445–459.

[37] M. Lavrauw. Scattered spaces with respect to spreads, and eggs in finite projective spaces. PhD Dissertation, Eindhoven University of Technology, Eindhoven, 2001.

[38] M. Lavrauw. Finite semifields with a large nucleus and higher secant varieties to Segre varieties. Adv. Geom. **11** (2011), 399–410.

[39] M. Lavrauw. Finite semifields and nonsingular tensors. *Des. Codes Cryptogr.* **68**, 1-3 (2013), 205–227.

[40] M. Lavrauw.*Scattered spaces in Galois geometry*. Contemporary developments in finite fields and applications, World Sci. Publ., Hackensack, NJ, (2016), 195–216.

[41] M. Lavrauw, G. Marino, O. Polverino and R. Trombetti. Solution to an isotopism question concerning rank 2 semifields. *J. Combin. Designs*. **23 (2)** (2015), 60–77.

[42] M. Lavrauw and O. Polverino O. *Finite semifields and Galois geometry*. Chapter in: De Beule J., Storme L. (eds.) Current Research Topics in Galois Geometry. NOVA Academic Publishers, 2011.

[43] M. Lavrauw, J. Sheekey and C. Zanella. On embeddings of minimum dimension of $\mathrm{PG}(n,q) \times \mathrm{PG}(n,q)$. To appear in *Des. Codes Cryptogr.*

[44] M. Lavrauw, L. Storme and G. Van de Voorde. A proof of the linearity conjecture for k-blocking sets in $\mathrm{PG}(n,p^3)$, p prime. *J. Combin. Theory, Ser. A* **118 (3)** (2011), 808–818.

[45] M. Lavrauw and G. Van de Voorde. On linear sets on a projective line. *Des. Codes Cryptogr.* **56 (2-3)** (2010), 89–104.

[46] M. Lavrauw and G. Van de Voorde. Scattered linear sets and pseudoreguli. *Electronic J. Combin* **20 (1)** (2013), P15.

[47] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1983. With a foreword by P. M. Cohn.

[48] M. Limbos. A characterisation of the embeddings of $\mathrm{PG}(m,q)$ into $\mathrm{PG}(n,q^r)$. *J. Geom.* **16 (1)** (1981), 50–55.

[49] J. Limbupasiriporn, Small sets of even type in finite projective planes of even order. *J. Geom.* 98 (2010), 139–149.

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

[51] G. Lunardon. Linear k-blocking sets. *Combinatorica* **21 (4)** (2001), 571–581.

[52] G. Lunardon, G. Marino, O. Polverino, R. Trombetti, Maximum scattered linear sets of pseudoregulus type and the Segre Variety $\mathcal{S}_{n,n}$. *J. Algebraic Combin.* 39 (2014), 807–831.

[53] G. Lunardon and O. Polverino. Translation ovoids of orthogonal polar spaces. *Forum Math.* **16 (5)** (2004), 663–669.

[54] G. Marino, O. Polverino, and R. Trombetti. On $\mathbb{F}_q$-linear sets of $\mathrm{PG}(3,q^3)$ and semifields. *J. Combin. Theory, Ser. A* **114 (5)** (2007), 769–788.

[55] G. Migliori. Insiemi di tipo $(0,2,q/2)$ in un piano proiettivo e sistemi di terne di Steiner. *Rend. Mat. Appl.*, **7** (1987), 77–82.

[56] O. Ore. On a special class of polynomials. *Trans. Amer. Math. Soc.*, 35(3) (1933), 559–584.

[57] V. Pepe. On the algebraic variety $\mathcal{V}_{r,t}$. *Finite Fields Appl.* **17 (4)** (2011), 343–349.

[58] P. Polito and O. Polverino. On small blocking sets. *Combinatorica* **18 (1)** (1998), 133–137.

[59] O. Polverino. Small blocking sets in $\mathrm{PG}(2,p^3)$. *Des. Codes Cryptogr.* **20 (3)** (2000), 319–324.

[60] O. Polverino. Linear sets in finite projective spaces. *Discrete Math.* **310 (22)** (2010), 3096–3107.

[61] L. Rédei. *Lückenhafte Polynome ber endlichen Korpern.* (German) Lehrbücher und Monographien aus dem Gebiete der exakten Wissenschaften. Mathematische Reihe, Band 42. Birkhäuser Verlag, Basel-Stuttgart, 1970.

[62] M. Richardson. On finite projective games. *Proc. Amer. Math. Soc.* **7** (1956), 458–465.

[63] S. Rottey, J. Sheekey and G. Van de Voorde. Subgeometries in the André/Bruck-Bose representation. *Finite Fields Appl* **35** (2015), 115–138.

[64] B. Segre. Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane. *Ann. Mat. Pura Appl.* **64** (1964), 1–76.

[65] J. Sheekey. A new family of linear maximum rank distance codes. *Advances in Mathematics of Communications*, 10 (3) (2016), 475–488.

[66] E.E. Shult and J. Thas. m-systems of polar spaces. *J. Combin. Theory Ser. A* **68 (1)** (1994), 184–204.

[67] L. Storme and P. Sziklai. Linear pointsets and Rédei type k-blocking sets in $\mathrm{PG}(n,q)$. *J. Algebraic Combin.* **14 (3)** (2001), 221–228.

[68] L. Storme and Zs. Weiner. On 1-blocking sets in $\mathrm{PG}(n,q)$, $n \geq 3$. *Des. Codes Cryptogr.* **21 (1–3)** (2000), 235–251.

[69] T. Szőnyi. Blocking sets in desarguesian affine and projective planes. *Finite Fields Appl.* **3 (3)** (1997), 187–202.

[70] T. Szőnyi and Zs. Weiner. Small blocking sets in higher dimensions. *J. Combin. Theory, Ser. A* **95 (1)** (2001), 88–101.

[71] P. Sziklai. On small blocking sets and their linearity. *J. Combin. Theory, Ser. A* **115 (7)** (2008), 1167–1182.

[72] P. Sziklai and G. Van de Voorde. A small minimal blocking set in $\mathrm{PG}(n,p^t)$, spanning a $(t-1)$-space, is linear. *Des. Codes Cryptogr.* **68 (1-3)** (2013), 25–32.

[73] J. Tits. Buildings of spherical type and finite BN-pairs. *Springer-Verlag, Berlin, Lecture Notes in Mathematics* **386**, 1974.

[74] G. Van de Voorde. Desarguesian spreads and field reduction for elements of the semilinear group. *Linear Algebra Appl.* **507** (2016), 96–120.

[75] G. Van de Voorde. *Blocking set in finite projective spaces and coding theory.* PhD thesis, Ghent University.

[76] G. Van de Voorde. On the linearity of higher-dimensional blocking sets. *Electronic J. Combin.* **17(1)** (2010), Research Paper 174, 16 pp.

[77] F.D. Veldkamp. Polar geometry. *Indag. Math.* **21** (1959), 512–551.

[78] Zs. Weiner. Small point sets of $\mathrm{PG}(n,q)$ intersecting each k-space in 1 modulo $\sqrt{q}$ points. *Innov. Incidence Geom.* **1** (2005), 171–180.

[79] B. Wu, Z. Liu. Linearized polynomials over finite fields revisited.*Finite Fields Appl.*, **22** (2013), 79–100.

[80] C. Zanella. Universal properties of the Corrado Segre embedding. *Bull. Belg. Math. Soc. Simon Stevin.* **3 (1)** (1996), 65–79.